

FlexNet Code Insight 2018 R3 User Guide

Legal Information

Book Name: FlexNet Code Insight 2018 R3 User Guide
Part Number: FNCI-2018R3-UG00
Product Release Date: October 2018

Copyright Notice

Copyright © 2018 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.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/producer/company/about/intellectual-property/>. 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 2018 R3 User Guide..... 9**
 - Contacting Us 10**
- 2 Using FlexNet Code Insight 11**
 - Intended Audience 11**
 - Opening FlexNet Code Insight 12**
 - Viewing Online Help and Online Guides..... 13
 - Creating a Project 13**
 - Applying a Scan Profile to the Project..... 14**
 - About Scan Profiles..... 14
 - Applying a Scan Profile..... 14
 - Uploading a Codebase..... 15**
 - What Is a FlexNet Code Insight Scan? 16**
 - Starting the Scan 16**
 - What Does an Analyst do?..... 17**
 - Analyzing (Auditing) Scan Results 17**
 - Using the Analysis Workbench 17**
 - The Analysis Workbench Layout 18
 - Searching for Codebase Files Based on Name 19
 - Searching for Codebase Files Based on Search Criteria 19
 - Creating a New File Search 20
 - Using the Codebase Files Pane Context Menu 20
 - Marking Files as Reviewed..... 21
 - Using the File Details Tab 21
 - Viewing the Evidence Summary for a File..... 22
 - Viewing Binary Strings..... 22
 - Viewing Exact Matches 23
 - Viewing Source Matches 23

Understanding the Exact or Partial Matches Panels	24
Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component	25
Using the Evidence Details Tab	26
Using the Inventory Details Tab	26
Adding Details to an Inventory Item	27
Using the Inventory Items Context Menu	27
Component Lookup	27
Guidelines for Component Lookup	28
Component Lookup Results	28
Performing Component Lookup	29
Creating an Inventory Item	29
Creating Inventory from the Inventory Items List	29
Creating Inventory from the Codebase Files List	30
Publishing Inventory	31
Automatically Publishing Inventory	31
Viewing Security Vulnerabilities for an Inventory Item	32
Using the Project Inventory Tab	34
Displaying Project Inventory	34
Dependency Inventory Items	35
Inventory Priority Calculation	35
Reviewing Inventory	35
Assigning Analysts, Reviewers and Observers to a Project	35
Quickly Filtering Published Inventory	36
Approving or Rejecting Inventory Items	37
Viewing Inventory License Details	37
Viewing As-Found License Text	38
Viewing Notes & Guidance	38
Viewing Associated Files	38
Creating and Managing Tasks for Project Inventory	39
Note About External Work Items	39
Manually Creating a Task	39
Editing a Task	41
Creating and Viewing External Work Items for a Project Inventory Task	43
Prerequisite	43
Manually Creating a Work Item	43
Viewing a Work Item	44
Recalling a Published Inventory Item	44
Understanding License Priorities	44
Security Vulnerability Alerts	45
Viewing Security Vulnerability Alerts	45
Receiving Security Vulnerability Alert Email Notifications	46
Using the Project Dashboard	47
Opening the Project Dashboard	47
Searching for Projects	47
Searching by Project Name	48
Searching by Security Vulnerability ID	48

Filtering Inventory on the Project Dashboard	49
Managing a Project	49
Using the Project Summary Page	49
Generating Reports	50
The Project Report	50
The Audit Report	50
The Notices Report	51
Adding Text for Notices Reports	52
Generating the Notices Report	52
Editing the Project Definition and General Settings	53
Updating Scan Settings for a Project	53
Connecting the Project to Remote Data Sources	53
Version Control Settings	54
ALM Settings	54
Changing Project Owners	56
Exporting Project Data	57
Creating a Private Project	57
Managing Policy Profiles	58
Understanding Policy Profiles	58
How Policy Profiles Work in the Automated Inventory-Review Process	58
Adding or Editing a Policy Profile	59
Copying a Policy Profile	59
Associating a Policy Profile with a Project	59
3 Performing Advanced Searches	61
Advanced Searches	61
Dependencies in Advanced Searches	65
4 Exporting & Importing Project Data	67
Exporting and Importing	67
What is Exported?	68
Exporting Project Data	68
Exporting Project Data Using the FlexNet Code Insight UI	69
Exporting Project Data Using the REST API	69
Types of Import	70
What is Imported?	70
How Files & Inventory Are Processed During Import	71
Import Options	71
Importing Project Data	71
Expected Results	73
Empty Inventory	73
Duplicate Inventory	74
Special Considerations for Standard Import	74

5	Automated Analysis	75
	What is Automated Analysis?	75
	Supported Package Managers	75
	Supported File Extensions	76
	Supported Archive Formats	76
	Additional Rule-based Detection Capabilities	77
6	Performing Inventory-Only Scanning.....	79
	Inventory-Only Scan	79
	Creating a Project Without Uploading a Codebase	79
	FlexNet Code Insight Plugins	80
7	Configuring Source Code Management	83
	Managing Source Code Management (SCM) Instances	83
	Adding an SCM Instance to the Code Insight Project	84
	Testing an SCM Instance	84
	Synchronizing an SCM Instance	84
	Deleting an SCM Instance	85
	Configuring a Git SCM Instance	85
	Adding a Git SCM Instance to the Code Insight Project	85
	Configuring the Git SCM Instance	86
	Configuring a Perforce SCM Instance	86
	Adding a Perforce SCM Instance to the Code Insight Project	86
	Configuring the Perforce SCM Instance	87
	Configuring a TFS SCM Instance.....	88
	Adding a TFS SCM Instance to the Code Insight Project.....	88
	Configuring the TFS SCM Instance.....	88
8	Pages and Panels.....	91
	The FlexNet Code Insight Dashboard	92
	Users Tab.....	93
	Add User Dialog	94
	Edit User Dialog	95
	Electronic Updates Tab	96
	Email Server Tab	96
	LDAP Tab	97
	ALM Tab	99
	Scan Servers Tab	100
	Scan Server Dialog.....	100
	Scan Profiles Tab	102
	Create/Edit Scan Profile Dialog	103
	Project Defaults Tab	104

Projects List Page	107
Project Summary Page	108
Edit Project: General Tab	111
Edit Project: Scan Settings Tab	115
Edit Project Users Dialog	116
Scan History Dialog	117
Select a New Project Owner Dialog	117
Analysis Workbench	118
File Search Results Pane	119
Advanced File Search Dialog	120
Advanced File Search Add Dialog	121
Inventory Details Pane	121
Evidence Details Pane	124
Project Inventory Review Page	124
Policies Page	125
Policy Details Page	126
License Details Dialog	129
Lookup Component Dialog	130
Add Project Dialog	130
Preferences Page	131
Add Token Dialog	132
Edit Token Dialog	133
Advanced Inventory Search Page	133
Import Project Data Dialog	136

FlexNet Code Insight 2018 R3 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 includes the following sections.

Table 1-1 • FlexNet Code Insight 2018 R3 User Guide

Topic	Content
Using FlexNet Code Insight	Provides basic information about FlexNet Code Insight that will enable you to quickly start using the product effectively.
Performing Advanced Searches	Overview and procedures for using advanced searches to find specific inventory.
Exporting & Importing Project Data	Explains the export and import of project data.
Automated Analysis	Contains information about FlexNet Code Insight automated analysis tools and features.
Performing Inventory-Only Scanning	Provides information about the various types of FlexNet Code Insight scans.
Configuring Source Code Management	Contains procedures for using source code management applications with FlexNet Code Insight.
Pages and Panels	Includes reference information for the pages and panels in the FlexNet Code Insight user interface.

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:

<http://www.flexera.com>

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/CCContactSupport>

2

Using FlexNet Code Insight

This section 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:

- [Intended Audience](#)
- [Opening FlexNet Code Insight](#)
- [Creating a Project](#)
- [Applying a Scan Profile to the Project](#)
- [Uploading a Codebase](#)
- [What Is a FlexNet Code Insight Scan?](#)
- [Starting the Scan](#)
- [What Does an Analyst do?](#)
- [Analyzing \(Auditing\) Scan Results](#)
- [Using the Analysis Workbench](#)
- [Using the Project Inventory Tab](#)
- [Using the Project Dashboard](#)
- [Managing a Project](#)
- [Creating a Private Project](#)
- [Managing Policy Profiles](#)

Intended Audience

The *FlexNet Code Insight 2018 R3 User Guide* is intended for anyone who uses FlexNet Code Insight for scanning, analyzing, and reviewing project codebases.

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 “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`.



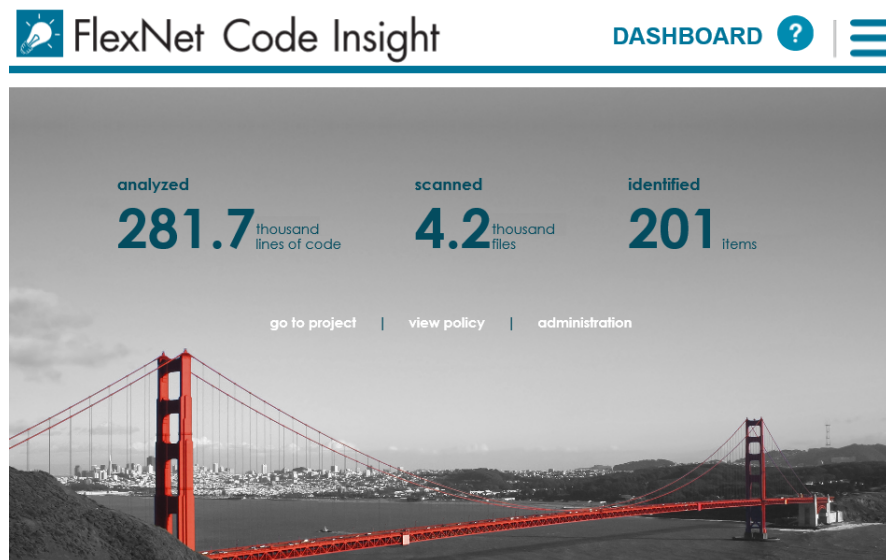
Note • If you are unsure about your server host name, contact your system administrator for guidance.

