Legal Information

**Book Name:** FlexNet Code Insight 2019 R3 User Guide  
**Part Number:** FNCI-2019R3-UG00  
**Product Release Date:** October 2019

**Copyright Notice**

Copyright © 2019 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 2019 R3 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
      Key Project Elements ....................................................................................... 16
      Common Project Configurations ................................................................. 16
   What is a Code Insight Project? .......................................................................... 15
      Creating a Project ............................................................................................ 17
   What Is a FlexNet Code Insight Scan? ............................................................... 18
   Applying a Scan Profile to the Project ............................................................. 18
      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
Contents

Analyzing (Auditing) Scan Results ................................................................. 37
  What Does an Analyst do? ........................................................................... 37

Scan Evidence ................................................................................................. 32
License Information Associated with Inventory ............................................ 33
  License Details from the Code Insight Data Library .................................. 33
  License Priority ............................................................................................ 34
Reporting of Detected License Text through the As-Found Text Inventory Field .................................................................................. 35
Notices Text ..................................................................................................... 36

Inventory Usage Information .......................................................................... 31

Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component ............................................................. 53

Component Lookup ........................................................................................ 56
  Guidelines for Component Lookup ............................................................. 56
  Component Lookup Results ....................................................................... 57

Component Lookup Results ........................................................................... 57

Opening the Analysis Workbench .................................................................. 38
The Analysis Workbench Layout .................................................................... 39
Searching for Codebase Files Based on Name .............................................. 40
Searching for Codebase Files Based on Search Criteria .................................. 41
Creating and Editing File Searches ............................................................... 41
  Creating a New File Search ....................................................................... 41
  Editing a File Search .................................................................................. 43
  Copying a File Search ................................................................................ 43
  Deleting a File Search ............................................................................... 44
Using the Filter Legend Options to Filter the Codebase .................................. 44
Using the Codebase Files Pane Context Menu .............................................. 46
Marking Files as Reviewed ........................................................................... 46
Viewing Details for Licenses Associated with Codebase Files ..................... 46
Using the File Details Tab ............................................................................ 48
  Viewing the Evidence Summary for a File ................................................. 48
  Viewing Binary Strings in a File ................................................................ 49
  Viewing Copyright, Email, URL, and License Evidence in a File ............... 49
  Viewing Exact Matches ............................................................................. 50
  Viewing Source Matches .......................................................................... 51
More About the “Remote Files” Panels on the Exact or Partial Matches Tabs ............................................................................................... 52
  Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component ............................................................. 53

Using the Evidence Details Tab ..................................................................... 48
Using the Inventory Details Tab .................................................................... 54
  Using the Inventory Items Context Menu .................................................. 55
  Viewing Security Vulnerabilities for Inventory in Analysis Workbench ....... 55

Viewing or Editing Inventory Usage Information from Analysis Workbench .................................................................................. 56

Component Lookup ........................................................................................ 56
  Guidelines for Component Lookup ............................................................. 56
  Component Lookup Results ....................................................................... 57
  Performing Component Lookup .................................................................. 57
Creating an Inventory Item from the Analysis Workbench ............................ 58
  Creating Inventory from the Inventory Items List ....................................... 58
  Creating Inventory from the Codebase Lists ............................................ 60
Editing Inventory from the Analysis Workbench ........................................... 61
  Publishing or Recalling Inventory from Analysis Workbench .................... 62
Contents

Reviewing Published Inventory .......................................................... 64
  Goal of the Reviewer ........................................................................ 64
  Displaying Project Inventory .......................................................... 65
  Searching Published Inventory ......................................................... 65
  Viewing Security Vulnerabilities for Project Inventory ...................... 66
  Viewing Details for the Licenses Associated with Project Inventory ..... 67
  Viewing and Updating Notes & Guidance ......................................... 68
  Viewing Usage Information for Project Inventory ............................ 68
  Viewing Associated Files ................................................................ 69
  Creating Inventory from the Project Inventory Tab ......................... 69
  Creating and Editing Custom Components ................................. 83
  Creating and Editing Custom Licenses ............................................ 94
  Viewing Usage Information for Project Inventory ............................ 68
  Viewing Details for the Licenses Associated with Project Inventory ..... 67
  Viewing and Updating Notes & Guidance ......................................... 68
  Viewing Usage Information for Project Inventory ............................ 68
  Viewing Associated Files ................................................................ 69
  Creating Inventory from the Project Inventory Tab ......................... 69
  Creating and Editing Custom Components ................................. 83
  Creating and Editing Custom Licenses ............................................ 94
  Creating a Custom Component ...................................................... 84
    Step 1: Access the Component Lookup Feature ............................. 84
    Step 2: Create the Custom Component ......................................... 84
      Create the Custom Component Based on a Keyword in Its Name or Title... 85
      Create the Custom Component Based on Its Project or Forge URL ....... 86
      Create the Custom Component Based on Its Forge .......................... 88
      Create the Custom Component in Free Form .............................. 89
    Step 3: Associate an Instance of the Custom Component with the Inventory Item 90
  Editing a Custom Component ....................................................... 91
  Custom Component Properties ....................................................... 92
  Supported Forge-URL Domains for Custom-Component Creation ....... 94

Managing Security Vulnerability Alerts ............................................. 78
  Accessing Security Vulnerability Alerts ......................................... 79
  Managing Security Vulnerability Alerts ......................................... 81
    Alert Details .................................................................................. 81
    Changing the Priority of an Alert ................................................. 83
    Changing the Status of an Alert ................................................... 83

Creating and Editing Custom Components ........................................ 83
  Creating a Custom Component ...................................................... 84
    Step 1: Access the Component Lookup Feature ............................. 84
    Step 2: Create the Custom Component ......................................... 84
      Create the Custom Component Based on a Keyword in Its Name or Title... 85
      Create the Custom Component Based on Its Project or Forge URL ....... 86
      Create the Custom Component Based on Its Forge .......................... 88
      Create the Custom Component in Free Form .............................. 89
    Step 3: Associate an Instance of the Custom Component with the Inventory Item 90
  Editing a Custom Component ....................................................... 91
  Custom Component Properties ....................................................... 92
  Supported Forge-URL Domains for Custom-Component Creation ....... 94

Creating and Editing Custom Licenses .............................................. 94
  Creating a Custom License ............................................................ 94
    Step 1: Initiate the Creation of a Custom License ............................ 95
      When Using Component Lookup to Register a Component Instance for a “component” Inventory Item 95
      When Selecting a New License for an Existing Inventory Item .......... 96
      When Creating or Editing a “License Only” Inventory Item ............. 97
    Step 2: Create the Custom License .............................................. 97
Managing Custom Detection Rules ................................................................. 100
Creating a Custom Detection Rule .............................................................. 101
Creating a Custom Detection Rule from Inventory of “Component” Type ........ 101
Creating a Custom Detection Rule from Scratch ......................................... 103
Viewing All Current Custom Detection Rules ........................................... 103
Editing a Custom Detection Rule ............................................................... 104
Deleting a Custom Detection Rule .............................................................. 104
Rule-Processing Considerations ............................................................... 104
Finalizing the Notices Text for the Notices Report .................................... 105
Accessing and Viewing Projects in the System ............................................ 107
Navigating to the Projects List ..................................................................... 107
Using the Project Dashboard ....................................................................... 108
Filtering Inventory for a Project from the Project Dashboard ....................... 110
Opening a Project ......................................................................................... 110
Showing Only Your Projects ....................................................................... 111
Searching the System .................................................................................. 111
Available Filters for Searching Across Projects ........................................... 112
Searching for Projects by Name .................................................................. 113
Searching All Projects for Inventory Based on a Specific Component and Version .................................................................................................................. 114
Searching All Projects for Inventory Associated with a Specific License ........ 115
Searching All Projects for a Security Vulnerability Advisory ...................... 115
Restoring the Full Project List ....................................................................... 116
Managing Items in the Project List ............................................................... 117
Managing a Project from the Summary Tab .................................................. 117
Opening the Project Summary Tab ............................................................... 118
Generating Reports ....................................................................................... 118
The Project Report ......................................................................................... 118
The Audit Report .......................................................................................... 119
The Notices Report ....................................................................................... 119
Generating the Notices Report ..................................................................... 120
Assigning Project Roles to Users ................................................................. 120
Editing the Project Definition and General Settings .................................... 121
Updating Scan Settings for a Project ........................................................... 122
Automatically Publishing Inventory ............................................................. 122
Updating Inventory Review and Remediation Settings for a Project ............ 123
Connecting the Project to Remote Data Sources ........................................ 123
Version Control Settings ............................................................................. 123
ALM Settings ............................................................................................... 124
Changing Project Owners ........................................................................... 126
Rescanning Your Codebase ......................................................................... 127
Change Events Resulting in Full or Incremental Rescans ............................. 127
Effects of Scan-Setting Changes on Rescans .............................................. 128
Handling of Edited Inventory During Rescans .......................................... 129
Initiating a Codebase Rescan ........................................................................ 130
<table>
<thead>
<tr>
<th>Scan Server Dialog</th>
<th>189</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Profiles Tab</td>
<td>192</td>
</tr>
<tr>
<td>Create/Edit Scan Profile Dialog</td>
<td>193</td>
</tr>
<tr>
<td>Project Defaults Tab</td>
<td>194</td>
</tr>
<tr>
<td>System Settings Tab</td>
<td>200</td>
</tr>
<tr>
<td>Projects List Page</td>
<td>200</td>
</tr>
<tr>
<td>Project Summary Tab</td>
<td>202</td>
</tr>
<tr>
<td>Edit Project: General Tab</td>
<td>205</td>
</tr>
<tr>
<td>Edit Project: Scan Settings Tab</td>
<td>206</td>
</tr>
<tr>
<td>Edit Project: Review and Remediation Settings Tab</td>
<td>207</td>
</tr>
<tr>
<td>Edit (Default) Project Users Page</td>
<td>212</td>
</tr>
<tr>
<td>Scan History Dialog</td>
<td>213</td>
</tr>
<tr>
<td>Select a New Project Owner Page</td>
<td>214</td>
</tr>
<tr>
<td>Analysis Workbench</td>
<td>215</td>
</tr>
<tr>
<td>File Search Results Pane</td>
<td>216</td>
</tr>
<tr>
<td>Advanced File Search Dialog</td>
<td>217</td>
</tr>
<tr>
<td>Advanced File Search Add Dialog</td>
<td>218</td>
</tr>
<tr>
<td>Inventory Details Pane</td>
<td>218</td>
</tr>
<tr>
<td>Evidence Details Pane</td>
<td>222</td>
</tr>
<tr>
<td>Project Inventory Review Page</td>
<td>222</td>
</tr>
<tr>
<td>Policy Page</td>
<td>223</td>
</tr>
<tr>
<td>Policy Details Page</td>
<td>224</td>
</tr>
<tr>
<td>Policy Fields</td>
<td>224</td>
</tr>
<tr>
<td>Impact on Policies When CVSS Version Changes on System</td>
<td>228</td>
</tr>
<tr>
<td>Custom Detection Rules Tab</td>
<td>228</td>
</tr>
<tr>
<td>Custom Detection Rule Dialog</td>
<td>230</td>
</tr>
<tr>
<td>Edit Custom Rule Dialog</td>
<td>233</td>
</tr>
<tr>
<td>License Details Window</td>
<td>235</td>
</tr>
<tr>
<td>Lookup Component Window</td>
<td>236</td>
</tr>
<tr>
<td>Add Project Dialog</td>
<td>237</td>
</tr>
<tr>
<td>Preferences Page</td>
<td>238</td>
</tr>
<tr>
<td>Add Token Dialog</td>
<td>239</td>
</tr>
<tr>
<td>Edit Token Dialog</td>
<td>240</td>
</tr>
<tr>
<td>Advanced Inventory Search Page</td>
<td>241</td>
</tr>
<tr>
<td>Import Project Data Dialog</td>
<td>244</td>
</tr>
</tbody>
</table>

A  FlexNet Code Insight User Roles and Permissions ......................... 247

System Roles and Permissions .................................................. 247
Project Roles and Permissions .................................................. 249
Roles and Permissions to Manage Project Task Flow .................... 251
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/
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
- Managing Policy Profiles
- Managing Authorization Tokens
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:

   Note • 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.

Task
To access online help and guides, do the following:

1. To access the online help, click the Help icon ( ) from any page in the product. Help is displayed for that page.
2. To access the online guides, click the Open Menu icon ( ) and select HELP from the menu. A list of available online documentation appears.

Changing Your Password

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

Task
To change your current Code Insight password, do the following:

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

2. Select Preferences to open the Preferences page.
3. Enter your new password in New Password, and then reenter it in New Password Confirm.
4. Click Update Password.

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.

- **Security-focused project**—The policy profile selected for the project triggers an automatic review of project inventory based on the presence of security vulnerabilities, on the CVSS scores and severity of these vulnerabilities, and on other criteria.

- **Project focused on intellectual-property protection**—The policy profile selected for the project triggers an automatic review of project inventory based on the presence of black-listed and white-listed components, version ranges, and licenses.
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.
   - **Policy Profile**—From the dropdown menu, select a policy profile to be used for this project. If you do not select a policy profile, the Default License Policy Profile will be used. For more information about policy profiles, see Managing Policy Profiles.

**Note** • The Project Visibility setting can also be accessed through the Edit Project option on the Manage Project menu on the Summary tab. For more information, see Editing the Project Definition and General Settings.
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 <strong>Summary</strong> 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>
<tr>
<td>5.</td>
<td>From the <strong>Edit Project</strong> dialog, navigate to the <strong>Scan Settings</strong> 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.)</td>
</tr>
</tbody>
</table>
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.
**Task** 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` archive. 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 jars.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.

