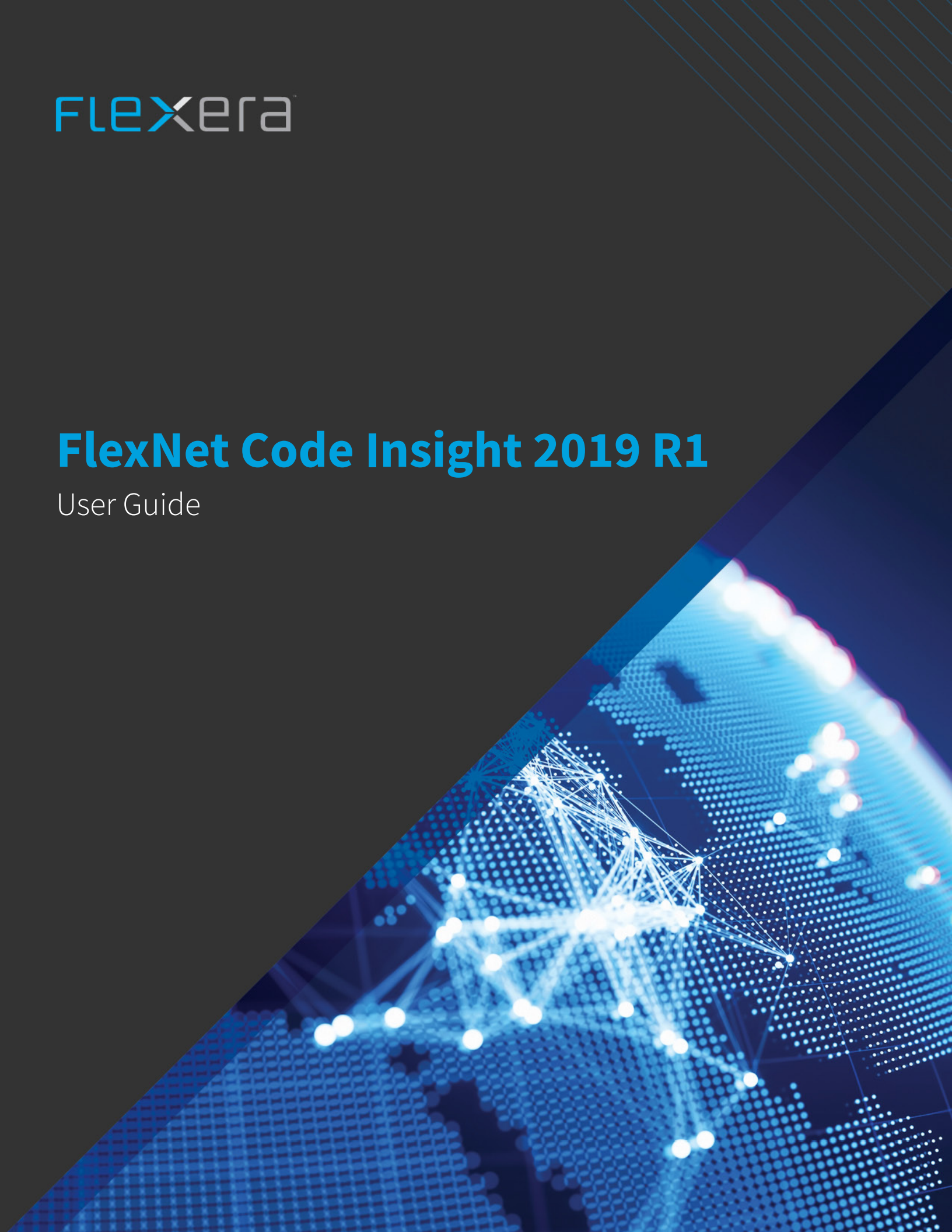




# FlexNet Code Insight 2019 R1

User Guide



# Legal Information

**Book Name:** FlexNet Code Insight 2019 R1 User Guide  
**Part Number:** FNCI-2019R1-UG00  
**Product Release Date:** March 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 R1 User Guide..... 9**
  - Intended Audience ..... 10**
  - Contacting Us ..... 10**
- 2 Using FlexNet Code Insight ..... 11**
  - Opening FlexNet Code Insight ..... 12**
    - Viewing Online Help and Online Guides..... 13
  - Roles and Permissions in FlexNet Code Insight ..... 13**
  - What is a Code Insight Project? ..... 13**
    - Key Project Elements ..... 14
    - Common Project Configurations ..... 14
  - Creating a Project ..... 14**
  - What Is a FlexNet Code Insight Scan? ..... 16**
  - Applying a Scan Profile to the Project..... 16**
    - About Scan Profiles..... 16
    - Applying a Scan Profile..... 17
  - Selecting Materials to Scan ..... 17**
    - Uploading a Codebase ..... 18
  - Scanning the Codebase ..... 18**
  - Overview of Scan Results ..... 19**
    - Inventory ..... 19
      - [Review Status of Inventory..... 20](#)
      - [Inventory Priority ..... 20](#)
      - [Inventory Confidence ..... 21](#)
      - [Security Vulnerabilities Associated with Inventory ..... 22](#)
      - [Inventory Usage Information..... 24](#)
    - Scan Evidence ..... 25
    - License Priority..... 26

<b>What Does an Analyst do?</b>	<b>27</b>
<b>Analyzing (Auditing) Scan Results</b>	<b>28</b>
Opening the Analysis Workbench	28
The Analysis Workbench Layout	29
Searching for Codebase Files Based on Name	30
Searching for Codebase Files Based on Search Criteria	31
Creating a New File Search	31
Using the Filter Legend Options to Filter the Codebase	32
Using the Codebase Files Pane Context Menu	33
Marking Files as Reviewed	34
Viewing License Details in Analysis Workbench	34
Using the File Details Tab	35
Viewing the Evidence Summary for a File	36
Viewing Binary Strings in a File	36
Viewing Copyright, Email, URL, and License Evidence in a File	37
Viewing Exact Matches	38
Viewing Source Matches	39
More About the “Remote Files” Panels on the Exact or Partial Matches Tabs	40
Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component	41
Using the Evidence Details Tab	42
Using the Inventory Details Tab	42
Using the Inventory Items Context Menu	43
Viewing Security Vulnerabilities for Inventory in Analysis Workbench	43
Viewing or Editing Inventory Usage Information in Analysis Workbench	44
Component Lookup	44
Guidelines for Component Lookup	44
Component Lookup Results	45
Performing Component Lookup	45
Creating an Inventory Item from the Analysis Workbench	45
Creating Inventory from the Inventory Items List	46
Creating Inventory from the Codebase Lists	48
Editing Inventory from the Analysis Workbench	49
Publishing Inventory	50
Automatically Publishing Inventory	50
<b>Reviewing Published Inventory</b>	<b>51</b>
Goal of the Reviewer	51
Displaying Project Inventory	52
Searching Published Inventory	52
Viewing Security Vulnerabilities for Project Inventory	53
Viewing License Details for Project Inventory	54
Viewing As-Found License Text	55
Viewing and Updating Notes & Guidance	55
Viewing Usage Information for Project Inventory	56
Viewing Associated Files	56
Creating Inventory from the Project Inventory Tab	56
Editing Inventory from the Project Inventory Tab	58

Approving or Rejecting Inventory Items .....	59
Creating and Managing Tasks for Project Inventory .....	60
Note About External Work Items .....	60
Manually Creating a Task .....	60
Editing a Task .....	62
Creating and Viewing External Work Items for a Project Inventory Task .....	64
Prerequisite .....	64
Manually Creating a Work Item .....	64
Viewing a Work Item .....	65
Recalling a Published Inventory Item .....	65
Understanding Security Vulnerability Alerts .....	66
Viewing Security Vulnerability Alerts .....	66
Receiving Security Vulnerability Alert Email Notifications .....	67
<b>Accessing and Viewing Projects in the System .....</b>	<b>67</b>
Navigating to the Projects List .....	67
Using the Project Dashboard .....	68
Filtering Inventory for a Project from the Project Dashboard .....	70
Opening a Project .....	70
Showing Only Your Projects .....	71
Searching the System .....	72
Available Filters for Searching Across Projects .....	72
Searching for Projects by Name .....	73
Searching All Projects for Inventory Based on a Specific Component and Version .....	74
Searching All Projects for Inventory Associated with a Specific License .....	75
Searching All Projects for a Security Vulnerability Advisory .....	76
Restoring the Full Project List .....	77
Managing Items in the Project List .....	77
<b>Managing a Project from the Summary Tab .....</b>	<b>77</b>
Opening the Project Summary Tab .....	78
Generating Reports .....	78
The Project Report .....	78
The Audit Report .....	79
The Notices Report .....	80
Adding Text for Notices Reports .....	80
Generating the Notices Report .....	81
Assigning Project Roles to Users .....	81
Editing the Project Definition and General Settings .....	82
Updating Scan Settings for a Project .....	83
Updating Inventory Review and Remediation Settings for a Project .....	83
Connecting the Project to Remote Data Sources .....	84
Version Control Settings .....	84
ALM Settings .....	84
Changing Project Owners .....	86
Rescanning Your Codebase .....	87
Change Events Resulting in Full or Incremental Rescans .....	88
Effects of Scan-Setting Changes on Rescans .....	88

Handling of Edited Inventory During Rescans .....	89
Initiating a Codebase Rescan.....	90
Exporting Project Data .....	91
<b>Creating a Private Project.....</b>	<b>92</b>
<b>Managing Policy Profiles.....</b>	<b>92</b>
Understanding Policy Profiles .....	93
How Policy Profiles Work in the Automated Inventory-Review Process.....	93
Adding or Editing a Policy Profile.....	93
Copying a Policy Profile .....	94
Associating a Policy Profile with a Project.....	94
<b>3 Performing Advanced Searches.....</b>	<b>95</b>
Advanced Searches .....	95
Dependencies in Advanced Searches .....	99
<b>4 Exporting &amp; Importing Project Data .....</b>	<b>101</b>
Exporting and Importing.....	101
What is Exported? .....	102
Exporting Project Data .....	102
Exporting Project Data Using the FlexNet Code Insight UI .....	103
Exporting Project Data Using the REST API .....	103
Types of Import .....	104
What is Imported? .....	104
How Files & Inventory Are Processed During Import.....	105
Import Options.....	105
Importing Project Data.....	105
Expected Results .....	107
Empty Inventory.....	107
Duplicate Inventory .....	108
Special Considerations for Standard Import .....	108
<b>5 Automated Analysis .....</b>	<b>109</b>
What is Automated Analysis? .....	109
Supported Development Ecosystems .....	109
Supported Ecosystems.....	110
Notes About Ecosystem Support.....	111
Notes about Dependencies Support.....	111
Supported Archive Formats .....	112
Additional Rule-based Detection Capabilities .....	112
<b>6 Performing Inventory-Only Scanning.....</b>	<b>113</b>
Inventory-Only Scan .....	113
Creating a Project Without Uploading a Codebase .....	113
FlexNet Code Insight Plugins .....	114

<b>7</b>	<b>Configuring Source Code Management</b>	<b>117</b>
	<b>Managing Source Code Management (SCM) Instances</b>	<b>117</b>
	Prerequisites	117
	Adding an SCM Instance to the Code Insight Project	118
	Testing an SCM Instance	118
	Synchronizing an SCM Instance	118
	Deleting an SCM Instance	119
	<b>Configuring a Git SCM Instance</b>	<b>119</b>
	Adding a Git SCM Instance to the Code Insight Project	119
	Configuring the Git SCM Instance	120
	<b>Configuring a Perforce SCM Instance</b>	<b>120</b>
	Adding a Perforce SCM Instance to the Code Insight Project	120
	Configuring the Perforce SCM Instance	121
	<b>Configuring a TFS SCM Instance</b>	<b>122</b>
	Adding a TFS SCM Instance to the Code Insight Project	122
	Configuring the TFS SCM Instance	123
<b>8</b>	<b>Pages and Panels</b>	<b>125</b>
	<b>The FlexNet Code Insight Dashboard</b>	<b>126</b>
	<b>Users/Permissions Tab</b>	<b>127</b>
	<b>Add User Dialog</b>	<b>128</b>
	<b>Edit User Dialog</b>	<b>128</b>
	<b>Electronic Updates Tab</b>	<b>129</b>
	<b>Email Server Tab</b>	<b>131</b>
	<b>LDAP Tab</b>	<b>132</b>
	<b>ALM Tab</b>	<b>134</b>
	<b>Scan Servers Tab</b>	<b>135</b>
	<b>Scan Server Dialog</b>	<b>135</b>
	<b>Scan Profiles Tab</b>	<b>137</b>
	<b>Create/Edit Scan Profile Dialog</b>	<b>138</b>
	<b>Project Defaults Tab</b>	<b>139</b>
	<b>Projects List Page</b>	<b>142</b>
	<b>Project Summary Tab</b>	<b>144</b>
	<b>Edit Project: General Tab</b>	<b>146</b>
	<b>Edit Project: Scan Settings Tab</b>	<b>147</b>
	<b>Edit Project: Review and Remediation Settings Tab</b>	<b>148</b>
	<b>Edit Project Users Dialog</b>	<b>153</b>
	<b>Scan History Dialog</b>	<b>154</b>
	<b>Select a New Project Owner Dialog</b>	<b>154</b>
	<b>Analysis Workbench</b>	<b>155</b>
	<b>File Search Results Pane</b>	<b>156</b>
	<b>Advanced File Search Dialog</b>	<b>157</b>

Advanced File Search Add Dialog .....	158
Inventory Details Pane .....	158
Evidence Details Pane .....	162
Project Inventory Review Page .....	162
Policies Page .....	163
Policy Details Page .....	164
License Details Dialog .....	167
Lookup Component Dialog .....	168
Add Project Dialog .....	168
Preferences Page .....	169
Add Token Dialog .....	170
Edit Token Dialog .....	171
Advanced Inventory Search Page .....	171
Import Project Data Dialog .....	175
<b>A FlexNet Code Insight User Roles and Permissions .....</b>	<b>177</b>
System Roles and Permissions .....	177
Project Roles and Permissions .....	179
Roles and Permissions to Manage Project Task Flow .....	180



# FlexNet Code Insight 2019 R1 User Guide

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**

Topic	Content
<b>Using FlexNet Code Insight</b>	“How to” information for using Code Insight functionality.
<b>Performing Advanced Searches</b>	Overview and procedures for using advanced searches to find specific inventory.
<b>Exporting &amp; Importing Project Data</b>	Explanation and procedures for exporting and importing project data.
<b>Automated Analysis</b>	Information about Code Insight automated analysis tools and features.
<b>Performing Inventory-Only Scanning</b>	Information about the Code Insight agent scan, performed remotely.
<b>Configuring Source Code Management</b>	Procedures for using Source Code Management (SCM) systems with Code Insight.
<b>Pages and Panels</b>	Reference to field descriptions on the pages, panes, tabs, and dialogs used in the Code Insight user interface.
<b>FlexNet Code Insight User Roles and Permissions</b>	A reference to the various user roles and permissions available in Code Insight to control access to Code Insight functionality.

# Intended Audience

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

# Contacting Us

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

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

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

<https://flexeracommunity.force.com/customer/>

# Using FlexNet Code Insight

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

- [Opening FlexNet Code Insight](#)
- [Roles and Permissions in FlexNet Code Insight](#)
- [What is a Code Insight Project?](#)
- [Creating a Project](#)
- [What Is a FlexNet Code Insight Scan?](#)
- [Applying a Scan Profile to the Project](#)
- [Selecting Materials to Scan](#)
- [Scanning the Codebase](#)
- [Overview of Scan Results](#)
- [What Does an Analyst do?](#)
- [Analyzing \(Auditing\) Scan Results](#)
- [Reviewing Published Inventory](#)
- [Accessing and Viewing Projects in the System](#)
- [Managing a Project from the Summary Tab](#)
- [Creating a Private Project](#)
- [Managing Policy Profiles](#)

# 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`.



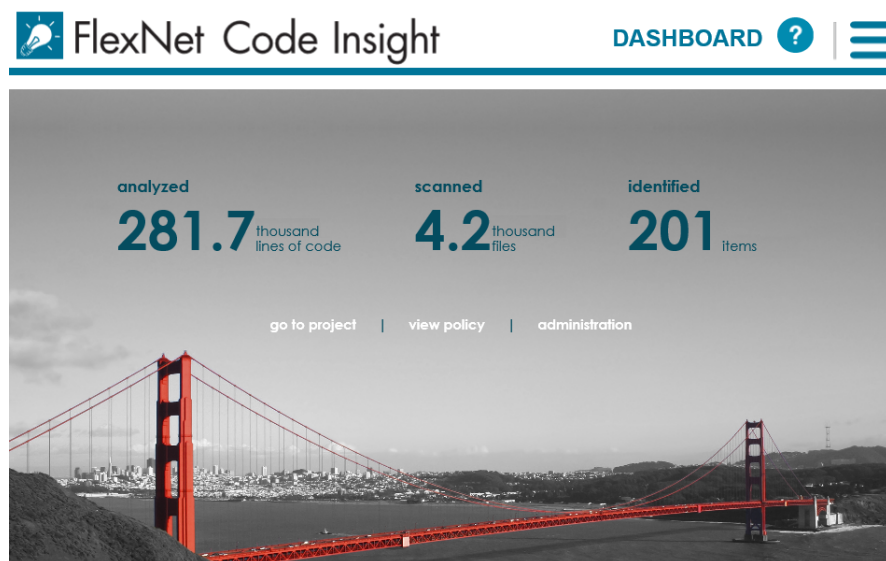
**Note** • If you are unsure about your server host name, contact your system administrator for guidance.

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.

## 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 to 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](#).



**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](#).

- **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](#).

The new project appears in the list of projects. At this point, the panes in the right panel will not contain data or graphs. If you created a Standard project, you will have to upload a codebase and scan it before data and graphs appear. To upload a codebase, see [Selecting Materials to Scan](#).

Additionally, if you want to change the currently assigned scan profile, see the later section, [Applying a Scan Profile](#).

# What Is a FlexNet Code Insight Scan?

The FlexNet Code Insight scanner 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 scanner uses automated detection rules to identify components, versions, licenses, and security vulnerabilities. In applying these rules, the scanner 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 scanner 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 scanner 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.



## Task

**To select a new scan profile, do the following:**

1. From the list of projects, select the project for which you want to apply a scan profile.  
  
(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](#).
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 (.
3. Click the **Summary** button at the top of the window to open the **Summary** tab for the project.
4. Click **Manage Project**, and select **Edit Project** from the popup menu.
5. From the **Edit Project** dialog, navigate to the **Scan Settings** tab, and select the desired scan profile for your project. (Click the information icon next to a selected scan profile to open a read-only view of its attributes.)

## Selecting Materials to Scan

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

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

Before FlexNet Code Insight can scan your code, you must upload a zip file containing your codebase. If your codebase changes, you can upload a new version of the codebase file by following the same procedure.

Refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix for role requirements to upload the 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 Zip File** to browse for a zip file containing your codebase.
4. (Optional) Click **Check to delete existing project codebase files** to have FlexNet Code Insight delete previously uploaded codebase files attached to this project.



**Note** • If you select to delete existing codebase files, a **Warning** dialog appears.

5. When the name of the zip file containing the codebase files appears in the field, click **Upload**. FlexNet Code Insight uploads your codebase file and attaches it to the selected project. You can now scan the uploaded codebase.



**Note** • Only zip file archives are supported. If you check the **delete existing files** option, all existing project codebase files will be permanently removed from the scan server. If you rescan the project without replacing these files via a new upload, the scan results for the removed files will be permanently deleted.

## Scanning the Codebase

After a codebase is uploaded and the appropriate scan profile is selected, you can scan the codebase.

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

#### Scan Status

<b>Scan Status:</b>	Project being scanned
<b>Scan Progress:</b>	In Scan Queue ( <a href="#">Show Details</a> )
<b>Last Scan:</b>	Scan of project Project2 <b>completed</b> . Scan Summary : 358 Files   6.03 MB   53 Lines of Code
<b>Past Scans:</b>	Click <a href="#">here</a> to view the scan history for this project.

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

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




---

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

For an overall understanding of the scan results, see [Overview of Scan Results](#).

3. Do any of the following:

- Manage the project. For example, you can assign users to project analyzer or reviewer roles, define the project's scan settings, configure an automated review and remediation workflow, configure a connection to a remote data source such as Perforce or Jira, and more. See [Managing a Project from the Summary Tab](#) for details.
- Analyze the scan results, as described in [Analyzing \(Auditing\) Scan Results](#).
- Generate the following reports:
  - [The Project Report](#)
  - [The Audit Report](#)
  - [The Notices Report](#)

## 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 Priority](#)

## Inventory

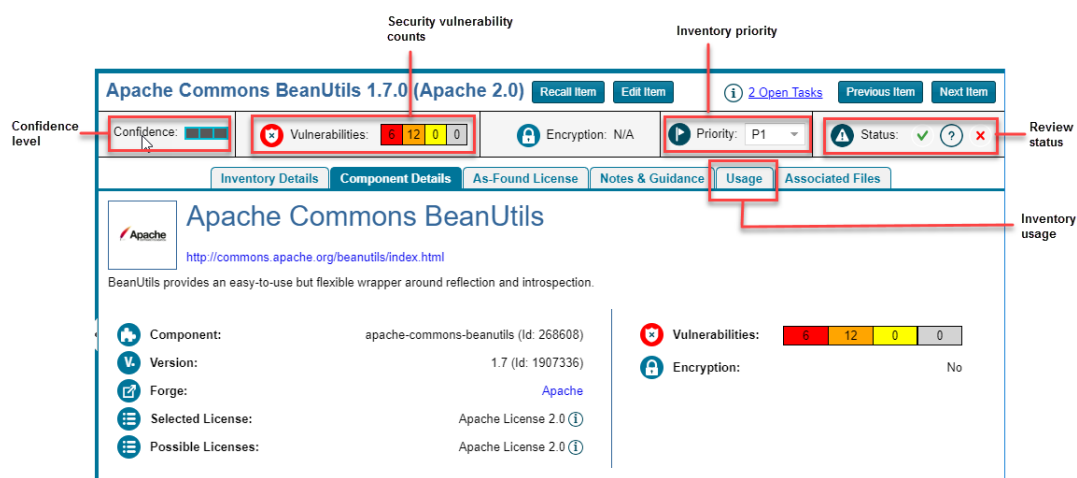
System-generated inventory is created by FlexNet Code Insight during a scan and is available for view both in **Analysis Workbench** and on the **Project Inventory** tab. An inventory item represents an explicit finding in the scanned codebase and can represent any of the following: top-level component, 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](#)
- [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

If the inventory item has at least one associated security vulnerability with a severity of HIGH or the selected license priority is P1 (see [License Priority](#)), the inventory priority is set to P1. 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 [License Priority](#)) *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.

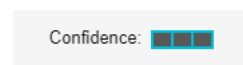
## Inventory Confidence

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

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

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

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



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

The following describes the Confidence levels:

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

- **Medium confidence**—An inventory item of Medium confidence means that the item was identified using a more generic technique or by the processing of a secondary indicator to produce an inventory item. A Medium-confidence inventory item might or might not have a match to a component in the Code Insight data library and might require triage or review in order to be validate or further refine the finding.
- **Low confidence**—An inventory item of Low confidence means that the inventory item was identified using a very generic rule or an exploratory detection technique, and thus might represent a component of unknown origin. Inventory of Low confidence rarely have a match to a component in the Code Insight data library and should be further triaged and reviewed by an Analyst for accuracy and completeness.

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

Table 2-1 •

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

## 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:



The color-coded segments represent the different severity levels as follows:

- **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)

For example, the **Vulnerabilities** graph above indicates 50 vulnerabilities of high severity, 33 of medium severity, 1 of low severity, and 80 of unknown severity.

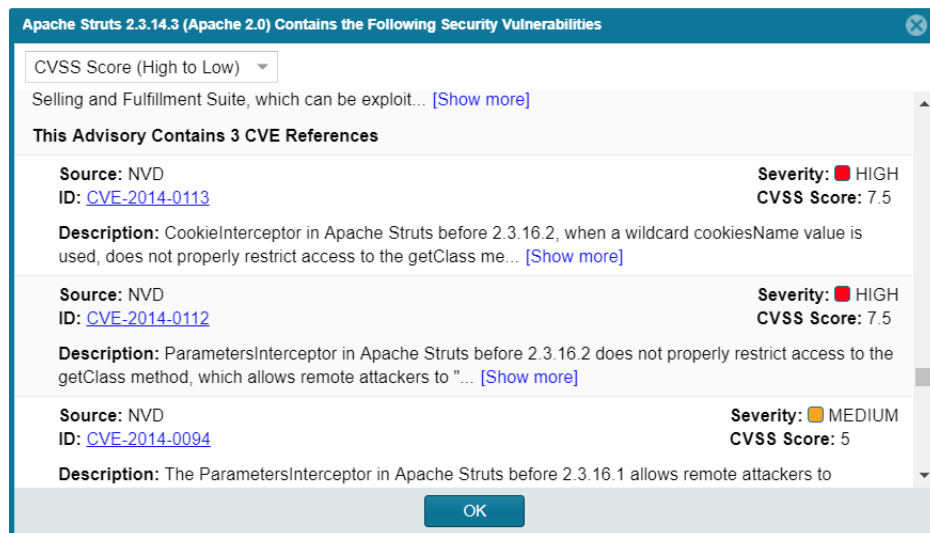
The following procedure explains how to use this graph to obtain details about the security vulnerabilities associated with the inventory item.