2. Enter your **username** and **password**.



Note • The default login name is **admin**; the default password is **Password123**. Your installation may require a different login name and password. If you are unsure about what to enter, contact your system 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.

Creating a Project

A project represents scan and analysis results from a codebase. Typically, a project would be created for each one of your products but you may also create projects for vendor code, to screen an open source component you are considering using, or to prepare for an open source contribution. 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.



Task To create a project, do the following:

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



The **Administration** menu opens.

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.
 - **Inventory Only:** 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 *Installation and Configuration* guide.
 - **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 **Manage Project** menu on the **Summary** page. 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 [Applying a Scan Profile to the Project](#).

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

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 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 matches based on the Compliance Library.
- **Comprehensive Scan profile:** Further expands the file-level third-party indicators with source matches based on the Compliance Library.

Additional scan profiles can be defined by the application administrator for use across projects (see the *FlexNet Code Insight Installation & Configure 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 of the **Project Summary** page. 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.



Task

To select a new scan profile:

1. From the list of projects, click the project for which you want to apply a scan profile. 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 **Project Summary** page 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. You can also click the information icon next to the scan profile you selected to view a read-only summary of the select scan profile.

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.



Task

To upload a project codebase, do the following:

1. Navigate to the **Project Summary** page, 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.

What Is a FlexNet Code Insight Scan?

The FlexNet Code Insight scanner performs a static analysis of files of any type (source or binary) and finds evidence of third-party code. This evidence includes:

- Third-party copyright statements.
- Open source license matches.
- Whole-file matches to files collected in the Compliance Library.
- Code-snippet matches to code collected in the Compliance Library.
- Email addresses and URLs.
- Search terms (strings).

Starting the Scan

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



Task

To start the scan, do the following:

1. Navigate to the **Project Summary** page, 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** portion of the **Project Summary** page.

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.

3. What do you want to do next?
 - [Filtering Inventory on the Project Dashboard](#)
 - [Analyzing \(Auditing\) Scan Results](#)
 - Generate the following reports:
 - [The Project Report](#)
 - [The Audit Report](#)
 - [The Notices Report](#)

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 auditor 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:

- 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.



Task

To audit scan results, do the following:

1. From the **Project Summary** page, click **Analysis Workbench**. The **Analysis Workbench** appears.
2. Use the **Analysis Workbench** to interact with the scan results. For more information, see [Using the Analysis Workbench](#).

Using the Analysis Workbench

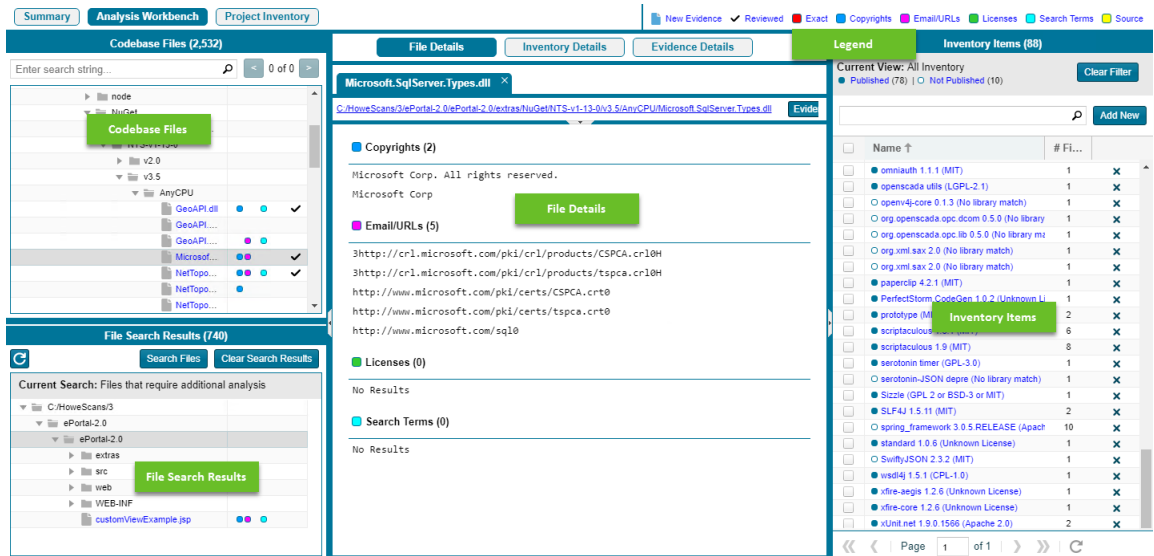
The following sections describe how to use the Analysis Workbench:

- [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 Codebase Files Pane Context Menu](#)
- [Marking Files as Reviewed](#)

- Using the File Details Tab
- Using the Evidence Details Tab
- Using the Inventory Details Tab

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 change 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/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/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](#).

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:
 - If you have more than one search criteria, select a Boolean value to limit the search: **AND** or **OR**. The default is **OR**.
 - Select a criterion from the drop-down **Criteria** menu.
 - Specify a search string by selecting **Contains** or **=** from the drop-down menu and typing a search string in the **Enter search string** field.
 - 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 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](#).

- **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 from the **Summary** page. 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.

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](#)
- [Viewing Exact Matches](#)
- [Viewing Source Matches](#)
- [Understanding the Exact or Partial Matches Panels](#)
- [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

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

Viewing Binary Strings



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:

icon_add.gif		File Inventory (0)		Type:	FILE	
Name:	icon_add.gif	Evidence	Exact Matches	Partial Matches	File Size:	0.93 KB
Path:	/home/palamida/scanroot/ePortal-2.0/web/images/icon_...				Lines of Code:	3
Digest:	1E902BEE3055A8BB654A6A7FA1B154C				Reviewed	No
Modified:	02/10/2009					

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. 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.
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 [Understanding the Exact or Partial Matches Panels](#) 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 are prioritized using the CodeRank™ metrics.



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 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 **Source** link in the legend at the top right of the page to easily find all files with source code matches. 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. Check the **Source Matches** checkbox to enable *source code fingerprint match* results.
5. Select a remote file in the **Remote Files** panel to turn on yellow highlights for the source code fingerprint matches and to see 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 [Understanding the Exact or Partial Matches Panels](#) for more information 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%)**: indicates the percentage of the matching third-party file contained in your scanned file.
- **Clustering (CL%)**: indicates the density/proximity of the source code matches within your scanned file.
- **Uniqueness (U%)**: indicates how common the set of discovered source code matches are in the Compliance Library (CL).
- **Matches**: indicates the number of unique matches in the scanned file.

Understanding the Exact or Partial Matches Panels

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

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

Note About Filtering in the Panels

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

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

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

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

Component Name ▼	bambod	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 content (source code fingerprint match) to the scanned file. The 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:

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:

- [Adding Details to an Inventory Item](#)
- [Component Lookup](#)
- [Creating an Inventory Item](#)

- [Publishing Inventory](#)
- [Automatically Publishing Inventory](#)
- [Viewing Security Vulnerabilities for an Inventory Item](#)

Adding Details to an Inventory Item

You can add details, such as license text and a description, to a published inventory item. Additional details help auditors to review the item.



Task

To add details to an inventory item, do the following:

1. In the **Inventory Items** pane, click the name of an item. The **Inventory Details** tab appears.
2. Enter or view information in the fields. For more information about the fields on this pane, see [Inventory Details Pane](#).
3. When you have finished changing or viewing the information on the **Inventory Details** tab, click **Save**.

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 inventory items that you would like to recall, 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.

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 a *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 one of the types of search:
 - Keyword
 - URL
 - Forge
5. Enter the required information for the specific type of search you are performing. For guidance on what to enter, see [Guidelines for Component Lookup](#)
6. 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

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 proceeds in the following way:

- 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 Name](#) and [Evidence Details](#).
- Research the findings and identify the origin of the files.
- 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.
- 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**.
- When you are finished creating Inventory Items, publish the ones you would like to report on. You may choose not to publish internal or test tools.

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

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

Creating Inventory from the Inventory Items List

In addition to creating inventory items from codebase files, you can create items from the **Inventory Items** list. This section describes how to do so.

**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**. The new item will appear in its own tab on the **Inventory Details** tab.
4. From the **Type** dropdown, select one of the following inventory types and perform the procedure under the selected inventory type:
 - **Work in Progress**
 - **Component:**
 - a. Click **Lookup Component** and search for a component of interest. For more information, see [Component Lookup](#).
 - b. Choose Component/Version/License from the results.
 - c. Complete the other fields as needed.
 - d. Select the **Associated Files** tab.
 - e. Drag and drop files from codebase file tree onto the **Associated Files** tab.
 - **License Only:**
 - a. Select a license from **License** dropdown. This dropdown appears when **License Only** is selected in the **Type** field.
 - b. Complete the other fields as needed.
 - c. Select the **Associated Files** tab.
 - d. Drag and drop files from the tree list in the **Codebase Files** pane onto the **Associated Files** tab.
5. When you finish editing the information for the new inventory item, click **Save**. The name of the inventory item appears in the **Inventory Items** pane.
6. (Optional) To report on newly created/edited inventory items, click **Publish**.

Creating Inventory from the Codebase Files List

In addition to creating inventory items from the **Inventory Items** list, you can create them from the **Codebase Files** list. This section describes how to do so.