<table>
<thead>
<tr>
<th>Scan Status:</th>
<th>Project being scanned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Progress:</td>
<td>In Scan Queue (Show Details)</td>
</tr>
<tr>
<td>Last Scan:</td>
<td>Scan of project Project2 completed</td>
</tr>
<tr>
<td>Past Scans:</td>
<td>Click here to view the scan history for this project</td>
</tr>
</tbody>
</table>

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 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. 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. 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.
For a “Component” Inventory Type

The inventory priority is set to P1 if either 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 What Does an Analyst do?).

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

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 What Does an Analyst do?) unless that would mean lowering an existing priority.

Note • Due to the algorithm used to calculate the priority, the 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>
<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:
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 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 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 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](image)

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 icon, you can view both CVSS score values.

- 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-2019-5407

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 the **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.

<table>
<thead>
<tr>
<th>Distribution Type</th>
<th>Inventory Details</th>
<th>Component Details</th>
<th>As-Found License</th>
<th>Notes &amp; Guidance</th>
<th>Usage</th>
<th>Associated Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Type</td>
<td>External</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part Of Product</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linking</td>
<td>Statically Linked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Distribution Type**—Indicates how you are distributing the item. The distribution type can affect license priority and obligations.
Chapter 2  Using FlexNet Code Insight
Overview of Scan Results

- **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 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 this license by simply clicking next to any license reference in Analysis Workbench or the Project Inventory tab.

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, as described in Viewing Details for Licenses Associated with Codebase Files.
- From Project Inventory, you view this information by inventory item, as described in Viewing Details for the Licenses Associated with Project Inventory.
- Whenever you create or edit an inventory item or preform 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>
<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>🟠</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>🔴</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 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 Licenses & Notices 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.
The following shows the License & Notices tab in Analysis Workbench:

![License & Notices tab in Analysis Workbench](image)

This shows the License & Notices tab in Project Inventory:

![License & Notices tab in Project Inventory](image)

The As-Found License Text content cannot be edited, but you can copy it to the Notices Text field (also on the Licenses & Notices tab as shown in the example) 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 Licenses & Notices 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.
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 2019 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 do to 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:

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:

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.
- **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 

   ![Folder] in its entry. A new file search is created with “Copy of...” in its title.
4. In the entry for the copy, click 

   ![Folder] 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 

   ![Folder] 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 

   ![Folder] 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 \( \times \) 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><img src="new-evidence" alt="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>!&lt;span class=&quot;check-mark&quot;&gt;&lt;/span&gt;</td>
<td>Reviewed</td>
<td>marked as “reviewed”.</td>
</tr>
<tr>
<td><img src="exact" alt="Icon" /></td>
<td>Exact</td>
<td>that are exact matches to known third-party files.</td>
</tr>
<tr>
<td><img src="copyrights" alt="Icon" /></td>
<td>Copyrights</td>
<td>containing copyright information.</td>
</tr>
<tr>
<td><img src="emailurls" alt="Icon" /></td>
<td>Email/URLs</td>
<td>containing email addresses or URLs.</td>
</tr>
<tr>
<td><img src="licenses" alt="Icon" /></td>
<td>Licenses</td>
<td>containing license information.</td>
</tr>
<tr>
<td><img src="search-terms" alt="Icon" /></td>
<td>Search Terms</td>
<td>containing search terms defined in the scan profile.</td>
</tr>
<tr>
<td><img src="source" alt="Icon" /></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:

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](example.png)

   - **Copyrights (0)**
   - **Email/URLs (4)**
     - http://getbootstrap.com
     - https://github.com/twbs/bootstrap/issues
     - jacobthornton@gmail.com
     - markdotta@gmail.com
   - **Licenses (1)**
     - MIT license (Expat) 🟢
   - **Search Terms (0)**
     - No Results

**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 (🗂️) 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 **What Does an Analyst do?** 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To view strings that are present in a binary file, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Ensure that you have selected a binary file in the <strong>Codebase Files</strong> panel, and click <strong>File Details</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Partial Matches</strong>. The <strong>File Details</strong> panel displays the strings that are output.</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional) Click the expand arrow (⏷), to view additional options. The top portion of the tab expands to show details about the binary file.</td>
</tr>
</tbody>
</table>

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

For the currently selected codebase file, use this procedure to view highlighted highlight 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To view copyright, email, URL, and license content in a file, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the <strong>Codebase Files</strong> pane or <strong>File Search Results</strong> 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.)</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>File Details</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the <strong>Partial Matches</strong> tab to show the contents of the file.</td>
</tr>
</tbody>
</table>

Color-code selection boxes at the top of the **Partial Matches** tab are used to indicate the type of evidence highlighted in the file. You can hover over a selection box to see a label indicating the type of evidence it highlights. Depending on the types of evidence existing in the file, certain selection boxes might already be selected; others might not be available. (By default, the Licenses selection box is not pre-selected even if license evidence exists in the file; you must manually select it to highlight license evidence.)
4. If necessary, select (or unselect) one or more color-coded selection boxes to highlight the evidence you want to view in the file. For example, the following color-coded selection will highlight (in the same color) each instance of email or URL evidence in the file:

![Color-coded selection example]

**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 have exact matches (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 **Remotes 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:

![Color-coded selection boxes](image)

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.

![Search filter](image)

**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 or Editing Inventory Usage Information from Analysis Workbench**
- **Component Lookup**
- **Creating an Inventory Item from the 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.

**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.)

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.
Chapter 2 Using FlexNet Code Insight
Analyzing (Auditing) Scan Results

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 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.

**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**.

**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”
Chapter 2  Using FlexNet Code Insight
Analyzing (Auditing) Scan Results

- **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

![Tip]

**To perform a Component Lookup, do the following:**

1. Open a project and navigate to **Analysis Workbench** (or the **Project Inventory** tab).
2. Select an inventory item from the list in the **Inventory Items** pane. The item appears in the **Inventory Details** pane. (For an item selected from the **Project Inventory** tab, you need to also click **Edit Item** to proceed with the next step.)
3. From the **Type** dropdown, select **Component** and click **Lookup Component**. The **Lookup Component** window appears.
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.)

<table>
<thead>
<tr>
<th>Task</th>
<th>To create inventory from the Inventory Items list, 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.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Add New at the top of the Inventory Items list. A new item, showing default values, opens in its own tab on the Inventory Details tab.</td>
</tr>
<tr>
<td>4.</td>
<td>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):</td>
</tr>
<tr>
<td></td>
<td>• 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:</td>
</tr>
<tr>
<td></td>
<td>&lt;COMPONENT_NAME&gt; &lt;VERSION&gt; (LICENSE_NAME)</td>
</tr>
</tbody>
</table>
• 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**.

7. (Recommended) On the **Notes** tab, add content to the **Audit Notes** pane 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 associate 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.

Task
To edit an inventory item in Analysis Workbench, do the following:

1. If not already on the Analysis Workbench, navigate to it.

2. Navigate to the Inventory Items list in the right pane.

3. Select the inventory item that you want to edit.

   A new tab, labeled with the inventory name and showing information about the inventory item, is opened within the Inventory Details tab.

4. 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.
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.

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).
Chapter 2  Using FlexNet Code Insight

Reviewing Published 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 for the Licenses Associated with Project Inventory
- Viewing and Updating Notes & Guidance
- Viewing Usage Information for Project Inventory
- Viewing Associated Files
- Creating Inventory from the Project Inventory Tab
- Editing Inventory from the Project Inventory Tab
- Approving or Rejecting Inventory Items
- Creating and Viewing External Work Items for a Project Inventory Task
- Recalling a Published Inventory Item
- Managing Security Vulnerability Alerts

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.

Task  To view project inventory, do the following:
1. Open a project and click the Project Inventory tab. The Inventory Items list pane is displayed on the left.
2. 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.
3. Select any of the tabs to display additional information about the inventory item.
4. To view the published inventory items sequentially:
   - Use the up and down arrows on your keyboard to step through inventory items quickly.
   - Use the Next Item and Previous Item buttons to move among inventory items.
5. 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.

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 inventory name, associated security vulnerabilities, and open security vulnerability alerts. In this way, you can easily find the inventory items of interest in 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.
Chapter 2 Using FlexNet Code Insight

Reviewing Published Inventory

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 Page.

- **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.)

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

1. If you are not there already, navigate to the Project Inventory tab.
2. Click a published inventory item from the Inventory Items list.
3. Select the Component Details tab. If known security vulnerabilities exist for the inventory item, the Vulnerabilities graph is displayed:

![Vulnerabilities: 0 1 7 2 7](image)

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 for the Licenses Associated with Project Inventory

You can view more details about the licenses that are part of your inventory on the License Details window. The information on this window is pulled from the FlexNet Code data library and 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).

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. Click a published inventory item from the Inventory Items list.
3. Select the Component Details tab. The license selected for this component is listed as the selected license.
4. Click the information icon (ℹ️) next to the Selected License value (the license currently associated with the inventory item) or the Possible Licenses (other valid license candidates with which you could associate the inventory item). 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 What Does an Analyst do? 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.

Viewing and Updating Notes & Guidance

The Notes & Guidance tab provides notes from the analysis and any guidance necessary to remediate the issue.

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 to view or edit notes that can help in reviewing or remediating the inventory item. For example, if the inventory item was manually created, you might include a note that specifies this.
4. Review or update content in the panes as needed.

Should no license information be available on the As-Found License tab (see Viewing and Updating Notes & Guidance), you can use the Notices Text pane on this tab to provide the exact notices text that you want to include for the inventory item in the Notices report. See Generating the Notices Report for more information.

5. 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:

  \(<\text{COMPONENT\_NAME}> \ <\text{VERSION}> \ (\text{LICENSE\_NAME})\)

- 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.

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.

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**.

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

### 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 **Creating Inventory from the Project Inventory Tab** 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.
   - 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 (-pencil) 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>To approve or reject inventory items, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Inventory Items list.</td>
</tr>
<tr>
<td>2.</td>
<td>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. 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.</td>
</tr>
</tbody>
</table>

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 Project Inventory 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 Advanced Search button to open the Advanced Inventory Search dialog. From here you can filter inventory items accordingly. When you select the specific inventory item, the Inventory Details tab for the item is displayed.</td>
</tr>
<tr>
<td>3.</td>
<td>In the Tasks section, click the Create Task button to open the Create Task 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.

---

**Task**

To edit a task, do the following:

1. Navigate to the **Project Inventory** page.
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.

![Create Task Dialog](image.png)

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.
Chapter 2 Using FlexNet Code Insight

Reviewing Published Inventory

**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.
   
   ![Resolution Type](image)

   - 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.

   ![Close Task](image)

   - 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**
Chapter 2  Using FlexNet Code Insight

Reviewing Published Inventory

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>
<tr>
<td>6.</td>
<td>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.</td>
</tr>
<tr>
<td>7.</td>
<td>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.</td>
</tr>
<tr>
<td>8.</td>
<td>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.</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.
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
- 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.
Task

**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.
Managing Security Vulnerability 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>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>The alert type. Currently, only New Vulnerability 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></td>
<td>• <strong>High</strong>—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></td>
<td>• <strong>Medium</strong>—The default when the severity level is Medium in either scoring system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong>—The default when the severity level is Low in either scoring system.</td>
</tr>
<tr>
<td></td>
<td>You can change this value as needed. See Changing the Priority of an Alert.</td>
</tr>
<tr>
<td></td>
<td>For more information about the severity levels for security vulnerabilities, see Viewing Security Vulnerabilities for Project Inventory.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The status of the alert in FlexNet Code Insight:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open</strong>—The alert needs to be addressed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>Change this value as needed. See Changing the Status of an Alert.</td>
</tr>
</tbody>
</table>
Filtering Alerts

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

Task

To filter the list of alerts, do the following:

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

   ![Alerts for openssl 1.0.2o (OpenSSL)](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.
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.

   ![New Custom Component Window]

   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 ![Help button](help-button.png) 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**.)
If Code Insight does not recognize the URL as belonging to a supported domain (that is, it is unable to parse the URL), the **New Custom Component** window opens showing the URL only. You must click **Get Details** to complete the component fields manually in **Free Form** mode. (Click **OK** on the “Unable to parse URL...” message box to proceed to Free Form mode.)

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 ![example](https://hub.com) 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.)

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 an 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**.)

   - 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

Note that New Custom Component window opens in the Free Form mode, 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 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 ![Exclamation Point](image) 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.

**Task**

**To associate an instance of the new custom component with the inventory item you are creating or editing, follow these steps:**

1. On the **Lookup Component** window showing the custom component you just created, click **Show Instances**.
2. Click **Register New Instance** to create a component instance.
3. Complete the instance registration by selecting **Create Custom Version** to specify a version and then selecting the license to associate with the instance.
4. Click **Use This Instance** next to the new instance to associate it with the inventory item.

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.

**Task**

**To edit a custom component, do the following:**

1. From the page on which you are creating or editing inventory, select **Component** in the **Type** field for the inventory item.

   ![New Inventory](image)

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

3. Search for the custom component by keyword, URL, or forge.

4. Locate the component in the search results, and update the component in any of these ways:
   - Click **Edit Custom Component** to update the component properties. See **Custom Component Properties** for field descriptions.
   - Click **Show Versions** to create one or more component-version-license instances for the component.

5. Click **Use This Instance** next to an instance to associate it with the inventory item or click **Cancel** to close the **Lookup Component** window.