#### Task

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

1. For a specific inventory item, click any of the **Vulnerabilities** counts (red, orange, yellow, or gray) in the graph. The **Security Vulnerabilities** dialog appears.



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 (Common Vulnerability Scoring System) score, and description.
- 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 **UNKNOWN**.



**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 link (if available) to further investigate the vulnerability and determine the severity and score of the vulnerability as it applies to your project.
  - The **Security Vulnerabilities** list represents vulnerabilities and advisories in a hierarchical fashion, with Secunia and other advisories at the top level, and CVEs at the secondary level of the hierarchy. This behavior is in place because advisories are often well-researched and provide additional information above what is provided by the NVD. CVEs that are not referenced by any advisories also appear at the top-level of the hierarchy. The hierarchy view is two levels deep.
  - A CVE that is referenced by multiple advisories for the given inventory item is shown in the secondary list under each of the advisory entries. However, the vulnerability itself will count only *once* in the **Vulnerabilities** count on **Inventory Details** tab.
  - All top-level entries (CVEs and advisories) are sorted by CVSS score. Similarly, CVE vulnerabilities in a secondary list under a top-level advisory entry are sorted by CVSS score within the secondary list.
  - The **Security Vulnerabilities** list shows only *explicit* CVE vulnerabilities, Secunia advisories, or other advisories (that is, those directly mapped to the component version identified by the inventory item) and lists them in their proper hierarchical position.
2. (Optional) Click the hyper-linked CVE in an entry to view the vulnerability details found on the NVD or other website. Accessing these links is recommended if conducting deeper research as it shows referenced CVEs (those that are not explicitly mapped to the component version but can be indirectly related).
  3. When you have finished viewing the reported vulnerabilities, click **OK** to close the dialog.

## Inventory Usage Information

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

The inventory usage fields are available on the **Usage** tab for a given inventory item, as found both on the **Project Inventory** tab (shown below) and in the inventory view in **Analysis Workbench**. You can update these fields when you manually create or edit inventory items.

	Inventory Details	Component Details	As-Found License	Notes & Guidance	Usage	Associated Files
Distribution Type:	External					
Part Of Product:	Yes					
Linking:	Statically Linked					
Modified:	Yes					
Encryption:	No					



- **Distribution Type**—Indicates how you are distributing the item. The distribution type can affect license priority and obligations.
  - **Externally** with your product, shipped to customers (outside of your organization, including a private cloud deployment at the customer's site)
  - As an application **hosted** in your company's data center (such as a SAAS application)
  - **Internally** only (such as an internal test framework included in the codebase but not distributed with the product)
  - Distribution method **unknown**
- **Part of Product**—Indicates whether the item is part of the core product or an infrastructure piece such as a build or test tool. This can affect whether third-party notices are required for this item.
- **Linking**—Indicates whether the libraries are statically linked (included in the materials), dynamically linked (brought in at runtime), or not linked at all. Linking can affect license priority and obligations.
- **Modified**—Indicates whether a project contributor, such as a developer, has modified the software from its original form. Modification can be an important factor for determining license obligations and distribution requirements that are governed by a specific license.
- **Encryption**—Indicates whether the component provides encryption capabilities used in the product. Encryption can affect export controls.

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

- [Viewing Security Vulnerabilities for Inventory in Analysis Workbench](#)
- [Viewing Usage Information for Project Inventory](#)
- [Editing Inventory from the Project Inventory Tab](#)

## Scan Evidence

Scan evidence is generated by FlexNet Code Insight during a scan and is available for view in **Analysis Workbench** to any analyst assigned to the project. Scan evidence is typically an indicator of third-party content in the codebase. It can be useful for verifying system-generated inventory, identifying and creating additional inventory not discovered during scan, finding embedded licenses and copyrights in bundled code or archives, determining file origin, and locating stolen or borrowed code.

You can quickly view filter on and view the following evidence for codebase files in **Analysis Workbench**. (For more details about viewing evidence in **Analysis Workbench**, see [Viewing License Details in Analysis Workbench](#) 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 Priority

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

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

**Table 2-2 • License Priorities**

Priority	Characteristics	Icon	Description
<b>P1</b>	Viral/Strong Copyleft		Usually, P1 licenses require immediate attention due to the possibility of tainting proprietary application code, an issue that can have significant business impact.
<b>P2</b>	Weak Copyleft/ Commercial/Uncommon		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.
<b>P3</b>	Permissive/Public Domain		In general, P3 licenses are allowed and have minimal impact to an organization as long as license obligations are satisfied. The most common license obligation is properly attributing the use of an open source component to its author.

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.

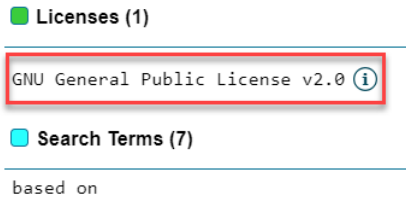
Inventory priority typically defaults to the license priority value unless you manually override the inventory priority value (as described in [Inventory Priority](#)).



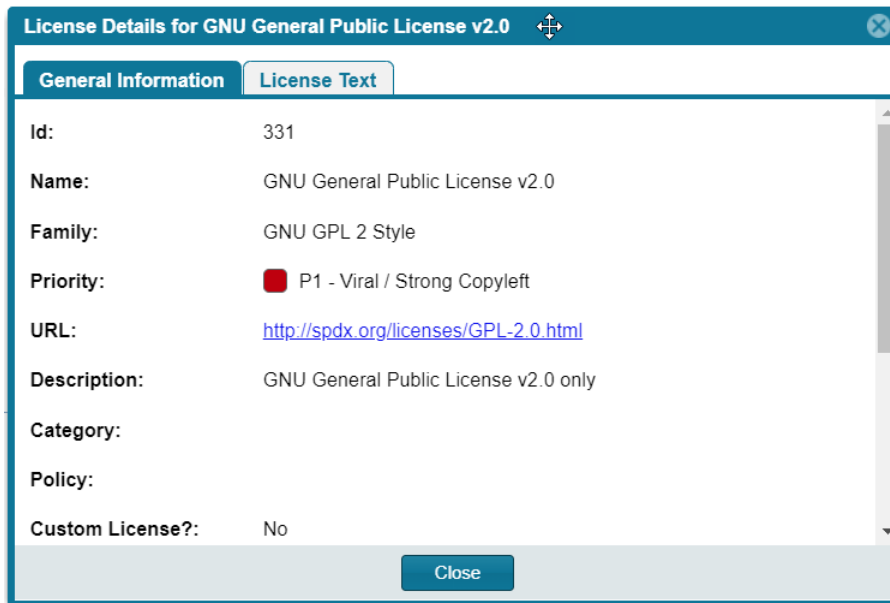
**Note •** FlexNet Code Insight REST APIs that reference the license entity, such as the Component Lookup API, include the license priority in the API response body.

### Viewing the License Priority

You can view the license priority from the **License Details** dialog associated with the license. To open this dialog, click the information ⓘ icon next to *any* license reference (see the following example license reference) in **Analysis Workbench** or on the **Project Inventory** tab.



The **License Details** dialog opens, showing information about the license, including its priority:



For explicit directions on opening the **License Details** dialog either in **Analysis Workbench** or on the **Project Inventory** tab, see the following:

- [Viewing License Details in Analysis Workbench](#)
- [Viewing License Details for Project Inventory](#)

## What Does an Analyst do?

The role of the Analyst is to transform the evidence uncovered by the scanner 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 *Mark Adler* and a license match to the *zlib* license. Then the Analysts would place these files in a group for the *zlib* open-source project and mark those files as **reviewed** to register progress.

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

# Analyzing (Auditing) Scan Results

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

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

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

## Section Overview

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

- [Opening the Analysis Workbench](#)
- [The Analysis Workbench Layout](#)
- [Searching for Codebase Files Based on Name](#)
- [Searching for Codebase Files Based on Search Criteria](#)
- [Creating a New File Search](#)
- [Using the Filter Legend Options to Filter the Codebase](#)
- [Using the Codebase Files Pane Context Menu](#)
- [Marking Files as Reviewed](#)
- [Viewing License Details in Analysis Workbench](#)
- [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**.



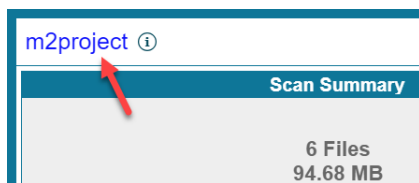
## Task

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:

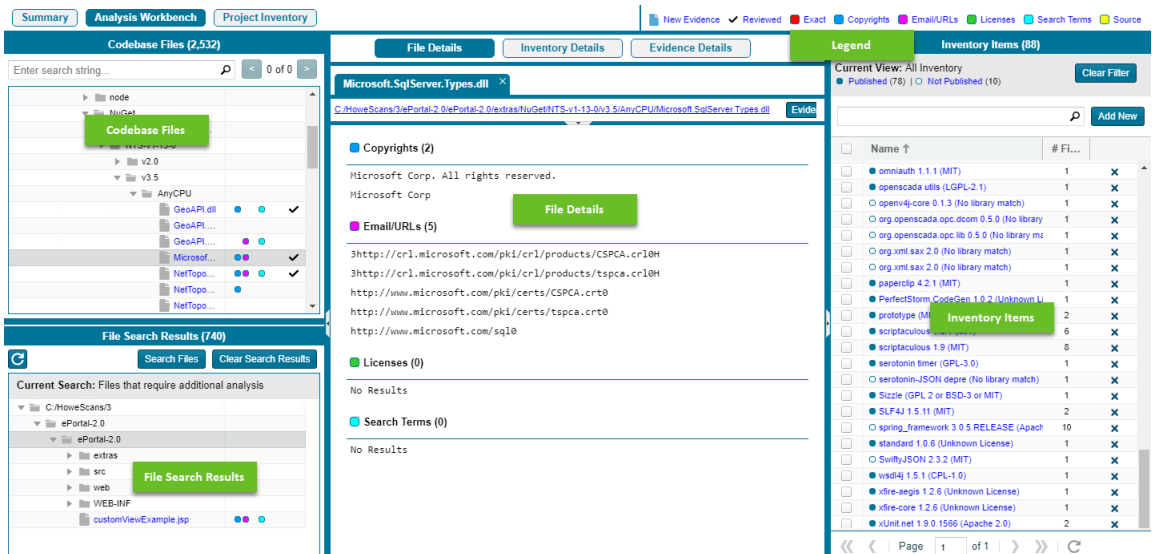


The project opens on either its **Project Inventory** or **Summary** tab (both are displayed). If you have permissions to analyze the scan results, the **Workbench Analysis** tab is displayed.

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 a New File Search](#).

Results are listed in the **File Search Results** pane.

## Creating a New File Search

You can supplement the built-in filters with custom filters to focus on scan data that are important to you.



### Task

**To create a new search filter, 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 filter.
5. (Optional) In the **Description** field, type a description of the filter. For example, type text that explains what the filter will search for.
6. Enter values in the **Criteria** fields:
  - a. If you have more than one search criteria, select the Boolean value to define how the criteria is applied: **AND** or **OR**. The default is **OR**.
  - b. Select a criterion from the drop-down **Criteria** menu.
  - c. Specify a search string by selecting **Contains** or **=** from the drop-down menu and typing a search string in the **Enter search string** field.
  - d. To add more criteria, click **Add Criteria** and repeat the bulleted steps above.

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

## 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.



The following describes the filter legend options:

**Table 2-3 • Filter Legend**

Icon	Label	Filters to files...
	<b>New Evidence</b>	...containing any evidence that the previous scan did <i>not</i> detect but that the most recent scan <i>did</i> .
	<b>Reviewed</b>	...marked as “reviewed”.
	<b>Exact</b>	...that are exact matches to known third-party files.
	<b>Copyrights</b>	...containing copyright information.
	<b>Email/URLS</b>	...containing email addresses or URLs.
	<b>Licenses</b>	...containing license information.
	<b>Search Terms</b>	...containing search terms defined in the scan profile.
	<b>Source</b>	...containing code-snippet matches (fingerprints) of known third-party code.

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](#)).



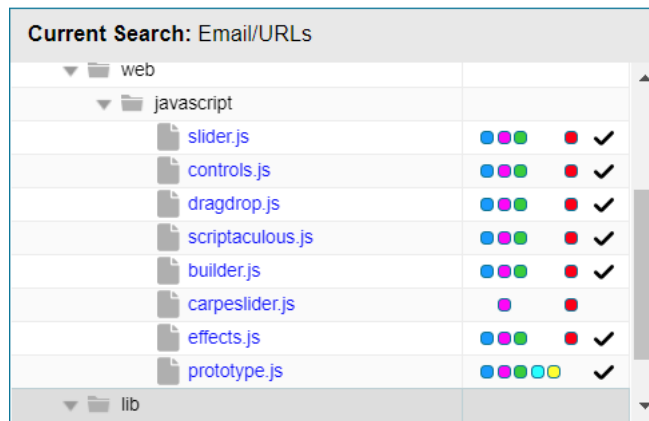


### Task

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 License Details in Analysis Workbench](#)
- [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.



### Task

**To mark files or directories as reviewed, do the following:**

1. 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.
2. Select **Mark as reviewed**.



**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 License Details in Analysis Workbench

You can view more details about the licenses that are part of your inventory on the **License Details** dialog. This dialog includes the following subtabs:

- 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** that displays the actual license content.

The following procedure describes how to access the **License Details** dialog from **Analysis Workbench**.



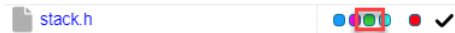
**Note** • This dialog is also accessible select or view a license as you create or edit an inventory item or perform a Component Lookup from the **Inventory Details** tab.



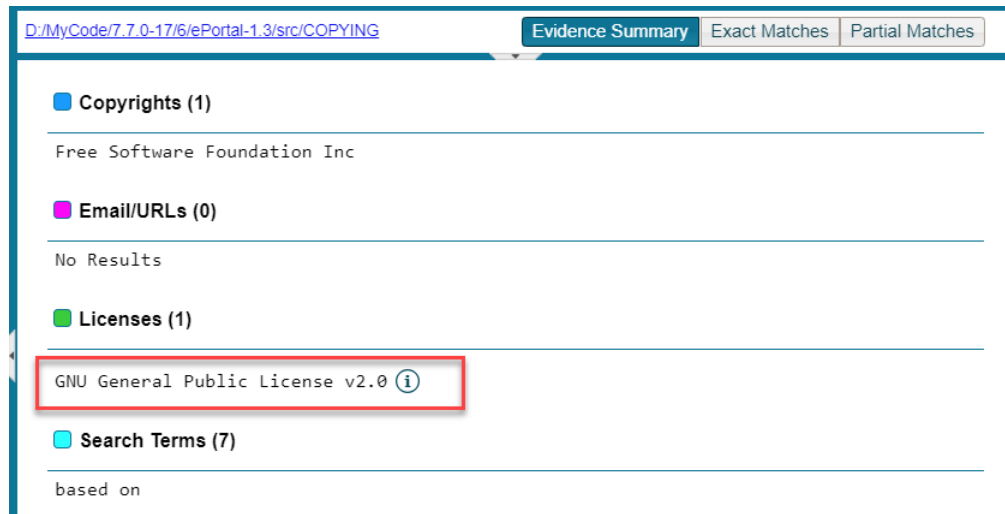
### Task

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:



**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 (i) next to the license name. The **License Details** dialog appears with the **General Information** tab in focus.

For descriptions of these fields on this tab, see [License Details Dialog](#). Also see [License Priority](#) for background on how the license priority is used.

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

## Using the File Details Tab

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

- [Viewing the Evidence Summary for a File](#)
- [Viewing Binary Strings in a File](#)

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

## Viewing the Evidence Summary for a File

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

- Copyrights
- Emails/URLs
- Licenses
- Search Terms

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



### Task

**To view the evidence summary, do the following:**

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

customViewExample.jsp			
<b>Name:</b>	customViewExample.jsp	<b>File Inventory (0)</b>	
<b>Path:</b>	/home/palamida/scanroot/ePortal-2.0/customViewExempl...	<b>Type:</b>	FILE
<b>Digest:</b>	120C0B559D5DE2D10DB5294E0278CD26	<b>File Size:</b>	6.46 KB
<b>Modified:</b>	03/06/2011	<b>Lines of Code:</b>	153
		<b>Reviewed</b>	Yes
		<b>Evidence</b>	<b>Exact Matches</b>
		<b>Partial Matches</b>	

## Viewing Binary Strings in a File

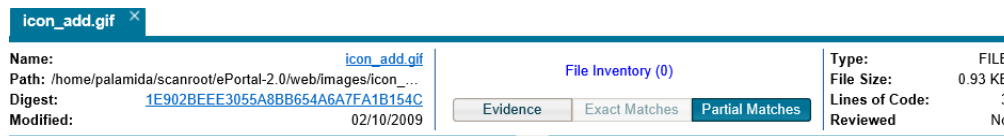
Use this procedure to view the list of strings (each string consisting of at least three consecutive printable characters) found in the content of a binary file. This list enables you to perform a deep search for evidence, such as a copyright or comment snippet, of third-party code in the file.



### Task

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

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



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

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

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

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

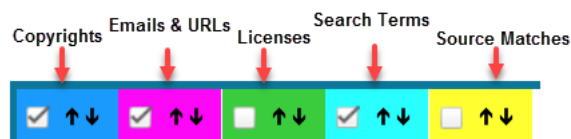


### Task


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

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

Color-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:



```

158         if ( returnreceipt ) {
159             sprintf( tmpstr, "Return-Receipt-To: %s\r\n",
160                     replytoid[0] ? replytoid : loginname );
161             bldHdrs.header->Add( tmpstr );
162         }
163
164         // Toby Korn tkorn@snl.com 8/4/1999
165         // If priority is specified on the command line, add it to the header
166         if ( priority [0] == '0' ) {
167             bldHdrs.header->Add( "X-MSMail-Priority: Low\r\nX-Priority: 5\r\n"

```

## 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.



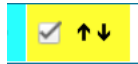
**Note** • The size limit for a file that you open in the **Partial Matches** tab is 2 MB. If the file you want to inspect is too large, you can download and open it outside of FlexNet Code Insight to inspect it manually for evidence.



### 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).

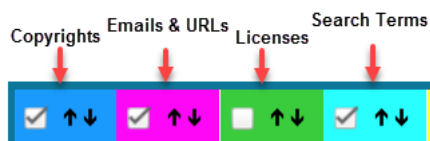
The information in the **Remote Files** panel consists of a set of files from the open source community that contain identical code to the scanned file. This means that the scanned file in the codebase possibly contains content that originated from outside the organization, and its origin needs to be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

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



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

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

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

- [Remote Files Panel](#)
- [Components Panel](#)
- [Licenses Panel](#)

### Note About Filtering in the Panels

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

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

For example, when you select a specific remote file in the **Remote Files** panel, 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.

Component Name	<input type="text" value="bamboo"/>	<input type="button" value="Apply"/>
----------------	-------------------------------------	--------------------------------------

### 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**, select the **File Details** tab.
2. Click the **Exact** or **Source** matches link in the legend at the top right of the page 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.
3. 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.
4. Select the **Exact Matches** or **Partial Matches** tab.

Additionally, if you are on the **Partial Matches** tab, select the **Source Matches** checkbox.

5. From the **Remotes File** 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).
6. In the **Components** panel, locate the component version that you believe is the origin of the matching code in the scanned database 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, or search for a new component altogether (see [Component Lookup](#)). 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.

7. 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, or search for a new component (see [Component Lookup](#)). 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.
8. Click the checkbox next to the inventory item to which you want to add the file.
9. (Optional) To mark the selected codebase file as reviewed, click **Mark file as reviewed**.
10. 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 holders 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 about inventory items:

- [Using the Inventory Items Context Menu](#)
- [Viewing Security Vulnerabilities for Inventory in Analysis Workbench](#)
- [Viewing or Editing Inventory Usage Information in Analysis Workbench](#)
- [Component Lookup](#)
- [Creating an Inventory Item from the Analysis Workbench](#)

- Editing Inventory from the Analysis Workbench
- Publishing Inventory
- Automatically Publishing Inventory

## 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.)



- Click any of the counts (red, orange, or yellow) 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](#).

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

## Viewing or Editing Inventory Usage Information in 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:**

- From the **Inventory Details** tab for a selected inventory item in **Analysis Workbench**, select the **Usage** tab.
- 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”

- **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, create your inventory item as **Work in Progress** and name it using the convention <COMPONENT> <VERSION> (<LICENSE>). For example, **myComponent 1.2 (MIT)**. When the component is added to the data library, the custom component instance is automatically remapped based on this information.

## 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.

## Performing Component Lookup



### Task

*To perform a component lookup, do the following:*

1. Open a project and navigate to the **Analysis Workbench**.
2. Select an inventory item from the list in the Inventory Items pane. The item appears in the **Inventory Details** pane.
3. From the **Type** dropdown, select **Component** and click **Lookup Component**. The **Lookup Component** dialog appears.
4. Select the search type (**Keyword**, **URL**, or **Forge**), and enter the required search criteria. See [Guidelines for Component Lookup](#).
5. 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 a copyright or text from an open source license. See [Searching for Codebase Files Based on Search Criteria](#) and [Using the Evidence Details Tab](#).

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

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

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

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

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

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

- [Creating Inventory from the Inventory Items List](#)
- [Creating Inventory from the Codebase Lists](#)

## Creating Inventory from the Inventory Items List

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



### Task

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

1. If not already on the **Analysis Workbench**, navigate to it.
2. Navigate to the **Inventory Items** list.
3. Click **Add New** at the top of the **Inventory Items** list. A new item, showing default values, opens in its own tab on the **Inventory Details** tab.
4. For the **Name** field, perform the appropriate step, based on the inventory type you intend to select for the **Type** field (see the next step):
  - For inventory of the type **Work in Progress**, specify a name for the inventory item. Best practice is to provide a name in the following conventional syntax used by Code Insight, even if the elements represented in the name are not available in the data library:  
`<COMPONENT_NAME> <VERSION> (LICENSE_NAME)`
  - For inventory of the type **Component** or **License only**, leave the **Name** field blank. The field will be automatically populated based on the registered component or license instance.
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 are able to locate it in the Code Insight data library using the Lookup Component feature. This type of inventory is associated with a registered component instance—that is, a unique component-version-license combination. It 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. A registered component instance represents a unique component-version-license combination currently in use in the system.

- Click the **Lookup Component** button to locate the component of interest. For more information about searching components, see [Component Lookup](#).
- In the list of results, navigate to the appropriate component, and click **Show Versions** to display the list of registered instances for that component.
- 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.

- 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](#).
- (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.
- When you completed the details for the new inventory item, click **Save**. The name of the inventory item appears in the **Inventory Items** pane.

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

## Creating Inventory from the Codebase Lists

This section describes how to “inventory” selected codebase files from the **Codebase Files** or **File Search Results** list in the **Analysis Workbench**, either by associating these files with existing inventory or by creating a new inventory item with which to associate them.

Alternatively, for instructions on creating inventory items from the **Inventory Items** list in the **Analysis Workbench**, see [Creating Inventory from the Inventory Items List](#).



### Task

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

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

### Add Selected Codebase Files to Existing Inventory

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



### Task

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

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

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

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





**Task**

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

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

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

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

## Editing Inventory from the Analysis Workbench

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



**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 Lookup Component feature to select a different registered instance (or create a new one to use). 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 Lookup Component 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 Inventory

If you have performed manual work on your inventory items, you must publish the items before anyone can review your work. Perform the following procedure to publish inventory.



**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.



### Task

**To publish inventory, 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.



**Note** • If you do not see an inventory item you want to publish, enter a term to search and click the search magnifier button.

2. Right click to open the context menu and choose **Publish Inventory**. The published items appear in the **Inventory Items** list with a filled box icon before their names.

## 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, you have the option to automatically mark the files associated with an auto-published inventory item as “reviewed”.