**Task**

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

1. Open a folder listed in the **Codebase Files** pane.
2. Right click on the code that you want to inventory. The **Inventory** popup menu appears.
3. Select **Add to inventory** from the popup menu. The **Add to inventory** dialog appears.
4. Click an inventory item from the list to select it.

5. (Optional) To mark the selected files as reviewed, click **Mark files as reviewed**.
6. (Optional) To add a new inventory item to the list of available items, do the following:
 - a. Click **Add New**. The **Create Inventory** dialog appears.
 - b. Enter a name and description for the new inventory item in the appropriate fields.
 - c. Click **Save**.
7. Click **Submit**. The item is added to inventory, but is not visible. To see the newly added inventory item in the **Inventory Items** pane, right-click the codebase file and select **Show Inventory Files**.

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. 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.



Task

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

1. Open the **Project 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.

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 select the **Mark associated file as reviewed** checkbox.
5. When you have set the auto-publish feature, click **Save**. The **Project Summary** page appears.



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

Viewing Security Vulnerabilities for an Inventory Item

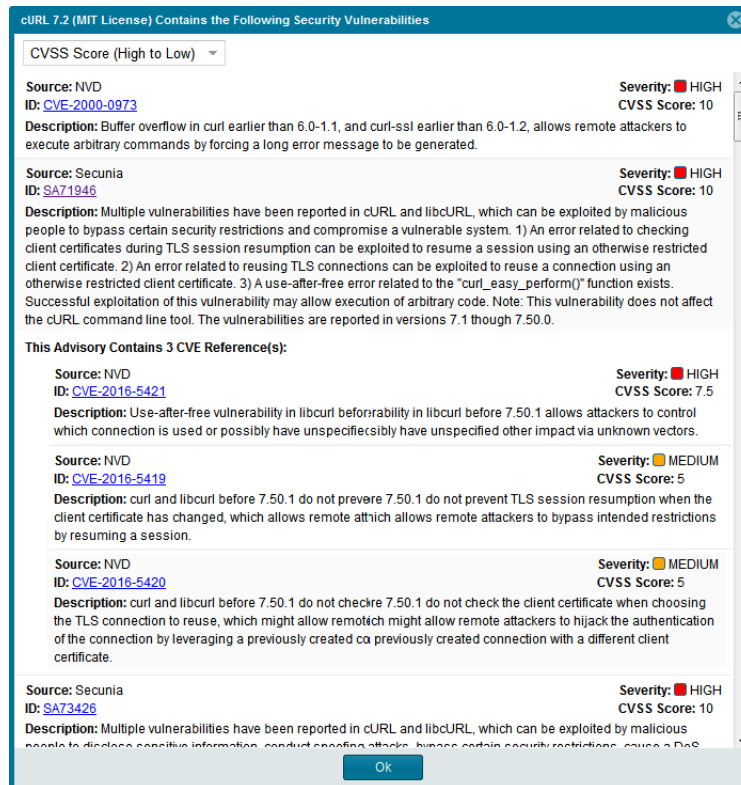
FlexNet Code Insight uses data from the National Vulnerability Database (NVD), Secunia advisories (as published by the Secunia Research team from Flexera), and other advisories such as RubySec to report security vulnerabilities associated with your inventory items. The vulnerabilities information from these sources is used to create vulnerability rankings and alerts. This section explains how to view the security vulnerabilities for an inventory item in the UI. For the procedure to display vulnerability alerts, see [Security Vulnerability Alerts](#).



Task

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

1. On the **Inventory Details** tab for the selected inventory item, click any of the **Vulnerabilities** counts (red, orange, or yellow). 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 of 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 0 and a severity of HIGH by default.



Note • A HIGH severity reported for vulnerabilities that are unscored ensures that these potentially critical vulnerabilities are not overlooked when filtering the inventory list using the Advanced Search feature or when sorting or reporting on vulnerabilities.

- You can click the vulnerability or advisory link to further investigate the vulnerability and determine the severity and score of the vulnerability as it applies to your project.



Note • Your feedback is welcome regarding 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](#)).

- 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 or advisory ID in an entry to view the vulnerability details found on the NVD, Secunia Community website, 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 return to the **Inventory Items** list.

Using the Project Inventory Tab

The **Project Inventory** tab shows a list of all the inventory items that have been published for the current project. Here you can set the status on inventory, change inventory priority and view details for the inventory item. Refer to the following sections for more information:

- [Displaying Project Inventory](#)
- [Dependency Inventory Items](#)
- [Inventory Priority Calculation](#)
- [Reviewing Inventory](#)
- [Quickly Filtering Published Inventory](#)
- [Approving or Rejecting Inventory Items](#)
- [Viewing Inventory License Details](#)
- [Viewing As-Found License Text](#)
- [Viewing Notes & Guidance](#)
- [Viewing Associated Files](#)
- [Creating and Viewing External Work Items for a Project Inventory Task](#)
- [Recalling a Published Inventory Item](#)
- [Understanding License Priorities](#)
- [Security Vulnerability Alerts](#)

Displaying Project Inventory

When an inventory item has been published, it can be reviewed, updated, and reported on in 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/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](#).

Dependency Inventory Items

Depending on how the codebase scan was configured, the inventory can include items that are first-level or transient dependencies of other inventory items. To distinguish a dependency inventory item from other inventory items, FlexNet Code Insight uses following naming convention for the dependency:

```
DEPENDENCY_COMPONENT DEPENDENCY_VERSION [Dependency of IMMEDIATE_PARENT_COMPONENT  
IMMEDIATE_PARENT_VERSION] (DEPENDENCY_SPDX_LICENSE_ID)
```

For example, an inventory item might look like this:

```
ant 1.7.1 [Dependency of ant-commons-logging 1.7.1] (Apache-2.0)
```

For transitive dependency inventory items, the parent is the top-most artifact in the dependency graph.

Inventory Priority Calculation

The priority of an inventory item is meant to highlight the importance of that item during the inventory review process. The following algorithm determines the default priority of an inventory item.

Inventory type component

If the inventory item has at least one associated security vulnerability with a severity of HIGH or the selected license priority is P1, 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.

Inventory type license-only

When a user selects a license for a license-only inventory item, the inventory priority is set to the 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.

Reviewing Inventory

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 to the project with a role of reviewer.

Assigning Analysts, Reviewers and Observers to a Project

The following are the available roles that users can have in a project:

- **Reviewers** have the ability to approve and reject inventory created by users in the analyst role.
- **Analysts** have the ability to create inventory items from evidence where appropriate, mark the analyzed files as reviewed, and **publish** inventory.

- **Observers** have read-only access to project inventory and can run reports. Development managers and executives are usually assigned the observer role. The observer role is available only for private projects.

In addition to assigning users to review public-view projects, the following procedure can be used to assign users and roles to specific private projects. For additional information about private projects, see [Creating a Private Project](#).



Task

To assign an analyst, a reviewer, or an observer to a project, do the following:

1. As the project owner, navigate to the **Project Summary** page.
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 user to the list of reviewers, drag the user from the **User** list on the left to the **Reviewers** list on the right. Repeat the drag and drop process to assign additional reviewers.
4. To assign a user to the list of analysts, drag the user from the **User** list on the left to the **Analysts** list on the right. Repeat the drag and drop process to assign additional analysts.
5. To assign a user to the list of observers, drag the user from the **User** list on the left to the **Observers** list on the right. Repeat the drag and drop process to assign additional observers.



Note • The **Observers** list is only visible for private projects.

6. (Optional) To add a user to the list of available users in the left pane, click **Add User** and complete the fields on the dialog. The user will appear in the list of available users.
7. Click **Close** when you finish adding reviewers and analysts.

Quickly Filtering Published Inventory

FlexNet Code Insight provides the ability 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.



Note • The following procedure assumes that you have already published inventory items.



Task

To quickly filter published inventory, do the following:

1. Navigate to the **Project Details** page and click **Project Inventory**. The **Inventory Items** pane appears, showing the list of inventory items.
2. Click the **Advanced Search** button at the top of the list.

3. From the **Advanced Inventory Search** dialog, select search criteria as needed. Options in the following categories enable you to search the inventory using multiple criteria as follows:
 - **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 [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.
4. Select **And** or **Or** from the **Apply Criteria** field.
5. Click **Apply** to filter the inventory to display only those inventory items that meet the selected criteria.
6. To refresh the list to show all inventory items, click **Show All Items**.

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 to indicate that it has been selected. A circle around the question mark indicates that no selection has been made.

Viewing Inventory License Details

You can view more details about the licenses that are part of your inventory on the **License Details** page. The **License Details** page has the **General Information** tab and the **License Text** tab. The **General Information** tab provides details such as the name of the license, its family and a priority assigned by FlexNet Code Insight. The **License Text** provides the actual text of the license.



Task

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

1. Click **Component Details**. The license selected for this component is listed as the selected license.
2. Click the info icon (i) next to the selected license. The **License Details** dialog appears with the **General Information** tab open.
3. View the information on the **General Information** tab. For descriptions of these fields, see [License Details Dialog](#).
4. Select the **License Text** tab to view the text of the license.

5. When you have finished viewing the license details, click **Close**.

Viewing As-Found License Text

During the scan, if FlexNet Code Insight found existing license text within the codebase, it will be displayed in the **As-Found License** tab.



Task

To view as-found license text, 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. Click the **As-Found License** tab . The as-found license text appears.
4. When you have finished viewing the license text, select another tab or click another item listed in the **Inventory Items** list.

Viewing 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. Click the **Notes & Guidance** tab in inventory details. The as-found license text appears.
2. When you have finished reviewing the list of associated files, select another tab or click another item listed in the **Inventory Items** pane.

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. Click the **Associated Files** tab in inventory details. A list of files associated with the selected inventory item appears.
2. When you have finished viewing the license text, select another tab or click another item listed in the **Inventory Items** pane.