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>
<thead>
<tr>
<th>Component Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create Using</strong></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 URL value, located beneath the Create Using section, which is either pre-populated from the Component Lookup window or manually entered here. If necessary, click Get Details 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 Component Lookup window. See the URL 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><strong>URL</strong></td>
<td>(Available under Create Using during component creation when the URL form is selected) The project or forge URL for which you are creating the custom component.</td>
</tr>
<tr>
<td></td>
<td>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 URL is automatically updated to the other field values when you click Get Details.</td>
</tr>
<tr>
<td></td>
<td>If the URL does not belong to a supported domain, you must manually provide all remaining necessary component details. (Click Get details to display the fields.)</td>
</tr>
<tr>
<td></td>
<td>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>Name</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 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>Title</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 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>Description</td>
<td>A description of the custom component to provide any additional meaningful information about the component.</td>
</tr>
<tr>
<td>URL</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 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 NA.</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. |
Chapter 2 Using FlexNet Code Insight

Creating and Editing Custom Licenses

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.

   The Edit Version/License dialog is displayed.

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 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**.

   ![Create Custom License Window](image)

   **Create Custom License**
   
   **Name:** Rose 1.5 License  
   **Short Name:** Rose-1.5  
   **Family:** Public Domain Style  
   **Priority:** P3 - Permissive/Public Domain  
   **URL:**  
   **Description:**  
   **License Text:**

   (The Rose License)
   Copyright © Red Rose
   Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the 'Software'), to deal in the Software without restriction.

   The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

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>Name</td>
<td>The full name of the license (for example, <em>The Rose License 1.5</em>).</td>
</tr>
<tr>
<td>Short Name</td>
<td>A unique shorthand representation of the license. This is usually the license SPDX short identifier (for example, <em>Rose-1.5</em>).</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 or 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 in the future inventory items created automatically by the rule.

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To edit an existing custom detection rule, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Custom Detection Rules tab, following the procedure in Viewing All Current Custom Detection Rules.</td>
</tr>
<tr>
<td>2.</td>
<td>In the Actions column for the entry you want to update, click the (Edit) icon. The Edit Custom Rule dialog opens.</td>
</tr>
<tr>
<td>3.</td>
<td>Edit fields as needed. See Edit Custom Rule Dialog for a description of each field.</td>
</tr>
<tr>
<td>4.</td>
<td>Manage the codebase files for the rules:</td>
</tr>
<tr>
<td></td>
<td>• To add a file, click the Add File button and provide the file’s name and MD5 value.</td>
</tr>
<tr>
<td></td>
<td>• To remove a file from the rule, click the (Delete File) icon.</td>
</tr>
<tr>
<td>5.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To remove a custom detection rule from the Code Insight data library, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Custom Detection Rules tab, following the procedure in Viewing All Current Custom Detection Rules.</td>
</tr>
<tr>
<td>2.</td>
<td>In the Actions column for the entry you want to remove, click the (Delete) icon. You are asked to confirm the deletion.</td>
</tr>
</tbody>
</table>

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 pane to provide the exact content to include in the Notices report. For example, you can copy the As-Found License Text content to the Notices Text field and modify it as needed, or provide your own license text. This text might also include rules that you developed during your manual research on the inventory item. (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 only this field 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.

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 pane contains content populated by the Scan Server, best practice is to leave the Notices Text pane empty as long as edits are not required so that the report uses the license information found in the As-Found License Text pane.

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 Licenses & Notices tab.
Chapter 2  Using FlexNet Code Insight

Finalizing the Notices Text for the Notices Report

From Project Inventory, select an inventory item and open the Licenses & Notices tab.

2. In the Notices Text field, enter (or paste from a source such as the content in the As-Found License Text field) the license content for the inventory item.

3. Modify and format the text exactly as you want it to appear in the Notices report.
4. Select **Save** to save your changes.

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.
Chapter 2  Using FlexNet Code Insight
Accessing and Viewing Projects in the System

Task  To open the Projects list, do the following:

1. From the FlexNet Code Insight Dashboard, select go to project.

   Alternatively, click the Open Menu icon in the upper right of any FlexNet Code Insight page:

   ![](image)

   The Projects list is displayed.

   ![](image)

   (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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To quickly filter inventory on the Project Dashboard, do the following:</strong></td>
</tr>
<tr>
<td>1. Open the <strong>Project Dashboard</strong> for a project. See Using the Project Dashboard.</td>
</tr>
<tr>
<td>2. Navigate to a chart and click a color-coded area. The project is opened to its <strong>Project Inventory</strong> 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. Click on a project inventory item listed to see more detail in the right pane of the <strong>Project Inventory</strong> 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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To open a project, do the following:</strong></td>
</tr>
<tr>
<td>1. Navigate to the <strong>Projects</strong> list. See Navigating to the Projects List for instructions.</td>
</tr>
<tr>
<td>2. Select a project in the <strong>Projects</strong> list. Its <strong>Project Dashboard</strong> is displayed on the right.</td>
</tr>
<tr>
<td>3. To open the project, either click the <strong>Open Project</strong> icon (Esp) next to the project entry in the <strong>Projects</strong> 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.

---

**Table 2-8 • Available Filters for Searching Across Projects (cont.)**

<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>Inventory impacted by a specific security vulnerability</td>
<td>Security Vulnerability</td>
<td>The complete ID of the security vulnerability</td>
<td>CVE-2018-11776 for an NVD vulnerability</td>
<td>Searching All Projects for a Security Vulnerability Advisory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SA40575 for a Secunia advisory</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DSA-4315 for a Debian advisory</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To search all projects for inventory based on a specific component and version, do the following:</strong></td>
</tr>
</tbody>
</table>

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 (for example, in the case of a zero-day vulnerability for which an ID has not been published)—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.

**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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To search for projects affected by a specific security vulnerability, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the <strong>Projects</strong> list. See Navigating to the Projects List for instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>At the top of the list, select <strong>Security Vulnerability</strong> from search dropdown on the left.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Enter Vulnerability ID</strong> field, specify the complete ID of the vulnerability (for example, <strong>CVE-2018-11776</strong> for an NVD vulnerability).</td>
</tr>
<tr>
<td>4.</td>
<td>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 <strong>Projects</strong> list header to show the number of projects returned by the search.</td>
</tr>
<tr>
<td></td>
<td>If no inventory items meet the specified criterion, the <strong>Projects</strong> list shows “No Projects”.</td>
</tr>
<tr>
<td>5.</td>
<td>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.)</td>
</tr>
</tbody>
</table>

**Restoring the Full Project List**

Use this step to remove the filter from the **Projects** list and restore the full list.

<table>
<thead>
<tr>
<th>Task</th>
<th>To restore the full list of projects, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the <strong>Projects</strong> list. See Navigating to the Projects List for instructions.</td>
</tr>
</tbody>
</table>
2. At the top of the list, click the \( \times \) icon in the criterion field to remove the current Projects list filter:

![Projects list filter]

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
- Deleting a Project
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 reports that describe your aspects of the project:

- The Project Report
- The Audit Report
- The Notices Report

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).
2. Click the Generate Report menu and select Project Report. A prompt will appear, explaining that the report is being generated in the background. When the report has been generated, the Download hyperlink appears in the Project Report field.
3. Click the Download hyperlink and respond to the prompts to save the report. The report is saved in a .zip file in both JSON and Excel formats:
   - **JSON**—Can be processed programmatically to integrate with other applications.
• **XLSX**—Can be viewed in Microsoft Excel.

4. Navigate to the folder where you saved the report .zip file, and unzip the file.

5. When the files have been unzipped, double-click one of the files to open it.

6. (Optional) Select the tabs (**Summary, Priority Legend, Inventory Items, Tasks**, and so forth) at the bottom of the sheet to view additional report information.

### 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.

#### Task

To generate an Audit report, do the following:

1. Navigate to the **Summary** tab for the project (see Opening the Project Summary Tab).

2. Click the **Generate Report** menu and select **Audit Report**. A prompt will appear, explaining that the report is being generated in the background. When the report has been generated, the **View | Download** hyperlink appears in the **Audit Report** field.

3. Determine if you want to view or download the report:
   - To view the report in your browser, click **View**.
   - To download the report, click **Download**. You will be prompted to save the report, which will be saved in the following formats in a .zip file:
     - **HTML**—Can be viewed in any browser.
     - **JSON**—Can be processed programmatically to integrate with other applications.
     - **XLSX**—Can be viewed in Microsoft Excel.

4. Navigate to the folder where you saved the report .zip file, and unzip the file.

5. When the files have been unzipped, double-click one of the files to open it.

6. (Optional) Select the tabs (**Summary, Priority Legend**, and so forth) at the bottom of the sheet to view additional report information.

### 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).

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 License & Notices 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 License & Notices 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>2.</td>
<td>Select Notices Report from the Generate Report dropdown. 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>3.</td>
<td>Click OK. When the report has been generated, the View</td>
</tr>
<tr>
<td>4.</td>
<td>Determine if you want to view or download the report:</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. On the prompt that appears, choose the next action for the report download:</td>
</tr>
<tr>
<td></td>
<td>Open—The report opens in your default text editor.</td>
</tr>
<tr>
<td></td>
<td>Save—The report is saved in the specified directory.</td>
</tr>
<tr>
<td></td>
<td>Cancel—The report is not downloaded.</td>
</tr>
</tbody>
</table>

### 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 switch 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).

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 set the minimum inventory confidence level for publishing inventory and to automatically mark files associated with an auto-published inventory as “reviewed”.

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, the associated options, Mark associated file as reviewed and Minimum inventory confidence level, are made available for updating. 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.

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.

Task

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 the 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>$COMPONENT_NAME</td>
<td>Name of the component associated with the inventory item</td>
</tr>
<tr>
<td>$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.
Chapter 2 Using FlexNet Code Insight

Managing a Project from the Summary Tab

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?**)

Both analysis types run separate scans. When you run the initial scan on your codebase, they each 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 or with your Code Insight configuration or version prior to the rescan. 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

**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>Details</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>
</tbody>
</table>

**Automated Analysis rule set**

<table>
<thead>
<tr>
<th></th>
<th>Full rescan</th>
<th>No rescan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules are automatically pushed to your Code Insight server through both an internal process and the weekly Electronic Update.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2-10 • Change Events Resulting in Full or Incremental Rescans (cont.)

<table>
<thead>
<tr>
<th>Changes to…</th>
<th>Automated Analysis</th>
<th>Advanced Analysis</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexNet Code Insight version</td>
<td>Full rescan</td>
<td>No rescan</td>
<td>This change is usually 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>
<tr>
<td>CL version</td>
<td>No rescan</td>
<td>Full rescan</td>
<td>This change is associated with a change to the CL Path value identified in the Scan Server setup. (This setup is handled by the Administrator, as described in the FlexNet Code Insight Installation and Configuration Guide.)</td>
</tr>
</tbody>
</table>

**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.
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:

- The component version string or the associated license
- Codebase-file associations (only in Analysis Workbench)
- Inventory properties 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 would remove the associations you defined and re-apply them to the inventory item identified in the rule set.

The following topics describe how the rescan process handles edited inventory:

- Rescan Rules to Preserve Your Inventory Edits
- Rescan Scenario: Handling of Files Manually Disassociated from Inventory Before Rescan
Rescan Rules to Preserve Your Inventory Edits

To ensure that inventory changes are preserved, the rescan applies the following rules to edited inventory:

- All the user-created inventory, its file associations, and edits are considered not system-updatable and therefore are preserved.

- Any change to a system-generated inventory item (including the 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 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 you 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>
</tbody>
</table>
2. Perform either step:
   - 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.
   - 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.)

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

<table>
<thead>
<tr>
<th>Scan Status</th>
<th>Project being scanned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Progress</td>
<td>In Scan Queue (Show Details)</td>
</tr>
<tr>
<td>Last Scan</td>
<td>Scan of project Project2 completed. Scan Summary: 358 Files</td>
</tr>
<tr>
<td>Past Scans</td>
<td>Click here to view the scan history for this project</td>
</tr>
</tbody>
</table>

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.

---

**Exporting Project Data**

FlexNet Code Insight allows you to export your project data to a JSON data file for use elsewhere. For detailed information on the export feature, see the Exporting and Importing Project Data chapter.

<table>
<thead>
<tr>
<th>Task</th>
<th>To export project data, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>As Project Owner, navigate to the <strong>Summary</strong> tab (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Manage Project</strong> and select <strong>Export Project Data</strong> from the dropdown menu.</td>
</tr>
<tr>
<td>3.</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

**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.

---

**Exporting Project Data**

FlexNet Code Insight allows you to export your project data to a JSON data file for use elsewhere. For detailed information on the export feature, see the Exporting and Importing Project Data chapter.