### Task

**To set the auto-publish feature, do the following:**

1. Open the **Summary** tab.
2. Open the **Manage Project** popup menu and select **Edit Project**
3. Select the **Scan Settings** tab. If this is the first time you have edited this project, the **Automatically publish system-created inventory items** and **Mark associated file as reviewed** options are already selected. See [Edit Project: Scan Settings Tab](#) in the “Pages and Panels” chapter for a description these options.
4. To disable the auto-publish feature, deselect the **Automatically publish system-created inventory items** checkbox. The **Mark associated file as reviewed** option will become grayed out. If you enable the **Automatically publish system-created inventory items** again, you must manually select the **Mark associated file as reviewed** checkbox if you want associated files to be automatically marked as “reviewed”.
5. When you have set the auto-publish feature, click **Save**. The **Summary** tab is opened.



**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 License Details for Project Inventory](#)
- [Viewing As-Found License Text](#)
- [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](#)
- [Understanding 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. Navigate to the **Project Details** page and click **Project Inventory**. The **Inventory Items list** pane appears with the **Inventory Details** tab displayed.
2. Select any of the tabs to display additional information about the inventory item.
3. 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.
4. 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. Navigate to the **Project Details** page 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.

**Advanced Inventory Search**

Inventory Items	Security Vulnerabilities	Licenses and Versions
<b>Inventory Name:</b> <input type="text" value="Enter Inventory Name"/>	<b>Security Vulnerability ID:</b> <input type="text" value="Enter Vulnerability ID"/>	<b>License Name:</b> <input type="text" value="Enter License Name"/>
<b>Inventory Priority:</b> <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4	<b>Security Vulnerability Severity:</b> <input type="checkbox"/> High Severity (CVSS 7.0 - 10.0) <input type="checkbox"/> Medium Severity (CVSS 4.0 - 6.9) <input type="checkbox"/> Low Severity (CVSS 0.1 - 3.9) <input type="checkbox"/> Unknown Severity (CVSS = N/A)	<b>License Priority:</b> <input type="checkbox"/> P1 - Viral / Strong Copyleft <input type="checkbox"/> P2 - Weak Copyleft / Commercial / Uncommon <input type="checkbox"/> P3 - Permissive / Public Domain <input type="checkbox"/> No License Found
<b>Inventory Review Status:</b> <input type="checkbox"/> Approved <input type="checkbox"/> Rejected <input type="checkbox"/> Not Reviewed	<b>Security Vulnerability Age:</b> <input type="text" value="Any"/>	<b>Version:</b> <input type="checkbox"/> No Associated Version
<b>Dependency Options:</b> <input type="text" value="All Inventory Items"/>		
<b>Inventory Age:</b> <input type="text" value="Any"/>		
<b>Inventory Notifications:</b> <input type="checkbox"/> Inventory with Open Alerts <input type="checkbox"/> Inventory Rejected Due to New Non-Compliant Security Vulnerabilities		
<b>Inventory Tasks Age:</b> <input type="text" value="Any"/>		
<b>Inventory Task Owner:</b> <input type="text" value="Any"/>		
<b>Inventory Confidence Level:</b> <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low		

Apply Or Criteria

Apply Clear Form Close

- 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 [Understanding 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.
  - Licenses**—Search for inventory items that have licenses of a certain of a certain name or license priority.
- Select **And** or **Or** from the **Apply Criteria** field.
- Click **Apply** to filter the inventory to display only those inventory items that meet the selected criteria.
- 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:**

- If you are not there already, navigate to the **Project Inventory** tab.
- 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:



4. Click any of the counts (red, orange, or yellow) 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 License Details for Project Inventory

You can view more details about the licenses that are part of your inventory on the **License Details** dialog. This dialog includes the following subtabs:

- 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** that displays the actual license content.

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



**Note** • This dialog 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 (i) 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** dialog appears with the **General Information** tab in focus.

For descriptions of these fields on this tab, see [License Details Dialog](#). Also see [License Priority](#) for background on how the license priority is used.

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

## Viewing As-Found License Text

The **As-Found License** tab shows the license text found in the codebase either by the system or by the Analyst. Depending on the detection technique, the tab can show actual license text for one or more licenses or be a reference to an license (such as Apache 2.0).

DOM4J 1.6.1 (DOM4J License)

Recall Item

Edit Item

Previous Item

Next Item

Confidence:

Vulnerabilities: No

Encryption: N/A

Priority: P3

Status:

Inventory Details

Component Details

As-Found License

Notes & Guidance




Usage

Associated Files

As-Found License Text

Save

Helvetica

B I U T<sup>+</sup> T<sup>-</sup>   

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.
4. Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.
5. Due credit should be given to the DOM4J Project - <http://www.dom4j.org>

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



### Task

**To view as-found license text, 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 **As-Found License** tab to view the license content. Any edits to this information should be made by an Analyst only. If no content is found on this tab, you can provide license notices information in the **Notices** pane on the **Notes & Guidance** tab. See [Viewing and Updating Notes & Guidance](#).
4. When you have finished with this tab, navigate to another tab for the inventory item, or select another inventory item.

## 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.
4. Review or update content in the panes as needed.

Should no license information be available on the **As-Found License** tab (see [Viewing As-Found License Text](#)), 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 [Adding Text for Notices Reports](#) 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.



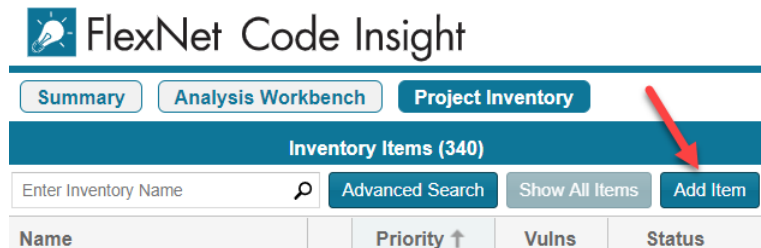
- No files can be associated with an inventory item when it is created from the **Project Inventory** tab.
- If you register a new component instance (a unique component-version-license combination) when creating inventory, the registered instance becomes available for selection across the system.
- 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:  
`<COMPONENT_NAME> <VERSION> (LICENSE_NAME)`
  - For inventory of the type **Component** or **License only**, leave the **Name** field blank. The field will be automatically populated based on the registered component or license instance.
4. From the **Type** dropdown, select the type of inventory item you want to create and perform the related step or steps:
  - **Work in Progress**—Create this type of inventory item if you want to quickly represent third-party code or an artifact without having to select an associated component, version, or license from the data library. (You can later edit this inventory item to convert it to one of the other inventory types.) This option is typically used if you need a placeholder or cannot find the associated element in the data library. Items of type **Work in Progress** are not affected by policies and do not receive vulnerability updates or alerts.
  - **Component**—Create this type of inventory item if you know the component, version, and license for the third-party code or artifact and are able to locate it in the Code Insight data library using the Lookup Component feature. This type of inventory is associated with a registered component instance—that is, a unique component-version-license combination. It 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. A registered component instance represents a unique component-version-license combination currently in use in the system.

- a. Click the **Lookup Component** button to locate the component of interest. For more information about searching components, see [Component Lookup](#).

- 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 Lookup Component feature to select a different registered instance (or create a new one to use). 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 the longer Lookup Component 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.



### Task

**To approve or reject inventory items, do the following:**

1. Navigate to the **Inventory Items** list.
2. On the line for the inventory item you want to approve or reject, click the green checkmark to approve the item or the red X to reject the item.

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

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

## Creating and Managing Tasks for Project Inventory

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

- **Manual Review Inventory**—A task to track the manual review of an inventory item, typically for an inventory item that has not already been auto-reviewed by policy. A manual inventory task alerts the assignee to the need to review the inventory item for use in the current context and to either approve or reject it based on the review. In the case that there is only one manual review task for the inventory item, the inventory status will be updated to Approved or Rejected.
- **Remediate Inventory**—A task to track the remediation efforts of an inventory item, typically for a rejected inventory item. A remediation task signals to the assignee to perform some action to make the inventory item acceptable for use (for example, to upgrade to a new version due to discovered vulnerabilities or to use a specific license and to comply with license obligations). Closing remediation tasks does not affect the inventory status.
- **Miscellaneous**—A task to track any other effort for an inventory item.

The following topics are described in this section:

- [Note About External Work Items](#)
- [Manually Creating a Task](#)
- [Editing a Task](#)

### Note About External Work Items

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

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

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

### Manually Creating a Task

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

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



## Task

To create a task manually, do the following:

1. Navigate to the **Project Inventory** page.
2. 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.

3. In the **Tasks** section, click the **Create Task** button to open the **Create Task** dialog.

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 **Reassign** 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.

The screenshot shows the 'Task Details' dialog box with the following fields and controls:

- Type:** Miscellaneous
- Summary:** Task for Apache Struts 2.3.14.3 (Apache 2.0)
- Details:** A rich text editor with a font dropdown set to 'Helvetica' and various formatting icons (bold, italic, underline, text color, background color, bulleted list, numbered list, indent, outdent).
- Status:** Open, with a 'Close Task' button.
- Priority:** Medium (dropdown menu).
- Owner:** Lois Smith (hyperlink), with a 'Reassign' button.
- Work Items:** None, with a 'Create Work Item' button.
- At the bottom are 'Save' and 'Close' buttons.

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](#).



### Task

**To close or reopen a Manual Inventory Review task, do the following:**

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

- To reopen a closed task, click the **Reopen** button.
2. Click **Close**.

## Closing or Reopening a Remediation or Miscellaneous Task

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

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



### Task

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

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

2. Click **Close**.

## Creating and Viewing External Work Items for a Project Inventory Task

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

The following topics are described in this section:

- [Prerequisite](#)
- [Manually Creating a Work Item](#)
- [Viewing a Work Item](#)

### Prerequisite

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

### Manually Creating a Work Item

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

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



#### Task

*To create a work item manually, do the following:*

1. Navigate to the **Project Inventory** page.
2. 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.

3. Click the **x Open Tasks** link to view the list of open tasks for the inventory item.
4. Locate the appropriate task from the **Tasks** list, and click the link in the **Summary** column to show the **Task Details** dialog.
5. Click the **Create Work Item** button. The **New Work Item** page is displayed.





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

6. Complete the fields to define the work item. See the inline help for field descriptions.

This page might already contain default field values based on the project or global application defaults; you can override these values as needed.

7. Click **Create Work Item**.

A “Success” message is displayed if the work item is created successfully on the corresponding ALM system (currently, a Jira server) associated to this project.

You are returned to the **Task Details** dialog.

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

## Viewing a Work Item

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



### Task

**To view a work item, do the following:**

1. Navigate to the **Inventory Details** tab for the inventory item associated with the task containing the work item.
2. Click the **# Open Tasks** link. The **Tasks** list is displayed.
3. 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.
4. Use the search filter at the top of the window to show **All**, **Open**, or **Closed** work items.
5. Click the **External ID** link for the work item to open the issue in Jira.

## 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. Recall is not required to make edits to the inventory item.



### Task

**To recall a published inventory item, do the following:**

1. Navigate to the **Inventory Details** page.
2. Click **Recall Inventory Item**. The item is removed from the **Inventory Items** list.

# Understanding Security Vulnerability Alerts

FlexNet Code Insight provides the ability to view and clear security vulnerability alerts. The Electronic Update process generates this type of alert for any new security vulnerability that impacts a published inventory item. Having such alerts allows you to stay on top of the most recent issues and address them through remediation or close them as false positives.

Refer to these topics for more information:

- [Viewing Security Vulnerability Alerts](#)
- [Receiving Security Vulnerability Alert Email Notifications](#)

## Viewing Security Vulnerability Alerts


When security vulnerability alerts are generated as part of an Electronic Update, email notifications are sent to the project owners. In addition to these email alerts, security vulnerability alerts can be viewed via the **Project Inventory** page.



### Task


**To view security vulnerability alerts, do the following:**

1. Navigate to the **Project Inventory** page. The page contains the following fields that inform you of alerts:

- **Alerts**—Displays the number of open and closed alerts for the selected inventory item.
-  **Open Alert Notice**—Displays the number of open alerts for the current inventory item.



**Note** • If there are no open security vulnerability alerts, the notice will not be shown.

2. Click the hyperlink (**x open alerts**) in one of the alert fields. The **Alerts** dialog appears.
3. View the following information:
  - **Type**—This column displays the alert type. In this release, only *New Vulnerability* alerts are available.
  - **Date**—The date that the alert was created.
  - **Priority**—The priority of the alert, shown as High, Medium, or Low. The priority defaults to the severity of the security vulnerability for the alert.
  - **Status**—The status, *Open* or *Closed*, of the alert in FlexNet Code Insight. Alerts that have been closed have an icon () to further identify them.
  - **Details**—This column contains the following information about the alert:
    - **Source**—Where the vulnerability was found, National Vulnerability Database (NVD) or Secunia Advisories (as published by the Secunia Research team from Flexera).
    - **ID**—The identification number of the vulnerability associated with the Common Vulnerabilities and Exposures (CVE). If this is a hyperlinked field, click it to go to the actual entry for the vulnerability on the advisory website.
    - **CVSS Score**—The score of the vulnerability based on the Common Vulnerability Scoring System (CVSS). The values of the CVSS score range from 0.1 to 10, with 10 being the most serious. If the vulnerability has no score, the value is **N/A**.

- **Description**—The description of the vulnerability as displayed in the National Vulnerability Database.
4. (Optional) To change the display based on the status of the vulnerability, select one of the following filters from the pulldown menu:
    - **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.
  5. When you finish viewing alert information, click **Close** to return to the **Project Inventory** page.

## Receiving Security Vulnerability Alert Email Notifications

In addition to viewing security vulnerability alerts in the FlexNet Code Insight application, you 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, you can click any of the hyperlinked text in the email to open FlexNet Code Insight and view additional information.

## 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.



### Task

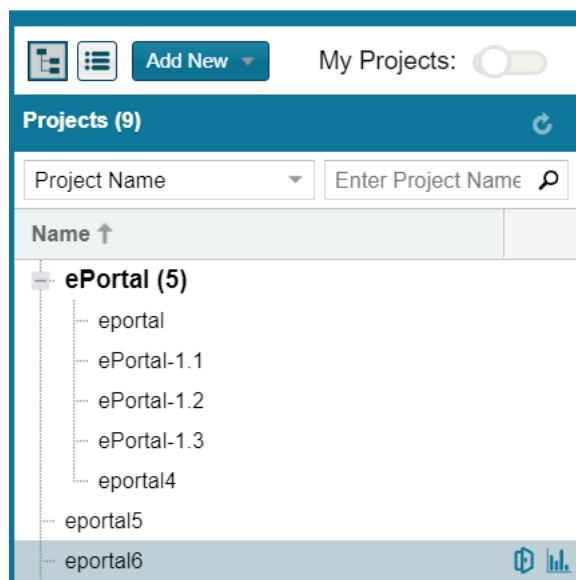
To open the Projects list, do the following:

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:



The **Projects** list is displayed.

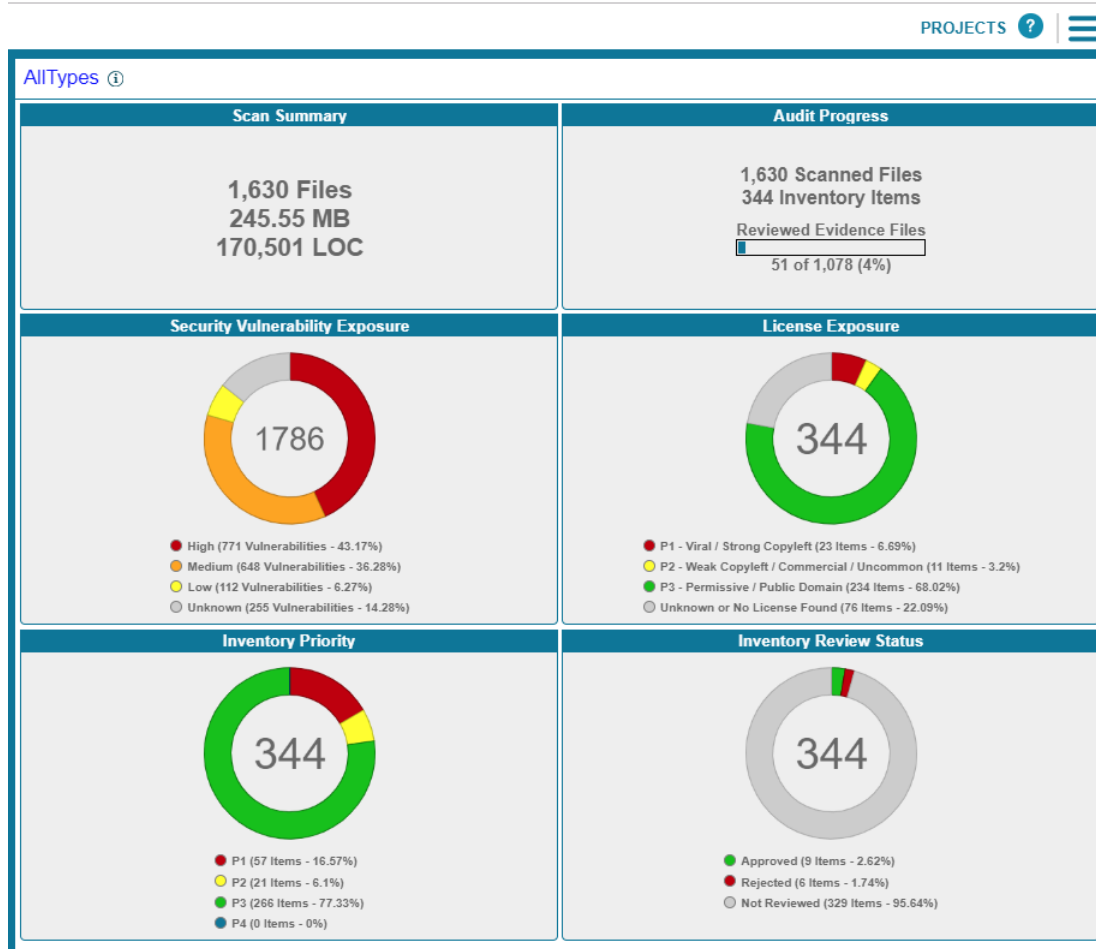


2. (Optional) Click the **My Projects** toggle at the top of the list to show only those projects with which you are associated as Project Owner or through a project role. (For details, see [Showing Only Your Projects](#).) You can also search projects by name, inventory, or security vulnerability as described in [Searching the System](#).

## Using the Project Dashboard


When you select a project from the Projects list, the **Project Dashboard** is displayed, providing you with an interactive view of your project, including security-vulnerability and license exposure, codebase and inventory review statistics, and other information.

The procedure that follows this image describes how to use **Project Dashboard** features.



## Task

To use the Project Dashboard, do the following:

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. Select a project from the **Projects** list. The **Project Dashboard** for the selected project is displayed in the right panel.  
(Alternatively, hover over the project entry, and click its **Load Project Dashboard** icon  in the project entry to display the dashboard.)

The **Project Dashboard** contains the following charts to provide an overview of the project's most recent scan and the resulting inventory:

- **Scan Summary**—A summary of your most recent scan, including number of files scanned, the size of the codebase/files, and the number lines of code.
- **Audit Progress**—A snapshot of the audit progress of the selected project.
- **Security Vulnerability Exposure**—An interactive color-coded chart and legend that provide an overview of the security vulnerabilities by severity across all the project inventory. The number in the center of the chart is the total number of security vulnerabilities found across all inventory items.

- **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.



### Task

*To quickly filter inventory on the Project Dashboard, do the following:*

1. Open the **Project Dashboard** for a project. See [Using the Project Dashboard](#).
2. Navigate to a chart and click a color-coded area. The project is opened to its **Project Inventory** tab, displaying the project inventory items associated with the information represented by color-code area. You can also click the corresponding colors in the legends below the charts to filter your inventory.
3. Click on a project inventory item listed to see more detail in the right pane of the **Project Inventory** tab. See [Reviewing Published Inventory](#) for details about this tab.

## Opening a Project

Use this basic procedure to open a project.

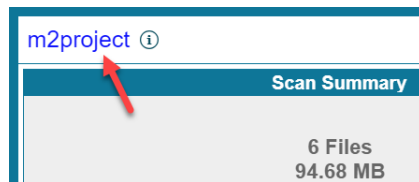


### Task

*To open a project, do the following:*

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. Select a project in the **Projects** list. Its **Project Dashboard** is displayed on the right.

- 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 (shown below):



The project is opened on either of the following tabs on its **Project Details** page:

- 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 Inventory](#).

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

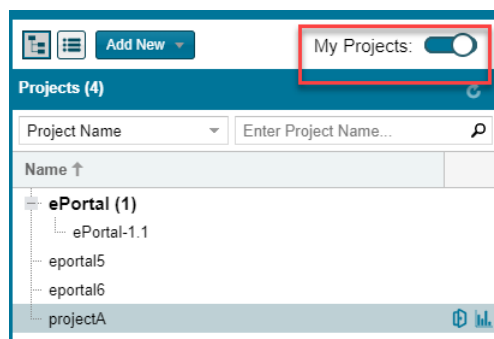
FlexNet Code Insight provides the option to filter the **Projects** list to show only those projects with which the current user is associated as either Project Owner, Analyst, Reviewer, or Observer. (For a description of these roles, see [Assigning Project Roles to Users](#).)

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:*

- Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
- At the top of the list, click the **My Projects** toggle.



- 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 2-4 •** Available Filters for Searching Across Projects

To search across all projects for...	...use this filter	Filter criterion	Criterion example	Refer to...
<b>Projects with a name containing a specific string</b>	Project Name	Project name	<a href="#">MyProject</a>	<a href="#">Searching for Projects by Name</a>
<b>Inventory based on a specific component and version</b>	Project Inventory	Component and version as it appears in the <b>Inventory Name</b> value	<a href="#">Apache Struts 2.3.14.3</a>	<a href="#">Searching All Projects for Inventory Based on a Specific Component and Version</a>
		Component name as it appears on the <b>Component Details</b> tab for the inventory item	<a href="#">struts2-core</a>	



**Table 2-4 • Available Filters for Searching Across Projects (cont.)**

To search across all projects for...	...use this filter	Filter criterion	Criterion example	Refer to...
<b>Inventory associated with a specific license</b>	Project Inventory	The <b>Selected License</b> value as it appears on the <b>Component Details</b> tab for the inventory item	<a href="#">GNU General Public License v2.0</a>	Searching All Projects for Inventory Associated with a Specific License
		The license name as it appears in the <b>Inventory Name</b> value	<a href="#">GNU General Public License</a> or <a href="#">GPL-2.0+</a>	
		The SPDX short identifier for the license	<a href="#">GPL-2.0+</a>	
<b>Inventory impacted by a specific security vulnerability</b>	Security Vulnerability	The complete ID of the security vulnerability	<a href="#">CVE-2018-11776</a> for an NVD vulnerability <a href="#">SA40575</a> for a Secunia advisory <a href="#">DSA-4315</a> for a Debian advisory	Searching All Projects for a Security Vulnerability Advisory

## Searching for Projects by Name

You can use the **Project Name** search filter available for the **Projects** list to search for a project by its full or partial name.

### Search Rules

When you search for projects by project name, the following rules apply:

- The name string value you enter is case-insensitive.
- All characters in the search string must be consecutive.
- A full or partial string value is supported as search criterion.
- The string can contain any characters (letters, numbers, and special characters).

### Searching for Projects by Name

This procedure shows how to search for projects by a full or partial name string.



#### Task

**To search projects by name, do the following:**

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Project Name** from search dropdown on the left.

3. Enter the project name (or a partial string in the name) in the **Enter Project Name** field. The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is provided in the **Projects** list header to show the number of projects returned by the search.

If no inventory items meet the specified criterion, the **Projects** list shows “No Projects”.

4. Select a project from the filtered list to open its dashboard. See [Using the Project Dashboard](#) for details.

Alternatively, open the project to view its inventory on the **Project Inventory** tab. See [Opening a Project](#) for details.

## Searching All Projects for Inventory Based on a Specific Component and Version

You can use the **Project Inventory** filter to search for those projects whose inventory contains items based on a specific component and version. The search returns a filtered list of projects; and, when a project in the list is opened, its inventory is also filtered by the search criterion.

This search method saves you time in locating specific inventory items that require attention across all projects. For example, you might also use this search method to pinpoint those projects containing inventory items affected by a recent component upgrade.

You can also use this search method to easily locate projects that contain inventory items impacted by a security vulnerability whose exact ID you do not know; you can search instead for projects with inventory based on a component and version known to be affected by the vulnerability. (This search method is an alternative to using the **Security Vulnerability** filter, which requires the exact vulnerability ID as the search criterion. See [Searching All Projects for a Security Vulnerability Advisory](#).)

### Search Rules

When you search projects for inventory based on a specific component and version, the following rules apply.

- A full or partial string value is supported as search criterion.
- All characters in the search string must be consecutive.
- The string value is case-insensitive and can contain letters, numbers, hyphens, and special characters. Spaces are also allowed.
- Only inventory items on the **Project Inventory** tab are supported in the search.