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 signals to the assignee 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](#)
- [Closing or Reopening a Review 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 **Task Flow Options** settings for the 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 Task Flow options that you can set up for the project. See [Editing the Project Definition and General Settings](#) for details on editing the project and [Edit Project: General Tab](#) to for **Task Flow Options** field descriptions.

**Task****To create a task manually:**

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 project owner, 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 open an external work item associated with the task, click the **Create Work Item** button. (See [Note About External Work Items](#) 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:

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.

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 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 tasks associated with it, the **Reject** status of a single task automatically sets the inventory item status to **Reject**.
- If an inventory item has two or more 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.

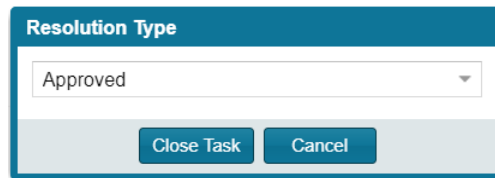
Note that, depending on the Task Flow options set for the project, the **Reject** status that is automatically set when you close a **Manual Inventory Review** task can automatically create a **Remediate Inventory** task. For more information about editing Task Flow options, see [Editing the Project Definition and General Settings](#).



Task

To close or reopen a Manual Inventory Review task:

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 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:

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 you 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 Task Flow options that you can set up for the project. See [Editing the Project Definition and General Settings](#) for details on editing the project and [Edit Project: General Tab](#) for **Task Flow Options** field descriptions.



Task

To create a work item manually:

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:

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. A 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 License Priorities

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

Each license you view in the **License Details** has one of the following priority values:

- **P1:** Viral/Strong Copyleft (red icon). Usually, P1 licenses require immediate attention due to the possibility of tainting proprietary application code which can have significant business impact.
- **P2:** Weak Copyleft/Commercial/Uncommon (yellow icon). 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.
- **P3:** Permissive/Public Domain (green icon). 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 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 electronic update.

Inventory priority typically defaults to the license priority value unless you manually override the inventory priority value. For information about changing the value, see [Displaying Project Inventory](#).



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.

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 (post-scan) 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 and send out email notifications 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) in the NVD or from the Secunia Advisories. This is a hyperlinked field; clicking on it will take you to the NVD entry or the Secunia Advisories entry for that file.
 - **CVSS Score**: The score of the vulnerability based on the Common Vulnerability Scoring System (CVSS). The values of the CVSS score range from 0 to 10, with 10 being the most serious.
 - **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.

Using the Project Dashboard

After you have created a project and scanned your codebase, the **Project Dashboard** provides you with an interactive view of your project, including security vulnerability exposure and license exposure. Refer to the following sections for details about using the dashboard:

- [Opening the Project Dashboard](#)
- [Searching for Projects](#)
- [Filtering Inventory on the Project Dashboard](#)


Opening the Project Dashboard

The **Project Dashboard** provides you with an overview of your scanned codebase, audit progress, and inventory in your project. This procedure assumes that you have logged into FlexNet Code Insight.



Task

To open the Project Dashboard, do the following:

1. From the **FlexNet Code Insight Dashboard**, select **go to project** and then select a project from the tree list. The **Project Dashboard** appears. You can also click the Load Project Dashboard icon () to display the **Project Dashboard**. The right panel of the page contains the following panes:
 - **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 [Displaying Project Inventory](#).
 - **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.
2. (Optional) Hover your pointer on the segments of the charts to view details about each section.
3. (Optional) Select another project from the **Project** list to view information about its inventory.

Searching for Projects

FlexNet Code Insight provides the ability to quickly search for and find projects that match specific criteria. You can search for a project by its name or by a security vulnerability that affects the project's published inventory.

Searching by Project Name

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

- The name you enter is case-insensitive.
- The name you enter can have any character (letters, numbers, and special characters) in it.
- Partial matches are supported.



Task

To search by project name, do the following:

1. Navigate to the **Project List** page.
2. Select **Project Name** from the first search drop down.
3. Type a project name in the **Enter Project Name** field. The list of projects will change to reflect the search result.
4. (Optional) Click the name of a project to display more information about the project:
 - If the project contains published inventory items, the **Inventory Items** pane appears.
 - If the project does not contain published inventory items, the **Project Summary** page appears. For information on publishing inventory, see [Publishing Inventory](#).

Searching by Security Vulnerability ID

When you search projects by inventory items with a specific associated security vulnerability, the following rules apply:

- Only one vulnerability may be entered as a search criteria.
- Spaces are not supported.
- Only exact matches by vulnerability name are supported. Partial matches are not supported.
- Only published inventory items are searched.
- Vulnerability IDs are not validated. If you enter an invalid ID, the search will not return any projects.



Task

To search by security vulnerability ID, do the following:

1. Navigate to the **Project List** page.
2. Select **Security Vulnerability** from the first search drop down.
3. Type the ID of the vulnerability in the **Enter Vulnerability ID** field and press **Enter**. The list of projects changes to reflect the search result. If there are no inventory items with the associated vulnerability for the specified ID, the project list will remain the same.
4. (Optional) Click the name of a project to display more information about the project:
 - If the project contains published inventory items, the **Inventory Items** pane appears.
 - If the project does not contain published inventory items, the **Project Summary** page appears. For information on publishing inventory, see [Publishing Inventory](#).

Filtering Inventory on the Project Dashboard

After you create a project, and upload and scan a codebase, you can quickly filter inventory to view potential problems and take steps to eliminate red (high exposure items) from your project inventory.



Task

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

1. Point to a chart and click on a colored area. The **Project Inventory** tab appears with the matching project inventory items listed in the **Inventory Items** pane. You can also point to corresponding colors in the legends below the charts to filter your inventory.
2. Click on a project inventory item listed to see more detail in the right pane of the **Project Inventory** tab.



Note • You can click on other vulnerability levels such as those in green or yellow to filter your project inventory.

Managing a Project

The following topics describe how to use features on the **Project Summary** page to manage the currently opened project:

- [Using the Project Summary Page](#)
- [Generating Reports](#)
- [Editing the Project Definition and General Settings](#)
- [Updating Scan Settings for a Project](#)
- [Connecting the Project to Remote Data Sources](#)
- [Changing Project Owners](#)
- [Exporting Project Data](#)


Using the Project Summary Page

When you open a project from the **Project List** page, the **Project Summary** page 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 Project Summary page:

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 **Project Summary** page for the project.

Generating Reports

From the **Project Summary** page, 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 the **Project Summary** page for the project (see [Using the Project Summary Page](#)).
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 Excel and JSON format:
 - **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 **Project Summary** page for the project (see [Using the Project Summary Page](#)).
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*, etc.) 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 that identifies all open source/third party components that it contains.



Note • Only published inventory items will be included in the **Notices** report.

The following items may appear in the **Notices** report:

- **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 blank, FlexNet Code Insight uses the associated component URL. If both are blank, no URL will appear in the report.
- **Inventory Notices Text**: If the **Notices Text** field of the **Inventory Details** panel is empty, FlexNet Code Insight uses the contents of the **As-Found License Text** field. If the **As-Found License Text** field is blank, FlexNet Code Insight uses the selected license's license text.



Note • If no selected license exists, the Notices report will contain the inventory name and the URL (if available) but no text below.

Adding Text for Notices Reports

If you want specific text to appear in the **Notices** report, you must first enter that text in the **Notice Text** field on the **Inventory Details** panel.



Task

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

1. Navigate to the **Analysis Workbench**. The **Analysis Workbench** appears.
2. Select an item from the list in the **Inventory Items** panel.
3. In the center panel, select **Inventory Details**. Information appears in the fields of the **Inventory Items** panel.
4. Scroll down the panel until the **Notice Text** field appears:

5. Type text that pertains to the select inventory item in the field. You can use the basic text editing tools to alter the look of your text.
6. Select **Save** to save your changes. The text you typed will appear in the Notices Report for this inventory item.

Generating the Notices Report



Task

To generate a Notices Report, do the following:

1. Navigate to the **Project Summary** page for the project (see [Using the Project Summary Page](#)).
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.

Editing the Project Definition and General Settings

After you create a project, you can edit its definition and general settings, including the project's association with a specific policy profile. You can also configure settings that automate the review and remediation task flow for the published inventory.



Task

To update project settings:

1. As the Project Owner, navigate to the **Project Summary** page (see [Using the Project Summary Page](#)).
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:

1. As the Project Owner, navigate to the **Project Summary** page (see [Using the Project Summary Page](#)).
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.

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 [Chapter 7, Configuring Source Code Management](#).

ALM Settings

FlexNet Code Insight provides plugins that allow integration with Application Lifecycle Management (ALM) systems. These ALM plugins are used to create and manage work items in the ALM system directly from Code Insight so that inventory requiring further review and remediation can be tracked externally as part of the user's existing workflow system. To configure an ALM plugin, the system or application administrator must create instances of the ALM system in Code Insight, a process described in the *FlexNet Code Insight Installation and Configuration Guide*.

In order to create and manage work items for a 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 offers a Jira plugin. 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:

1. As the Project Owner, navigate to the **Project Summary** page (see [Using the Project Summary Page](#)).
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.
 - 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 2-1 • 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
\$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:

1. As the Project Owner, navigate to the **Project Summary** page.
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 first created the project will automatically become the 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 **Project Summary** page (see [Using the Project Summary Page](#)).
3. Open the **Manage Project** dropdown menu and select **Change Owner**. The **Select new project owner** dialog appears.



Note • If you have not logged in as *administrator* or *project owner*, you will not see the **Change Owner** button in the **Owner** field.

4. Highlight a name in the list and click **Apply**. The **Project Summary** page appears 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 **Project Summary** page.

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 [Exporting & Importing Project Data](#).



Task

To export project data, do the following:

1. As Project Owner, navigate to the **Project Summary** page (see [Using the Project Summary Page](#)).
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 [Exporting & Importing Project Data](#).