<table>
<thead>
<tr>
<th>Task</th>
<th>To export project data, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>As Project Owner, navigate to the <strong>Summary</strong> tab (see Opening the Project Summary Tab).</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Manage Project</strong> and select <strong>Export Project Data</strong> from the dropdown menu.</td>
</tr>
<tr>
<td>3.</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

**Note** • You can also use the public REST API to export your project data. For more information, see the Exporting and Importing Project Data chapter.
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 your 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To add a new policy profile or edit an existing one, 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 Policy from the menu to open the Policies page, showing the list of current policy profiles.</td>
</tr>
<tr>
<td>3.</td>
<td>To edit an existing policy profile, select it from the list, and click the Edit icon.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>To add a new policy profile, click Add Policy.</td>
</tr>
<tr>
<td></td>
<td>The Policy Details page is displayed.</td>
</tr>
<tr>
<td>4.</td>
<td>Refer to the associated help (or to Policy Details Page) for details about the fields used to define the policy profile.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Save to save the updates or to add the new policy profile.</td>
</tr>
</tbody>
</table>

Copying a Policy Profile

The following procedure describes how to create a copy of 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 Open Menu icon in the upper right of any FlexNet Code Insight page:</td>
</tr>
<tr>
<td>2.</td>
<td>Select Policy from the menu to open the Policies 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 Copy icon.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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
- 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>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, click <strong>Add Token</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter a name for the new token and specify an expiration date (or choose <strong>Never Expires</strong>).</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Save</strong>.</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>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 copy, and click the <strong>Copy to clipboard</strong> icon (/button) in the <strong>Actions</strong> column.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Select Token Text</strong> to select the entire token value, and then press Ctrl + C to copy it.</td>
</tr>
<tr>
<td>4.</td>
<td>Paste token in the appropriate location for use by the REST interface.</td>
</tr>
</tbody>
</table>

# 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 <strong>Edit</strong> icon (/button).</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 Preferences page (see Accessing the Preferences Page).</td>
</tr>
<tr>
<td>2.</td>
<td>From the AUTH Tokens pane, locate the token you want to edit, and click the Edit icon (X).</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 Page

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>
</table>
| Any             | By Notification           | 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. | Inventory with Open Alerts = checked  
Inventory Rejected Due to New Non-Compliant Security Vulnerabilities = checked |
| Any             | By Inventory Task Age     | Inventory tasks (review or remedial tasks) created within the specified date range.  
Useful for filtering on inventory items that have recently created tasks to determine what new work needs to be performed. | Inventory Tasks Age = Last 7 days  
Inventory Tasks Age = Custom Date Range  
From: 09/05/2018 To: 10/31/2018 |
| Any             | By Inventory Task Owner   | Inventory tasks (review or remedial tasks) owned by a specific user. | Inventory Tasks Owner = Any  
Inventory Tasks Owner = Only mine (current user)  
Inventory Tasks Owner = <Username> (selected user) |
| Analyst, Reviewer | By Confidence Level       | 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. | Inventory Confidence Level = High (or Medium or Low) |
### 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>Security Analyst</td>
<td>By Vulnerability ID</td>
<td>Inventory with a specific vulnerability (NVD CVE or Secunia Advisory). Use useful when you are looking for inventory exposing you to a specific security issue, typically a newsworthy event.</td>
<td>Security Vulnerability ID = SA71946</td>
</tr>
<tr>
<td></td>
<td>By Security Risk Exposure</td>
<td>Inventory containing security vulnerabilities of a specified severity. Useful 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>Security Vulnerability Severity = High</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By Security Vulnerability Age</td>
<td>Inventory with new security vulnerabilities since a specified date. Useful to see which inventory items have new security vulnerabilities reported against them based on the specified date range.</td>
<td>Security Vulnerability Age = Last day</td>
</tr>
<tr>
<td></td>
<td>By Security Risk Exposure and Vulnerability Age</td>
<td>Inventory with new security vulnerabilities of a specified severity since a specified date. Useful to see which inventory items have new security vulnerabilities reported against them based on the specified date range and a certain severity.</td>
<td>Security Vulnerability Age = Last day and Security Vulnerability Severity = High</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>By Inventory Alert</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 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>
</tbody>
</table>
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.

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>Security Analyst</td>
<td>By New Vulnerabilities (Requires re-review)</td>
<td>Inventory that has gained a new security vulnerability since a specified date.</td>
<td>Review Status = Approved and Security Vulnerability Age = Last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useful to determine which inventory items require another look from a security analyst due to new associated vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>By License Risk Exposure</td>
<td>Most critical inventory that requires legal review (contains a P1 license - Viral/Strong Copyleft).</td>
<td>License Priority = P1 - Viral/Strong Copyleft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useful to prioritize legal work based on license classification.</td>
<td></td>
</tr>
<tr>
<td>Analyst</td>
<td>Requires Re-Review based on Missing License</td>
<td>Approved inventory with a missing license.</td>
<td>Inventory Review Status = Approved and License Priority = No License Found</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Useful to catch scenarios where items were approved without an associated license. This should be a rare event.</td>
<td></td>
</tr>
<tr>
<td>Eng. Mgr./Final Reviewer</td>
<td>Stop Shipment!</td>
<td>Approved inventory that may require a stop shipment due to high severity vulnerability or P1 license.</td>
<td>Inventory Review Status = Approved or License Priority = P1 - Viral/Strong Copyleft or Security Vulnerability Severity = High</td>
</tr>
</tbody>
</table>

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”.

By default, only inventory from the source project that remains relevant in the target project (based on associated codebase files that match in both the source and target projects) is processed during import. For example, “foo-v1” inventory without a matching associated file match in “foo-v2” is considered an “empty” inventory item and therefore will not be imported. If you want to change this default behavior to process all inventory (including empty inventory), use the `createEmptyInventory=true` flag during the import (see Available Import Options to Control Import Behavior for details).

- **Audit work reuse**—As in the versioning example above, you can use the export-import process to apply analysis work performed on one project to another project containing a subset of similar files. Export data from “project1”, scan “project2” (pointed to “project2” codebase), and import the data into “project2”. Likewise, this process can be used to apply analysis work from several different projects to the current project.
- **Sharing of live audit results between teams**—Use the export-import process to share live audit results between teams or with Flexera Professional Services. For example, you can export data from “project 1” on “instance 1” and import the data into “project 2” on “instance 2”. Results are imported either into an empty project for a live view of inventory or into a scanned project for a live view of inventory with file associations and access to the codebase file tree. To ensure that all inventory is processed, use the `createEmptyInventory=true` flag during the import (see Available Import Options to Control Import Behavior for details).

- **Migrating audited projects from FlexNet Code Insight v6 to v7**—Use import to create live project inventory in Code Insight v7 from exported v6 project or workspace data. After exporting data from a v6 project, run the Audit Data Migration Tool (available for download in the Flexera Product and License Center) to map inventory fields from Code Insight v6 to v7 and to convert the exported data to the proper JSON data format required for import into v7. Then perform an import into a Code Insight v7 project. Import into an empty project for a live view of inventory only or into a scanned project for a live view of inventory with file associations.

- **Creating inventory from an external system**—Use import to create project inventory in Code Insight from a data file containing legacy or external data. This type of import requires the conversion of the legacy data to the JSON format used by imported data prior to importing into the new project.

## 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 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)

Or

- 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 product 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.qV2j8ZLgLrGJns78OdPRwvE9-8y1x7w-0zrSh7jz2d9uqY8tvAcSv68posEU09tD-YX1gXznX-1GrrnopOU7G3w"
```
Exporting Project Data

The following sections provide the details about exporting project data:

- About an Export
- Types of Data Exported
- Prerequisites for Exporting Data
- Exporting Project Data Using the Web UI
- Exporting Project Data Using the REST Interface
- Verifying a Successful Export

**Important** • The instructions in this section assume that you are exporting data from the FlexNet Code Insight version for which this current documentation was published. These instructions might not apply to other Code Insight versions. If exporting project data to a different Code Insight version, consult the documentation included with that version for export instructions.

About an Export

During the export process, the project data is exported into a JSON data file and then compressed into a .zip archive. The archive file can be stored for backup purposes or imported into a project (described in Importing Project Data).

The export runs as a background process that does not interfere with scanning or analysis work.

Project data export is accessible through either of these options:

- The FlexNet Code Insight Web UI, as described in Exporting Project Data Using the Web UI.
- The FlexNet Code Insight REST interface, as described in Exporting Project Data Using the REST Interface.

**Note** • Currently, the Code Insight Web UI supports the export of data from only those projects created as “standard” (that is, with the Standard project-type attribute). To export data from projects created as “inventory only” (with the Inventory Only project-type attribute), you must use the Code Insight REST interface. You can view a project’s type on the Project Summary page. For more information about project types, see Creating a Project.
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.

**Task**

To export project data using the Code Insight Web UI, do the following:

1. Ensure that all requirements in Prerequisites for Exporting Data are met.
2. Log into Code Insight as the owner of the project you want to export.
3. Navigate to the **Project Summary** tab. See Project Summary Tab for information about the fields on this tab.
4. Open the **Manage Project** dropdown and select **Export Project Data**.

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.
Chapter 4  Exporting and Importing Project Data

Exporting Project Data

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:sers\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=55" -H "accept: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJJZCI6MSwiaWF0IjoxNTY2ODU5NTg2fQ.qV2j8ZLgNGNJsT8OdPRwvE0-0y1x7w-0zr5h7jz2d9uqY8tvACsV68posEU9tD-YX1lgXznX-IgnrnpoU7G3w" > ProjectKDR.zip

   The status of the export process appears in the command prompt window:

   ![Export Status]
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.

<table>
<thead>
<tr>
<th>Task</th>
<th>To verify a successful completion of the export process, do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Unzip the archive. If the export process was not successful, the .zip archive includes a file containing the appropriate status code and error message.</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional) Open the JSON data file with a utility that supports JSON, such as Textpad or Notepad++, to determine noticeable errors.</td>
</tr>
<tr>
<td>3.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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
- Importing Project Data Using the REST API
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 available through the FlexNet Code Insight REST interface, as described in Importing Project Data. The following sections provide overview information about the import process.

Input Used in the Import Process

The input to the API 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 to the API 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 the codebase files through Analysis Workbench. The inventory is live—that is, ready to be edited and reviewed.

Alternatively, an import can be performed on a project that was created as an “inventory only” project and that 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 through Analysis Workbench.

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 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>Performs a full import (that is, both inventory and codebase files are processed):</td>
<td>Performs a partial import:</td>
</tr>
<tr>
<td></td>
<td>• Processes all inventory items (published and unpublished).</td>
<td>• Processes inventory only.</td>
</tr>
<tr>
<td></td>
<td>• Per inventory item, provides inventory details, status, and associated repository item (component-version-license).</td>
<td>• Does not process codebase files (reviewed or unreviewed).</td>
</tr>
<tr>
<td></td>
<td>• Lists associated file paths for inventory.</td>
<td></td>
</tr>
<tr>
<td><strong>File processing</strong></td>
<td>Does the following:</td>
<td>Does not process files (reviewed or unreviewed).</td>
</tr>
<tr>
<td></td>
<td>• Processes all files marked as reviewed in the data file to be imported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provides absolute file paths and MD5s for processed files.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does not import unreviewed files.</td>
<td></td>
</tr>
<tr>
<td><strong>Custom-data processing</strong></td>
<td>Imports custom versions, custom licenses, and custom mappings.*</td>
<td>Imports custom versions, custom licenses, and custom mappings.*</td>
</tr>
<tr>
<td><strong>Required type for target project</strong></td>
<td>Requires a project created with the <strong>Standard</strong> attribute.</td>
<td>Requires a project created with the <strong>Inventory Only</strong> attribute.</td>
</tr>
<tr>
<td><strong>Target project codebase requirement</strong></td>
<td>Requires a codebase that is uploaded (or synchronized) to the target project and scanned.</td>
<td>Requires no codebase.</td>
</tr>
<tr>
<td><strong>Access to imported inventory and codebase files</strong></td>
<td>Provides direct access to the following:</td>
<td>Provides direct access to imported inventory through <strong>Project Inventory</strong>. (Access to inventory and codebase files through <strong>Analysis Workbench</strong> is not available.)</td>
</tr>
<tr>
<td></td>
<td>• Imported inventory through <strong>Project Inventory</strong> and <strong>Analysis Workbench</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Imported codebase files through <strong>Analysis Workbench</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
The import does not process custom components. Instead, FlexNet Code Insight creates target inventory of the work-in-progress (WIP) type or license-only type to represent inventory with custom components.

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.

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.

---

**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 export using REST API).
Import Behavior

The import process is initiated when you issue a cURL command that calls the REST API `importProjectData`, as described in Importing Project Data Using the REST API. The following sections provide information about the default import and options you can include with this API to reconfigure the import behavior.

- Default File and Inventory Processing During an Import
- Available Import Options to Control 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 Control 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 `checkInventory (default: false)` 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 `checkReviewed (default: true)` for more information.
- 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 `createEmptyInventory (default: false)` for more information.

Available Import Options to Control Import Behavior

The following options can be included with the `importProjectData` API to override the default import behavior (described in the previous section, Default File and Inventory Processing During an Import) as needed. See Importing Project Data Using the REST API for complete details about setting up the command for executing the import process.

If these options are not set, the default values apply.
checkInventory (default: false)

This option specifies whether file MD5 should be used as criteria (in instead of file path) when associating files to inventory in the target project during the import process. By default, this option is disabled, so that only files that match based on file path between the data file to be imported 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. However, if the file or the directory containing the file has been renamed in the target project codebase, but the file contents have not changed, you can use the file MD5 as criteria for associating files to inventory instead of using the file path.

With this option enabled, only files that match based on MD5 in the data file and the target project codebase will be associated with inventory in the target project. To change the default setting and thus enable the use of MD5 checks when associating files with inventory in the target project, include the `checkInventory=true` option as shown:

```
curl -X POST --data-binary @$PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/ importProjectData?projectId=PROJECT_ID&checkInventory=true"
```

checkReviewed (default: true)

This option specifies whether file MD5 should be used as criteria (instead of file path) when marking files as reviewed in the target project during the import process. By default, this option is enabled, so that only files that match based on MD5 between the data file to be imported and the target project codebase, are marked as reviewed in the target project. For example, the file “/ePortal-1.3/src/gettext.c”, marked as the “reviewed” in the data file, will be considered for marking as reviewed 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 and MD5.

However, with this option disabled, files need to have only a matching file path between the data file and the scanned target codebase in order to be processed as reviewed in the target project. To change the default setting and thus disable the use of MD5 checks when marking files as reviewed, include the `checkReviewed=false` option as shown:

```
curl -X POST --data-binary @$PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/ importProjectData?projectId=PROJECT_ID&checkReviewed=false"
```

createEmptyInventory (default: false)

This option determines whether “empty” 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.

By default, this option is disabled, preventing empty inventory items from being created in the target project. However, with this option enabled, all inventory items—with or without matching associated files in the target codebase—are created during the import. To change the default setting and thus enable the creation of empty inventory during the import, include the `createEmptyInventory=true` option as shown:

```
curl -X POST --data-binary @$PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/ importProjectData?projectId=PROJECT_ID&createEmptyInventory=true"
```

Other Import Considerations

Consider the following additional behavior during import processing.
Duplicate Inventory

Two inventory items are considered identical between the source and target project if they are associated with the same repository item (by component ID). Duplicate inventory is resolved during the import by overriding all fields in the target project with information from the data file to be imported, with the exception of empty data in the data file.

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 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>To initiate the import process, execute the following curl command to invoke the importProjectData REST API using the POST method. Replace the highlighted variables with your server host ID (hostname or IP address) and port, the project ID, and the authorization token. Also, replace PROJECT_DATA_FILE with the name of .zip archive containing the JSON data file you are importing.</td>
</tr>
</tbody>
</table>

```bash
```

The following is an example:

```bash
```

Note • Inventory items without file associations are never imported by default. If you are importing from a scanned project into an inventory-only project, you must add the createEmptyInventory=true option for inventory to be generated in the new project. See Available Import Options to Control Import Behavior for details.
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.

3. To verify that the import has completed successfully, follow these steps:
   
   a. Open the target project in FlexNet Code Insight and navigate to the **Inventory** page (see Searching the System).
   
   b. 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.)
   
   c. Confirm that the inventory items contain accurate inventory details and file path associations.
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**—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, BitBake recipe</td>
<td>Yocto</td>
<td>N/A</td>
<td>.bb</td>
<td>✔</td>
<td>N/A</td>
<td>N/A</td>
<td>See Notes for Yocto Ecosystems.</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-">https://go-</a> search.org</td>
<td>glide.yaml</td>
<td>✔</td>
<td>—</td>
<td>—</td>
<td>See Notes for Supported 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>http:// search.maven.org/</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>https:// registry.bower.io/packages/</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>https:// api.nuget.org/v3-flatcontainer/</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>
<tr>
<td>NodeJS</td>
<td>NPM</td>
<td>https:// registry.npmjs.org/</td>
<td>package.json</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.

**Notes for Supported 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.

**Notes for Supported 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.
Notes for 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.

Notes for Supported 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></td>
<td></td>
</tr>
<tr>
<td>Eclipse</td>
<td>An Eclipse workspace in the Eclipse IDE environment.</td>
<td></td>
</tr>
<tr>
<td>Visual Studio</td>
<td>A Visual Studio solution.</td>
<td></td>
</tr>
<tr>
<td><strong>CI Tools</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure DevOps</td>
<td>An Azure DevOps workspace as part of the build process.</td>
<td></td>
</tr>
<tr>
<td>Bamboo</td>
<td>A Bamboo workspace as part of the build process (on Local Agents only)</td>
<td></td>
</tr>
<tr>
<td>GitLab</td>
<td>GitLab projects as part of the build process.</td>
<td></td>
</tr>
<tr>
<td>Jenkins</td>
<td>A Jenkins workspace as part of the build process.</td>
<td></td>
</tr>
<tr>
<td>TeamCity</td>
<td>TeamCity projects as part of the build process.</td>
<td></td>
</tr>
<tr>
<td><strong>Package Manager</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Build Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ant</td>
<td>Apache Ant as part of the build process.</td>
<td></td>
</tr>
<tr>
<td>Gradle</td>
<td>Gradle projects as part of the build process.</td>
<td></td>
</tr>
<tr>
<td>Maven</td>
<td>Maven projects as part of the build process.</td>
<td></td>
</tr>
<tr>
<td><strong>Binary Repositories</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JFrog Artifactory</td>
<td>Artifactory repositories to identify non-compliant artifacts.</td>
<td></td>
</tr>
<tr>
<td><strong>Container Platforms</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Docker Images</td>
<td>Docker images on a Docker server.</td>
<td></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 <strong>Version Control Settings</strong> tab, navigate to it.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the <strong>Instance</strong> tab for the instance you want to delete.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Delete Instance</strong>. 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**
- **Configuring the 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 <strong>Adding an SCM Instance to the Code Insight Project</strong> to navigate to the <strong>Version Control Settings</strong> tab and add a Git SCM instance, selecting <strong>Git</strong> from the <strong>Application</strong> dropdown.</td>
</tr>
<tr>
<td>2.</td>
<td>See <strong>Configuring the Git SCM Instance</strong> 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 <strong>Testing an SCM Instance</strong>.</td>
</tr>
</tbody>
</table>
Configuring the 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>
<tbody>
<tr>
<td>Git Repository URL</td>
<td>Provide the repository URL in either format:</td>
</tr>
<tr>
<td></td>
<td>• http(s)://&lt;host.xz&gt;/&lt;path&gt;/to/repo.git</td>
</tr>
<tr>
<td></td>
<td>• &lt;user&gt;@&lt;host&gt;:&lt;path&gt;/repo.git</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>&lt;scanroot&gt;/&lt;projectID&gt;/&lt;instanceID&gt;</td>
</tr>
<tr>
<td>Git Username</td>
<td>Provide the user name for Authenticated access to the repository.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Git Password</td>
<td>Enter the password associated with the user name provided.</td>
</tr>
<tr>
<td>Git Branch, Git Tag, or Git Commit ID</td>
<td>Specify either the Git branch, tag, or commit ID to identify the source code version to which to synchronize.</td>
</tr>
<tr>
<td></td>
<td>Alternatively, leave these fields blank to synchronize to the master branch.</td>
</tr>
</tbody>
</table>
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 Configuring the 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. If SSL has been configured for communication between the Perforce server and the Perforce client on Code Insight, execute the following command in p4 to establish the trust between the server and client. Unless this trust is established, connections between the Perforce server and client will fail.

   ```
   p4 -p ssl:<p4ServerHostID>:<p4Port> trust
   ```

   where p4ServerHostID and p4Port identify the hostID (hostname or IP address) and port of the Perforce server.

   When prompted to establish trust, enter yes.

4. Once you save the Perforce SCM instance, test the Code Insight connection with Perforce SCM instance, as described in Testing an SCM Instance.

Configuring the Perforce SCM Instance

The following settings are used to configure a Perforce 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>
</table>
| **URL (P4PORT)**            | Provide the URL of the Perforce instance with which to synchronize. Note the following example URL formats: **For a TCP connection**
  tcp:<p4ServerHostID>:<p4Port>  |
|                             | **For an SSL connection**
  ssl:<p4ServerHostID>:<p4Port>  |
| **Username (P4USER)**       | Provide the user name that has access to the Perforce depot to which this instance is synchronizing. |
| **Password (P4PASSWD)**     | Provide the password associated with the user name provided. If you are using a P4 ticket provided by the Perforce administrator, this field is optional. |
| **Branch Spec (P4CLIENT)**  | Provide the path to the branch to which this instance is synchronizing. |
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>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>

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
- Configuring the 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.

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 TFS SCM instance, selecting TFS from the Application dropdown.

2. See Configuring the 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.
Configuring the 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>
<tbody>
<tr>
<td><strong>TFS URL</strong></td>
<td>Provide the URL of the TFS with which to synchronize. Note the following example URL formats. For the latest version of TFS: <code>&lt;protocol&gt;://&lt;tfs_host&gt;:&lt;port&gt;/&lt;collection&gt;/&lt;project&gt;</code> For earlier versions of TFS: <code>&lt;protocol&gt;://&lt;tfs_host&gt;:&lt;port&gt;/&lt;collection&gt;/&lt;tfsroot&gt;/&lt;project&gt;</code></td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Changeset</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td>(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.</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring Source Code Management

Configuring a TFS SCM Instance
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 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>
<tr>
<td>identified</td>
<td>Displays the number of OSS items that were identified in your codebase.</td>
</tr>
</tbody>
</table>
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>
<tr>
<td>Actions</td>
<td>This column contains the pencil icon (✏️). Click it to open the Edit User dialog, where you can edit information about the selected user.</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
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>

See Also
Users/Permissions Tab

See Also
Add User Dialog
Edit User Dialog
“Configuring FlexNet Code Insight” in the FlexNet Code Insight Installation & Configuration Guide
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 8-4 • Edit User dialog**

<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 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 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 <strong>Submit</strong> 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 <strong>Cancel</strong> 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**
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><strong>General</strong></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 <a href="#">Specifying an Update as Server or Local</a>.</td>
</tr>
</tbody>
</table>
| **Electronic Update Type** | Select the type of Electronic Update to run based on how the FlexNet Code Insight server obtains the Update Manifest and Update Data files required to perform the update:  
  - **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.  
  - **Server**—The most recent Electronic Update files are automatically downloaded from Flexera to the Code Insight server as part of the Electronic Update process. |
| **Local Electronic Update configuration** | 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. |
Chapter 8  Pages and Panels

Electronic Updates Tab

Table 8-5  Electronic Updates tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration for automatic Electronic Updates (server update only)</td>
<td>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.</td>
</tr>
<tr>
<td>Update Frequency</td>
<td>Select from one of the available frequencies for running an incremental Electronic Update automatically:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Daily—If you select Daily, a second dropdown is displayed to choose the time of day when you want the Electronic Update to occur.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Save Schedule</td>
<td>Click this button to save the schedule. Your future incremental updates will run automatically according to the frequency you defined.</td>
</tr>
<tr>
<td>Configuration for manually running an Electronic Update</td>
<td>You can manually run an Electronic Update at any time. The update is run immediately or placed in queue and initiated once all pending scans have completed. Currently, this is the only way to schedule a local update. If automatic server updates are also configured, a manually-run update is in addition to the automatic updates.</td>
</tr>
<tr>
<td>Run Update Now</td>
<td>Select the scope of the manually-run update:</td>
</tr>
<tr>
<td></td>
<td>• Incremental Update—Schedule an incremental Electronic Update. However, if no changes have occurred in the Electronic Update data since it was last run, the update is not executed.</td>
</tr>
<tr>
<td></td>
<td>• Full Update—Force a full Electronic Update to run whether or not changes have occurred in the Electronic Update data since it was last run. Use this option judiciously as a full Electronic Update takes several hours to complete, similar to the time required to run the initial update when FlexNet Code Insight was installed.</td>
</tr>
<tr>
<td>Update</td>
<td>Click this button to initiate the Electronic Update immediately or once pending scans are completed.</td>
</tr>
</tbody>
</table>

See Also
“Configuring FlexNet Code Insight” chapter in the FlexNet Code Insight Installation & Configuration Guide
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 8-6 • Email Server tab

<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>
<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>

LDAP Tab

The LDAP tab on the Administration page allows you to enable LDAP logins for FlexNet Code Insight and edit information about your LDAP setup. The tab contains the following columns and fields:

Table 8-7 • LDAP tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP</td>
<td>Select Yes or No to determine if LDAP will be used for user authentication. The default is No.</td>
</tr>
</tbody>
</table>

LDAP Connection Details

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP URL</td>
<td>Specify the URL of your LDAP server in this format: ldap://&lt;ldap_server_host&gt;:&lt;ldap_port&gt; The following is an example LDAP server URL: ldap://ad.mycompany.com:389</td>
</tr>
</tbody>
</table>
Table 8-7 • LDAP tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select the type of LDAP authentication that will be used:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anonymous</strong>—If you select this option, the LDAP <strong>Username</strong> and <strong>Password</strong> fields in this section remain disabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authenticated</strong>—If you select this option, the following LDAP fields are enabled.</td>
</tr>
<tr>
<td><strong>LDAP Username</strong></td>
<td>Enter the LDAP user name used for authentication, providing the user’s full Distinguished Name (DN). Note that the user must have permissions to query the LDAP server. This field is disabled if anonymous authentication is selected.</td>
</tr>
<tr>
<td><strong>LDAP Password</strong></td>
<td>Enter the password for the user name specified in the previous field. This field is disabled if anonymous authentication is selected.</td>
</tr>
<tr>
<td><strong>LDAP Query Details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LDAP Base</strong></td>
<td>Specify the base node of the LDAP server.</td>
</tr>
<tr>
<td><strong>LDAP Search Base</strong></td>
<td>Specify the Search Base, which, along with the Search Query, is used to query a list of users for synchronizing with FlexNet Code Insight.</td>
</tr>
<tr>
<td><strong>LDAP Search Query</strong></td>
<td>Specify the search query for your LDAP server. The following is an example search query:</td>
</tr>
<tr>
<td></td>
<td>(&amp;(objectClass=person)(memberOf=CN=SCAGroup,CN=Users,DC=ad,DC=mycompany,DC=com))</td>
</tr>
<tr>
<td><strong>Use Paging</strong></td>
<td>Select <strong>Yes</strong> if the LDAP server has paging enabled. Select <strong>No</strong> if the server does not have paging enabled. If you select <strong>Yes</strong>, the <strong>LDAP Page Size</strong> field is enabled.</td>
</tr>
<tr>
<td><strong>LDAP Page Size</strong></td>
<td>Indicate the page size. The default page size is 1000 elements.</td>
</tr>
<tr>
<td><strong>LDAP User Sync Frequency</strong></td>
<td>Specify the frequency at which FlexNet Code Insight will synchronize user data with the LDAP server:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Never</strong>—Select this option to disable the automatic user sync. A user sync will occur only if the user clicks the <strong>Sync Now</strong> button. For all other values, automatic user sync is enabled per the configured frequency. (This is the default value.)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hourly</strong>—Enter an integer value representing the number of hours between user syncs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong>—Select a time at which the user sync will run every day.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly</strong>—Select a day of the week and a time of the day when the user sync will run each week.</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>
<tbody>
<tr>
<td><strong>Existing Issues Sync Frequency</strong></td>
<td>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.)</td>
</tr>
<tr>
<td></td>
<td>• Never</td>
</tr>
<tr>
<td></td>
<td>• Hourly (enter number of hours)</td>
</tr>
<tr>
<td></td>
<td>• Daily (enter time of day)</td>
</tr>
<tr>
<td></td>
<td>• Weekly (enter day of the week and time of day)</td>
</tr>
<tr>
<td></td>
<td>Click ✓ to accept the updated synchronization frequency or ✗ to restore the previous frequency.</td>
</tr>
<tr>
<td><strong>Test Connection</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Delete Instance</strong></td>
<td>Click to delete the current ALM instance after verifying that no project references to this instance exist.</td>
</tr>
<tr>
<td><strong>ALM_type Instance Name</strong></td>
<td>Unique name of the ALM instance.</td>
</tr>
<tr>
<td><strong>ALM_type Server URL</strong></td>