### Searching All Projects by Component and Version

Use this procedure to locate projects with inventory based on a specific component and version.



#### Task

**To search all projects for inventory based on a specific component and version, do the following:**

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Project Inventory** from search dropdown on the left.
3. In the **Enter Search Criteria** field, specify the complete name or a partial string for one of the following:
  - The name of the component as it appears on the **Component Details** tab (for example, **struts2-core**) for an inventory item

- The name of the component and version as it appears in the **Inventory Name** value (for example, [Apache Struts 2.3.14.3](#))

The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is also provided in the **Projects** list header to show the number of projects returned by the search.

4. Open one of the projects to see a filtered list of inventory items that contain the component or component and version. (See [Opening a Project](#) for details.)

## Searching All Projects for Inventory Associated with a Specific License

You can use the **Project Inventory** filter to search for those projects containing inventory items associated with a specific license. The search returns a filtered list of projects; and, when a project in the list is opened, its inventory is also filtered by the search criterion.

This search method saves you time in locating inventory items with license-related issues, such as those items that are associated with a high-risk license, across all projects.

### Search Rules

When you search projects for inventory associated with a specific license, the following rules apply:

- A full or partial string value is supported as search criterion.
- All characters in the search string must be consecutive.
- The string value is case-insensitive and can contain letters, numbers, hyphens, and special characters. Spaces are also allowed.
- Only inventory items on the **Project Inventory** tab are supported in the search.

### Searching All Projects by License

Use this procedure to locate projects with inventory associated with a specific license.



#### Task

*To search all projects for inventory associated with specific license, do the following:*

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Project Inventory** from search dropdown on the left.
3. In the **Enter Search Criteria** field, specify the complete name or a partial string for one of the following:
  - The name of the **Selected License** as it appears on the **Component Details** tab (for example, [GNU General Public License v2.0](#)) for an inventory item
  - The license SPDX short identifier (for example, [GPL-2.0+](#))
  - The license name as it appears in the **Inventory Name** value (for example, [GNU General Public License](#) or [GPL-2.0+](#))

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 license. (See [Opening a Project](#) for details.)

## 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.



#### Task

**To search for projects affected by a specific security vulnerability, do the following:**

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Security Vulnerability** from search dropdown on the left.
3. In the **Enter Vulnerability ID** field, specify the complete ID of the vulnerability (for example, **CVE-2018-11776** for an NVD vulnerability, **SA40575** for a Secunia advisory, **DSA-4315** for a Debian advisory, and so forth).
4. Press Enter. The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is also provided in the **Projects** list header to show the number of projects returned by the search.

If no inventory items meet the specified criterion, the **Projects** list shows “No Projects”.

5. Open one of the projects to see a filtered list of inventory items that are impacted by the security vulnerability. (See [Opening a Project](#) for details.)

## Restoring the Full Project List

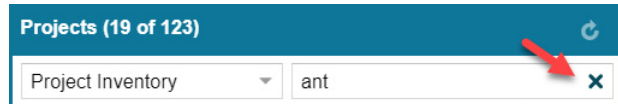
Use this step to remove the filter from the **Projects** list and restore the full list.



### Task

**To restore the full list of projects, do the following:**

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, Click the **X** icon in the criterion field to remove the current **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](#)
- [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](#)

## 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 “notices” text associated with the inventory item. It is pulled from the **Notices Text** pane on the **Inventory Details** panel in the Analysis Workbench (or on the **Notes & Guidances** tab on the **Project Inventory** page). If this pane is empty, FlexNet Code Insight uses the content in the **As-Found License Text** pane, which shows the verbatim text license text found in the codebase either by the system or the Analyst. If no **As-Found License Text** or **Notices Text** information is available, no notices are generated for the inventory item in the Notices report (although the report will still show the inventory name and the URL, if available).

## Adding Text for Notices Reports

If the **As-Found License Text** pane is empty for a given inventory item, you can use the **Notices Text** pane to provide the exact content to include in the Notices report.



**Note** • If the **As-Found License Text** pane contains content, best practice is to leave the **Notices Text** pane empty so that the report uses the license information found in the **As-Found License Text** pane.



### Task

**To add text for the Notices report, do the following:**

1. Navigate to one of these locations:

#### Analysis Workbench

- a. In the Analysis Workbench for your project, select an item from the list in the **Inventory Items** panel.
- b. In the center panel, select **Inventory Details**. Information appears in the fields of the **Inventory Items** panel.



- c. Scroll down the panel until the **Notices Text** pane appears:

**Notices  
Text:**



#### Project Inventory Page

- a. On the **Project Inventory** page for your project, select an inventory item from the inventory list.
  - b. On the right, select the **Notes & Guidance** tab, and locate the **Notices Text** pane.
2. In the **Notices Text** pane, enter the license content for the inventory item. No special formatting (such fonts, character formats, lists, and so forth) is permitted.
  3. Select **Save** to save your changes. The content you entered will appear for this inventory item in the Notices report.

## Generating the Notices Report



#### Task

*To generate a Notices Report, do the following:*

1. Navigate to the **Summary** tab for the project (see [Opening the Project Summary Tab](#)).
2. 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.
3. Click **OK**. When the report has been generated. When the report has been generated, the **View | Download** hyperlink appears in the **Basic Report:** field.
4. 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**. On the prompt that appears, choose the next action for the report download:
    - **Open**—The report opens in your default text editor.
    - **Save**—The report is saved in the specified directory.
    - **Cancel**—The report is not downloaded.

## 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 as 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 a role to a given user, drag and drop the user name from the **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 another role to the same user or to assign a role to a different user.
5. Click **Close** when you finish adding reviewers, analysts, and reviewers.

## 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 and update default settings for automatically publishing inventory after the scan.



### 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](#) to for field descriptions.
5. Click **Save** to save the changes.

## Updating Inventory Review and Remediation Settings for a Project

You can overwrite default settings that configure the automation of the review, remediation, and status notification processes for published inventory in your project. These settings, which work in conjunction with the set of policies in the project's policy profile, are used to set up the following in your project:

- The policy profile to associate with the project. The policies in the selected profile work in conjunction with the review, remediation, and notification configuration defined on this tab.
- Automatic creation of manual review tasks for inventory items not reviewed by policy during publication performed as part of a scan. The tasks are automatically assigned to the default legal or security contact that you specify.
- Automatic creation of remediation tasks and associated external work items for inventory that is rejected either automatically by policy or during manual publication by an analyst. The tasks are automatically assigned to the default engineering contact that you specify.
- Automatic rejection of published inventory impacted by new vulnerabilities detected in the latest scan or Electronic Update.
- The automatic generation of email notifications only (instead of assigned tasks), which are sent to the project owner as alerts concerning the rejected or non-reviewed published inventory items.



### Task

*To update settings that automate review, remediation, and status notification processes for published inventory, do the following:*

1. As the Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Edit Project** from the popup menu. The **Edit Project** page opens.
3. Select the **Review and Remediation Settings** tab.
4. Update the fields as needed. Refer [Edit Project: Review and Remediation Settings Tab](#) to for field descriptions.
5. Click **Save** to save the changes.

## Connecting the Project to Remote Data Sources

If your system is configured to connect to a remote data source, you will have access to update the following:

- [Version Control Settings](#)
- [ALM Settings](#)

### Version Control Settings

Use the **Version Control Settings** tab on the **Edit Project** page to connect to one or more Source Code Management (SCM) repositories directly from FlexNet Code Insight so you can scan and audit code without manually moving that data to the scan server. For information about connecting to a remote data sources, see the [Using FlexNet Code Insight](#) 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 **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 2-5 • Supported Code Insight Variables for Use in Work Item Summary and Description Text**

\$PROJECT_NAME	Name of the Code Insight project containing the issue
\$INVENTORY_ITEM_NAME	Name of the inventory item containing the issue
\$COMPONENT_NAME	Name of the component associated with the inventory item
\$VERSION_NAME	Version of the component associated with the inventory item
\$LICENSE_NAME	Name of the selected license for the inventory item
\$NUMBER_VULNERABILITIES	Total number of security vulnerabilities associated with the inventory item

**Table 2-5 • Supported Code Insight Variables for Use in Work Item Summary and Description Text (cont.)**

\$NUMBER_FILES	Total number of files associated with the inventory item
\$INVENTORY_URL	Link to the inventory item

When the work item is created, the included variables are replaced by their respective values.

### Example Use of Variables

The following is example text you might enter in the **Default Summary Text** field. The text includes some of the available variables:

The \$INVENTORY\_ITEM\_NAME inventory item in the project \$PROJECT\_NAME contains \$NUMBER\_VULNERABILITIES vulnerabilities that require review. Go to \$INVENTORY\_URL to see the vulnerable inventory item.

If your Code Insight project name is *MySampleProject* and the name of the inventory item name for which you create a work item is *Apache Commons BeanUtils*, the work item and Jira issue will display the following summary:

The Apache Commons BeanUtils 1.7.0 (Apache 2.0) inventory item in the project MySampleProject contains 18 vulnerabilities that require review. Go to <https://my.sample.server:8888/codeinsight> to see the vulnerable inventory item.

## Unassociating an ALM Instance from a Project

The Project Owner may unassociate an ALM instance from a project at any time. If the association is removed, any existing work items will remain with the project, but the **Create Work Item** option becomes disabled.



### Task

**To unassociate an ALM instance from a project, do the following:**

1. As the Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Edit Project** from the popup menu. The **Edit Project** page opens.
3. Select the **ALM Settings** tab.
4. In the **ALM Instance** dropdown, change the selection to **None**.

## Changing Project Owners

FlexNet Code Insight provides the ability to change the owner of a project. This feature enables you to transfer the ownership of a project to a new user when the current project owner is unavailable to administer the project. Any user who is an Administrator or the current Project Owner can change the owner. (The user who created the project automatically becomes the initial Project Owner.)



**Note •** Changing a Project Owner is a silent transaction. No email notifications will be sent as part of this operation.



**Task**

**To change the project owner, do the following:**

1. Log into FlexNet Code Insight as an *Administrator* or the current *Project Owner*.
2. Navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
3. Open the **Manage Project** dropdown menu and select **Change Owner**, or click the **Change Owner** button, whichever is visible. The **Select new project owner** dialog appears.



**Note** • If you have not logged in as *Administrator* or *Project Owner*, neither the **Manage | Change Owner** menu option nor the **Change Owner** button is visible.

4. Highlight a name in the list and click **Apply**. The **Summary** tab is opened with the selected name displayed in the **Owner** field.



**Note** • If you change the owner to a user without *Administrator* or *Project Management* permissions, only the **Generate Audit Report** option will be available at the bottom of the **Summary** tab.

## Rescanning Your Codebase

During a codebase scan, FlexNet Code Insight uses a combination of Automated Analysis and Advanced Analysis techniques to identify open-source and third-party code in your product (see [What Is a FlexNet Code Insight Scan?](#))

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 2-6 •** Change Events Resulting in Full or Incremental Rescans

Changes to...	Automated Analysis	Advanced Analysis	Details
<b>Codebase files</b>	Incremental rescan	Incremental rescan	Changes in codebase files are determined by the MD5 hash digest of the files.
<b>Automated Analysis rule set</b>	Full rescan	No rescan	Rules are automatically pushed to your Code Insight server through both an internal process and the weekly Electronic Update.
<b>FlexNet Code Insight version</b>	Full rescan	No rescan	This change is usually an upgrade in the Code Insight version.
<b>Scan profile settings</b>	Full rescan	Full rescan	<p>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 <i>expensive</i> Advanced Analysis full rescan. See <a href="#">Effects of Scan-Setting Changes on Rescans</a> for more information.</p> <p>Scan profiles are configured by the Administrator as described in the <i>FlexNet Code Insight Installation and Configuration Guide</i>.</p>
<b>CL version</b>	No rescan	Full rescan	This change is associated with a change to the <b>CL Path</b> value identified in the scan server setup. (This setup is handled by the Administrator, as described in the <i>FlexNet Code Insight Installation and Configuration Guide</i> .)

## Effects of Scan-Setting Changes on Rescans

One type of change event that does effect a full rescan by either Automated Analysis or Advanced Analysis (or both) is an update to settings in the scan profile associated with the rescan. Depending on which settings have changed, the full rescan could be more expensive (requiring more time and resources) than other full rescans.



**Note •** *Keep in mind that, if you have applied a new scan profile to your project, only those profile settings that are different from the settings in the previously associated profile will impact the rescan.*

The following table provides a list of the scan profile settings and the type of full rescan to expect should any of the settings be updated prior to a codebase rescan.



**Table 2-7 •** Types of Full Rescan to Expect Should Scan Profile Settings Change

Scan Profile Settings	Automated Analysis	Advanced Analysis
A change to any of these settings: <ul style="list-style-type: none"> <li>● <b>Perform Package/License Discovery in Archive</b></li> <li>● <b>Dependency Support</b></li> <li>● <b>Automatically Add Related Files to Inventory</b></li> </ul>	Full rescan	—
A change to any of these settings: <ul style="list-style-type: none"> <li>● <b>Source Code Matches</b></li> </ul> Related fields: <ul style="list-style-type: none"> <li>● <b>Include System Identified Files</b></li> <li>● <b>Include Files with Exact Matches</b></li> </ul>	—	Full rescan (expensive)
A change to any of these settings: <ul style="list-style-type: none"> <li>● <b>Exact Matches</b></li> <li>● <b>Search Terms</b></li> <li>● <b>Scan Inclusions</b></li> </ul>	—	Full rescan (expensive but less expensive than that performed when <b>Source Code Matches</b> or related fields change)

## Handling of Edited Inventory During Rescans

FlexNet Code Insight enables you to make changes to inventory both in **Analysis Workbench** and on the **Project Inventory** tab. You create inventory items as well as edit both user-created and system-generated inventory. Edits to existing inventory can include changes to the following elements:

- 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 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.



### Task

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

1. Navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).

2. Perform either step:

- Click the **here** link in the **Scan Status** field to schedule the rescan. If other events are scheduled, the rescan will be queued and automatically run based on queue order.
- Click the **Start Scan** button.

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

- Scan Status -	
<b>Scan Status:</b>	Project being scanned
<b>Scan Progress:</b>	In Scan Queue ( <a href="#">Show Details</a> )
<b>Last Scan:</b>	Scan of project Project2 <b>completed</b> . Scan Summary : 358 Files   6.03 MB   53 Lines of Code
<b>Past Scans:</b>	Click <a href="#">here</a> to view the scan history for this project.

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

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



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

For an overall understanding of the scan results, see [Overview of Scan Results](#).

## 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 & Importing Project Data](#) chapter.



**Task**

**To export project data, do the following:**

1. As Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Export Project Data** from the dropdown menu.
3. When prompted, select a location to store the exported data. FlexNet Code Insight creates a JSON data file, archives it in a .zip file and saves it in to a location specified in your browser settings.



**Note** • You can also use the public REST API to export your project data. For more information, see the [Exporting & Importing Project Data](#) chapter.

## Creating a Private Project

Security-conscious project owners can control access to their projects within the enterprise by setting a project's visibility to **Private**. This feature gives project owners the ability to hide sensitive information from general view and select specific users who can view the project. The default project visibility is **Public**, which means that all FlexNet Code Insight users can view all projects. For information about assigning roles, see [Assigning Project Roles to Users](#).



**Note** • Users who have Administrator privileges but are not part of a Private project can see the project in the **Projects** list, view the **Summary** tab for the project, and change the owner of the project.



### Task

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

1. If you are not viewing the **Project** list, navigate to it.
2. Click **Add New**. The **Add Project** dialog appears with default values appearing in all the fields but **Name**.
3. In the **Name** field, enter a name for the new private project.
4. From the **Project Visibility** dropdown, select **Private**.
5. (Optional) Select a different project type from the **Project Type** dropdown.
6. (Optional) Select a different policy profile from the **Policy Profile** dropdown.
7. 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.

8. (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.




### Task

**To add a new policy profile or edit an existing one, do the following:**

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



2. Select **Policy** from the menu to open the **Policies** page, showing the list of current policy profiles.

3. To edit an existing policy profile, select it from the list, and click the **Edit** icon .  
  
or  
  
To add a new policy profile, click **Add Policy**.  
  
The **Policy Details** page is displayed.
4. Refer to the associated help (or to [Policy Details Page](#)) for details about the fields used to define the policy profile.
5. Click **Save** to save the updates or to add the new policy profile.

## Copying a Policy Profile

The following procedure describes how to create a copy an existing policy profile. This can be useful for providing a template to create a new policy profile or for backing up an existing one.




### Task

*To copy an existing policy, do the following:*

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



2. Select **Policy** from the menu to open the **Policies** page, showing the list of current policy profiles.
3. Select the policy profile to copy from the policy list, and click **Copy** icon .

A new policy with the name **Copy of policy name** is added to the **Policy** list. You can then edit the new policy to change its name or update its criteria. See [Adding or Editing a Policy Profile](#).

## Associating a Policy Profile with a Project

The Project Owner can associate a project with a policy profile when the project is created (see [Creating a Project](#)) or later by editing the project (see [Updating Inventory Review and Remediation Settings for a Project](#)). If no policy is explicitly selected for a project, the Default License Policy Profile is used.

# 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

Persona	Search Type	Finds...	Example
<b>Any</b>	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 = <i>zlib 1.2.8 (zlib/libpng License)</i>  Inventory Name = <i>zlib</i>  License Name = <i>EPL</i>

**Table 3-1 • Sample Advanced Searches**

Persona	Search Type	Finds...	Example
<b>Any</b>	By Criticality (Priority)	<p>Most critical inventory that requires security or legal review based on presence of high-severity vulnerabilities or P1 licenses.</p> <p>Useful when you want to prioritize your inventory review by most important findings.</p>	<p><b>Option 1:</b> Inventory Priority = <i>P1</i></p> <p><b>Option 2:</b> Security Vulnerability Severity = <i>High Severity (CVSS 7.0 - 10.0)</i> or License Priority = <i>P1 - Viral/Strong Copyleft</i></p>
<b>Any</b>	By Review Status	<p>Inventory that requires further review (Not Reviewed), is Approved, or is Rejected.</p> <p>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.</p>	Inventory Review Status = <i>Approved</i>
<b>Any</b>	By Dependencies	<p>Only dependency inventory items (both first-level and transitive dependencies), only top-level inventory items (excluding all dependency inventory items), or all inventory items.</p> <p>Useful for focusing on or filtering out dependency inventory items.</p>	<p>Dependency Options = <i>All Inventory Items</i></p> <p>Dependency Options = <i>Only Top-Level Inventory Items</i></p> <p>Only Dependency Inventory Items = <i>Only Dependency Inventory Items</i></p>
<b>Any</b>	By Inventory Age	<p>Inventory created within the specified time range.</p> <p>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.).</p>	Inventory Age = <i>Last 7 Days</i>



**Table 3-1 • Sample Advanced Searches**

Persona	Search Type	Finds...	Example
<b>Any</b>	By Notification	<p>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.</p> <p>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.</p>	<p>Inventory with Open Alerts = <i>checked</i></p> <p>Inventory Rejected Due to New Non-Compliant Security Vulnerabilities = <i>checked</i></p>
<b>Any</b>	By Inventory Task Age	<p>Inventory tasks (review or remedial tasks) created within the specified date range.</p> <p>Useful for filtering on inventory items that have recently created tasks to determine what new work needs to be performed.</p>	<p>Inventory Tasks Age = <i>Last 7 days</i></p> <p>Inventory Tasks Age = <i>Custom Date Range</i> From: 09/05/2018 To: 10/31/2018</p>
<b>Any</b>	By Inventory Task Owner	<p>Inventory tasks (review or remedial tasks) owned by a specific user.</p>	<p>Inventory Tasks Owner = <i>Any</i></p> <p>Inventory Tasks Owner = <i>Only mine</i> (current user)</p> <p>Inventory Tasks Owner = <i>&lt;Username&gt;</i> (selected user)</p>
<b>Analyst, Reviewer</b>	By Confidence Level	<p>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 <a href="#">Inventory Confidence</a> in the “Using FlexNet Code Insight” chapter.)</p> <p>Useful for determining whether the item should be triaged or reviewed to validate or further refine the finding.</p>	<p>Inventory Confidence Level = <i>High</i> (or <i>Medium</i> or <i>Low</i>)</p>

**Table 3-1 • Sample Advanced Searches**

Persona	Search Type	Finds...	Example
<b>Security Analyst</b>	By Vulnerability ID	Inventory with a specific vulnerability (NVD CVE or Secunia Advisory).  Useful when you are looking for inventory exposing you to a specific security issue, typically a newsworthy event.	Security Vulnerability ID = <i>SA71946</i>
<b>Security Analyst</b>	By Security Risk Exposure	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.	Security Vulnerability Severity = <i>High Severity (CVSS 7.0 - 10.0)</i>
<b>Security Analyst</b>	By Security Vulnerability Age	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.	Security Vulnerability Age = <i>Last day</i>
<b>Security Analyst</b>	By Security Risk Exposure and Vulnerability Age	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.	Security Vulnerability Age = <i>Last day</i> and Security Vulnerability Severity = <i>High Severity (CVSS 7.0 - 10.0)</i>
<b>Security Analyst</b>	By Inventory Alert	Published inventory items that have new security vulnerability alerts or that have been rejected due to new non-compliant security vulnerabilities. You can select one or both options.  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.	Inventory with Open Alerts = <i>checked</i>  Inventory Rejected Due to New Non-Compliant Security Vulnerabilities = <i>checked</i>

**Table 3-1 • Sample Advanced Searches**

Persona	Search Type	Finds...	Example
<b>Security Analyst</b>	By New Vulnerabilities (Requires re-review)	Inventory that has gained a new security vulnerability since a specified date.  Useful to determine which inventory items require another look from a security analyst due to new associated vulnerabilities.	<i>Review Status = Approved and Security Vulnerability Age = Last 7 days</i>
<b>Legal</b>	By License Risk Exposure	Most critical inventory that requires legal review (contains a P1 license - Viral/Strong Copyleft).  Useful to prioritize legal work based on license classification.	<i>License Priority = P1 - Viral/Strong Copyleft</i>
<b>Analyst</b>	Requires Re-Review based on Missing License	Approved inventory with a missing license.  Useful to catch scenarios where items were approved without an associated license. This should be a rare event.	<i>Inventory Review Status = Approved and License Priority = No License Found</i>
<b>Eng. Mgr./ Final Reviewer</b>	Stop Shipment!	Approved inventory that may require a stop shipment due to high severity vulnerability or P1 license.  Useful to identify cases that would break the build. These are items that were approved at the time of review, but since then have a different license or high-severity vulnerability.	<i>Inventory Review Status = Approved or License Priority = P1 - Viral/Strong Copyleft or Security Vulnerability Severity = High Severity (CVSS 7.0 - 10.0)</i>

## 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 & Importing Project Data

This section discusses the export and import features of FlexNet Code Insight.

## Exporting and Importing

FlexNet Code Insight provides the ability to export project data from one project and import that data into another project on the same server or across different servers. The functionality can be useful in any of these following scenarios:

- **Backup and restoration of project and audit data:** Use export to create a full backup of a project. The backup data file includes information about the project and scan, all inventory (with inventory details, field values, file associations, and inventory status), review status of the files, and custom data. The project data may be restored to a new project for an archived view or for ongoing scanning and auditing.
- **Audit work reuse:** Use export/import to apply audit and analysis work performed on one project to another project with a similar codebase. The default import behavior processes only inventory from the source project that is relevant to the target project, so that only inventory with matched files is processed during the import.
- **Sharing of live audit results:** Use export/import to share live audit results between teams, such as in the case of a Professional Services engagement with a customer. Export a project from one instance of FlexNet Code Insight and import into a project on another instance on a different server. Results can be imported as inventory only or as a starting point for continued scanning and auditing.
- **Creating inventory from external or legacy data:** Use import to create live project inventory in FlexNet Code Insight from a datafile containing legacy or external data. This type of import requires conversion of the legacy data (such as from a 6.x project or an external system) to the import data JSON format before importing it into a new FlexNet Code Insight project.
- **Copy and branch a project:** Use export/import to create an exact copy of a project for future scanning and audit work. Export the project data and import it into a scanned project that is pointed to the same codebase (usually on the same instance) for ongoing scanning and auditing.

Project data export and import functionality is available through a REST interface. The Export Project Data API exports the project data into a JSON data file, and then compresses it into a zip archive. The archive file can be used as input to the Import Project Data API, which decompresses the archive and processes the JSON data file. For additional details and usage for the Project Data Export and Import APIs, reference this document or see the online REST API Swagger documentation.

The export and import APIs may be invoked locally or remotely from any REST client or command line tool that supports Curl. The export and import processes run in the background and do not interfere with other scan or analysis work.