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 Analysts, Reviewers and Observers to a Project](#).



Note • Users who have Administrator privileges but are not part of a Private project will be able to see projects in the project folders tree, view only the Summary page 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 projects unless the user has the rights to see private projects.

8. (Optional) Assign roles to users who will interact with the private project. For more information, see [Assigning Analysts, Reviewers and Observers to a Project](#).

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 system administrator grants the **Policy Management** permission to users who have rights to manage policy profiles. Typically, these would be legal or security users. (For more information, see “Creating a User” in the *FlexNet Code Insight Installation and Configuration Guide*.)

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.

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:

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:

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

You can associate the project with a policy profile when the project is created (see [Creating a Project](#)) or later by editing project (see [Editing the Project Definition and General Settings](#)) as described here. 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. There are many combinations of search criteria you can use depending upon the type of inventory you want to find. The following table, which is arranged by persona (job function/department), presents a number of advanced searches and their typical results:

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
Any	By Inventory, Component or License keyword	Inventory of interest based on full or partial inventory, component or license name. Useful when you want a quick search for a specific component or license across all of your inventory items.	Inventory Name = <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
Any	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>Option 1: Inventory Priority = <i>P1</i></p> <p>Option 2: Security Vulnerability Severity = <i>High Severity (CVSS 7.0 - 10.0)</i> or License Priority = <i>P1 - Viral/Strong Copyleft</i></p>
Any	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>
Any	By Dependencies	<p>Only dependency inventory items (both first-level and transient 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>
Any	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
Any	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>
Any	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>
Any	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><Username></i> (selected user)</p>
Security Analyst	By Vulnerability ID	<p>Inventory with a specific vulnerability (NVD CVE or Secunia Advisory).</p> <p>Useful when you are looking for inventory exposing you to a specific security issue, typically a newsworthy event.</p>	<p>Security Vulnerability ID = <i>SA71946</i></p>
Security Analyst	By Security Risk Exposure	<p>Inventory containing security vulnerabilities of a specified severity.</p> <p>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.</p>	<p>Security Vulnerability Severity = <i>High Severity (CVSS 7.0 - 10.0)</i></p>

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
Security Analyst	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>
Security Analyst	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>
Security Analyst	By Inventory Alert	Published inventory items that have new security vulnerability alerts or that have been rejected due to new non-compliant security vulnerabilities. You can select one or both options. 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>
Security Analyst	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.	Review Status = <i>Approved</i> and Security Vulnerability Age = <i>Last 7 days</i>
Legal	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.	License Priority = <i>P1 - Viral/Strong Copyleft</i>

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
Analyst	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.	Inventory Review Status = <i>Approved</i> and License Priority = <i>No License Found</i>
Eng. Mgr./ Final Reviewer	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.	Inventory Review Status = <i>Approved</i> or License Priority = <i>P1 - Viral/Strong Copyleft</i> or Security Vulnerability Severity = <i>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 **Project Summary** page. 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 may 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 **Project Summary** page. See [Project Summary Page](#) 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.eyJzdWIiOiJqcWVhW4iLCJ1c2VySWQiOiJEWLCjYXQjE1MTA5NjM2NzZ9" > 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 for Projects](#). 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)
Target Project: Inventory Only	<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>
Target Project: Standard (scanned data)	Not supported.	 <p>Note • <i>Requires a scan before import.</i></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.

Automated Analysis

This section discusses the automated analysis features of FlexNet Code Insight. The following topics are covered in this section:

- [What is Automated Analysis?](#)
- [Supported Package Managers](#)
- [Supported File Extensions](#)
- [Supported Archive Formats](#)
- [Additional Rule-based Detection Capabilities](#)

What is Automated Analysis?

FlexNet Code Insight provides automated analysis capability to scan specific software packages and create inventory items that can be manually reviewed by analysts. Each electronic update provides additional data and quality to the automated analysis capability.

The following are ways to use the automated analysis capabilities:

- FlexNet Code Insight standard scan that results in the creation of inventory items.
- Scan plugins that perform a scan remotely on an engineering server, and send data back to FlexNet Code Insight to create inventory.

Supported Package Managers

FlexNet Code Insight is capable of analyzing the following types of files:

- Bower
- Maven/Gradle
- Ruby Gem

- NPM
- CocoaPods
- NuGet
- RPM packages

Security vulnerabilities are verified against the [National Vulnerability Database](#).

Supported File Extensions

The following filename extensions are processed during automated discovery scanning:

Table 5-1 • Supported File Extensions

deb	dll	dmg
dylib	exe	gem
gemspec	gz	gradle
htm	html	js
json	jsp	lock
nuget	nupkg	nuspec
patch	podspec	rpm
sig	sign	udeb
xml		



Note • The automated analysis returns optimal results when access to the internet is available.

Supported Archive Formats

During automated discovery scanning, archive files are deflated and the contents of those archives are scanned. The following archive formats as expressed by the filename extensions are supported:

Table 5-2 • Supported Archive Formats

bz2	bzip2	cab
cpio	dmg	ear

Table 5-2 • Supported Archive Formats

gzip	.gz	iso
jar	msi	tar
tarz	tbz2	tgz
7z	war	xz
zip		

Additional Rule-based Detection Capabilities

The automated detection 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. FlexNet Code Insight provides the facility to create a project and scan it without having to upload a codebase, providing integration between FlexNet Code Insight and the development system. The FlexNet Code Insight scanner can scan a codebase wherever it resides and represent the identified inventory items for stakeholder review. This is inventory-only scanning.

The following is the overall process for creating an inventory-only project and performing a scan on a remote codebase:

1. Create an inventory-only project in FlexNet Code Insight. See [Creating a Project](#).
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 Installation and Configuration Guide*.
3. Install and configure a scan agent plugin. For information on installing and configuring a scan agent plugin, see “Installing & Configuring FlexNet Code Insight Plugins” in the *FlexNet Code Insight Installation and Configuration Guide*. 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. FlexNet Code Insight ships with a set of standard plugins that are described in the *FlexNet Code Insight Installation and Configuration Guide*.
4. 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 provides the following plugins:

- **Jenkins**: Allows automated scanning of a Jenkins workspace as part of the build process.
- **Artifactory**: Allows automated scanning of Artifactory repositories as to identify non-compliant artifacts.
- **Docker**: Allows automated scanning of Docker images on a Docker server.
- **Bamboo**: Allows automated scanning of a Bamboo workspace as part of the build process.
- **Maven**: Allows automated scanning of Maven projects as part of the build process.
- **Gradle**: Allows automated scanning of Gradle projects as part of the build process.
- **Ant**: Allows automated scanning of Apache Ant as part of the build process.
- **Visual Studio**: Allows automated scanning of a VSTS workspace as part of the build process.
- **TeamCity**: Allows automated scanning of TeamCity projects as part of the build process.
- **GitLab**: Allows automated scanning of GitLab projects as part of the build process.
- **Generic plugin**: Can be copied and altered to perform specific FlexNet Code Insight scanning tasks that you want to incorporate into your workflow. You can download the generic plugin example from the Flexera Product License Center (PLC).

Requirement Considerations

The following lists general plugin requirements:

- In general, the Code Insight plugins require a minimum of 4GB heap for scanning. The heap size may need to be adjusted based on the number of parallel scans to be executed.
- For the Docker images plugin, ensure that your environment has a minimum of 2GB heap space and is configured with a 64-bit JRE to support that amount of heap space.
- The Jenkins Scan Agent plugin requires 64-bit JVM and that you run the scan agent as a Jenkins Slave.

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 on 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](#)



Note • Ensure that you have read the “Integrating with SCM” section in the “FlexNet Code Insight Installation and Configuration Guide” before performing the procedures in this section.

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:

1. Navigate to the **Project Summary** page. For more information about editing projects, see [Editing the Project Definition and General Settings](#).
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:**

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
Git Repository URL	<p>Provide the repository URL in either format:</p> <ul style="list-style-type: none">• <code>http(s)://<host.xz>/<path>/to/repo.git</code>• <code><user>@<host>:<path>/repo.git</code> <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><scanroot>/<projectID>/<instanceID></code></p>
Git Username	<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>
Git Password	<p>Enter the password associated with the user name provided.</p>
Git Branch, Git Tag, or Git Commit ID	<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:

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. 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
URL (P4PORT)	<p>Provide the URL of the Perforce instance with which to synchronize. Note the following example URL formats.</p> <p>For a TCP connection:</p> <p style="text-align: center;">tcp:<P4 Server>:<P4 Port></p> <p>For an SSL connection:</p> <p style="text-align: center;">ssl:<P4 Server>:<P4 Port></p>
Username (P4USER)	Provide the user name that has access to the Perforce depot to which this instance is synchronizing.
Password (P4PASSWD)	<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>
Branch Spec (P4CLIENT)	Provide the path to the branch to which this instance is synchronizing.
Changelist No	(Optional) Provide a changelist number only if this instance is synchronizing to a particular changelist. Otherwise, this value defaults to the latest revision.
Label	(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 Performe SCM instance:

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

Performe SCM Instance Setting	Description
TFS URL	<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> <p style="text-align: center;"><code><protocol>:<tfs_host>:<port>/<collection>/<project></code></p> <p>For earlier versions of TFS:</p> <p style="text-align: center;"><code><protocol>:<tfs_host>:<port>/<collection>/<tfsroot>/<project></code></p>

Table 7-3 • Settings Used to Configure a TFS SCM Instance

Perforce SCM Instance Setting	Description
Username	<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>
Password	<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>
Changeset	<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 Label description next), the label is ignored, and the instance synchronizes to the changeset.</p>
Label	<p>(Optional) Provide a specific label to which the TFS SCM instance is synchronizing.</p> <p>If a label and changeset (see the previous Changeset description) are both specified, the label is ignored, and the instance synchronizes to the changeset instead.</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 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 Page](#)
- [Edit Project: General Tab](#)
- [Edit Project: Scan 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
analyzed	Displays the number of lines of code that have been analyzed since FlexNet Code Insight was installed.
scanned	Displays the number of lines of code that have been scanned since FlexNet Code Insight was installed.
identified	Displays the number of OSS items that were identified in your codebase.
go to project	Select this option to go to the list of projects that have been created.
view policy	Select this option to view a list of policies that have been created.
administration	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 Tab](#)[Electronic Updates Tab](#)[Email Server Tab](#)[LDAP Tab](#)[ALM Tab](#)[Scan Servers Tab](#)[Scan Profiles Tab](#)

Users Tab

The **Users** tab is where you can 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
Add User	Click to display the Add User dialog.
Login	Displays the login of each user that has been added.
First Name	Displays the first name of each defined user.
Last Name	Displays the last name of each defined user.
Email	Displays the email address of the user associated with the login.
Actions	This column contains the pencil icon (✎). Click it to open the Edit User dialog, where you can edit information about the selected user.
Search	Click this button to open the Search for Users dialog, on which you can search for specific users who fit the criteria you enter.