<td>URL of the ALM server to which to connect in the format http(s):&lt;server_name_or_ip&gt;.</td>
</tr>
<tr>
<td><strong>ALM_type Username</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>ALM_type Password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Default Project Key</strong></td>
<td>Key for the project for which issues will be created on the ALM server.</td>
</tr>
<tr>
<td><strong>Default Issue Type</strong></td>
<td>The default issue type created on the ALM server.</td>
</tr>
<tr>
<td><strong>Default Priority</strong></td>
<td>Default priority of the issued created on the ALM server.</td>
</tr>
<tr>
<td><strong>Default Assignee</strong></td>
<td>The default user to whom to assign work items created for this instance.</td>
</tr>
<tr>
<td><strong>Default Summary Text</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Default Description Text</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alias</strong></td>
<td>The user-defined name for the Scan Server, as well as the server’s</td>
<td>The following icons represent the server status:</td>
</tr>
<tr>
<td></td>
<td>current status. The following icons represent the server status:</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></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></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><strong>Host</strong></td>
<td>The localhost value is used if the Scan Server is on the same instance</td>
<td>The localhost value is used if the Scan Server is on the same instance as the Core Server.</td>
</tr>
<tr>
<td></td>
<td>as the Core Server.</td>
<td></td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port used by the Scan Server on the host instance. By default, the port is 8888.</td>
<td></td>
</tr>
<tr>
<td><strong>CL Path</strong></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</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><strong>Codebase Path</strong></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>
<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>
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. 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.

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.

See Also
Scan Server Dialog

Scan Server Dialog

Click this button to add a new Scan Server. The Scan Server dialog is displayed.

### Table 8-9 • Scan Servers tab (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>![actions for scan server entry]</td>
<td>Select the appropriate icon for the desired action:</td>
</tr>
<tr>
<td>![action]</td>
<td>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.</td>
</tr>
<tr>
<td>![Add Scan Server]</td>
<td>Click this button to add a new Scan Server. The Scan Server dialog is displayed.</td>
</tr>
</tbody>
</table>
**Dialog Fields**

The **Scan Server** dialog contains the following fields:

**Table 8-10 • Scan Server dialog**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alias</strong></td>
<td>Enter a common name for the Scan Server.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Provide the hostname (such as <code>kr1.eng.companyA.com</code>) or IP address of the instance hosting the Scan Server. If the Scan Server is on the same instance as the Core Server, enter <code>localhost</code>. The same host-and-port combination must be unique among the enabled Scan Servers. (See <strong>Status</strong> is this table for a description of enabled Scan Servers.)</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Specify the port used by the Scan Server on the host instance. By default, the port is <code>8888</code>. The same host-and-port combination must be unique among the enabled Scan Servers. (See <strong>Status</strong> is this table for a description of enabled Scan Servers.)</td>
</tr>
<tr>
<td><strong>CL Path</strong></td>
<td>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 <strong>Save</strong>. 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 <em>FlexNet Code Insight Installation and Configuration Guide</em>. 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:</td>
</tr>
<tr>
<td></td>
<td>• “Managing Scan Profiles” in the <em>FlexNet Code Insight Installation and Configuration Guide</em> for more information about the “Basic Scan Profile (without CL)” and about creating and managing scan profiles in general.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Applying a Scan Profile</strong> in the “Using FlexNet Code Insight” chapter in this book for instructions on associating a scan profile with a project.</td>
</tr>
<tr>
<td></td>
<td>• <strong>What Is a FlexNet Code Insight Scan?</strong> in the “Using FlexNet Code Insight” chapter in this book for information about Code Insight scans in general.</td>
</tr>
</tbody>
</table>
Table 8-10 • Scan Server dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
| **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. |
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. 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 to identify those codebase files that exactly match file information in the CL (Compliance Library).</td>
</tr>
<tr>
<td></td>
<td>• Source Code Matches—Whether the Scan Server is to identify code strings in the scanned codebase files that exactly match strings in the CL (Compliance Library).</td>
</tr>
<tr>
<td></td>
<td>• Edit icon—Click at the end of a scan profile entry to edit the profile. The Create (or Edit) Scan Profile dialog is opened, showing the scan profile details.</td>
</tr>
<tr>
<td>Add Scan Profile button</td>
<td>Select this button to create a new scan profile.</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 following fields to define a scan profile:

Table 8-12 • Create/Edit Scan Profile dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</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>
</tr>
<tr>
<td></td>
<td>• No Dependencies: Only top-level inventory items are reported without any dependencies. (Default)</td>
</tr>
<tr>
<td></td>
<td>• Only First Level Dependencies: Only first-level (or direct) dependencies are reported along with top-level inventory items.</td>
</tr>
<tr>
<td></td>
<td>• All Transitive Dependencies: 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. For a description of Code Insight dependency support for supported ecosystems, see the Automated Analysis chapter.</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>
</tr>
<tr>
<td>Exact Matches</td>
<td>Select this option to have the Scan Server record exact matches for scanned files based on data from the Compliance Library (CL).</td>
</tr>
<tr>
<td>Source Code Matches</td>
<td>Select this option to have the Scan Server record source code matches for scanned files based on data from the Compliance Library (CL).</td>
</tr>
<tr>
<td>Include System Identified Files</td>
<td>(Available only when Source Code Matches is selected) 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 through automated analysis.</td>
</tr>
<tr>
<td>Include Files with Exact Matches</td>
<td>(Available only when Source Code Matches is selected) Select this option if you want the Scan Server to perform source-code matching for files that have already been identified as having exact matches.</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>
</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.</td>
</tr>
</tbody>
</table>
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>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><strong>Scan Settings</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Scan Profile</strong></td>
<td>Select the scan profile to default for projects. Click 📋 to view the details of the scan profile.</td>
</tr>
<tr>
<td><strong>Scan Server</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Automated Inventory Publish Options</strong></td>
<td>These options configure defaults for automatically publishing project inventory once a scan completes. Users can change these settings at the project level by navigating to `Manage Project</td>
</tr>
<tr>
<td><strong>Automatically publish system-created inventory items</strong></td>
<td>Select this option to automatically publish inventory items that Code Insight creates as part of the scan (that is, system-generated inventory items). If you select this option, the <strong>Minimum inventory confidence level for auto-publish</strong> field is enabled.</td>
</tr>
<tr>
<td><strong>Minimum inventory confidence level for auto-publish</strong></td>
<td>Select the default minimum Inventory Confidence level required to automatically publish a system-generated inventory item:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>Low</strong>—Automatically publish all system-generated inventory.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>Medium</strong>—Automatically publish only those system-generated inventory items with Medium and High confidence levels.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>High</strong>—Automatically publish only those system-generated inventory items with a High confidence level.</td>
</tr>
<tr>
<td></td>
<td>For a description of the Confidence levels and how they are used, see <strong>Inventory Confidence</strong>.</td>
</tr>
<tr>
<td><strong>Mark associated file as reviewed</strong></td>
<td>Select this option if you want Code Insight to automatically mark the files associated with each automatically published inventory item as “reviewed”.</td>
</tr>
</tbody>
</table>
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.

### Policy Profile

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.

### 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.
Manual Review Options 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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>• do nothing—Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</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>
<tr>
<td></td>
<td>Note • This option has no effect when the do nothing value is selected.</td>
</tr>
</tbody>
</table>
Chapter 8  Pages and Panels

Project Defaults Tab

Table 8-13 • Project Defaults tab (cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Review Options</td>
<td>Set the default type of manual review tasks to be generated:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></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 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.</td>
</tr>
<tr>
<td></td>
<td>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.)</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>
Remediation Options

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.

**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.
See Also
Policy Page
Policy Details Page
Edit Project: General Tab
Edit Project: Scan Settings Tab
Edit Project: Review and Remediation Settings Tab
Edit Project: (Default) Project Users Page
Managing Policy Profiles
Assigning Project Roles to Users
Creating Inventory from the Project Inventory Tab
Creating and Viewing External Work Items for a Project Inventory Task
ALM Settings

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 Options</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>

See Also
Security Vulnerabilities Associated with Inventory
Managing Policy Profiles
Policy Details Page
“Setting the Common Vulnerability Scoring System” in the FlexNet Code Insight Installation and Configuration Guide

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>
</tbody>
</table>
| Projects (x)         | 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)”
| 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 \( \times \) 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.                                                                                         |
Project Summary Tab

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></td>
</tr>
<tr>
<td>Name</td>
<td>The name given to the selected project and its Id number.</td>
</tr>
<tr>
<td>Owner</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>
<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>
</tbody>
</table>
Table 8-16 • Project Summary tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Project Type of the target project (project that will accept the imported data) controls the type of import to be performed. The following are the possible project types:</td>
</tr>
<tr>
<td></td>
<td>• Inventory Only: processes all published inventory, with inventory details, fields and file associations.</td>
</tr>
<tr>
<td></td>
<td>• Standard: processes all inventory, with inventory details, fields and file associations, as well as all files that are marked as reviewed.</td>
</tr>
<tr>
<td>Project Visibility</td>
<td>The visibility of the project:</td>
</tr>
<tr>
<td></td>
<td>• Public: 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>• Private: Only users assigned to roles in this project have access to it.</td>
</tr>
<tr>
<td>Project Risk</td>
<td>The project vulnerability risk value (Low, Medium, or High).</td>
</tr>
<tr>
<td>Scan Settings</td>
<td></td>
</tr>
<tr>
<td>Policy Profile</td>
<td>The name of the profile associated with this project.</td>
</tr>
<tr>
<td>Scan Profile</td>
<td>The name of the scan profile associated with this project. Click [1] to view the details of the scan profile.</td>
</tr>
<tr>
<td>Scan Paths</td>
<td>The location of your codebase. Click [1] to view the details about the Scan Server.</td>
</tr>
<tr>
<td>Scan Status</td>
<td></td>
</tr>
<tr>
<td>Scan Status</td>
<td>Notifies you when the scan is scheduled and waiting in queue. Click the hyperlinked term here to schedule a scan. If other events are scheduled, the scan is placed in a queue. Otherwise, it is run immediately. If the Scan Server is disabled, the link is also disabled.</td>
</tr>
</tbody>
</table>
### Project Summary Tab

#### 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.

#### Reports

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Report</td>
<td>Displays the status of the audit report. If a report is not available, click Generate Audit Report to create one.</td>
</tr>
<tr>
<td>Notices Report</td>
<td>Displays the status of the notices report. If a report is not available, click Generate Notices Report to create one.</td>
</tr>
<tr>
<td>Start Scan</td>
<td>Click to start your codebase scan.</td>
</tr>
<tr>
<td>Generate Report</td>
<td>Click to generate a Project, Audit, or Notices report in the background to display later.</td>
</tr>
<tr>
<td>Upload Project Codebase</td>
<td>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.</td>
</tr>
<tr>
<td>Manage Project</td>
<td>A dropdown menu that allows you to perform actions on the selected project:</td>
</tr>
<tr>
<td></td>
<td>• Edit Project</td>
</tr>
<tr>
<td></td>
<td>• Edit Project Users</td>
</tr>
<tr>
<td></td>
<td>• Export Project Data</td>
</tr>
<tr>
<td></td>
<td>• Delete Project</td>
</tr>
<tr>
<td></td>
<td>• Change Owner</td>
</tr>
</tbody>
</table>

### See Also
- Creating a Project
- Projects List Page
- Uploading a Project Codebase
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>
<tr>
<td>Project Folder</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Select a New Folder dropdown—Click the down arrow to locate and select an available folder to which to move the project.</td>
</tr>
</tbody>
</table>
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 this information on this tab. The tab contains the following fields:

**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>Scan Profile</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>Scan Server</td>
<td>The Scan Server assigned to this project. This field is not editable.</td>
</tr>
<tr>
<td>Auto-Publish</td>
<td>These options configure the automatic publication of project inventory once a scan completes.</td>
</tr>
<tr>
<td>Automatically publish system-created inventory items</td>
<td>Select this option to auto-publish inventory items that Code Insight automatically creates based on internal system policies. If you select this option, the <strong>Minimum inventory confidence label</strong> and <strong>Mark associated files as reviewed</strong> fields are enabled.</td>
</tr>
</tbody>
</table>
| Minimum confidence level for auto-publish | Select the minimum Inventory Confidence level required to auto-publish a system-generated inventory item:  
  - **Low**—Auto-publish all system-generated inventory.  
  - **Medium**—Auto-publish only those system-generated inventory items with Medium and High confidence levels.  
  - **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. |
| Mark associated files as reviewed | Select this option to automatically mark the files associated with each auto-published inventory item as “reviewed”. |
### Table 8-18  Edit Project: Scan Settings tab (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Codebase for Scan Server</strong></td>
<td>These settings enable you to limit which directories are scanned in your codebase.</td>
</tr>
<tr>
<td><strong>Path</strong></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>
</tbody>
</table>

![Project Codebase For Scan Server: Scanner1](image)

If the Scan Server is down, no project tree is displayed.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selected Paths</strong></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><strong>Save</strong></td>
<td>These buttons control whether you save your updates to scan settings.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Click this button to return to the Summary tab without saving your edits.</td>
</tr>
</tbody>
</table>

**See also**
- Updating Scan Settings for a Project
- Automatically Publishing Inventory

## 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.
• 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><strong>Automated Review Options</strong></td>
<td><strong>Policy Profile</strong> 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. |
What should happen if inventory items are not reviewed by policy?

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.

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of manual reviews will be performed on this project?</td>
<td>Determine the 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 meet no 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 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.</td>
</tr>
</tbody>
</table>

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. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</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, if the current reviewer reassigns a specific task to another user, the “reviewer” role is not automatically assigned to that user.</td>
</tr>
</tbody>
</table>
What should happen if inventory items are rejected?

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:

- **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. (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.)