---

**Note** • A standard Import assumes that the codebase has been scanned on the destination instance.

## What is Exported?

The Export Project Data API processes all project data (export/project/scan information, all inventory and file associations, statuses, and custom data). Some of this data is for informational purposes only and not necessarily used during import. The following content is exported:

- **Export information:** Date and time, owner, FlexNet Code Insight version, CL and Electronic Update version, and more.
- **Project and scan settings:** Name, description, scan profile, policy profile, and scanroot path.
- **Inventory:** All inventory data, fields, publish and review status, associated files, and associated repository item.
- **Custom data:** Custom versions, licenses and vulnerabilities, and custom mappings.
- **Reviewed files:** Absolute files paths and MD5s for all files marked as reviewed.

## Exporting Project Data

Projects can be exported in one of the following ways:

- By selecting **Export Project Data** from the **Manage Project** dropdown menu on the **Summary** tab. See [Exporting Project Data Using the FlexNet Code Insight UI](#).
- By using the Export Project Data REST API. See [Exporting Project Data Using the REST API](#).

To export data, the following are required:

- A running FlexNet Code Insight instance.
- An existing, non-empty project, which can be unscanned if you are exporting only the project information and configuration.



---

**Note** • Running an export on a project currently being scanned is not recommended.

- A valid JWT token for the project owner of the project to be exported. The token is required only if exporting via REST API. For more information, see “Generating a JWT Authorization Token” in the *FlexNet Code Insight Installation and Configuration Guide*.

- A REST client or command line interface with Curl support. The client or command line interface is required only if exporting via REST API.

## Exporting Project Data Using the FlexNet Code Insight UI

Exported project data is saved in JSON format and placed in a zip file.



### Task

**To export project data in the UI, do the following:**

1. Log into FlexNet Code Insight as the project owner of the project you want to export.
2. Navigate to the **Summary** tab. See [Project Summary Tab](#) for information about the fields on the page.
3. Open the **Manage Project** dropdown and select **Export Project Data**.
4. When prompted, select a location to store the exported data. FlexNet Code Insight generates a zip file containing a JSON data file and saves it to the specified location.

## Exporting Project Data Using the REST API

In addition to doing so within the user interface, FlexNet Code Insight provides a REST API to do the exporting.



### Task

**To export project data using the REST API, do the following:**

1. Modify the following Curl command by substituting the variables based on your server and project information. Specify the name of the zip file into which the command output will be redirected.

```
curl -X GET "HOST:PORT/codeinsight/api/project/exportProjectData?projectId=PROJECT_ID" -H "accept: application/json" -H "Authorization: Bearer JWT_TOKEN" > PROJECT_DATA_FILE.zip
```

The following is an example:

```
curl -X GET "http://localhost:8888/codeinsight/api/project/exportProjectData?projectId=55" -H "accept: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJqcniVlaW4iLCJ1c2VySWQiOiJEWLCjYpYXQiOiJlMTA5NjM2NzZ9" > MyProjectDataFile.zip
```

2. Run the statement with a command line utility that supports Curl.



**Note** • You may use the *Get Project Id API* (*/project/id*) to determine the ID of the project. If the project name contains a space or special character, replace it with its encoded version. For example, use “project%20foo” for a project named “project foo”.

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

```
Export Zip
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   100    33917   0 33917   0     0  11305      0  --:--:--  0:00:03  --:--:-- 11253
```

When the export completes, a zip archive will be available in the directory from which you ran the statement. The archive contains a JSON data file with the project data. Unless specified otherwise, the zip archive and the data file will include the project Id at the beginning of the file and a timestamp at the end of the file, as in the following:

```
C:/fnci/project_export/MyProject.zip/5-export-12-22-2020_10-42.zip  
C:/fnci/project_export/MyProject.zip/MyProject-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. Unzip the archive.
4. (Optional) To verify that the export process completed successfully, open the JSON data file with a utility that supports JSON, such as Textpad or Notepad++. If the data appears to be correct, the data file is ready for import.



**Note** • If the export process is not successful, the zip archive will contain a file with the status code and error message. Resolve the error, delete the invalid archive file, and run the script again.

## Types of Import

The following are the available types of import:

- **Inventory-only import:** Processes all published inventory, with inventory details, fields and file associations. Requires an Inventory Only project without a scan.
- **Standard import:** Processes all inventory, with inventory details, fields and file associations, as well as all **files** that are marked as reviewed. Requires a Standard project with a completed scan before import.

The **Project Type** of the target project (the project that will accept the imported data) controls the type of import to be performed.

## What is Imported?

Different items are imported with each type of import.

### Inventory-Only Import

- **Inventory**—Only published inventory items, along with their details, review status, associated files, and associated repository item.
- **Custom data**—Custom versions, licenses and vulnerabilities, and custom mappings.

### Standard Import

- **Inventory**—All inventory (published & unpublished), along with inventory fields, details, reviewed status, associated files and associated repository item.
- **Custom data**—Custom versions, licenses and vulnerabilities, and custom mappings.
- **Reviewed files**—Absolute files paths and MD5s for all files marked as reviewed.





**Note** • Import does not process custom components. Instead, FlexNet Code Insight creates work-in-progress (WIP) or license-only type inventory to represent inventory with custom components.

## How Files & Inventory Are Processed During Import

During import, the file path (and optionally the MD5) is the key between data in the data file and the codebase files on the target server. File paths are matched between the data file and codebase files by subtracting the root path from the absolute path. For 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 files that match based on file path are processed for inventory-to-file association in the target project.
- Only files that match based on file path and MD5 are processed when marking files as reviewed in the target project.
- Only Inventory containing files that match based on file path is processed during import into the target project (empty inventory is not created).

## Import Options

The following options may be applied during import to override the default settings as needed:

### **checkInventory (default: false)**

If enabled, only files with matching MD5 in the import data file and the scanned file will be associated to inventory in the target project.

### **checkReviewed (default: true)**

If enabled, only files with matching MD5 in the import data file and the scanned file will be marked as reviewed.

### **createEmptyInventory (default: false)**

If enabled, all inventory (with or without matched files based on file path) is processed during import.



**Note** • If the `checkInventory`, `checkReviewed`, and `createEmptyInventory` options are not set, the default values apply.

## Importing Project Data

To import data, the following are required:

- A running instance of FlexNet Code Insight.

- An existing project to import data into, which can be either an Inventory Only project if performing an Inventory Only import or a Standard project with a scanned codebase if performing a standard import.
- A valid zip archive containing the JSON data file with the project data to be imported. The data file may be generated by the export process or created manually. It must be in the correct import format.
- The Electronic Update has completed on the target server.
- A valid JWT token for the project owner of the project to be imported.
- A REST client or command line interface with Curl support.

**Task****To run an import, do the following:**

1. Create a Standard or Inventory Only project for import, depending on the type of import. For information on creating a project, see [Creating a Project](#).



**Note** • 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 Jenkins plugin or another scan agent plugin.

2. For Standard import only, upload and scan the same or a similar codebase. A scan is not required for an Inventory-only project.
3. Modify the following Curl command by substituting the variables based on your server and project information:

```
curl -X POST --data-binary "@PROJECT_DATA_FILE.zip" "HOST:PORT/codeinsight/api/importer/importProjectData?projectId=PROJECT_ID" -H "accept: application/json" -H "authorization: Bearer JWT_TOKEN" -H "cache-control: no-cache" -H "Content-Type: application/octet-stream"
```

The following is an example:

```
curl -X POST --data-binary "@MyProjectDataFile.zip" "http://localhost:8888/codeinsight/api/importer/importProjectData?projectId=1" -H "accept: application/json" -H "authorization: Bearer eyJzdWIiOiJqcnViaW4iLCJ1c2VySwQiOiJlLCJpYXQiOiJlMTA5NmM2NzZ9" -H "cache-control: no-cache" -H "Content-Type: application/octet-stream"
```



**Note** • Empty inventory items without file associations are never imported by default. If you are importing from a scanned project into an inventory project, you must add the “createEmptyInventory=true” option for inventory to be generated in the new project.




**Note** • The `PROJECT_DATA_FILE` parameter refers to the name of the project data file containing the data you wish to import. The `PROJECT_ID` refers to the ID of the project you want to import the data into.

4. Run the statement from a command-line utility that supports Curl. When the import is done, a status message with the term **OK** will appear in the command prompt window. If the import is not successful, a status code and error message will appear.
5. To verify that the import completed successfully, open the target project in FlexNet Code Insight and navigate to the **Inventory** page. See [Searching the System](#). Confirm the total number of inventory items based (only inventory with matched files is imported by default) and that the inventory items contain accurate inventory details and file path associations.

## Expected Results

The following table summarizes the type of export/import combinations that can be performed in FlexNet Code Insight and their expected results. In the table, *source project* is the project from which data is exported, and *target project* is the project into which data is imported.

**Table 4-1 • Export/Import Expected Results**

	Source Project: Inventory Only	Source Project: Standard (scanned data)
<b>Target Project: Inventory Only</b>	<p>Components are matched against the target system compliance library.</p> <p>Custom vulnerabilities may be imported.</p> <p>Policy is applied.</p> <p>All inventory is published.</p>	<p>Component IDs are imported.</p> <p>Imported file paths are listed in inventory but not processed.</p> <p>Custom vulnerabilities may be imported.</p> <p>Policy is <i>not</i> applied.</p> <p>Inventory is Published/Recalled based on imported data.</p> <p>Inventory is Approved/Rejected/Unknown based on imported data.</p> <p>File reviewed status is not applicable.</p>
<b>Target Project: Standard (scanned data)</b>	Not supported.	 <p><b>Note •</b> Requires a scan before import.</p> <p>Component IDs are imported.</p> <p>Imported file paths listed in inventory and matched to existing scanned files.</p> <p>Vulnerabilities are not imported (obtained during scan).</p> <p>Policy is not applied.</p> <p>Inventory Published/Recalled status based on imported data.</p> <p>Inventory is Approved/Rejected/Unknown based on imported data.</p> <p>Files are marked as reviewed based on imported data.</p>

## Empty Inventory

An empty inventory item is one that does not contain any associated files. By default, empty inventory is not processed during import and no empty inventory items are created in the target project.

## 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 import and all fields in the target project are overridden by the data in the data file, with the exception of empty data in the data file.

## Special Considerations for Standard Import

Because a Standard import requires a local scan on the target server before import, the scan may override some manual audit work performed on the source project. Be aware of the following scenarios that only apply to a Standard Import:

### Unreviewed Files

Files that are manually *unreviewed* in the source project, do not retain the *unreviewed* status after standard import to the target project. This occurs because the project data file stores information only about reviewed files.

If you wish to retain both reviewed and unreviewed file status after standard import, manually mark all of the codebase files in the target project as *unreviewed* before importing the data file.

### Deleted Inventory and Removed File Associations

System-generated inventory that is manually deleted from the source project is brought back after standard import to the target project. Files that are manually removed from system-generated inventory in the source project are brought back after standard import to the target project. This occurs because the pre-import scan brings back the deleted or removed data.

To ensure that deleted inventory and file associations remain deleted after standard import, do one of the following:

- Turn off all automated detection when scanning the target project before performing the import.
- After scanning the target project, delete all project inventory before performing the import.

### Repository Item modifications

Modifying the associated repository item for a given system-generated inventory item in the source project may result in two similar inventory items (with the same name and file path) in the target project after a standard import. This occurs because the pre-import scan generates the same inventory item as in the source project before user edits.

To avoid two identical inventory items, do one of the following:

- Turn off all automated detection when scanning the target project before performing the import.
- After scanning the target project, delete all project inventory before performing the import.

# 5

## Automated Analysis

This chapter covers the following topics to describe the Automated Analysis of features in FlexNet Code Insight:

- [What is Automated Analysis?](#)
- [Supported Development Ecosystems](#)
- [Supported Archive Formats](#)
- [Additional Rule-based Detection Capabilities](#)

### What is Automated Analysis?

FlexNet Code Insight provides Automated Analysis capability to automatically inventory various package formats without the need for manual analysis. New automated detection rules are delivered to FlexNet Code Insight as part of the Electronic Update process and through internal processes.

Automated Analysis is used in both scanning scenarios outlined below:

- Traditional scanning where the codebase is uploaded to the scan server or synchronized using a source code management system like Git or Perforce.
- Scan agent plugins that perform a scan remotely on an Engineering build server and send results back to FlexNet Code Insight.

### Supported Development Ecosystems

FlexNet Code Insight provides native support for operating in many development ecosystems (each encompassing a language, package type, and public registry). See the following topics for more information:

- [Supported Ecosystems](#)
- [Notes About Ecosystem Support](#)
- [Notes about Dependencies Support](#)

## Supported Ecosystems

The table below provides the following information about each ecosystem that Code Insight supports in the Automated Analysis process:

- **Language/File Type**—The code language or file type supported by the ecosystem.
- **Package**—The name of a package type in the ecosystem.
- **Registry**—The URL for the public registry or repository that hosts the package type.
- **Manifest File**—The file for which the Code Insight scan searches to locate a package of this type.
- **Top-level Inv.**—The indicator ✓ for “yes” or a dash (—) for “no”, showing whether the Code Insight scan supports the detection of third-party software in the package (displayed as top-level inventory).
- **Direct Dep., Trans. Dep.**—If top-level inventory is supported, the discovery of this component’s direct (first-level) dependencies and transitive dependencies (that is, dependencies of dependencies).
- **Notes**—Specific information pertaining to Code Insight’s support of the ecosystem.

**Table 5-1 • Supported Ecosystems**

Language/ File Type	Package	Registry	Manifest File	Top-level Inv.	Direct Dep.	Trans. Dep.	Notes
<b>DLL/EXE</b>	PE Header	N/A	.dll, .exe	✓	N/A	N/A	—
<b>Go</b>	glide	<a href="https://go-search.org">https://go-search.org</a>	glide.yaml	✓	—	—	See <a href="#">Notes for Supported Go Ecosystems</a> .
	godep		godeps.json	✓	—	—	
	govendor		vendor.json	✓	—	—	
	module		go.mod	✓	—	—	
<b>Java</b>	Gradle	<a href="http://search.maven.org/">http://search.maven.org/</a>	build.gradle	✓	✓	✓	—
	Maven		pom.xml	✓	✓	✓	—
<b>JavaScript</b>	Bower	<a href="https://registry.bower.io/packages/">https://registry.bower.io/packages/</a>	bower.json	✓	✓	—	—
			.bower.json	✓	✓	—	—
			package.json	✓	✓	—	—
<b>.NET</b>	NuGet	<a href="https://api.nuget.org/v3-flatcontainer/">https://api.nuget.org/v3-flatcontainer/</a>	.nupkg	✓	✓	✓	—
			.nuspec	✓	✓	✓	—
<b>NodeJS</b>	NPM	<a href="https://registry.npmjs.org/">https://registry.npmjs.org/</a>	package.json	✓	✓	✓	—
<b>PHP</b>	Composer	<a href="https://packagist.org/">https://packagist.org/</a>	composer.json	✓	✓	—	—
			composer.lock	✓	✓	—	—

Table 5-1 • Supported Ecosystems (cont.)

Language/ File Type	Package	Registry	Manifest File	Top-level Inv.	Direct Dep.	Trans. Dep.	Notes
RPM	RPM Header	N/A	.rpm	✓	N/A	N/A	—
Ruby	Gem	<a href="https://rubygems.org/api/v1/">https://rubygems.org/api/v1/</a>	.gem	✓	✓	—	See <a href="#">Notes for Supported Ruby Ecosystems</a> .
			Gemfile	✓	✓	—	
			.gemspec	✓	✓	—	
Swift, Obj-C	CocoaPods	N/A	Podfile.lock	✓	—	—	—
			.podspec	✓	—	—	—

## 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 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 of 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://sevenzzip.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 JWT authorization token for the user whose account will be used to connect to FlexNet Code Insight. See “Generating a JWT Authorization Token” in the *FlexNet Code Insight Plugins Guide*.

**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 access token.

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

Build Environment	Code Insight Plugin	Performs automated scanning of...
<b>IDEs</b>	Eclipse	An Eclipse workspace in the Eclipse IDE environment.
	Visual Studio	Selected codebase paths included in a Visual Studio project.
<b>CI Tools</b>	Azure DevOps	An Azure DevOps workspace as part of the build process.
	Bamboo	A Bamboo workspace as part of the build process (on Local Agents only)
	GitLab	GitLab projects as part of the build process.
	Jenkins	A Jenkins workspace as part of the build process.  A separate plugin is available (called the Scan Schedule Plugin) that enables you to simply schedule the scan of a codebase residing on the Code Insight scan server via the Jenkins scheduler.
	TeamCity	TeamCity projects as part of the build process.
<b>Package Manager and Build Tools</b>	Ant	Apache Ant as part of the build process.
	Gradle	Gradle projects as part of the build process.
	Maven	Maven projects as part of the build process.
<b>Binary Repositories</b>	JFrog Artifactory	Artifactory repositories to identify non-compliant artifacts.
<b>Container Platforms</b>	Docker Images	Docker images on a Docker server.

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 more information about editing projects, see [Assigning Project Roles to Users](#).
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, 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, navigate to it.
2. Click **Sync Now** to get files from the repository. Files are stored in the root folder for the Code Insight scan server, which contains subfolders with project IDs. Under each project ID folder, subfolders with names such as `git.0` or `git.1` are generated. The number of subfolders is equal to the number of instances created inside your FlexNet Code Insight project.



**Note** • 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.

## Deleting an SCM Instance

This section shows you how to delete an SCM instance if it is no longer needed.



**Task**      **To delete an SCM instance, do the following:**

1. If you are not already on the **Version Control Settings** tab, navigate to it.
2. Select the **Instance** tab for the instance you want to delete.
3. Click **Delete Instance**. The selected instance is deleted from the system.

## 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.



**Task**      **To configure a Git 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 Git SCM instance, selecting **Git** from the **Application** dropdown.
2. See [Configuring the Git SCM Instance](#) for a description of the settings used to define a Git SCM instance, or use the inline help provided for each setting on the tab.
3. Once you save the Git SCM instance, test the Code Insight connection with Git SCM instance, as described in [Testing an SCM Instance](#).

## 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

Git SCM Instance Setting	Description
<b>Git Repository URL</b>	<p>Provide the repository URL in either format:</p> <ul style="list-style-type: none"><li>• <code>http(s)://&lt;host.xz&gt;/&lt;path&gt;/to/repo.git</code></li><li>• <code>&lt;user&gt;@&lt;host&gt;:&lt;path&gt;/repo.git</code></li></ul> <p>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:</p> <p><code>&lt;scanroot&gt;/&lt;projectID&gt;/&lt;instanceID&gt;</code></p>
<b>Git Username</b>	<p>Provide the user name for Authenticated access to the repository.</p> <p>Leave this field blank for “anonymous” or SSH access (the system automatically looks for an SSH keypair on the server). See the <i>FlexNet Code Insight Installation and Configuration Guide</i> for instructions on configuring Git over SSH.</p>
<b>Git Password</b>	<p>Enter the password associated with the user name provided.</p>
<b>Git Branch, Git Tag, or Git Commit ID</b>	<p>Specify either the Git branch, tag, or commit ID to identify the source code version to which to synchronize.</p> <p>Alternatively, leave these fields blank to synchronize to the master branch.</p>

## Configuring a Perforce SCM Instance

Flexnet Code Insight provides an SCM connector that enables you to scan a codebase hosted on a Perforce server. To perform the scan, you must first configure a Perforce SCM instance for the Code Insight project. Refer to the following topics for more information:

- [Adding a Perforce SCM Instance to the Code Insight Project](#)
- [Configuring the Perforce SCM Instance](#)

## Adding a Perforce SCM Instance to the Code Insight Project

The following procedure describes how to add a Perforce SCM instance to the Code Insight project.





**Task**

**To configure a Perforce SCM instance, do the following:**

1. Use the instructions in [Adding an SCM Instance to the Code Insight Project](#) to navigate to the **Version Control Settings** tab and add a Perforce SCM instance, selecting **Perforce** from the **Application** dropdown.
2. See [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**

Perforce SCM Instance Setting	Description
<b>URL (P4PORT)</b>	<p>Provide the URL of the Perforce instance with which to synchronize. Note the following example URL formats:</p> <p><b>For a TCP connection</b></p> <pre>tcp:&lt;p4ServerHostID&gt;:&lt;p4Port&gt;</pre> <p><b>For an SSL connection</b></p> <pre>ssl:&lt;p4ServerHostID&gt;:&lt;p4Port&gt;</pre> <p>p4ServerHostID and p4Port identify the hostID (hostname or IP address) and port of the Perforce server</p>
<b>Username (P4USER)</b>	Provide the user name that has access to the Perforce depot to which this instance is synchronizing.
<b>Password (P4PASSWD)</b>	<p>Provide the password associated with the user name provided.</p> <p>If you are using a P4 ticket provided by the Perforce administrator, this field is optional.</p>
<b>Branch Spec (P4CLIENT)</b>	Provide the path to the branch to which this instance is synchronizing.

**Table 7-2 •** Setting Used to Configure a Performer SCM Instance

Perforce SCM Instance Setting	Description
<b>Changelist No</b>	(Optional) Provide a changelist number only if this instance is synchronizing to a particular changelist. Otherwise, this value defaults to the latest revision.
<b>Label</b>	(Optional) Provide a label for the perforce branch.

## 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 Performer 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**

Perforce SCM Instance Setting	Description
<b>TFS URL</b>	<p>Provide the URL of the TFS with which to synchronize. Note the following example URL formats.</p> <p>For the latest version of TFS:</p> <pre>&lt;protocol&gt;:&lt;tfs_host&gt;:&lt;port&gt;/&lt;collection&gt;/&lt;project&gt;</pre> <p>For earlier versions of TFS:</p> <pre>&lt;protocol&gt;:&lt;tfs_host&gt;:&lt;port&gt;/&lt;collection&gt;/&lt;tfsroot&gt;/&lt;project&gt;</pre>
<b>Username</b>	<p>Provide the user name that has access to the TFS collection to which this instance is synchronizing.</p> <p>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 <i>FlexNet Code Insight Installation and Configuration Guide</i>.</p>
<b>Password</b>	<p>Provide the password associated with the user name provided.</p> <p>If you are synchronizing with a VSTS project in TFS, enter the password from the alternate authentication credentials enabled in VSTS.</p>
<b>Changeset</b>	<p>(Optional) Provide a changeset number to which the TFS SCM instance is synchronizing. Otherwise, this value defaults to the latest revision.</p> <p>If a changeset and label are both specified (see the <b>Label</b> description next), the label is ignored, and the instance synchronizes to the changeset.</p>
<b>Label</b>	<p>(Optional) Provide a specific label to which the TFS SCM instance is synchronizing.</p> <p>If a label and changeset (see the previous <b>Changeset</b> description) are both specified, the label is ignored, and the instance synchronizes to the changeset instead.</p>



# 8

## Pages and Panels

Reference information for the following pages and panels in FlexNet Code Insight appears in this section:

- [The FlexNet Code Insight Dashboard](#)
- [Users/Permissions Tab](#)
- [Add User Dialog](#)
- [Edit User Dialog](#)
- [Electronic Updates Tab](#)
- [Email Server Tab](#)
- [LDAP Tab](#)
- [ALM Tab](#)
- [Scan Servers Tab](#)
- [Scan Server Dialog](#)
- [Scan Profiles Tab](#)
- [Create/Edit Scan Profile Dialog](#)
- [Project Defaults Tab](#)
- [Projects List Page](#)
- [Project Summary Tab](#)
- [Edit Project: General Tab](#)
- [Edit Project: Scan Settings Tab](#)
- [Edit Project: Review and Remediation Settings Tab](#)
- [Edit Project Users Dialog](#)
- [Scan History Dialog](#)

- [Select a New Project Owner Dialog](#)
- [Analysis Workbench](#)
- [File Search Results Pane](#)
- [Advanced File Search Dialog](#)
- [Advanced File Search Add Dialog](#)
- [Inventory Details Pane](#)
- [Evidence Details Pane](#)
- [Project Inventory Review Page](#)
- [Policies Page](#)
- [Policy Details Page](#)
- [License Details Dialog](#)
- [Lookup Component Dialog](#)
- [Add Project Dialog](#)
- [Preferences Page](#)
- [Add Token Dialog](#)
- [Edit Token Dialog](#)
- [Advanced Inventory Search Page](#)
- [Import Project Data Dialog](#)

## The FlexNet Code Insight Dashboard

The Dashboard is displayed when you access FlexNet Code Insight. The Dashboard contains the following options:

**Table 8-1** • FlexNet Code Insight Dashboard

Column/Field	Description
<b>analyzed</b>	Displays the number of lines of code that have been analyzed since FlexNet Code Insight was installed.
<b>scanned</b>	Displays the number of lines of code that have been scanned since FlexNet Code Insight was installed.
<b>identified</b>	Displays the number of OSS items that were identified in your codebase.
<b>go to project</b>	Select this option to go to the list of projects that have been created.
<b>view policy</b>	Select this option to view a list of policies that have been created.
<b>administration</b>	Select this option to perform administration tasks related to FlexNet Code Insight.



**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](#)  
[Policies Page](#)  
[Users/Permissions Tab](#)  
[Electronic Updates Tab](#)  
[Email Server Tab](#)  
[LDAP Tab](#)  
[ALM Tab](#)  
[Scan Servers Tab](#)  
[Scan Profiles Tab](#)

## Users/Permissions Tab

The **Users/Permissions** tab on the **Administration** page allows you to add and edit users who can work in FlexNet Code Insight. The tab contains the following columns and fields:

**Table 8-2** • Users tab

Column/Field	Description
<b>Add User</b>	Click to display the <b>Add User</b> dialog.
<b>Manage Permissions</b>	Click to display the <b>Manage Permissions</b> dialog used to assign the following permissions to users: Administrator, Manage Policy, and Create Projects.
<b>Login</b>	Displays the login of each user that has been added.
<b>First Name</b>	Displays the first name of each defined user.
<b>Last Name</b>	Displays the last name of each defined user.
<b>Email</b>	Displays the email address of the user associated with the login.
<b>Actions</b>	This column contains the pencil icon (✎). Click it to open the <b>Edit User</b> dialog, where you can edit information about the selected user.
<b>Enter Search Criteria</b>	Enter a string by which to filter the list of users. A full or partial match to any of the user details is allowed. Click ✕ to remove the filter.

#### See Also

[Add User Dialog](#)  
[Edit User Dialog](#)  
 “Configuring FlexNet Code Insight” in the *FlexNet Code Insight Installation & Configuration Guide*

## 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

Column/Field	Description
<b>Login</b>	Enter the login of the new user.
<b>First Name</b>	Enter the first name of new user.
<b>Last Name</b>	Enter the last name of new user.
<b>Email</b>	Displays the email address of the user associated with the login. To change the user's email address, type over the existing email address.
<b>Password</b>	The current password is not displayed in this field. A user with <i>Administrator</i> permission can type a new password in this field.
<b>Password Confirm</b>	The current password is not displayed in this field. A user with <i>Administrator</i> permission can type a new password in this field.
<b>Question</b>	The prompt that the user must answer to retrieve a forgotten password.
<b>Answer</b>	The answer to the question in the previous field.
<b>Submit</b>	Select <b>Submit</b> to have the system save your user edits. A prompt appears to notify you that your edits have been saved.
<b>Cancel</b>	Select Cancel to return to the Administration Users tab without saving your changes.

**See Also**

[Users/Permissions Tab](#)

## 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

Column/Field	Description
<b>Login</b>	Displays the login of the selected user. This field is read-only and cannot be changed.



Table 8-4 • Edit User dialog (cont.)

Column/Field	Description
<b>First Name</b>	Displays the first name of selected user. To change the user's first name, type over the existing name.
<b>Last Name</b>	Displays the last name of selected user. To change the user's last name, type over the existing name.
<b>Email</b>	Displays the email address of the user associated with the login. To change the user's email address, type over the existing email address.
<b>Password</b>	The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.
<b>Password Confirm</b>	The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.
<b>Question</b>	The prompt that the user must answer to retrieve a forgotten password.
<b>Answer</b>	The answer to the question in the previous field.
<b>Submit</b>	Select <b>Submit</b> to have the system save your user edits. A prompt appears to notify you that your edits have been saved.
<b>Cancel</b>	Select <b>Cancel</b> to return to the Administration Users tab without saving your changes.

**See Also**[Users/Permissions Tab](#)

## Electronic Updates Tab

The **Electronic Updates** tab on the **Administration** page allows you to update the frequency by which to run incremental Electronic Updates automatically. This tab also provides an option to force an incremental or full update outside of the regularly scheduled updates. (For example, you might need to force a full update if the most recent update did not complete properly; or, if you cannot wait for the next scheduled update to determine whether critical vulnerabilities are impacting your product, you can force an incremental update.)



**Note** • Codebase scans cannot be performed during the Electronic Update process, but a scan that is already underway will not be interrupted when an automatic update is scheduled to begin or a forced update is triggered. The Electronic Update will be queued and automatically run based on queue order.

The tab contains the following columns and fields:

**Table 8-5 •** Electronic Updates tab

Column/Field	Description
<b>Electronic Update</b>	
<b>Schedule Update</b>	<p>Use this button to force an incremental or full Electronic Update:</p> <ul style="list-style-type: none"> <li>● <b>Request an incremental update</b>—Click <b>Schedule Update</b> to request an incremental update to obtain any changes since the last update. If Code Insight determines that changes have occurred since the last update, the update is run immediately (or placed in queue if a codebase scan is in progress). If no changes exist, no update is run.</li> <li>● <b>Force a full update</b>—Select the <b>Force Full Electronic Update</b> option and then click <b>Schedule Update</b> to force a full update whether or not changes have occurred since the last update. (If a codebase scan is in progress, the update is placed in queue.) Use this option with caution as the full update requires more overhead than an incremental update.</li> </ul> <p>Note that the regularly scheduled automatic updates are also configured using the <b>Update Frequency</b> fields.</p>
<b>Force Full Electronic Update</b>	<p>Select this option, and then click <b>Schedule Update</b> to force a full update whether or not changes have occurred since the last update. Use this option with caution as the full update requires more overhead than an incremental update.</p>
<b>Update Frequency</b>	
“frequency” dropdown	<p>In the first dropdown, select from one of the available frequencies for running an update automatically:</p> <ul style="list-style-type: none"> <li>● <b>Never</b>—If you select <b>Never</b>, no Electronic Update is run automatically. (When you select this option, the other <b>Update Frequency</b> dropdowns are hidden.) If you need to run an update, you can do so using the <b>Schedule Update</b> button (and the <b>Force Full Electronic</b> option if necessary).</li> <li>● <b>Daily</b>—If you select <b>Daily</b>, choose a clock time from the second, or “time”, dropdown down to indicate at what time of day to run the update.</li> <li>● <b>Weekly</b>—If you select <b>Weekly</b>, choose a clock time from the “time” dropdown and a weekday from the <b>Select a day...</b> dropdown to indicate when to run the weekly update.</li> </ul>
“time” dropdown	<p>If you selected <b>Daily</b> or <b>Weekly</b> from the “frequency” dropdown, this dropdown is made available. From it, select a clock time when you want the Electronic Update to occur.</p>

Table 8-5 • Electronic Updates tab (cont.)

Column/Field	Description
<b>Select a day...</b> dropdown	If you selected <b>Weekly</b> from the “frequency” dropdown, the <b>Select a day...</b> dropdown also becomes available. From it, select the day of the week when the Electronic Update is to occur. (This value works in conjunction with the “time” value to schedule the weekly update.)
<b>Save</b>	Select <b>Save</b> to save your edits to the <b>Update Frequency</b> fields. A prompt appears to notify you that your edits have been saved.

**See Also**

“Configuring FlexNet Code Insight” 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

Column/Field	Description
<b>Enable Email Server</b>	Select <b>Yes</b> to enable FlexNet Code Insight to use the email server or <b>No</b> to leave it disabled. The default is <b>No</b> . The rest of the fields on this page are not available until you select <b>Yes</b> .
<b>Sender’s Email Address</b>	Enter the email address of the sender.
<b>SMTP Host Name</b>	Enter the Simple Mail Transfer Protocol (SMTP) host name.
<b>SMTP Host Port</b>	Enter the port number of the SMTP host.
<b>SMTP User Name</b>	Enter the SMTP user name. This field is optional. Leave it blank if you are using anonymous SMTP.
<b>SMTP User Password</b>	Enter the SMTP user password. This field is optional. Leave it blank if you are using anonymous SMTP.
<b>Enable SMTP over TLS</b>	Select <b>Yes</b> to use Transport Layer Security (TLS) to secure email over SMTP or select <b>No</b> to leave this option disabled.


## 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

Column/Field	Description
<b>Enable LDAP</b>	Select <b>Yes</b> or <b>No</b> to determine if LDAP will be used for user authentication. The default is <b>No</b> .
<b>LDAP Connection Details</b>	
<b>LDAP URL</b>	Specify the URL of your LDAP server. The following is an example LDAP server URL: <code>ldap://&lt;ldap_server_host&gt;:&lt;ldap_port&gt; ldap://ad.mycompany.com:389</code>
<b>Authentication Type</b>	Select the type of LDAP authentication that will be used: <ul style="list-style-type: none"><li>● <b>Anonymous</b>—If you select this option, the <b>LDAP Username</b> and <b>LDAP Password</b> fields in this section remain disabled.</li><li>● <b>Authenticated</b>—If you select this option, the following LDAP fields are enabled.</li></ul>
<b>LDAP Username</b>	Enter the LDAP username 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.
<b>LDAP Password</b>	Enter the password for the username specified in the field above. This field is disabled if anonymous authentication is selected.
<b>LDAP Query Details</b>	
<b>LDAP Base</b>	Specify the base node of the LDAP server.
<b>LDAP Search Base</b>	Specify the Search Base, which, along with the Search Query, is used to query a list of users for synchronizing with FlexNet Code Insight.
<b>LDAP Search Query</b>	Specify the search query for your LDAP server. The following is an example search query: <code>(&amp;(objectClass=person)(memberOf=CN=SCAGroup,CN=Users,DC=ad,DC=mycompany,DC=com))</code>
<b>Use Paging</b>	Select <b>Yes</b> if the LDAP server has paging enabled. Select <b>No</b> if the server does not have paging enabled. If you select <b>Yes</b> , the <b>LDAP Page Size</b> field is enabled.
<b>LDAP Page Size</b>	Indicate the page size. The default page size is 1000 elements.

Table 8-7 • LDAP tab (cont.)

Column/Field	Description
<b>LDAP User Sync Frequency</b>	<p>Specify the frequency at which FlexNet Code Insight will synchronize user data with the LDAP server:</p> <ul style="list-style-type: none"> <li>● <b>Never</b>—Select this option to disable the automatic user sync. A user sync will occur only if the user clicks the <b>Sync Now</b> button. For all other values, automatic user sync is enabled per the configured frequency. (This is the default value.)</li> <li>● <b>Hourly</b>—Enter an integer value representing the number of hours between user syncs.</li> <li>● <b>Daily</b>—Select a time at which the user sync will run every day.</li> <li>● <b>Weekly</b>—Select a day of the week and a time of the day when the user sync will run each week.</li> </ul>
<b>Search Sub-tree</b>	Select this checkbox to enable deep searches through the subtree of the path defined by <b>LDAP Base</b> + <b>LDAP Search Base</b> . Note that, while helpful in locating users in certain cases, a deep search can negatively affect performance (and therefore, by default, is not enabled).
<b>LDAP User Property Mappings</b>	
<b>Login</b>	Enter the LDAP user property field representing the user's login.
<b>First Name</b>	Enter the LDAP user property field representing the user's first name.
<b>Last Name</b>	Enter the LDAP user property field representing the user's last name.
<b>Email</b>	Enter the LDAP user property field representing the user's email address.
<b>Login Filter</b>	Specify a filter that will limit the user search performed in the search base location. For example, you could specify (uid={0}, which, when used with the LDAP Search Base and LDAP Search Query specified above, will search for an entry where the uid is equal to the user name.
<b>[actions]</b>	
<b>Save</b>	Click this button to save any changes you made to the fields on the <b>LDAP</b> tab.
<b>Test LDAP Server Connection</b>	Click this button to test the connection to the LDAP server.
<b>Sync Now</b>	Click this button to force a user sync.
	 <p><b>Note</b> • This button is disabled if a user sync is currently running.</p>

# ALM Tab

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




Column/Field	Description
<b>Application</b>	Name of the ALM application for which to add an instance.
<b>Add Instance</b>	Click to open a new <b>Instance</b> tab to configure an instance to point to a server in the ALM system.
<b>Existing Issues Sync Frequency</b>	<p>Click the  to the right of this field, and select the synchronization frequency that will apply to <i>all</i> the configured ALM instances. (The default value is <b>Hourly</b> repeated every <b>1</b> hour.)</p> <ul style="list-style-type: none"><li>● <b>Never</b></li><li>● <b>Hourly</b> (enter number of hours)</li><li>● <b>Daily</b> (enter time of day)</li><li>● <b>Weekly</b> (enter day of the week and time of day)</li></ul> <p>Click  to accept the updated synchronization frequency or  to restore the previous frequency.</p>
<b>Test Connection</b>	Click to validate that Code Insight can connect to the current instance based on the supplied <b>ALM_type Instance Name</b> , <b>ALM_type Server URL</b> , <b>ALM_type Username</b> , and <b>ALM_type Password</b> .
<b>Delete Instance</b>	Click to delete the current ALM instance after verifying that no project references to this instance exist.
<b>ALM_type Instance Name</b>	Unique name of the ALM instance.
<b>ALM_type Server URL</b>	URL of the ALM server to which to connect in the format <code>http(s):&lt;server_name_or_ip&gt;</code> .
<b>ALM_type Username</b> <b>ALM_type Password</b>	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.
<b>Default Project Key</b>	Key for the project for which issues will be created on the ALM server.
<b>Default Issue Type</b>	The default issue type created on the ALM server.
<b>Default Priority</b>	Default priority of the issued created on the ALM server.

Table 8-8 • ALM tab (cont.)

Column/Field	Description
<b>Default Summary Text</b>	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.
<b>Default Description</b>	Default text to display as a description for the issue on the ALM server. The text supports the following Code Insight variables: \$PROJECT_NAME, \$INVENTORY_ITEM_NAME, \$COMPONENT_NAME, \$VERSION_NAME, \$LICENSE_NAME, \$NUMBER_VULNERABILITIES, \$NUMBER_FILES, or \$INVENTORY_URL.

## Scan Servers Tab

The **Scan Servers** tab on the **Administration** page allows you to edit information about your scan server. The tab contains the following columns and fields:

Table 8-9 • Scan Servers tab

Column/Field	Description
<b>Scan Servers</b>	The name of your scan server.
<b>Edit</b>	Select this button to edit the server configuration for the scanner you selected in the Scan Servers field.
<b>New</b>	Select this button to create a new scanner.