See Also[Add User Dialog](#)[Edit User Dialog](#)

Add User Dialog

The **Add User** dialog is where you can 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
Login	Enter the login of the new user.
First Name	Enter the first name of new user.
Last Name	Enter the last name of new user.
Email	Displays the email address of the user associated with the login. To change the user's email address, type over the existing email address.
Password	The current password is not displayed in this field. A user with <i>Administrator</i> permission can type a new password in this field.
Password Confirm	The current password is not displayed in this field. A user with <i>Administrator</i> permission can type a new password in this field.
Question	The prompt that the user must answer to retrieve a forgotten password.
Answer	The answer to the question in the previous field.
Permissions	<p>Displays the permission that the selected user has or can have:</p> <ul style="list-style-type: none">● Administrator: Grants the new user permission to add other users and perform additional FlexNet Code Insight administration tasks.● Policy Management: Grants the new user permission to create, edit, and delete policies. <p>To grant a permission, select the checkbox in front of the permission type. A user may have both permissions.</p>
Submit	Select Submit to have the system save your user edits. A prompt appears to notify you that your edits have been saved.
Cancel	Select Cancel to return to the Administration Users tab without saving your changes.

See Also
[Users 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
Login	Displays the login of the selected user. This field is read-only and cannot be changed.
First Name	Displays the first name of selected user. To change the user's first name, type over the existing name.
Last Name	Displays the last name of selected user. To change the user's last name, type over the existing name.
Email	Displays the email address of the user associated with the login. To change the user's email address, type over the existing email address.
Password	The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.
Password Confirm	The current password is not displayed in this field. A user with Administrator permission can type a new password in this field.
Question	The prompt that the user must answer to retrieve a forgotten password.
Answer	The answer to the question in the previous field.
Permissions	<p>Displays the permission that the selected user has or can have:</p> <ul style="list-style-type: none">● Administrator: Grants the new user permission to add other users and perform additional FlexNet Code Insight administration tasks.● Policy Management: Grants the new user permission to create, edit, and delete policies. <p>To grant a permission, select the checkbox in front of the permission type. A user may have both permissions.</p>
Submit	Select Submit to have the system save your user edits. A prompt appears to notify you that your edits have been saved.
Cancel	Select Cancel to return to the Administration Users tab without saving your changes.

See Also
[Users Tab](#)

Electronic Updates Tab

The **Electronic Updates** tab is where you can select the frequency of electronic updates. The tab contains the following columns and fields:

Table 8-5 • Electronic Updates tab

Column/Field	Description
Schedule Update	Displays the login of the selected user. This field is read-only and cannot be changed.
Update Frequency	
Frequency Dropdown	Select from one of the available frequencies: <ul style="list-style-type: none">• Never• Daily• Weekly
Time Dropdown	If you selected Daily or Weekly from the Frequency dropdown, the Time dropdown becomes available. Select a time of day when you want the Electronic Update to occur.
Day Dropdown	If you chose Weekly from the Frequency dropdown, select a day of the week when the Electronic Update is to occur.
Save	Select Save to save your user edits. A prompt appears to notify you that your edits have been saved.

Email Server Tab

The **Email Server** tab is where you can enable email and set email options. The tab contains the following columns and fields:

Table 8-6 • Email Server tab

Column/Field	Description
Enable Email Server	Select Yes to enable FlexNet Code Insight to use the email server or No to leave it disabled. The default is No . The rest of the fields on this page are not available until you select Yes .
Sender's Email Address	Enter the email address of the sender.
SMTP Host Name	Enter the Simple Mail Transfer Protocol (SMTP) host name.
SMTP Host Port	Enter the port number of the SMTP host.

Table 8-6 • Email Server tab (cont.)

Column/Field	Description
SMTP User Name	Enter the SMTP user name. This field is optional. Leave it blank if you are using anonymous SMTP.
SMTP User Password	Enter the SMTP user password. This field is optional. Leave it blank if you are using anonymous SMTP.
Enable SMTP over TLS	Select Yes to use Transport Layer Security (TLS) to secure email over SMTP or select No to leave this option disabled.


LDAP Tab

The **LDAP** tab is where you can 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
Enable LDAP	Select Yes or No to determine if LDAP will be used for user authentication. The default is No .
LDAP Connection Details	
LDAP URL	The URL of your LDAP server. For example, <code>ldap://<ldap_server_host>:<ldap_port> ldap://ad.mycompany.com:389</code> .
Authentication Type	Select the type of LDAP authentication that will be used: <ul style="list-style-type: none">● Anonymous: If you select this option, the LDAP Username and LDAP Password fields in this section remain disabled.● Authenticated: If you select this option, the following LDAP fields are enabled.
LDAP Username	A text field in which you can specify the LDAP username. This field is disabled if anonymous authentication is selected.
LDAP Password	A masked text field in which you can specify the password for the username specified in the field above. This field is disabled if anonymous authentication is selected.
LDAP Query Details	
LDAP Base	The base node of the LDAP server.
LDAP Search Base	The Search Base, along with the Search Query, are used to query a list of users for synchronizing with FlexNet Code Insight.

Table 8-7 • LDAP tab (cont.)

Column/Field	Description
LDAP Search Query	The search query for your LDAP server. For example, (&(objectClass=person)(memberOf=CN=SCAGroup,CN=Users,DC=ad,DC=mycompany,DC=com)).
Use Paging	Select Yes if the LDAP server has paging enabled. Select No if the server does not have paging enabled. If you select Yes , the LDAP Page Size field is enabled.
LDAP Page Size	The default page size is 1000 elements.
LDAP User Sync Frequency	<p>These fields are used to set the frequency at which FlexNet Code Insight will synchronize user data with the LDAP server:</p> <ul style="list-style-type: none"> ● Never: The default value, which indicates that automatic user sync is disabled and will only occur if the user clicks the Sync Now button. For all other values, automatic user sync is enabled per the configured frequency. ● Hourly: Enter an integer value representing the number of hours between user syncs ● Daily: Select a time at which the user sync will run every day. ● Weekly: Select a day of the week and a time of the day when the user sync will run each week.
LDAP User Property Mappings	
Login	Enter the LDAP user property field representing the user's login.
First Name	Enter the LDAP user property field representing the user's first name.
Last Name	Enter the LDAP user property field representing the user's last name.
Email	Enter the LDAP user property field representing the user's email address.
Login Filter	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.
Save	Click this button to save any changes you made to the fields on the LDAP tab.
Test LDAP Server Connection	Click this button to test the connection to the LDAP server.
Sync Now	Click this button to force a user sync.
	 <p>Note • This button is disabled if a user sync is currently running</p>

ALM Tab

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

Table 8-8 • ALM tab (cont.)

Column/Field	Description
Default Summary Text	Default text to display as a summary for the issue on the ALM server. The text supports the following Code Insight variables: \$PROJECT_NAME, \$INVENTORY_ITEM_NAME, \$COMPONENT_NAME, \$VERSION_NAME, \$LICENSE_NAME, \$NUMBER_VULNERABILITIES, \$NUMBER_FILES, or \$INVENTORY_URL.
Default Description	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 is where you can edit information about your scan server. The tab contains the following columns and fields:

Table 8-9 • Scan Servers tab

Column/Field	Description
Scan Servers	The name of your scan server.
Edit	Select this button to edit the server configuration for the scanner you selected in the Scan Servers field.
New	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
Alias	The name of your scan server.
Host	The IP address of your scan server host computer. If the scan server is on the same machine as the core server, enter localhost .
Port	The number of your scan server host port. By default, the port is 8888.

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

Column/Field	Description
CL Path	The FlexNet Code Insight Compliance Library will be provided on an USB SSD drive. Using FlexNet Code Insight's automated discovery, you are able to perform a scan even before obtaining the Compliance Library or setting up a scan server. For more information, see the FlexNet Code Insight User Guide.
Codebase Path	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.
Save	Click this button to save any changes you made to the fields on the Scan Server dialog.
Cancel	Click this button to cancel any changes you made to the fields on the Scan Server dialog.


See Also

[Scan Servers Tab](#)

Scan Profiles Tab

The **Scan Profiles** tab is where you can 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
Scan Profiles 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">● Standard Scan Profile● Basic Scan Profile (without CL)● Comprehensive Scan Profile <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 Create/Edit Scan Profile Dialog.</p> <ul style="list-style-type: none">● Scan Archives—Whether the scanner will perform package discovery and license detection within all archive files in the project codebase.● Dependencies—The level of component-dependency scanning to be performed by the scanner.● Exact Matches—Whether scanner is to identify those codebase files that exactly match file information in the CL (Compliance Library).● Source Code Matches—Whether the scanner is to identify code strings in the scanned codebase files that exactly match strings in the CL (Compliance Library).● Edit icon—Click  at the end of a scan profile entry to edit the profile. The Create (or Edit) Scan Profile dialog is opened, showing the scan profile details.
Add Scan Profile button	Select this button to create a new scan profile.