- **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. (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.)
  - 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.

Assignee for remediation work

If desired, designate a new default development contact to which to assign remediation tasks.

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 in the “Using FlexNet Code Insight” chapter.

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.

Table 8-19 • Edit Project: Review and Remediation Settings tab (cont.)

<table>
<thead>
<tr>
<th>Section/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
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 X next to the user name in the pane.</td>
</tr>
</tbody>
</table>
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>
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>
Analysis Workbench

The Analysis Workbench is where you can interact with the items in your project inventory. The Analysis Workbench has the following fields:

Note • Some panes do not contain data until you choose a file in another pane.

Table 8-23 • Analysis Workbench

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legend</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 Files Search Results pane.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed</strong>: Click this link to display files in the File Search Results pane that have been reviewed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exact</strong>: Click this link to display files in the File Search Results pane that are exact matches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Copyrights</strong>: Click this link to display files in the File Search Results pane that contain copyright text.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Email/URLS</strong>: Click this link to display files in the File Search Results pane that contain email addresses and URLs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Licenses</strong>: Click this link to display files in the File Search Results pane that contain licenses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search Terms</strong>: Click this link to display files in the File Search Results pane that match default search terms.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source</strong>: Click this link to display files in the File Search Results 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
The **File Search Results** pane displays the results of your file search. The **File Search Results** pane has the following fields.

**Table 8-23 • Analysis Workbench (cont.)**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyrights</td>
<td>Lists the copyright text found in the selected file.</td>
</tr>
<tr>
<td>Emails/URLs</td>
<td>Lists the emails and URLs found in the selected file.</td>
</tr>
<tr>
<td>Licenses</td>
<td>Lists the licenses found in the selected file.</td>
</tr>
<tr>
<td>Search Terms</td>
<td>Lists the search terms that were found in the selected file.</td>
</tr>
<tr>
<td>Inventory Items (x)</td>
<td></td>
</tr>
<tr>
<td>Current View</td>
<td>Lists what portion of the project inventory that is being displayed.</td>
</tr>
<tr>
<td>Quick Filters</td>
<td>Provides options to quickly filter the inventory items listed:</td>
</tr>
<tr>
<td></td>
<td>• Published (x)</td>
</tr>
<tr>
<td></td>
<td>• Not Published (x)</td>
</tr>
<tr>
<td>Clear Filter</td>
<td>Clears any search terms that have been entered.</td>
</tr>
<tr>
<td>Search</td>
<td>Enter terms to search for in the inventory.</td>
</tr>
<tr>
<td>Add New</td>
<td>Click to create a new inventory item on the <strong>New Inventory Item</strong> tab.</td>
</tr>
<tr>
<td>Publish</td>
<td>Highlight an inventory item from the list and click <strong>Publish</strong> to publish the item.</td>
</tr>
<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.</td>
</tr>
<tr>
<td>Delete</td>
<td>Highlight an inventory item from the list and click <strong>Delete</strong> to delete the item from inventory.</td>
</tr>
</tbody>
</table>

**See Also**
Reviewing Published Inventory

---

**Note** • Some panes do not contain data until you choose a file in another pane.
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 8-24 • File Search Results pane

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click</td>
<td>Click to refresh the search.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Click to open the Advanced File Search dialog on which you can choose a standard search or add a new one.</td>
</tr>
<tr>
<td>Clear Search Results</td>
<td>Click to clear the results of the search.</td>
</tr>
<tr>
<td>Current Search</td>
<td>Displays the criteria for the current search.</td>
</tr>
<tr>
<td>Results Tree</td>
<td>The results of the current search.</td>
</tr>
</tbody>
</table>

### Table 8-25 • Advanced File Search dialog

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>Click this button to access the Advanced File Search Add dialog.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the search. For example, Files not in inventory.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the search. For example, Files not associated with inventory items.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click to delete a search.</td>
</tr>
<tr>
<td>Search</td>
<td>Click to execute the selected search.</td>
</tr>
<tr>
<td>Close</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 allow you to select a standard search, create your own search, or delete an existing search. The dialog has the following fields:

Table 8-26 • Advanced File Search Add dialog

<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 Add Criteria 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 Search Files dialog without searching.</td>
</tr>
</tbody>
</table>

Inventory Details Pane

The Inventory Details pane in the Analysis Workbench or on the Project Inventory tab provides details about the inventory, component, and files in the inventory. The pane has the following fields:

Table 8-27 • Inventory Details pane

<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 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>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 Inventory Details pane without saving changes.</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>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>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 <em>x Open Alerts</em> or <em>x Closed Alerts</em> link to view their details. If no alerts exist, <em>None</em> is displayed. For more information about alerts, 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.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Vulnerabilities</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If no vulnerabilities have been found for the inventory item, the value <strong>No</strong> is displayed in place of the graph. (In Analysis Workbench, if the Type value for the inventory item is <strong>Work in Progress</strong> or <strong>License Only</strong>, the value <strong>N/A</strong> is displayed.)</td>
</tr>
<tr>
<td>Created By</td>
<td>The name of the person or process that created the inventory item.</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>Created On</td>
<td>The date that the inventory item was created.</td>
</tr>
<tr>
<td>Updated On</td>
<td>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.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the inventory item.</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><strong>Type</strong></td>
<td>The type of finding of this item:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Work in Progress</strong>—A set of files with something in common. The work in progress will become a component or license only via manual audit work.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Component</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>License Only</strong>—Files under a specific license without a known component.</td>
</tr>
<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 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.</td>
</tr>
</tbody>
</table>

#### Usage tab

<table>
<thead>
<tr>
<th>Distribution Type</th>
<th>The option indicating how the inventory item is distributed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Internal</strong></td>
<td>Internally only (such as test framework that might be included in the codebase but is not distributed with the product).</td>
</tr>
<tr>
<td>• <strong>External</strong></td>
<td>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>• <strong>Hosted</strong></td>
<td>Hosted in your company’s data center (such as a SAAS application).</td>
</tr>
<tr>
<td>• <strong>Unknown</strong></td>
<td>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. |
**Table 8-27 • Inventory Details pane (cont.)**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Linking</strong></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><strong>Modified</strong></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><strong>Encryption</strong></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>

**Notes tab**

<table>
<thead>
<tr>
<th>Detection Notes</th>
<th>System notes that specify the automated detection technique that was used to locate the component; license information in the case that the license has changed from one version to another or if the component has multiple licenses; attributes extracted from a POM or manifest file containing project and configuration details.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Notes</td>
<td>Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis.</td>
</tr>
<tr>
<td>As-Found License Text</td>
<td>The actual license text for the license associated with the inventory item; this text is manually added by the analyst during the audit or, in some cases, automatically added by the system based on a high-confidence detection rule. You can enter text in this field for future reference.</td>
</tr>
<tr>
<td>Notices Text</td>
<td>The text to be shown in the Notices report for the selected inventory item. For more information about the Notices report, see generating the Notices Report.</td>
</tr>
</tbody>
</table>

**Associated Files tab**

Click this tab to view a list of the files that are part of the inventory for this project. Click the X to delete a listed file.
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. The 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>
</tbody>
</table>
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 8-30 • Policy page**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Search criteria** | The prompt for this field changes based upon your selection in the **Search type** field:  
  - If you select **Inventory Name** in the **Search type** field, you must enter a full or partial name to search for.  
  - If you select **Security Vulnerability** in the **Search type** field, you must enter a valid vulnerability ID to search for.  
  - If you select **Inventory with Vulnerabilities** in the **Search type** field, the list will automatically display the inventory items that meet your criteria.  
  - If you select **Inventory with Open Alerts** in the **Search type** field, the list will automatically display the inventory items that meet your criteria. |
| **Policy list** | 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.  
  - **Edit icon**—Click to edit the selected policy profile. The **Policy Details** page is opened, showing the profile details.  
  - **Copy icon**—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`. |
| **Add Policy button** | Click the **Add Policy** button to create a new policy profile. The **Policy Details** page is opened. |
Policy Details Page

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 8-31 • Policy Details page**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>These fields identify the policy profile you are creating or editing.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the policy profile that you are editing or copying. If you are copying a profile, the name will read <em>Copy of 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><strong>Description</strong></td>
<td>The policy profile description, if it exists. You can edit or add a description.</td>
</tr>
<tr>
<td><strong>Created</strong></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><strong>Updated</strong></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>
### Table 8-31 • Policy Details page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>The following criteria automatically approve or reject inventory items with security vulnerabilities during publication.</td>
</tr>
</tbody>
</table>

| | 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.

<table>
<thead>
<tr>
<th><strong>Licenses</strong></th>
<th>The following fields create policies that automatically approve or reject inventory associated with a given license.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a License... (dropdown)</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 8-31 • Policy Details page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses (list)</td>
<td>The list of license policies (in a grid format) currently used by this profile for automatically reviewing inventory items.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—The name of the license.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Usage Guidance icon</strong>—Click  to display the <strong>Usage Guidance</strong> dialog, in which you can add or edit text that will help reviewers in reviewing this license.</td>
</tr>
<tr>
<td></td>
<td>• <strong>License Details icon</strong>—Click  to display the <strong>License Details</strong> window for the selected license.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Action</strong>—Select one of the following to indicate what status to automatically assign to any inventory item associated with this license:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Approve</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Reject</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>No Action</strong> (same as the “Not Reviewed” inventory status, thus requiring a manual review)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete icon</strong>—Click  to delete the license from the policy.</td>
</tr>
</tbody>
</table>
### Components
The following fields create policies that automatically approve or reject inventory based on the component associated with the inventory.

<table>
<thead>
<tr>
<th>Add Component button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Components (list)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The list of current components and version (in a grid format) currently used by this profile for automatically reviewing inventory items.</td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong>—The name of the component.</td>
<td></td>
</tr>
<tr>
<td><strong>Versions</strong>—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:</td>
<td></td>
</tr>
<tr>
<td>• To enter a specific version, select the same version in the Versions from and to fields.</td>
<td></td>
</tr>
<tr>
<td>• To enter an explicit range, select a minimum version in the Versions from field and the maximum version in the to field.</td>
<td></td>
</tr>
<tr>
<td>• To specify any version for the given component, select the wild card * in both Versions from and to fields.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Action</strong>—Select one of the following to indicate what status to automatically assign to inventory items associated with this component-version:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Approve</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Reject</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>No Action</strong> (same as the “Not Reviewed” inventory status, thus requiring a manual review)</td>
<td></td>
</tr>
<tr>
<td><strong>Delete icon</strong>—Click ✗ to delete the component entry from the policy.</td>
<td></td>
</tr>
</tbody>
</table>
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 8-32 • Custom Detection Rules tab

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[actions]</strong></td>
<td></td>
</tr>
<tr>
<td>Enter Component</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>Name search string</td>
<td></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>

<table>
<thead>
<tr>
<th>[Custom rule entry]</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td>The name of the component on which the custom detection rule is based.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The component version.</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>The license found in the FlexNet Code Insight data library and associated with the component.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>The forge URL for the component.</td>
</tr>
</tbody>
</table>

[actions for custom rule entry]

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 **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 8-33 • Custom Detection 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. If you have accessed this dialog from the <em>Inventory Details</em> tab for an inventory item in <em>Analysis Workbench</em>, these fields are auto-populated with component information from the inventory item and are not editable. If you have accessed this dialog from the <em>Custom Detection Rules</em> 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 <em>Custom Detection Rules</em> tab, click <strong>Lookup Component</strong> to select the component and its version, license, and forge URL. The <strong>License</strong> and <strong>URL</strong> fields are populated accordingly. If you accessed this dialog from the <em>Inventory Details</em> 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 <em>Custom Detection Rules</em> 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 <strong>License</strong> to switch to another license and, optionally, change the component version. Additionally, click <strong>License</strong> 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 <em>Inventory Details</em> tab, this field is not editable.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the component. If you accessed this dialog from the <em>Custom Detection Rules</em> tab, this field is editable. It is not editable if you accessed the dialog from the <em>Inventory Details</em> tab.</td>
</tr>
<tr>
<td>URL</td>
<td>The forge URL for the component. If you accessed this dialog from the <em>Custom Detection Rules</em> tab, this field is editable. It is not editable if you accessed the dialog from the <em>Inventory Details</em> tab.</td>
</tr>
</tbody>
</table>
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.