### See Also

[Scan Server Dialog](#)

## Scan Server Dialog

The **Scan Server** dialog is where you can edit information about your scan server. The dialog contains the following columns and fields:

Table 8-10 • Scan Server dialog

Column/Field	Description
<b>Alias</b>	The name of your scan server.
<b>Host</b>	The IP address of your scan server host computer. If the scan server is on the same machine as the core server, enter <b>localhost</b> .
<b>Port</b>	The number of your scan server host port. By default, the port is 8888.

**Table 8-10 •** Scan Server dialog (cont.)

Column/Field	Description
<b>CL Path</b>	<p>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 scanner 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.</p> <p>Alternatively, you can 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 <i>FlexNet Code Insight Installation and Configuration Guide</i>. 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.</p> <p>For additional information, see the following:</p> <ul style="list-style-type: none"> <li>• “Managing Scan Profiles” in the <i>FlexNet Code Insight Installation and Configuration Guide</i> for more information about the “Basic Scan Profile (without CL)” and about creating and managing scan profiles in general.</li> <li>• <a href="#">Applying a Scan Profile</a> in the “Using FlexNet Code Insight” chapter in this book for instructions on associating a scan profile with a project.</li> <li>• <a href="#">What Is a FlexNet Code Insight Scan?</a> in the “Using FlexNet Code Insight” chapter in this book for information about Code Insight scans in general.</li> </ul>
<b>Codebase Path</b>	The directory on the scan server where FlexNet Code Insight will store and manage all uploaded code. You should have adequate disk space to store the codebases. The recommended starting size for this directory is 500GB.
<b>Save</b>	Click this button to save any changes you made to the fields on the Scan Server dialog.
<b>Cancel</b>	Click this button to cancel any changes you made to the fields on the Scan Server dialog.

**See Also**

[Scan Servers Tab](#)


[What Is a FlexNet Code Insight Scan?](#)



# Scan Profiles Tab

The **Scan Profiles** tab on the **Administration** page allows you to add a scan profile and edit information about an existing scan profile. The tab contains the following columns and fields:

**Table 8-11** • Scan Profiles tab

Column/Field	Description
<b>Scan Profiles</b> list	<p>A list (in grid format) of available scan profiles. The following are the predefined scan profiles:</p> <ul style="list-style-type: none"><li>● Standard Scan Profile</li><li>● Basic Scan Profile (without CL)</li><li>● Comprehensive Scan Profile</li></ul> <p>The list will contain additional profiles if you have added them.</p> <p>The following are key attributes shown for each scan profile in the list. These attributes are described in detail in <a href="#">Create/Edit Scan Profile Dialog</a>.</p> <ul style="list-style-type: none"><li>● <b>Scan Archives</b>—Whether the scanner will perform package discovery and license detection within all archive files in the project codebase.</li><li>● <b>Dependencies</b>—The level of component-dependency scanning to be performed by the scanner.</li><li>● <b>Exact Matches</b>—Whether scanner is to identify those codebase files that exactly match file information in the CL (Compliance Library).</li><li>● <b>Source Code Matches</b>—Whether the scanner is to identify code strings in the scanned codebase files that exactly match strings in the CL (Compliance Library).</li><li>● <b>Edit icon</b>—Click  at the end of a scan profile entry to edit the profile. The <b>Create</b> (or <b>Edit</b>) <b>Scan Profile</b> dialog is opened, showing the scan profile details.</li></ul>
<b>Add Scan Profile</b> button	Select this button to create a new scan profile.

## 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

Field	Description
<b>Perform Package/License Discovery in Archives</b>	Select this option to have the scanner recursively perform package discovery and license detection within all archive files encountered in the project codebase. By default, this option is selected.
<b>Dependency Support</b>	<p>Determine the level of dependency scanning to be performed by the scanner. The available options include:</p> <ul style="list-style-type: none"><li>• <b>No Dependencies</b>: Only top-level inventory items are reported without any dependencies. (Default)</li><li>• <b>Only First Level Dependencies</b>: Only first-level (or direct) dependencies are reported along with top-level inventory items.</li><li>• <b>All Transitive Dependencies</b>: All first-level and transitive dependencies are reported along with top-level inventory items. The scanner calls out to the relevant package management repository to obtain transitive dependency information.</li></ul> <p>For a description of Code Insight dependency support for supported ecosystems, see the <a href="#">Automated Analysis</a> chapter.</p>
<b>Automatically Add Related Files to Inventory</b>	Select this option to have the system associate additional files to existing inventory items based on the data available in automatic detection rules.
<b>Exact Matches</b>	Select this option to have the scanner record exact matches for scanned files based on data from the Compliance Library (CL).
<b>Source Code Matches</b>	Select this option to have the scanner record source code matches for scanned files based on data from the Compliance Library (CL).
<b>Include System Identified Files</b>	(Available only when <b>Source Code Matches</b> is selected) Select this option if you want the scanner to perform source-code matching for files that have already been associated with one or more inventory items through automated analysis.
<b>Include Files with Exact Matches</b>	(Available only when <b>Source Code Matches</b> is selected) Select this option if you want the scanner to perform source-code matching for files that have already been identified as having exact matches.
<b>Search Terms</b>	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.
<b>Scan Exclusions</b>	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.

### See Also

[Scan Profiles Tab](#)

[What Is a FlexNet Code Insight Scan?](#)

[Applying a Scan Profile to the Project](#)

## Project Defaults Tab

The settings on **Project Defaults** tab on the **Administration** page work in conjunction with a project's policies to configure the automation of review, remediation, and status notification processes for published inventory. These settings, which are global across all projects but can be overridden at the project level, are used to set up the following:

- Automatic creation of manual review tasks for inventory items not reviewed by policy during the publication performed as part of a scan. The tasks are automatically assigned to a default legal or security contact (defined at the project level, as described in [Edit Project: Review and Remediation Settings Tab](#)).
- 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 a default engineering contact (defined at the project level, as described in [Edit Project: Review and Remediation Settings Tab](#)).
- 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.

See the following field descriptions for more information.

**Table 8-13** • Project Defaults tab

Section/Field	Description
<b>Automated Review Options</b>	

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



Section/Field	Description
<b>automatically reject inventory items impacted by a new vulnerability that violates your policy</b>	<p>Determine what action the system should take for published inventory affected by a new security vulnerability discovered during a post-publication scan or Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the <b>Project Inventory</b> tab.</p> <ul style="list-style-type: none"> <li>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 <i>greater than</i> 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.</li> </ul> <p>If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.</p> <ul style="list-style-type: none"> <li>Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability.</li> </ul> <p>For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see <a href="#">Policies Page</a> and <a href="#">Policy Details Page</a>. For information about associating these policies with a project, see <a href="#">Managing Policy Profiles</a>.</p>
<b>Manual Review Options</b>	
<b>What should happen if inventory items are not reviewed by policy?</b>	<p>Determine what action should be triggered for those inventory items that are <i>not</i> affected by policy (and therefore have a <b>Not Reviewed</b> status) during the publication of inventory either as part of a scan or manually by a user:</p> <ul style="list-style-type: none"> <li><b>do nothing</b>—Simply show the status of the inventory item as <b>Not Reviewed</b> on the <b>Project Inventory</b> tab.</li> <li><b>send an email notification to the project owner</b>—Automatically send an email to the project owner, stating the need for a manual review of the item. The value for <b>Select the minimum priority...</b> (described in the next table entry) affects this option.</li> <li><b>automatically create a manual review task</b>—Automatically create a manual review task assigned to the default legal or security reviewer, and send an email, notifying the reviewer about assigned task. (Default reviewers are defined at the project level on the <b>Edit Project</b> dialog, as described in <a href="#">Edit Project: Review and Remediation Settings Tab</a>.)</li> </ul> <p>Information about managing such a task to track the progress of a manual review is found in <a href="#">Creating and Managing Tasks for Project Inventory</a> in the “Using FlexNet Code Insight” chapter.)</p> <p>The value for <b>Select the minimum priority...</b> (described in the next table entry) affects this option.</p>

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

Section/Field	Description
<b>Select the minimum priority to perform the action selected above</b>	<p>(Enabled when an option other than <b>do nothing</b> is selected for the previous field.)</p> <p>Select the minimum inventory priority (<b>P1</b>, <b>P2</b>, <b>P3</b>, or <b>P4</b>) to which the value for the previous field applies.</p> <p>For example, if the previous field is set to <b>send an email notification to the project owner</b> and minimum priority is set to <b>P3</b>, 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.</p>  <p><b>Note</b> • This option has no effect on the <b>do nothing</b> value.</p>
<b>What should happen if inventory items are rejected?</b>	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>do nothing</b>—Simply show the status of the inventory item as Reject on the Project Inventory tab.</li> <li>● <b>send an email notification to the project owner</b>—Automatically send an email to the project owner, stating the need for remediation work on the inventory item.</li> <li>● <b>automatically create a remediation task</b>—Automatically create a remediation task assigned to the default development contact (for example, an engineering manager), and send an email, notifying the contact about the assigned task. (The default development contact is defined at the project level on the <b>Edit Project</b> dialog, as described in <a href="#">Edit Project: Review and Remediation Settings Tab</a>.)</li> <li>● <b>automatically create a remediation task and an external work item</b>—Automatically do the following: <ul style="list-style-type: none"> <li>● Create a remediation task assigned to the default development contact (for example, an engineering manager), and send an email, notifying the contact about the assigned task. (See the previous bulleted item for more information.)</li> <li>● 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 <a href="#">ALM Settings</a> in the “Using FlexNet Code Insight” chapter.</li> </ul> </li> </ul>

- See Also**
- [Policies Page](#)
  - [Policy Details Page](#)
  - [Edit Project: Review and Remediation Settings Tab](#)
  - [Managing Policy Profiles](#)
  - [Creating Inventory from the Project Inventory Tab](#)
  - [Creating and Viewing External Work Items for a Project Inventory Task](#)
  - [ALM Settings](#)

# 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 8-14 • Projects List page




Column/Field	Description
<b>Tree view</b> 	Click to change the display to a tree view.
<b>List view</b> 	Click to change the display to a list view.
<b>Add New</b>	Click to add a new folder or project to the list. (This button is displayed only if you have permission to create projects.)
<b>My Projects</b>	Click to show only those projects with which you are associated, either as Project Owner or with a project role (Analyst, Reviewer, or Observer).
<b>Projects (x)</b>	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)”).

Table 8-14 • Projects List page (cont.)

Column/Field	Description
<b>Project Search fields</b>	<p>From the search filters on the left, select the filter based on the type of search you want to perform (<b>Project Name</b>, <b>Project Inventory</b>, or <b>Security Vulnerability</b>).</p> <p>In the field on the right, enter the string criterion for the search:</p> <ul style="list-style-type: none"><li>• When searching for a project name, enter a partial string or full project name.</li><li>• 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.</li><li>• When searching for a security vulnerability, enter the exact vulnerability ID.</li></ul> <p>Press Enter to view the filtered list. If no inventory items meet the specified criterion, the <b>Projects</b> list shows “No Projects”.</p> <p>To clear the search filter and restore the full project list, click  in the criterion field.</p> <p>See for <a href="#">Searching the System</a> for full details.</p>
<b>Name</b>	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 <b>Summary</b> tab. Click the arrow to toggle the list from A to Z or from Z to A.
<b>Selected Project Name</b>	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.
<b>Owner</b>	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.
<b>Profile</b>	Displays the name of the profile attached to the selected project. If no profile is attached to the project, “No profile selected” appears.
<b>Created</b>	Displays the data that the project was created.
<b>Last Scan</b>	Displays the date that the codebase was last scanned.
<b>Project Summary Graphs</b>	The panes in this panel display overview information about the files and inventory associated with the selected project. The graphs do not appear unless you select a project from the project list.

**See Also**

[Creating a Project](#)  
[Project Summary Tab](#)  
[Using the Project Dashboard](#)  
[Searching the System](#)

# 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 8-15 • Project Summary tab**

Column/Field	Description
<b>Project Details</b>	
<b>Name</b>	The name given to the selected project and its Id number.
<b>Owner</b>	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.
<b>Legal Contact</b>	<p>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.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See <a href="#">Updating Inventory Review and Remediation Settings for a Project</a> for details.</p>
<b>Security Contact</b>	<p>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.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See <a href="#">Updating Inventory Review and Remediation Settings for a Project</a> for details.</p>
<b>Developer Contact</b>	<p>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.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See <a href="#">Updating Inventory Review and Remediation Settings for a Project</a> for details.</p>
<b>Description</b>	A description, if entered, of the project appears in this field.
<b>Project Type</b>	<p>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:</p> <ul style="list-style-type: none"><li>● <b>Inventory Only:</b> processes all published inventory, with inventory details, fields and file associations.</li><li>● <b>Standard:</b> processes all inventory, with inventory details, fields and file associations, as well as all files that are marked as reviewed.</li></ul>



Table 8-15 • Project Summary tab

Column/Field	Description
<b>Project Visibility</b>	<p>The visibility of the project:</p> <ul style="list-style-type: none"> <li>● <b>Public:</b> All users in the system can view and change the project.</li> <li>● <b>Private:</b> Sensitive information is hidden from general view, and only select users can view the project.</li> </ul>
<b>Project Risk</b>	<p>The project vulnerability risk value:</p> <ul style="list-style-type: none"> <li>● Low</li> <li>● Medium</li> <li>● High</li> </ul>
<b>Scan Settings</b>	
<b>Policy Profile</b>	The name of the profile attached to this project.
<b>Scan Profile</b>	The name of the scan profile associated with this project. Click ⓘ to view the details of the scan profile.
<b>Scan Paths</b>	The location of your codebase. Click ⓘ to view the details about the scan server.
<b>Scan Status</b>	
<b>Scan Status</b>	Notifies you of scheduled scans. Click the hyperlinked <b>here</b> to schedule a scan. If other events are scheduled, the scan is placed in a queue. Otherwise, it is run immediately.
<b>Last Scan</b>	Displays the date that the codebase was last scanned.
<b>Past Scans</b>	Click the hyperlinked <b>here</b> 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 been performed, the list will be empty.
<b>Reports</b>	
<b>Audit Report</b>	Displays the status of the audit report. If a report is not available, click <b>Generate Audit Report</b> to create one.
<b>Notices Report</b>	Displays the status of the notices report. If a report is not available, click <b>Generate Notices Report</b> to create one.
<b>Start Scan</b>	Click to immediately scan your codebase.
<b>Generate Report</b>	Click to generate a Project, Audit, or Notices report in the background to display later.

Table 8-15 • Project Summary tab

Column/Field	Description
<b>Upload Project Codebase</b>	Click to add or change the codebase that will be scanned for the selected project.
<b>Manage Project</b>	<p>A dropdown menu that allows you to perform actions on the selected project:</p> <ul style="list-style-type: none"><li>• Edit Project</li><li>• Edit Project Users</li><li>• Export Project Data</li><li>• Delete Project</li><li>• Change Owner</li></ul>

**See Also**[Creating a Project](#)[Projects List Page](#)

## 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 8-16 • Edit Project: General tab

Column/Field	Description
<b>Project Name</b>	The name of the selected project. You can change the name by typing over the current project name.
<b>Description</b>	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.
<b>Project Visibility</b>	The option defining whether the project is defined as public or private. When private, only project owner can upload the codebase, run scans, manage scan results, and manage the project in general.
<b>Project Risk</b>	The current vulnerability risk value (Low, Medium, or High) for the project. To edit, select another value from the dropdown.
<b>Project Folder</b>	<p>The folder in the <b>Projects</b> list under which the project is currently grouped. To edit the project location in the list, select one of the following:</p> <ul style="list-style-type: none"><li>• <b>Clear Project Folder button</b>—Click this button to remove the project from the current folder in the <b>Projects</b> list and place it in the root folder.</li><li>• <b>Select a New Folder dropdown</b>—Click the down arrow to locate and select an available folder to which to move the project.</li></ul>

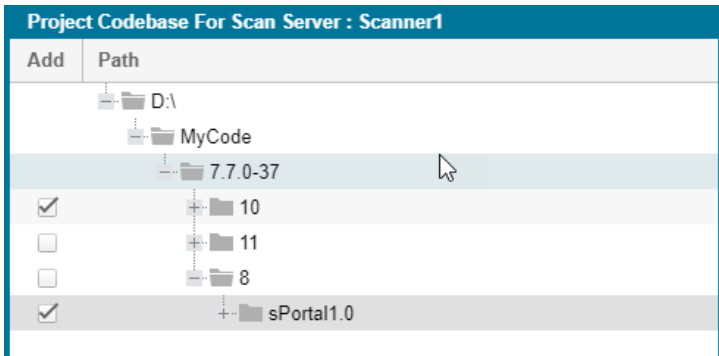
# Edit Project: Scan Settings Tab

The **Edit Project: Scan Settings** tab on the **Edit Project** dialog displays information about the scan settings defined for the selected project. You can edit this information on this tab. The tab contains the following fields:

**Table 8-17** • Edit Project: Scan Settings tab

Column/Field	Description
<b>Scan Profile</b>	The name of the scan profile associated with the selected project. You can pick a different scan profile from the dropdown list.
<b>Scan Server</b>	The name of your scan server.
<b>Auto-Publish</b>	
<b>Automatically publish system-created inventory items</b>	Select to automatically publish those inventory items that are system-created based on internal system policies. If you select this option, the <b>Mark associated files as reviewed</b> and <b>Minimum inventory confidence label</b> are enabled.
<b>Mark associated files as reviewed</b>	Select to automatically mark the files associated with each auto-published inventory item as “reviewed”.
<b>Minimum confidence level</b>	<p>Select the minimum Confidence level for the system-generated inventory items you want to auto-publish:</p> <ul style="list-style-type: none"> <li>● <b>Low</b>—Auto-publish all inventory.</li> <li>● <b>Medium</b>—Auto-publish only inventory items with Medium and High confidence levels.</li> <li>● <b>High</b>—Auto-publish only inventory items with Medium and High confidence levels.</li> </ul> <p>For a description of the Confidence levels and how they are used, see <a href="#">Inventory Confidence</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Project Codebase for Scan Server</b>	

**Table 8-17 •** Edit Project: Scan Settings tab (cont.)

Column/Field	Description
<b>Path</b>	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, or drill down in the tree to locate and select specific subdirectories.
	
<b>Selected Paths</b>	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 <b>X</b> next to the directory in this pane.
<b>Save</b>	Click this button to save your edits to the scan settings.
<b>Cancel</b>	Click this button to return to the <b>Summary</b> tab without saving your edits.

## 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. 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.

See the following field descriptions for more information.

**Table 8-18 •** Edit Project: Review and Remediation Settings tab



Section/Field	Description
<b>Automated Review Options</b>	
<b>Select your policy profile</b>	<p>Select policy profile you want to associate with your project. (By default, <b>Default Policy Profile</b> is selected.)</p> <p>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). To view the policies defined in the selected policy profile, click the down arrow next to <b>View Policy Details</b>.</p> <p>For more information about policy profiles in general, see <a href="#">Managing Policy Profiles</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>automatically reject inventory items impacted by a new vulnerability that violates your policy</b>	<p>Determine what action the system should take for published inventory affected by a new security vulnerability discovered during a post-publication scan or Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the <b>Project Inventory</b> tab.</p> <ul style="list-style-type: none"> <li>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 <i>greater than</i> 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.</li> </ul> <p>If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.</p> <ul style="list-style-type: none"> <li>Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability.</li> </ul> <p>For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see <a href="#">Policies Page</a> and <a href="#">Policy Details Page</a>. For information about associating these policies with a project, see <a href="#">Managing Policy Profiles</a>.</p>
<b>Manual Review Options</b>	

Table 8-18 • Edit Project: Review and Remediation Settings tab (cont.)

Section/Field	Description
<b>What should happen if inventory items are not reviewed by policy?</b>	<p>Determine what action should be triggered for those inventory items that are <i>not</i> affected by policy (and therefore have a <b>Not Reviewed</b> status) during the publication of inventory either as part of a scan or manually by a user:</p> <ul style="list-style-type: none"> <li>● <b>do nothing</b>—Simply show the status of the inventory item as <b>Not Reviewed</b> on the <b>Project Inventory</b> tab.</li> <li>● <b>send an email notification to the project owner</b>—Automatically send an email to the project owner, stating the need for a manual review of the item. The value for <b>Select the minimum priority...</b> (described in the next table entry) affects this option.</li> <li>● <b>automatically create a manual review task</b>—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 <a href="#">Creating Inventory from the Project Inventory Tab</a> in the “Using FlexNet Code Insight” chapter.) The value for <b>Select the minimum priority...</b> (described in the next table entry) affects this option.</li> </ul>
<b>Select the minimum priority to perform the action selected above</b>	<p>(Enabled when an option other than <b>do nothing</b> is selected for the previous field.)</p> <p>Select the minimum inventory priority (<b>P1</b>, <b>P2</b>, <b>P3</b>, or <b>P4</b>) to which the value for the previous field applies.</p> <p>For example, if the previous field is set to <b>send an email notification to the project owner</b> and minimum priority is set to <b>P3</b>, 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.</p> <p></p> <p><b>Note</b> • This option has no effect on the <b>do nothing</b> value.</p>

**Table 8-18 •** Edit Project: Review and Remediation Settings tab (cont.)

Section/Field	Description
<b>What type of manual reviews will be performed on this project?</b>	<p>Determine the type of manual review tasks to be generated:</p> <ul style="list-style-type: none"> <li>● <b>Legal Only</b>—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.</li> <li>● <b>Security Only</b>—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.</li> <li>● <b>both Legal and Security</b>—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.</li> </ul> <p>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.</p>
<b>Select reviewers for this project</b>	<p>Designate a new default Legal reviewer or Security reviewer as needed to which to assign the generated manual review tasks. (By default, the project owner is designated as both reviewers.)</p> <p>Then, depending on the type of manual reviews selected for the project (see the <b>What type of manual reviews will be performed...</b> option described previously), Code Insight determines to which reviewer to assign the task and notify by email. The reviewer can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see <a href="#">Creating and Managing Tasks for Project Inventory</a> in the “Using FlexNet Code Insight” chapter.</p> <p>To select a new reviewer, click <b>Change User</b> next to the name of the current <b>Legal reviewer</b> or <b>Security reviewer</b> assignee, select a user from the <b>Select new...contact</b> dialog, and click <b>Apply</b>.</p> <p>The selected user is automatically given the role of project “reviewer” if the user is not already assigned this role. However, if the default reviewer then reassigns the task to another user, the “reviewer” role is not automatically assigned to that user if the user does not already have that role.</p>

Table 8-18 • Edit Project: Review and Remediation Settings tab (cont.)

Section/Field	Description
<b>What should happen if inventory items are rejected?</b>	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>do nothing</b>—Simply show the status of the inventory item as Reject on the Project Inventory tab.</li> <li>● <b>send an email notification to the project owner</b>—Automatically send an email to the project owner, stating the need for remediation work on the inventory item.</li> <li>● <b>automatically create a remediation task</b>—Automatically create a remediation task assigned to the default development contact (for example, an engineering manager), 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 <a href="#">Creating and Managing Tasks for Project Inventory</a> in the “Using FlexNet Code Insight” chapter.)</li> <li>● <b>automatically create a remediation task and an external work item</b>—Automatically do the following: <ul style="list-style-type: none"> <li>● Create a remediation task assigned to the default development contact (for example, an engineering manager), 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 <a href="#">Creating and Managing Tasks for Project Inventory</a> in the “Using FlexNet Code Insight” chapter.)</li> <li>● 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 <a href="#">ALM Settings</a> in the “Using FlexNet Code Insight” chapter.</li> </ul> </li> </ul>
<b>Assignee for remediation work</b>	<p>If needed, designate a new default development contact to which to assign the generated remediation tasks. (By default, the project owner is the designated contact.)</p> <p>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 <a href="#">Creating and Managing Tasks for Project Inventory</a> in the “Using FlexNet Code Insight” chapter.</p> <p>To select a new contact, click <b>Change User</b> next to the name of the current assignee, select a user from the <b>Select new...contact</b> dialog, and click <b>Apply</b>.</p>



### See also

[Policies Page](#)  
[Policy Details Page](#)  
[Project Defaults Tab](#)  
[Managing Policy Profiles](#)  
[Creating Inventory from the Project Inventory Tab](#)  
[Creating and Viewing External Work Items for a Project Inventory Task](#)  
[ALM Settings](#)

## Edit Project Users Dialog

The **Edit Project Users** dialog displays a list of defined project users. On this dialog, you can edit the project permissions for existing project users.



**Note** • User permissions are not mutually exclusive. A user can have analyst, reviewer and observer permissions or any combination of permissions.

The dialog contains the following fields:

**Table 8-19** • Edit Project Users dialog

Column/Field	Description
<b>Select Users</b>	
<b>Add User</b>	Click this button to assign the selected user the Analyst and/or Reviewer permission.
<b>Search</b>	Enter a full or partial user name to search for a user in the system.
<b>User List</b>	Lists all the currently defined FlexNet Code Insight users.
<b>Analysts</b>	Displays the names of the users who have analyst permission. You can drag and drop users from the <b>User</b> list into this list.
<b>Reviewers</b>	Displays the names of the users who have reviewer permission. You can drag and drop users from the User list into this list.
<b>Observers</b>	Displays the names of the users who have observer permission. You can drag and drop users from the <b>User</b> list into this list.
 <b>Note</b> • The <b>Observers</b> list is only visible for private projects. For more information, see <a href="#">Creating a Private Project</a> .	


### See Also

[Searching Published Inventory](#)

## 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 8-20** • Scan History dialog

Column/Field	Description
	Click to view messages about the scan. If no messages were generated during the scan, the message field will be blank.
<b>Scheduled On</b>	The date and time that the scan was scheduled.
<b>Started On</b>	The date and time that the scan was started.
<b>Completed On</b>	The date and time that the scan completed.
<b>Duration</b>	The amount of time the scan took.
<b>Scheduled By</b>	The user name of the person who scheduled the scan.
<b>Status</b>	The status of the scan: <i>Completed</i> or <i>Failed</i> .
<b>Ok</b>	Click <b>Ok</b> to exit the <b>Scan History</b> dialog and return to the <b>Scan Summary</b> page.

**See Also**

[Analyzing \(Auditing\) Scan Results](#)

## Select a New Project Owner Dialog

The **Select a New Project Owner** dialog is where you can change the owner of a selected project. The dialog contains the following fields:

**Table 8-21** • Select a New Project Owner dialog

Column/Field	Description
<b>List of Users</b>	The names of all the users in the system are listed in this field. Highlight a name and click <b>Apply</b> to change the project's owner.
<b>Apply</b>	Click this button to assign the selected owner to the project.
<b>Cancel</b>	Click this button to cancel changes without saving.

# 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 8-22** • Analysis Workbench

Column/Field	Description
<b>Legend</b>	<p>A color-coded and hyperlinked guide to the files and inventory in your scanned codebase:</p> <ul style="list-style-type: none"><li>● <b>New Evidence</b>: 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 <b>Files Search Results</b> pane.</li><li>● <b>Reviewed</b>: Click this link to display files in the <b>File Search Results</b> pane that have been reviewed.</li><li>● <b>Exact</b>: Click this link to display files in the <b>File Search Results</b> pane that are exact matches.</li><li>● <b>Copyrights</b>: Click this link to display files in the <b>File Search Results</b> pane that contain copyrighted code.</li><li>● <b>Email/URLS</b>: Click this link to display files in the <b>File Search Results</b> pane that contain email addresses and URLs.</li><li>● <b>Licenses</b>: Click this link to display files in the <b>File Search Results</b> pane that contain licenses.</li><li>● <b>Search Terms</b>: Click this link to display files in the <b>File Search Results</b> pane that match default search terms.</li><li>● <b>Source</b>: Click this link to display files in the <b>File Search Results</b> pane that match</li></ul>
<b>Codebase Files Panel</b>	
<b>Enter Path</b>	<p>To display codebase files in the <b>Analysis Workbench</b>, 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.</p>
<b>Path/Folder/File Tree</b>	<p>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.</p>
<b>File Details</b>	

Table 8-22 • Analysis Workbench (cont.)

Column/Field	Description
<b>Copyrights</b>	Lists the copyright holders found in the selected file.
<b>Emails/URLs</b>	Lists the emails and URLs found in the selected file.
<b>Licenses</b>	Lists the licenses found in the selected file.
<b>Search Terms</b>	Lists the search terms that were found in the selected file.
<b>Inventory Items (x)</b>	
<b>Current View</b>	Lists what portion of the project inventory that is being displayed.
<b>Quick Filters</b>	Provides options to quickly filter the inventory items listed: <ul style="list-style-type: none"><li>● Published (x)</li><li>● Not Published (x)</li></ul>
<b>Clear Filter</b>	Clears any search terms that have been entered.
<b>Search</b>	Enter terms to search for in the inventory.
<b>Add New</b>	Click to create a new inventory item on the <b>New Inventory Item</b> tab.
<b>Publish</b>	Highlight an inventory item from the list and click <b>Publish</b> to publish the item.
<b>Recall</b>	Click to recall (remove) a published inventory item from <b>Inventory Items</b> list if it does not fit the criteria for inclusion.
<b>Delete</b>	Highlight an inventory item from the list and click <b>Delete</b> to delete the item from inventory.

**See Also**

[Reviewing Published Inventory](#)