See Also

[Create/Edit Scan Profile Dialog](#)

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
Perform Package/License Discovery in Archives	Select this option to have the scanner recursively perform package discovery and license detection within all archive files encountered in the project codebase.
Dependency Support	<p>Determine the level of dependency scanning to be performed by the scanner. The available options include:</p> <ul style="list-style-type: none"> ● No Dependencies: Only top-level inventory items are reported without any dependencies. (Default) ● Only First Level Dependencies: Only first-level (or direct) dependencies are reported along with top-level inventory items. ● All Transitive Dependencies: 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. <p>This option is supported only for Java/Maven through <code>pom.xml</code> files and NPM through <code>package.json</code> files. Additional technologies will be supported in future releases.</p>
Automatically Add Related Files to Inventory	Select this option to have the system associate additional files to existing inventory items based on the data available in automatic detection rules. The automatic file mappings are marked with either high or low confidence.
Exact Matches	Select this option to have the scanner record exact matches for scanned files based on data from the Compliance Library (CL).
Source Code Matches	Select this option to have the scanner record source code matches for scanned files based on data from the Compliance Library (CL).
Include System Identified Files	(Available only when Source Code Matches is selected) Select this option if you want the scanner <i>not</i> to perform source code matching for files that are already associated with one or more inventory items.
Include Files with Exact Matches	(Available only when Source Code Matches is selected) Select this option if you want the scanner <i>not</i> to perform source code matching for files that have exact matches.
Search Terms	Provide a list of search terms to be used in the scan.
Scan Exclusions	Provide a list of file extensions to be excluded from the scan.

See Also
[Scan Profiles Tab](#)

Project Defaults Tab

The **Project Defaults** tab defines options that are global for all projects, but you can override them at the project level.

Currently this tab enables you to set **Task Flow Options** settings only.

Task Flow Options settings can automate the status notification, review, and remediation process for published inventory and generally work in conjunction with the policy profile associated with the project. For example, you can define the automatic creation of tasks and work items that track the review and remediation process for inventory items rejected by policy. You can also define the task flow for those items that result in a **Not Reviewed** status because policies do to apply to the items.

To override the **Task Flow Options** settings at the project level, see [Editing the Project Definition and General Settings](#).

For more information about policies, refer to [Managing Policy Profiles](#) in the “Using FlexNet Code Insight” chapter. (Also see [Policies Page](#) and [Policy Details Page](#) for information about the criteria you can define in policies.)

The **Project Defaults** tab contains the following fields:


Table 8-13 • Project Defaults tab

Column/Field	Description
When an inventory item is: impacted by a new vulnerability that violates your policy, auto-reject the inventory item	<p>This field defines what action the system should take if an inventory item is affected by a new security vulnerability (discovered during scanning or via electronic update).</p> <p>When a new security vulnerability with a CVSS score or severity <i>greater than</i> the threshold configured as policy for the Code Insight project, select this checkbox to automatically reject those project inventory items impacted by the vulnerability. (This rejection also applies to inventory items previously approved.) To indicate that an inventory item has been rejected due to new vulnerabilities, an alert icon is automatically added to the entry for each impacted inventory item on the Project Inventory tab.</p> <p>If you leave the checkbox unselected, the status of inventory items impacted by the new vulnerability remains as is.</p> <p>Note that security alerts are generated only when an electronic update, performed <i>post-scan</i>, discovers new vulnerabilities.</p> <p>For information about setting policies that define vulnerability CVSS and severity thresholds for automatic rejection or approval of inventory items, see Policies Page and Policy Details Page.</p>

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

Column/Field	Description
When an inventory item is: neither approved nor rejected by policy	<p>This field defines what action the system should take if the inventory item is <i>not</i> affected by policy (during publishing of inventory as part of a scan or manual publishing by a user).</p> <p>When Code Insight automatically publishes the inventory, define the action or action sequence that should be triggered automatically for those inventory items not automatically approved or rejected by policy:</p> <ul style="list-style-type: none">● take no action—Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab.● send an email notification—In addition to showing the Not Reviewed status for the inventory item, automatically send an email to the project owner, informing the project owner of the need to manually review the item. The minimum priority value affects this option.● create a review task—In addition to showing the Not Reviewed status for the inventory item, automatically create a review task assigned to the project owner and send an email, notifying the project owner about task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) The minimum priority value affects this option.● create a review task with an external work item—In addition to showing the Not Reviewed status for the inventory item, perform the following:<ul style="list-style-type: none">● Automatically create a review task assigned to the project owner and send an email to notify the project owner about the task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.)● Automatically associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). Code Insight creates the work item using the settings for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter. <p>The minimum priority value affects this option.</p>

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

Column/Field	Description
When an inventory item is: rejected by policy	<p>This field defines what action the system should take if an inventory item is automatically rejected by policy (during publishing of inventory as part of a scan or manual publishing by a user).</p> <p>Select the action or action sequence that should be automatically triggered when an inventory item is rejected by policy:</p> <ul style="list-style-type: none"> • take no action—Simply show the status of the inventory item as Reject on the Project Inventory tab. • send an email notification—Automatically send an email, informing the project owner of the need to perform remediation work on the component. • create a remediation task—Automatically create a remediation task assigned to the project owner and send an email, notifying the project owner about task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) • create a remediation task with an external work item—Perform the following: <ul style="list-style-type: none"> • Automatically create a remediation task assigned to the project owner and send an email, informing the project owner about the task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) • Automatically associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). Code Insight creates the work item using the settings for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter.
minimum priority	<p>Select the minimum inventory priority (P1, P2, P3, or P4) to which the values for neither approved nor rejected apply.</p> <p>For example, if neither approved nor rejected by policy is set to send email notification and minimum priority is set to P3, then the email notification will only be sent out for P1, P2, and P3 inventory items that are not affected by policy. No email notification will be sent for P4 items.</p> <p></p> <p>Note • This option has no effect on the take no action value for neither approved nor rejected by policy.</p>

See Also[Policies Page](#)[Policy Details Page](#)[Managing Policy Profiles](#)[Creating and Managing Tasks for Project Inventory](#)[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
Tree view 	Click to change the display to a tree view.
List view 	Click to change the display to a list view.
Add New	Click to add a new folder or project to the list.
Projects (x)	Lists the number of projects in the system.
Project Search fields	The first dropdown allows you to search projects by project name or security vulnerability name. The second dropdown allows you to specify a name to search for.
Name	A hyperlinked list of the names of all projects in the system. When you select a project from the list, information about the project appears in the panes of the Project Summary page. Click the arrow to toggle the list from A to Z or from Z to A.
Selected Project Name	When you select a project from the list, the name of the selected project appears in this field. You can click the selected project name to open the project.
Owner	The hyperlinked name of the person who owns the project. Click the name to open your default email program to send an email to the project owner.
Profile	Displays the name of the profile attached to the selected project. If no profile is attached to the project, “No profile selected” appears.
Created	Displays the data that the project was created.
Last Scan	Displays the date that the codebase was last scanned.

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

Column/Field	Description
Project Summary Graphs	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 Page](#)

Project Summary Page

The **Project Summary** page is where you can 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 • Projects Summary page

Column/Field	Description
Project Details	
Name	The name given to the selected project and its Id number.
Owner	The hyperlinked name of the person who owns the project. Click the name to open your default email program to send an email to the project owner.
Description	A description, if entered, of the project appears in this field.
Project Type	<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">● Inventory Only: processes all published inventory, with inventory details, fields and file associations.● Standard: processes all inventory, with inventory details, fields and file associations, as well as all files that are marked as reviewed.
Project Visibility	<p>The visibility of the project:</p> <ul style="list-style-type: none">● Public: All users in the system can view and change the project.● Private: Sensitive information is hidden from general view, and only select users can view the project.

Table 8-15 • Projects Summary page (cont.)



Column/Field	Description
Project Risk	The project vulnerability risk value: <ul style="list-style-type: none"> • Low • Medium • High
Scan Settings	
Policy Profile	The name of the profile attached to this project.
Scan Profile	The name of the scan profile associated with this project. Click  to view the details of the scan profile.
Scan Paths	The location of your codebase. Click  to view the details about the scan server.
Scan Status	
Scan Status	Notifies you of scheduled scans. Click the hyperlinked here to schedule a scan.
Last Scan	Displays the date that the codebase was last scanned.
Past Scans	Click the hyperlinked text 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.
Reports	
Audit Report	Displays the status of the audit report. If a report is not available, click Generate Audit Report to create one.
Notices Report	Displays the status of the notices report. If a report is not available, click Generate Notices Report to create one.
Start Scan	Click to immediately scan your codebase.
Generate Report	Click to generate a Project, Audit, or Notices report in the background to display later.
Upload Project Codebase	Click to add or change the codebase that will be scanned for the selected project.

Table 8-15 • Projects Summary page (cont.)