### 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 exact content to include in the Notices report. This is usually a modification of the content in As-Found License Text. (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.

### [associated codebase files]

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.

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.

### File MD5

If you accessed this dialog from the **Inventory Details** tab:

- To add one or more files, click the check-box next to each desired file.
- To remove a from the rule, click its check-box to deselect it.

If you accessed this dialog from the **Custom Detection Rules** tab:

- To add a file, click **Add File** and enter the exact file name and MD5 value for the file.
- To remove a file from the rule, click **X** in the file entry.
Table 8-33 • Custom Detection Rule dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>The following are actions conclude the rule-creation session.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Click <strong>Save</strong> to save the new custom detection rule to the Code Insight data library. You will be asked for confirmation to proceed with the creation.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Click <strong>Cancel</strong> 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 8-34 • 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>
<tr>
<td>License</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Additionally, you can click 🔍 to view the details and text of the selected license as stored in the FlexNet Code Insight data library.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the component.</td>
</tr>
<tr>
<td>URL</td>
<td>The forge URL for the component.</td>
</tr>
<tr>
<td><strong>License, notices, and note content</strong></td>
<td>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.</td>
</tr>
<tr>
<td>As-Found License Text</td>
<td>The license content you want to associate with the inventory item. If no <strong>Notices Text</strong> 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 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.)</td>
</tr>
<tr>
<td></td>
<td>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>
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 8-35 • License Details window

<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>
Chapter 8  Pages and Panels

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 8-36 • Lookup Component window**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search by</strong></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><strong>Keywords</strong></td>
<td>Enter the name or title keyword by which to search components or to create a custom component.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Enter the project or forge URL by which to search components or to create a custom component.</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 8-36 • Lookup Component window**

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search by</strong></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><strong>Keyword</strong></td>
<td>Search for a component or create a custom component that uses a specific keyword in its name.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Search for a component or create a custom component that uses a specific project or forge URL.</td>
</tr>
<tr>
<td><strong>Forge</strong></td>
<td>Search for a component or create a custom component that is based on a specific forge.</td>
</tr>
</tbody>
</table>

**Description**

A short description of the license.

**Category**

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.

**Custom License**

A designation of whether this license is a custom license.

**Commercial**

A designation of whether the licenses is classified as commercial.

**Copyleft**

A designation of whether the licenses is considered a copyleft license.

**Free Software License**

A designation of whether the license is a free software license.

**GPL V2 Compatible**

A designation of whether a license is compatible with GPL-2.0.

**License Text Tab**

The complete text of the selected license as stored in the FlexNet Code Insight data library. This text represents the external forge license text.
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 8-37 • 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 token are associated with the current user account.) The page has the following fields:

### Table 8-38 • Preferences page

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Password</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 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 <strong>Update Password</strong> to save your changes.</td>
</tr>
<tr>
<td>AUTH Tokens</td>
<td></td>
</tr>
</tbody>
</table>
Table 8-39 • Preferences page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Token</td>
<td>Click this button to display the Add Token dialog.</td>
</tr>
<tr>
<td>Name</td>
<td>A list of the names of previously created tokens.</td>
</tr>
<tr>
<td>Token</td>
<td>The system-generated token associated with the name.</td>
</tr>
<tr>
<td>Create Date</td>
<td>The date on which the token was created.</td>
</tr>
</tbody>
</table>

Actions

A group of icons that indicate actions you can take on each token:

- **Edit ( )**: Click to open the Edit Token dialog.
- **Delete (X)**: Click to delete the selected token. The token is deleted immediately.
- **Copy to clipboard ( )**: Click to copy the selected token to the clipboard. You can use this option to copy tokens so that you paste them 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).

See Also

Add Token Dialog
Edit Token Dialog
Exporting and Importing Project Data
Performing Inventory-Only Scanning

**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 8-39 • 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>• <strong>Never Expires</strong>: The authorization token never expires.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Expires On</strong>: The authorization token is valid until the date you pick on the Validity Calendar.</td>
</tr>
</tbody>
</table>
Edit Token Dialog

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 8-40 • 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 <strong>Token</strong> 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 <strong>Edit Token</strong> dialog without saving your edits.</td>
</tr>
</tbody>
</table>
Advanced Inventory Search Page

The Advanced Inventory Search page appears when you click the Advanced Search button on the Inventory Items page. This Advanced Inventory Search page lets you search your inventory in a variety of ways. The page has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Items</td>
<td>Enter the whole or partial name of an item for which to search. For example, if you enter apache in this field, FlexNet Code Insight will find all inventory items that have the word apache in their name.</td>
</tr>
<tr>
<td>Inventory Name</td>
<td>Select one or more of these checkboxes (P1, P2, P3, or P4) to search the inventory by inventory priority.</td>
</tr>
<tr>
<td>Inventory Priority</td>
<td>For more information about inventory priority, see Inventory Priority in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td>Inventory Review Status</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>• Approved—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>• Rejected—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>• Not Reviewed—Show only items that have not yet been reviewed.</td>
</tr>
<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>• All Inventory Items—Display all inventory items—top-level inventory and first-level and transitive dependencies.</td>
</tr>
<tr>
<td></td>
<td>• Only Top-Level Inventory Items—Display only top-level inventory items only. No first-level or transitive dependencies are listed.</td>
</tr>
<tr>
<td></td>
<td>• Only Dependency Inventory Items—Display only first-level and transitive dependencies.</td>
</tr>
</tbody>
</table>
### Chapter 8  Pages and Panels

Advanced Inventory Search Page

<table>
<thead>
<tr>
<th><strong>Column/Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **Inventory Age**    | Search by inventory publication date. This dropdown field has the following choices:  
  - **Any**—Show any published inventory.  
  - **Last 1 day**—If today is Feb 6th, search from Feb 5th 12 AM.  
  - **Last 7 days**—If today is Feb 6th, search from Jan 30th 12 AM.  
  - **Last month**—If today is Feb 6th, search from Jan 7th 12 AM (30 days).  
  - **Custom Date Range**—Select a beginning (**From**) and ending (**To**) date from the popup calendar.                                                                 |

**Note**: To appear in search results based on inventory age, an inventory item must have been published. The search will not find items that were created but not published.

| **Inventory Notifications** | Select one or more of the following checkboxes to filter the inventory display based on security vulnerabilities:  
  - **Inventory with Open Alerts**—Display 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**—Inventory items that have been rejected due to new security alerts that are non-compliant with policy. |

| **Inventory Tasks Age**    | Search for published inventory items with tasks of a certain age (based on creation date). This dropdown field has the following choices:  
  - **Any**—Show any published inventory.  
  - **Last day**—If today is Feb 6th, search from Feb 5th 12 AM.  
  - **Last 7 days**—If today is Feb 6th, search from Jan 30th 12 AM.  
  - **Last month**—If today is Feb 6th, search from Jan 7th 12 AM (30 days).  
  - **Custom Date Range**—Select a beginning (**From**) and ending (**To**) date from the popup calendar.                                                                 |

| **Inventory Task Owner**   | Search for published inventory items with tasks assigned to a specific user (or any user):  
  - **Any**—Inventory with tasks assigned to any user.  
  - **Only Mine**—Inventory with tasks assigned to you (current user).  
  - **Specific User**—Inventory with tasks assigned to a specific user. (A **Select user** pop-up enables you to select the user.) |

---

Table 8-41 • Advanced Inventory Search page (cont.)
Inventory Confidence Level
Search for system-generated published inventory items that have a Confidence level of either **High**, **Medium**, or **Low**.

The Confidence level is the measure of the strength of the discovery technique used to generate the inventory item. For a description of the Confidence levels and how they are used, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.

Security Vulnerabilities

Security Vulnerability ID
Enter a valid vulnerability ID for which to search.

Security Vulnerability Severity
Search for inventory associated with vulnerabilities having the severity levels you specify here. The severity list differs depending on the CVSS version used by FlexNet Code Insight.

If CVSS v3.0 is used, the following severities are listed:

- 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 severities are listed:

- 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.

Security Vulnerability Age
Vulnerability age means how long ago a vulnerability was detected in the inventory. This could be 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. Select one of the following age ranges to limit your search:

- **Last day**—If today is Feb 6th, search from Feb 5th 12 AM.
- **Last 7 days**—If today is Feb 6th, search from Jan 30th 12 AM.
- **Last 30 days**—If today is Feb 6th, search from Jan 7th 12 AM.
- **Custom Date Range**—Select a beginning and ending date from the popup calendar.
Import Project Data Dialog

The Import Project Data dialog appears when you select Import Project Data from the Manage Project dropdown menu on the Summary tab. It lets you set options that FlexNet Code Insight uses to import data. The dialog has the following fields:

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Type</td>
<td>Select the type of import you want to perform:</td>
</tr>
<tr>
<td></td>
<td>• Inventory Only Import</td>
</tr>
<tr>
<td></td>
<td>• Standard Import (Default)</td>
</tr>
<tr>
<td>Import File Location</td>
<td>Select this option to browse for the project data file you want to import.</td>
</tr>
</tbody>
</table>

Table 8-41 • Advanced Inventory Search page (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Name</td>
<td>The full or partial name of the license for which to search.</td>
</tr>
<tr>
<td>License Priority</td>
<td>Select one or more of the following license priorities to limit your search:</td>
</tr>
<tr>
<td></td>
<td>• P1 — Viral/Strong Copyleft</td>
</tr>
<tr>
<td></td>
<td>• P2 — Weak Copyleft/Commercial/Uncommon</td>
</tr>
<tr>
<td></td>
<td>• P3 — Permissive/Public Domain</td>
</tr>
<tr>
<td></td>
<td>• No License Found</td>
</tr>
<tr>
<td></td>
<td>For more information about license priority, see What Does an Analyst do? in the “Using FlexNet Code Insight” chapter.</td>
</tr>
<tr>
<td>Apply And/Or Criteria</td>
<td>Select one of the boolean criteria to apply to the search selections:</td>
</tr>
<tr>
<td></td>
<td>• Or — The item may contain any one or more of the chosen criteria to be displayed. This is the default boolean operator.</td>
</tr>
<tr>
<td></td>
<td>• And — The item must meet all chosen criteria to be displayed.</td>
</tr>
<tr>
<td>Apply</td>
<td>Click this button to apply the selected search criteria and return to the Inventory Items page to view the results. The title bar of the Inventory Items page denotes that the display shows only filtered results.</td>
</tr>
<tr>
<td>Clear Form</td>
<td>Click this button to remove any previously specified search criteria.</td>
</tr>
<tr>
<td>Close</td>
<td>Click this button to close this page and return to the Inventory Items page without applying your search criteria.</td>
</tr>
</tbody>
</table>

Table 8-42 • Import Project Data dialog
Table 8-42 • Import Project Data dialog (cont.)

<table>
<thead>
<tr>
<th>Column/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create inventory with no matching files</strong></td>
<td>Select this option to import inventory if no matching files are present in the target project codebase. The default is not to import this type of inventory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> • If you choose to import inventory without matching files, you will have to manually delete the empty inventory that is not applicable to the current project.</td>
</tr>
<tr>
<td><strong>Only add files to inventory with matching MD5</strong></td>
<td>This option is unchecked by default.</td>
</tr>
<tr>
<td><strong>Only mark files as reviewed with matching MD5</strong></td>
<td>This option is checked by default.</td>
</tr>
</tbody>
</table>
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>Administrators</th>
<th>Manage Policy</th>
<th>Create Project</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administer Code Insight:</strong></td>
<td>🍁</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>• Set system settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage users and permissions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Schedule or run Electronic Updates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure an email server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure LDAP users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure Application Lifecycle (ALM) instances</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure a Scan Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure scan profiles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Define global project defaults</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage policies:</strong></td>
<td>—</td>
<td>🍁</td>
<td>—</td>
</tr>
<tr>
<td>• Create and edit policy profiles</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Create projects:</strong></td>
<td>—</td>
<td>—</td>
<td>🍁</td>
</tr>
<tr>
<td>• Create projects (and thereby automatically become Project Owner for each)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create project folders (in Projects list)</td>
<td></td>
<td></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>Roles</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage a project:</td>
<td></td>
<td><em>The project creator automatically becomes Project Owner, who can then reassign ownership to another user.</em></td>
</tr>
<tr>
<td>• Reassign project ownership</td>
<td></td>
<td><em>See the previous section, System Roles and Permissions, for information about the Create Project role needed to create projects.</em></td>
</tr>
<tr>
<td>• Manage project users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rename project</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Move projects in Project Folder Tree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage scan settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage inventory review/remediation settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Manage Source Control Management (SCM) and Application Lifecycle (ALM) instances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View project inventory</td>
<td></td>
<td><em>Any user (not just one with a project role) can view the Project Inventory tab and the associated inventory details.</em></td>
</tr>
</tbody>
</table>
**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 <strong>Notices Text</strong> (on the <strong>Licenses &amp; Notices</strong> tab) and <strong>Notes &amp; Guidance</strong> text (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 <strong>Notices Text</strong> on the <strong>Licenses &amp; Notices</strong> tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Edit <strong>Audit Notes</strong> on the <strong>Notes</strong> tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Invoke a scan</strong></td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td><strong>Upload codebase</strong></td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td><strong>Import/export project data</strong></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”.

---

Chapter A  FlexNet Code Insight User Roles and Permissions  Project Roles and Permissions
# 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>Notes</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create/edit tasks</td>
<td>Any user assigned to a project role can create and edit tasks.</td>
<td>Project Owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Reassign task</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Close manual review</td>
<td></td>
<td>–</td>
</tr>
<tr>
<td>Close remediation</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Close miscellaneous</td>
<td>Any user assigned to a project role can close a miscellaneous task.</td>
<td>✓</td>
</tr>
<tr>
<td>task</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter A  FlexNet Code Insight User Roles and Permissions
Roles and Permissions to Manage Project Task Flow