## File Search Results Pane

The **File Search Results** pane displays the results of your file search. The **File Search Results** pane has the following fields.



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


Table 8-23 • File Search Results pane

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

## 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 • Advanced File Search dialog

Column/Field	Description
<b>Add New</b>	Click this button to access the <b>Advanced File Search Add</b> dialog.
<b>Name</b>	The name of the search. For example, <i>Files not in inventory</i> .
<b>Description</b>	A short description of the search. For example, <i>Files not associated with inventory items</i> .
	Click to delete a search.
<b>Search</b>	Click to execute the selected search.
<b>Close</b>	Click to close the Search Files dialog without searching.

## 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 8-25** • Advanced File Search Add dialog

Column/Field	Description
<b>Name</b>	The name of the search. For example, <i>Files not in inventory</i> .
<b>Description</b>	A short description of the search. For example, <i>Files not associated with inventory items</i> .
<b>Criteria</b>	
<b>Add Criteria</b>	Click the dropdown menu and select search criteria. To add more criteria, click <b>Add Criteria</b> 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.
<b>Add Criteria Group</b>	Click to add a group of criteria.
<b>Save</b>	Click to save the new search.
<b>Save and Search</b>	Click to execute the new search without saving the search for future use.
<b>Search without saving</b>	Click to execute the new search without saving the search for future use.
<b>Cancel</b>	Click to close the <b>Search Files</b> dialog without searching.

## 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 8-26** • Inventory Details pane

Column/Field	Description
<b>Recall</b>	Click to recall (remove) a published inventory item from <b>Inventory Items</b> list if it does not fit the criteria for inclusion. The selected items are removed from the <b>Project Inventory</b> view and are only visible in the <b>Analysis Workbench</b> .
<b>Save</b>	Click to save any changes you have made to the inventory details.
<b>Close</b>	Click to close the <b>Inventory Details</b> pane without saving changes.

Table 8-26 • Inventory Details pane (cont.)

Column/Field	Description
<b>Review Status</b>	<p>The status of the inventory item:</p> <ul style="list-style-type: none"><li>● <b>Approved</b>—The item is approved for use in the software project.</li><li>● <b>Not Reviewed</b>—The item has not been reviewed.</li><li>● <b>Rejected</b>—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.</li></ul>
<b>Alerts</b>	<p>Notifies you whether or not security alerts exist for this item.</p>
<b>Priority</b>	<p>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.</p> <p>You can change the priority for this inventory item by selecting a different priority from the dropdown list and clicking <b>Save</b>. For more information about priorities, see <a href="#">Inventory Priority</a>.</p>
<b>Vulnerabilities</b>	<p>A bar graph showing the count of known vulnerabilities by severity—red (high), orange (medium), yellow (low), or unknown (gray)—for the inventory item. Click the graph to view the list of vulnerabilities and their details.</p> <p>If no vulnerabilities have been found for the inventory item, the value <b>No</b> is displayed in place of the graph.</p>
<b>Created By</b>	<p>The name of the person or process that created the inventory item.</p>
<b>Confidence</b>	<p>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.</p> <p>For more information about the Confidence levels, see <a href="#">Inventory Confidence</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Created On</b>	<p>The date that the inventory item was created.</p>
<b>Updated On</b>	<p>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.</p>
<b>Name</b>	<p>The name of the inventory item.</p>

Table 8-26 • Inventory Details pane (cont.)

Column/Field	Description
<b>Type</b>	<p>The type of finding of this item:</p> <ul style="list-style-type: none"> <li>• <b>Work in Progress</b>—A set of files with something in common. The work in progress will become a component or license only via manual audit work.</li> <li>• <b>Component</b>—Files from a specific component version with known or unknown license. If this type is selected, the <b>Lookup Component</b> button becomes active, enabling you to select a new component instance for the inventory item.</li> <li>• <b>License Only</b>—Files under a specific license without a known component.</li> </ul>
<b>Component</b>	<p>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.</p>
<b>License</b>	<p>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.</p>
<b>Description</b>	<p>A description of the inventory item. You can update the description as needed.</p>
<b>Url</b>	<p>The URL of the license for this inventory item. You can update the URL as needed.</p>
<b>Disclosed</b>	<p>The <b>Yes</b> or <b>No</b> 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.</p> <p>This field is used most often by analysts to denote information about the state of the inventory item.</p>
<b>Usage tab</b>	
<b>Distribution Type</b>	<p>The option indicating how the inventory item is distributed:</p> <ul style="list-style-type: none"> <li>• <b>Internal</b>—Internally only (such as test framework that might be included in the codebase but is not distributed with the product).</li> <li>• <b>External</b>—Externally with the product, shipped to customers (outside of your organization, including a private cloud deployment at the customer's site)</li> <li>• <b>Hosted</b>—Hosted in your company's data center (such as a SAAS application).</li> <li>• <b>Unknown</b>—Unknown distribution type.</li> </ul>
<b>Part of Product</b>	<p>The <b>Yes</b>, <b>No</b>, or <b>unknown</b> 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.</p>





Table 8-26 • Inventory Details pane (cont.)

Column/Field	Description
<b>Linking</b>	<p>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 <b>Unknown</b> value indicates that linking status is not known.</p> <p>Linking can affect license priority and obligations.</p>
<b>Modified</b>	<p>The <b>Yes</b>, <b>No</b>, or <b>Unknown</b> 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.</p>
<b>Encryption</b>	<p>The <b>Yes</b>, <b>No</b>, or <b>Unknown</b> option indicating whether the component provides the encryption capabilities used in the product. Encryption can affect export controls.</p>
<b>Notes tab</b>	
<b>Detection Notes</b>	<p>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.</p>
<b>Audit Notes</b>	<p>Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis.</p>
<b>As-Found License Text</b>	<p>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.</p>
<b>Notices Text</b>	<p>The text to be shown in the <b>Notices</b> report for the selected inventory item. For more information about the <b>Notices</b> report, see <a href="#">Generating the Notices Report</a>.</p>
<b>Associated Files tab</b>	<p>Click this tab to view a list of the files that are part of the inventory for this project. Click the <b>X</b> to delete a listed file.</p>

## 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 8-27 •** Evident Details pane

Column/Field	Description
<b>Expand All/Collapse All</b>	Click to toggle between expanded and collapsed display.
<b>Search field</b>	Enter search criteria.
<b>Tree view</b> 	Click to change the display to a tree view.
<b>List view</b> 	Click to change the display to a list view.
<b>Select Evidence Types</b>	Click to select evidence types to display

## Project Inventory Review Page

The **Project Inventory Review** page lets you search project inventory. The page has the following fields:

**Table 8-28 •** Project Inventory Review page

Column/Field	Description
<b>Inventory Items (x)</b>	The title of this pane includes the number of inventory items displayed in the list below.
<b>Search type</b>	From the dropdown list, select the type of search to perform: <ul style="list-style-type: none"><li>• Inventory Name</li><li>• Security Vulnerability</li><li>• Inventory with Vulnerabilities</li><li>• Inventory with Open Alerts</li></ul>

**Table 8-28** • Project Inventory Review page (cont.)



Column/Field	Description
<b>Search criteria</b>	<p>The prompt for this field changes based upon your selection in the <b>Search type</b> field:</p> <ul style="list-style-type: none"><li>• If you select <b>Inventory Name</b> in the <b>Search type</b> field, you must enter a full or partial name to search for.</li><li>• If you select <b>Security Vulnerability</b> in the <b>Search type</b> field, you must enter a valid vulnerability ID to search for.</li><li>• If you select <b>Inventory with Vulnerabilities</b> in the <b>Search type</b> field, the list will automatically display the inventory items that meet your criteria.</li><li>• If you select <b>Inventory with Open Alerts</b> in the <b>Search type</b> field, the list will automatically display the inventory items that meet your criteria.</li></ul>

## Policies Page

The **Policies** page lets you edit, copy, and create policies for your projects. See [Managing Policy Profiles](#) for more details about policies.

The page has the following fields:

**Table 8-29** • Policy page

Column/Field	Description
<b>Policy list</b>	<p>The list of current policies in a grid format. Each entry shows the policy name and its description, the user who last updated the policy, and date of the last update for each policy.</p> <p>Select a policy to edit or copy.</p> <ul style="list-style-type: none"><li>• <b>Edit icon</b>—Click  to edit the selected policy. The <b>Policy Details</b> page is opened, showing the policy details.</li><li>• <b>Copy icon</b>—Click  to copy the selected policy. The Policy Details page is opened, showing a new instance of the selected policy. (The selected policy is always saved first.) This new instance has the name Copy of <i>selected_policy_name</i>.</li></ul>
<b>Add Policy button</b>	Click the <b>Add Policy</b> button to create a new policy. The <b>Policy Details</b> page is opened.

### See Also

[Policy Details Page](#)

[License Details Dialog](#)

[Managing Policy Profiles](#)

# Policy Details Page

The **Policy Details** page lets you define or edit a policy 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 can be automatically approved or rejected (or flagged for a manual review) based on the policy definition. See [Managing Policy Profiles](#) for more information.

The page has the following fields:

**Table 8-30 •** Policy Details page

Column/Field	Description
<b>General</b>	
<b>Name</b>	The name of the policy that you are editing or copying.  If you are copying a policy, the name will read <i>Copy of <code>selected_policy</code></i> , where <i>selected_policy</i> is the name of the policy you selected to copy. To change the name of the policy, type a new name in this field.
<b>Description</b>	The policy description, if it exists. You can edit or add a description.
<b>Created</b>	The name of the user who created the policy, and the date and time the policy was created. You can click the hyperlinked name to send an email to the user who created the policy.
<b>Updated</b>	The name of the user who last updated the policy, and the date and time the policy was updated. You can click the hyperlinked name to send an email to the user who updated the policy.
<b>Security Vulnerabilities</b>	
<b>Only auto-approve inventory items if there are no associated security vulnerabilities</b>	Select this checkbox to have Code Insight skip any matching license-based or component policies if the inventory item has any associated security vulnerabilities.
<b>Reject inventory items if any associated security vulnerabilities have a CVSS score above...</b>	Select this checkbox to have Code Insight automatically reject any inventory items with any associated security vulnerabilities that have a CVSS score above the specified value.  This policy takes precedence over any other automated approval policy.
<b>Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than ...</b>	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 selected value.  This policy takes precedence over any other automated approval policy.
<b>Licenses</b>	

**Table 8-30 •** Policy Details page (cont.)





Column/Field	Description
<b>Select a License</b> drop-down list	<p>The list of licenses available to add to the policy as criteria for automatically reviewing inventory items.</p> <p>Select a license from the list, and click <b>Add License</b> to add it to the policy.</p>
<b>Add License</b> button	Click the <b>Add License</b> button to add the selected license as a criterion for the policy.
<b>License</b> list	<p>The list of licenses (in a grid format) currently used by this policy as criteria for automatically reviewing inventory items.</p> <ul style="list-style-type: none"> <li>● <b>Name</b>—The name of the license.</li> <li>● <b>Usage Guidance icon</b>—Click  to display the <b>Usage Guidance</b> dialog, in which you can add or edit text that will help reviewers in reviewing this license.</li> <li>● <b>License Details icon</b>—Click  to display the <b>License Details</b> dialog for the selected license.</li> <li>● <b>Action</b>—Select one of the following to indicate what status is automatically assigned based on the license: <ul style="list-style-type: none"> <li>● <b>Approve</b></li> <li>● <b>Reject</b></li> <li>● <b>No Action</b> (same as the “Not Reviewed” inventory status, thus requiring a manual review)</li> </ul> </li> <li>● <b>Delete icon</b>—Click  to delete the license from the policy.</li> </ul>
<b>Components</b>	
<b>Add Component</b> button	<p>Click the <b>Add Component</b> button to select the component and enter the version range as a criterion for the automated inventory review.</p> <p>When you click this button, the <b>Lookup Component</b> dialog is opened, enabling you to enter search criteria to filter the available components. You can then select the component and specify the version range in the <b>Versions</b> field (see below). (See <a href="#">Lookup Component Dialog</a> for information about the <b>Lookup Component</b> dialog.)</p>

Table 8-30 • Policy Details page (cont.)

Column/Field	Description
<b>Component list</b>	<p>The list of current components with a version range (in a grid format) that this policy uses as criteria for automated inventory review.</p> <ul style="list-style-type: none"> <li>● <b>Name</b>—The name of the component.</li> <li>● <b>Versions</b>—Select a specific version or a range of versions for the given component. (The <b>Versions from</b> and <b>to</b> drop-down lists are populated with available versions for the component.) Here are some example ways to specify a version or version range: <ul style="list-style-type: none"> <li>● To enter a specific version, select the same version in the <b>Versions from</b> and <b>to</b> fields.</li> <li>● To enter an explicit range, select a minimum version in the <b>Versions from</b> field and the maximum version in the <b>to</b> field.</li> <li>● To specify any version for the given component, select the wild card * in both <b>Versions from</b> and <b>to</b> fields.</li> <li>● To specify any version up to a specific version, enter the wild card * in the <b>Versions from</b> field and the maximum version in the <b>to</b> field.</li> <li>● To specify any version after a specific version, select the specific version in the <b>Versions from</b> field and the wild card * in the <b>to</b> field.</li> </ul> </li> </ul> <p>The <b>unknown</b> option applies to certain components that were collected without a version value. To specifically handle unknown versions, set both <b>Versions from</b> and <b>to</b> fields to <b>unknown</b>.</p> <ul style="list-style-type: none"> <li>● <b>Action</b>—Select one of the following to indicate what status is automatically assigned based on the component version: <ul style="list-style-type: none"> <li>● <b>Approve</b></li> <li>● <b>Reject</b></li> <li>● <b>No Action</b> (same as the “Not Reviewed” inventory status, thus requiring a manual review)</li> </ul> </li> <li>● <b>Delete icon</b>—Click  to delete the component entry from the policy.</li> </ul>
<b>Policy Details page actions</b>	
<b>Save</b>	Click to save the changes you have made to this policy.
<b>Close</b>	Click to close the <b>Policy Details</b> page. If you have made changes the policy, be sure that you have clicked <b>Save</b> before closing the page; otherwise, changes are lost.

**See Also**

[Policy Details Page](#)  
[License Details Dialog](#)  
[Lookup Component Dialog](#)  
[Managing Policy Profiles](#)

# License Details Dialog

The **License Details** dialog lets you view general information and license text for a selected license. The dialog has the following fields:

**Table 8-31** • License Details dialog

Column/Field	Description
<b>General Information Tab</b>	
<b>Id</b>	The identification number of the license in the database.
<b>Name</b>	The name of the license. For example, <i>Academic Free License v1.1</i> .
<b>Priority</b>	The priority ranking as determined by FlexNet Code Insight. For more information, see <a href="#">Understanding Security Vulnerability Alerts</a> .
<b>URL</b>	The URL where the license is available on the internet.
<b>Description</b>	A short description of the license.
<b>Category</b>	A license attribute that supports arbitrary classification of a license.
<b>Custom License</b>	Tells you if this license is a custom license.
<b>Commercial</b>	A designation of whether the licenses is classified as commercial.
<b>Copyleft</b>	A designation of whether the licenses is considered a copyleft license.
<b>Free Software License</b>	A designation of whether the licenses is a free software license.
<b>GPL V2 Compatible</b>	A designation of whether a license is compatible with GPL-2.0.
<b>License Text Tab</b>	Displays the actual text of the selected license.

## Lookup Component Dialog

The **Lookup Component** dialog lets you search for a component in the CL and display additional information about the component, such as vulnerabilities and license issues. The dialog has the following fields:

**Table 8-32** • Lookup Component dialog

Column/Field	Description
<b>Search by</b>	Select the type of search you want to perform: <ul style="list-style-type: none"><li>● Keyword</li><li>● URL</li><li>● Forge</li></ul>
<b>Keywords</b>	Enter a search term to look it up in the CL.
<b>Select this Component</b>	Click this button to select the displayed component to add to an existing inventory item or to create a new one.
<b>Show Instances</b>	Select this hyperlink to display all instances that match your search criteria. By default, FlexNet Code Insight shows only one matching instance.
<b>Register New Instance</b>	Click this button to add a new instance using information in the CL.

## 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 8-33** • Add Project dialog

Column/Field	Description
<b>Name</b>	Enter a name for the new project.
<b>Project Type</b>	From the dropdown menu, select the type of scan that will be run on this project: <ul style="list-style-type: none"><li>● <b>Standard</b>—This is the default scan type. It requires that you upload your codebase to FlexNet Code Insight.</li><li>● <b>Inventory Only</b>—This type of scan allows for remote scanning and does not require that you upload your codebase to FlexNet Code Insight. To learn more about inventory-only projects, see “Creating a Project Without Uploading a Codebase” in the <i>FlexNet Code Insight Installation and Configuration</i> guide.</li></ul>



Table 8-33 • Add Project dialog (cont.)

Column/Field	Description
<b>Project Visibility</b>	From the dropdown menu, select whether this will be a public or private project. The default is public, which allows all users to view all the details of this project. If you select <b>Private</b> , you will have to specify users who will have access to the details of this project beyond the permission to view the <i>project name, owner, and change owner</i> .
<b>Policy Profile</b>	From the dropdown menu, select a policy profile to be used for this project. This field is optional.


## Preferences Page

The **Preferences** page appears when you select **Preferences** from the main menu. It lets you change a user's password associated with an authorization token. In addition, you can view and add authorization (AUTH) tokens for use with FlexNet Code Insight REST APIs. The page has the following fields:

Table 8-34 • Preferences page

Column/Field	Description
<b>Change Password</b>	
<b>New Password</b>	Enter a new password for the selected authorization token. The password must be a minimum of 8 characters, one of which must be numeric and one of which must be a capital letter. No spaces are allowed in the password.
<b>New Password Confirm</b>	Reenter the password you entered in the <b>New Password</b> field.
<b>Update Password</b>	After entering the password in both fields, click Update Password to save your changes.
<b>Authorization Tokens</b>	
<b>Add Token</b>	Click this button to display the <b>Add Token</b> dialog.
<b>Name</b>	A list of the names of previously created tokens.
<b>Token</b>	Displays the system-generated token associated with the name.
<b>Create Date</b>	The date on which the token was created.

Table 8-34 • Preferences page (cont.)

Column/Field	Description
<b>Actions</b>	A group of icons that indicate actions you can take on each token: <ul style="list-style-type: none"><li>• Edit (<p><b>See Also</b></p></li></ul>

[Add Token Dialog](#)

[Edit Token Dialog](#)

## 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 to be used to authenticate calls to FlexNet Code Insight REST APIs. The dialog has the following fields:

Table 8-35 • Add Token dialog

Column/Field	Description
<b>Name</b>	Enter a name for the token you are creating.
<b>Token Validity</b>	Select one of the validity periods: <ul style="list-style-type: none"><li>• <b>Never Expires</b>: The authorization token never expires.</li><li>• <b>Expires On</b>: The authorization token is valid until the date you pick on the Validity Calendar.</li></ul>
<b>Validity Calendar</b>	If you check the <b>Expires On</b> option, the validity calendar becomes active. type an expiration date (for example, 10/10/10) or click the calendar icon and pick a date.

**See Also**

[Preferences Page](#)

[Edit Token Dialog](#)

# Edit Token Dialog

The **Edit Token** dialog appears when you click the **Edit Token** icon on the **Preferences** page. It lets you create an authorization token to be used to authenticate calls to FlexNet Code Insight REST APIs. The dialog has the following fields:

**Table 8-36** • Edit Token dialog

Column/Field	Description
<b>Name</b>	Enter a name for the token you are creating.
<b>Token</b>	Displays the actual characters of the system-generated token.
<b>Select Token Text</b>	Click this button to highlight the token characters displayed in the <b>Token</b> field. To copy the token to the clipboard, press <b>CTRL-C</b> .
<b>Expiration</b>	A read-only field that displays the expiration date of the token, or the text, “Token has no expiration date.”
<b>Save</b>	Click this button to save your edits.
<b>Cancel</b>	Click this button to exit the <b>Edit Token</b> dialog without saving your edits.

**See Also**

[Preferences Page](#)

[Add Token Dialog](#)


# 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 8-37** • Advanced Inventory Search page

Column/Field	Description
<b>Inventory Items</b>	
<b>Inventory Name</b>	Enter the whole or partial name of an item for which to search. For example, if you enter <b>apache</b> in this field, FlexNet Code Insight will find all inventory items that have the word <i>apache</i> in their name.
<b>Inventory Priority</b>	Select one or more of these checkboxes ( <b>P1</b> , <b>P2</b> , <b>P3</b> , or <b>P4</b> ) to search the inventory by inventory priority.  For more information about inventory priority, see <a href="#">Inventory Priority</a> in the “Using FlexNet Code Insight” chapter.

**Table 8-37 •** Advanced Inventory Search page (cont.)

Column/Field	Description
<b>Inventory Review Status</b>	<p>Select one or more of the following checkboxes to filter the inventory display based on the review status of inventory items:</p> <ul style="list-style-type: none"> <li>● <b>Approved</b>—Show only inventory that has been reviewed and approved, either manually by a reviewer or automatically during the auto-publish process.</li> <li>● <b>Rejected</b>—Show only inventory that has been reviewed and rejected, either manually by a reviewer or automatically during the auto-publish process.</li> <li>● <b>Not Reviewed</b>—Show only items that have not yet been reviewed.</li> </ul> <p>For more information about the review status, see <a href="#">Review Status of Inventory</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Dependency Options</b>	<p>Select one of the following options to filter the inventory display based on dependency level:</p> <ul style="list-style-type: none"> <li>● <b>All Inventory Items</b>—Display all inventory items—top-level inventory and first-level and transitive dependencies.</li> <li>● <b>Only Top-Level Inventory Items</b>—Display only top-level inventory items only. No first-level or transitive dependencies are listed.</li> <li>● <b>Only Dependency Inventory Items</b>—Display only first-level and transitive dependencies.</li> </ul>
<b>Inventory Age</b>	<p>Search by inventory publication date. This dropdown field has the following choices:</p> <ul style="list-style-type: none"> <li>● <b>Any</b>—Show any published inventory.</li> <li>● <b>Last 1 day</b>—If today is Feb 6th, search from Feb 5th 12 AM.</li> <li>● <b>Last 7 days</b>—If today is Feb 6th, search from Jan 30th 12 AM.</li> <li>● <b>Last month</b>—If today is Feb 6th, search from Jan 7th 12 AM (30 days).</li> <li>● <b>Custom Date Range</b>—Select a beginning (<b>From</b>) and ending (<b>To</b>) date from the popup calendar.</li> </ul> <div>  <p><b>Note •</b> 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.</p> </div>

**Table 8-37 •** Advanced Inventory Search page (cont.)

Column/Field	Description
<b>Inventory Notifications</b>	<p>Select one or more of the following checkboxes to filter the inventory display based on security vulnerabilities:</p> <ul style="list-style-type: none"> <li>● <b>Inventory with Open Alerts</b>—Display only inventory items that have open vulnerability alerts (that is, alerts for vulnerabilities that were discovered post-publication and have not been closed).</li> <li>● <b>Inventory Rejected Due to New Non-Compliant Security Vulnerabilities</b>—Inventory items that have been rejected due to new security alerts that are non-compliant with policy.</li> </ul>
<b>Inventory Tasks Age</b>	<p>Search for published inventory items with tasks of a certain age (based on creation date). This dropdown field has the following choices:</p> <ul style="list-style-type: none"> <li>● <b>Any</b>—Show any published inventory.</li> <li>● <b>Last day</b>—If today is Feb 6th, search from Feb 5th 12 AM.</li> <li>● <b>Last 7 days</b>—If today is Feb 6th, search from Jan 30th 12 AM.</li> <li>● <b>Last month</b>—If today is Feb 6th, search from Jan 7th 12 AM (30 days).</li> <li>● <b>Custom Date Range</b>—Select a beginning (<b>From</b>) and ending (<b>To</b>) date from the popup calendar.</li> </ul>
<b>Inventory Task Owner</b>	<p>Search for published inventory items with tasks assigned to a specific user (or any user):</p> <ul style="list-style-type: none"> <li>● <b>Any</b>—Inventory with tasks assigned to any user.</li> <li>● <b>Only Mine</b>—Inventory with tasks assigned to you (current user).</li> <li>● <b>Specific User</b>—Inventory with tasks assigned to a specific user. (A <b>Select user</b> pop-up enables you to select the user.)</li> </ul>
<b>Inventory Confidence Level</b>	<p>Search for system-generated published inventory items that have a Confidence level of either <b>High</b>, <b>Medium</b>, or <b>Low</b>.</p> <p>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 <a href="#">Inventory Confidence</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Security Vulnerabilities</b>	
<b>Security Vulnerability ID</b>	Enter a valid vulnerability ID for which to search.

**Table 8-37** • Advanced Inventory Search page (cont.)

Column/Field	Description
<b>Security Vulnerability Severity</b>	<p>Select one or more of the following severities to include in your search:</p> <ul style="list-style-type: none"> <li>● High Severity (CVSS 7.0 - 10.0)</li> <li>● Medium Severity (CVSS 4.0 - 6.9)</li> <li>● Low Severity (CVSS 0.1 - 3.9)</li> <li>● Unknown Severity (N/A)</li> </ul> <p>For more information about vulnerability severities, see <a href="#">Security Vulnerabilities Associated with Inventory</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Security Vulnerability Age</b>	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>Last day</b>—If today is Feb 6th, search from Feb 5th 12 AM.</li> <li>● <b>Last 7 days</b>—If today is Feb 6th, search from Jan 30th 12 AM.</li> <li>● <b>Last 30 days</b>—If today is Feb 6th, search from Jan 7th 12 AM.</li> <li>● <b>Custom Date Range</b>—Select a beginning and ending date from the popup calendar.</li> </ul>
<b>Licenses</b>	
<b>License Name</b>	The full or partial name of the license for which to search.
<b>License Priority</b>	<p>Select one or more of the following license priorities to limit your search:</p> <ul style="list-style-type: none"> <li>● <b>P1</b>—Viral/Strong Copyleft</li> <li>● <b>P2</b>—Weak Copyleft/Commercial/Uncommon</li> <li>● <b>P3</b>—Permissive/Public Domain</li> <li>● No License Found</li> </ul> <p>For more information about license priority, see <a href="#">License Priority</a> in the “Using FlexNet Code Insight” chapter.</p>
<b>Apply And/Or Criteria</b>	<p>Select one of the boolean criteria to apply to the search selections:</p> <ul style="list-style-type: none"> <li>● <b>Or</b>—The item may contain any one or more of the chosen criteria to be displayed. This is the default boolean operator.</li> <li>● <b>And</b>—The item must meet all chosen criteria to be displayed.</li> </ul>
<b>Apply</b>	Click this button to apply the selected search criteria and return to the <b>Inventory Items</b> page to view the results. The title bar of the <b>Inventory Items</b> page denotes that the display shows only filtered results.


Table 8-37 • Advanced Inventory Search page (cont.)

Column/Field	Description
<b>Clear Form</b>	Click this button to remove any previously specified search criteria.
<b>Close</b>	Click this button to close this page and return to the <b>Inventory Items</b> page without applying your search criteria.

## 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 8-38 • Import Project Data dialog

Column/Field	Description
<b>Import Type</b>	Select the type of import you want to perform: <ul style="list-style-type: none"><li>● Inventory Only Import</li><li>● Standard Import (Default)</li></ul>
<b>Import File Location</b>	Select this option to browse for the project data file you want to import.
<b>Create inventory with no matching files</b>	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.  <b>Note</b> • 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.
<b>Only add files to inventory with matching MD5</b>	This option is unchecked by default.
<b>Only mark files as reviewed with matching MD5</b>	This option is checked by default.







# 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

		Roles		
		Administrators	Manage Policy	Create Project
Permissions	Notes			
<b>Administer Code Insight:</b>		✓	—	—
<ul style="list-style-type: none"><li>● Manage users and permissions</li><li>● Schedule or run electronic updates</li><li>● Configure an email server</li><li>● Configure LDAP users</li><li>● Configure Application Lifecycle (ALM) instances</li><li>● Configure a scan server</li><li>● Configure scan profiles</li><li>● Define global project defaults</li></ul>				
<b>Manage policies:</b>		—	✓	—
<ul style="list-style-type: none"><li>● Create and edit policy profiles</li></ul>				
<b>Create projects:</b>	The Project Creation role is controlled by the <b>Allow All Users to Create Projects</b> option on the <b>Manage Permissions</b> dialog. If <b>Yes</b> (default), any user has this role. If <b>No</b> , 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 <i>FlexNet Code Insight Installation and Configuration Guide</i> .) Users who have this role can also create project folders in the <b>Projects</b> list.	—	—	✓
<ul style="list-style-type: none"><li>● Create projects (and thereby automatically become Project Owner for each)</li><li>● Create project folders (in <b>Projects</b> list)</li></ul>				

# 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**

		Roles			
		Project Owner	Analyst	Reviewer	Observer
Permissions	Notes				
<b>Manage project:</b> <ul style="list-style-type: none"> <li>Change project owner</li> <li>Manage project users</li> <li>Rename project</li> <li>Move projects in Project Folder Tree</li> <li>Manage scan settings</li> <li>Manage and inventory review/ remediation settings</li> <li>Manage Source Control Management (SCM) and Application Lifecycle (ALM) instances</li> </ul>	<p>The project creator automatically becomes Project Owner, who can then reassign ownership to another user.</p> <p>See the previous section, <a href="#">System Roles and Permissions</a>, for information about the Create Project role needed to create projects.</p>	✓	—	—	—
<b>View project inventory</b>	Any user (not just one with a project role) can view the <b>Project Inventory</b> tab and the associated inventory details.	✓	✓	✓	✓*
<b>Edit/create project inventory</b>	<p>The Reviewer role has limited inventory-editing capabilities on the <b>Project Inventory</b> tab. Reviewers can neither edit nor add new inventory (that is, the <b>Edit</b> and <b>Add</b> buttons are not available). However, reviewers can recall inventory and edit inventory priority, review status, alerts, as-found license text, and notes (except detection notes).</p>	✓	✓	✓	—
<b>Access and use Analysis Workbench</b> <ul style="list-style-type: none"> <li>View codebase file tree</li> <li>Edit inventory in the Workbench</li> </ul>		✓	✓	—	—

**Table A-2 • Project Roles and Permissions (cont.)**

		Roles			
		Project Owner	Analyst	Reviewer	Observer
Permissions	Notes				
Invoke a scan		✓	✓	—	—
Upload codebase		✓	✓	—	—
Import/export project data		✓	✓	—	—

\* 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”.

## 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**

		Roles				
		Project Owner	Analyst	Reviewer	Observer	Task Assignee
Permissions	Notes					
Create/edit tasks	Any user assigned to a project role can create and edit tasks.	✓	✓	✓	✓	✓
Reassign task		✓	—	—	—	✓
Close manual review task		—	—	✓	—	—
Close remediation task		✓	—	—	—	✓
Close miscellaneous task	Any user assigned to a project role can close a miscellaneous task.	✓	✓	✓	✓	✓