Column/Field	Description
Manage Project	A dropdown menu that allows you to perform actions on the selected project: <ul style="list-style-type: none">• Edit Project• Edit Project Users• Export Project Data• Delete Project• Change Owner

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
Project Name	The name of the selected project. You can change the name by typing over the current project name.
Description	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.
Project Visibility	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.
Project Risk	The current vulnerability risk value (Low, Medium, or High) for the project. To edit, select another value from the dropdown.
Project Folder	<p>The folder in which the project is currently stored. To edit, select a different folder from the Select a New Folder dropdown. Alternatively, click Clear Project Folder to move the project to the root folder:</p> <ul style="list-style-type: none">● Clear Project Folder button—Click this button to remove the project from the current folder and place it in the root folder.● Select a New Folder dropdown—Click the down arrow to locate and select the folder to which to move the project.
Policy Profile	<p>The policy profile currently enabled for the project. To associate the project with a policy profile or switch to another profile, select the policy profile from the Policy Profile dropdown.</p> <p>To view the policies defined in the selected policy profile, click the down arrow next to View Policy Details. These policies enable Code Insight to automatically review published items and mark them as Approve, Reject, or Not Reviewed. For a description of policies available for a policy profile, see Policy Details Page.</p> <p>For more information about policy profiles in general, see Managing Policy Profiles in the “Using FlexNet Code Insight” chapter.</p>
Task Flow Options	
Once inventory items are marked as Approve , Reject , or Not Reviewed , you can use the following options to define an automated workflow to help you obtain a final, approved inventory more efficiently.	


Table 8-16 • Edit Project: General tab (cont.)

Column/Field	Description
When an inventory item is: impacted by a new vulnerability that violates your policy, auto-reject the inventory item	<p>This field defines what action the system should take if an inventory item is affected by a new security vulnerability (discovered during scanning or via electronic update).</p> <p>When a new security vulnerability with a CVSS score or severity <i>greater than</i> the threshold configured as policy for the Code Insight project, select this checkbox to automatically reject those project inventory items impacted by the vulnerability. (This rejection also applies to inventory items previously approved.) To indicate that an inventory item has been rejected due to new vulnerabilities, an alert icon is automatically added to the entry for each impacted inventory item on the Project Inventory tab.</p> <p>If you leave the checkbox unselected, the status of inventory items impacted by the alert remains as is.</p> <p>Note that security alerts are generated only when an electronic update, performed <i>post-scan</i>, discovers new vulnerabilities.</p> <p>For information about setting policies that define vulnerability CVSS and severity thresholds for automatic rejection or approval of inventory items, see Policies Page and Policy Details Page.</p>
When an inventory item is: neither approved nor rejected by policy	<p>This field defines what action the system should take if the inventory item is not affected by policy (during publishing of inventory as part of a scan or manual publishing by a user).</p> <p>When Code Insight automatically publishes the inventory, define the action or action sequence that should be triggered for those inventory items not automatically reviewed by policy:</p> <ul style="list-style-type: none"> ● take no action—Simply show the status of the inventory item as “Not Reviewed” on the Project Inventory tab. ● send an email notification—In addition to showing the Not Reviewed status for the inventory item, automatically send an email to the project owner, informing the project owner of the need to manually review the item. The minimum priority value affects this option. ● create a review task—In addition to showing the Not Reviewed status for the inventory item, automatically create a review task assigned to the project owner and send an email, notifying the project owner about task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) The minimum priority value affects this option.

Table 8-16 • Edit Project: General tab (cont.)

Column/Field	Description
neither approved nor rejected by policy (cont.)	<ul style="list-style-type: none"> ● create a review task with an external work item—In addition to showing the Not Reviewed status for the inventory item, perform the following: <ul style="list-style-type: none"> ● Automatically create a review task assigned to the project owner and send an email to notify the project owner about the task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) ● Automatically associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). Code Insight creates the work item using the settings for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter. <p>The minimum priority value affects this option.</p>

Table 8-16 • Edit Project: General tab (cont.)

Column/Field	Description
When an inventory item is: rejected by policy	<p>This field defines what action the system should take if an inventory item is automatically rejected by policy (during publishing of inventory as part of a scan or manual publishing by a user).</p> <p>Select the action or action sequence that should be automatically triggered when an inventory item is rejected by policy:</p> <ul style="list-style-type: none"> ● take no action—Simply show the status of the inventory item as Reject on the Project Inventory tab. ● send an email notification—Automatically send an email, informing the project owner of the need to perform remediation work on the component. ● create a remediation task—Automatically create a remediation task assigned to the project owner and send an email, notifying the project owner about task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) ● create a remediation task with an external work item—Perform the following: <ul style="list-style-type: none"> ● Automatically create a remediation task assigned to the project owner and send an email, informing the project owner about the task. (The project owner can then reassign the task to the appropriate user, such as an engineer or a legal or security expert. For details about reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) ● Automatically associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). Code Insight creates the work item using the settings for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter.
minimum priority	<p>Select the minimum inventory priority (P1, P2, P3, or P4) to which the values for neither approved nor rejected apply.</p> <p>For example, if neither approved nor rejected by policy is set to send email notification and minimum priority is set to P3, then the email notification will only be sent out for P1, P2, and P3 inventory items that are not affected by policy. No email notification will be sent for P4 items.</p> <p></p> <p>Note • This option has no effect on the take no action value for neither approved nor rejected by policy.</p>

See Also
[Policies Page](#)
[Policy Details Page](#)
[Managing Policy Profiles](#)
[Creating and Managing Tasks for Project Inventory](#)
[Creating and Viewing External Work Items for a Project Inventory Task](#)
[ALM Settings](#)

Edit Project: Scan Settings Tab

The **Edit Project: Scan Settings** tab 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
Scan Profile	The name of the scan profile associated with the selected project. You can pick a different scan profile from the dropdown list.
Scan Server	The name of your scan server.
Auto-Publish	<p>Select whether to automatically publish inventory items based on internal system policies:</p> <ul style="list-style-type: none"> • Automatically publish system-created inventory items: Automatically publish inventory items. If you select this option, the Mark associated files as reviewed is enabled. • Mark associated files as reviewed: Automatically mark the files associated with the system-created inventory item as “reviewed”.
Enter or select directory	<p>A text box used to quickly navigate to a directory in the File System Tree.</p> <p>Simply enter the directory path, and click the Navigate to path icon.</p> <p>For more information about the File System Tree list, see the next description.</p>
File System Tree	<p>An interactive list in tree format showing all the directories on the scan server.</p> <p>Initially, the top-level directory in the codebase for the current project is selected for the scan. However, if you want to limit the scan to one or more subdirectories in the codebase, add directories to the scan, or reselect the top-level directory, you can drill down in the list to locate these directories.</p> <p>To select a directory for scanning, click the checkbox next to directory in the tree.</p>
Selected Paths	The pane showing the path for each directory currently selected for the scan. As a quick method for removing a given directory from the scan without having to drill down in the tree to locate it, simply click the X next to the directory in this pane.
Save	Click this button to save your edits to the scan settings.

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

Column/Field	Description
Cancel	Click this button to return to the Project Summary page without saving your edits.

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 8-18 • Edit Project Users dialog

Column/Field	Description
Select Users	
Add User	Click this button to assign the selected user the Analyst and/or Reviewer permission.
Search	Enter a full or partial user name to search for a user in the system.
User List	Lists all the currently defined FlexNet Code Insight users.
Analysts	Displays the names of the users who have analyst permission. You can drag and drop users from the User list into this list.
Reviewers	Displays the names of the users who have reviewer permission. You can drag and drop users from the User list into this list.
Observers	Displays the names of the users who have observer permission. You can drag and drop users from the User list into this list.



Note • The **Observers** list is only visible for private projects. For more information, see [Creating a Private Project](#).


See Also

[Assigning Analysts, Reviewers and Observers to a Project](#)

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 8-19 • 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.
Scheduled On	The date and time that the scan was scheduled.
Started On	The date and time that the scan was started.
Completed On	The date and time that the scan completed.
Duration	The amount of time the scan took.
Scheduled By	The user name of the person who scheduled the scan.
Status	The status of the scan: <i>Completed</i> or <i>Failed</i> .
Ok	Click Ok to exit the Scan History dialog and return to the Scan Summary 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 8-20 • Select a New Project Owner dialog

Column/Field	Description
List of Users	The names of all the users in the system are listed in this field. Highlight a name and click Apply to change the project's owner.
Apply	Click this button to assign the selected owner to the project.
Cancel	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 8-21 • Analysis Workbench

Column/Field	Description
Legend	<p>A color-coded and hyperlinked guide to the files and inventory in your scanned codebase:</p> <ul style="list-style-type: none">● New Evidence: Click this link to filter the search results to display only files that are new since the last scan. If only a single scan took place, all files with evidence are displayed in the Files Search Results pane.● Reviewed: Click this link to display files in the File Search Results pane that have been reviewed.● Exact: Click this link to display files in the File Search Results pane that are exact matches.● Copyrights: Click this link to display files in the File Search Results pane that contain copyrighted code.● Email/URLS: Click this link to display files in the File Search Results pane that contain email addresses and URLs.● Licenses: Click this link to display files in the File Search Results pane that contain licenses.● Search Terms: Click this link to display files in the File Search Results pane that match default search terms.● Source: Click this link to display files in the File Search Results pane that match
Codebase Files Panel	
Enter Path	<p>To display codebase files in the Analysis Workbench, enter a directory path that contains the codebase files you are interested in or click the browse button to navigate to the path. If no path is entered, FlexNet Code Insight defaults to the path that was specified during the scan.</p>
Path/Folder/File Tree	<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>
File Details	

Table 8-21 • Analysis Workbench (cont.)

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

See Also

[Using the Project Inventory Tab](#)


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 8-22 • File Search Results pane

Column/Field	Description
	Click to refresh the search.
Advanced Search	Click to open the Advanced File Search dialog on which you can choose a standard search or add a new one.
Clear Search Results	Click to clear the results of the search.
Current Search	Displays the criteria for the current search.
Results Tree	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 8-23 • Advanced File Search dialog

Column/Field	Description
Add New	Click this button to access the Advanced File Search Add dialog.
Name	The name of the search. For example, <i>Files not in inventory</i> .
Description	A short description of the search. For example, <i>Files not associated with inventory items</i> .
	Click to delete a search.
Search	Click to execute the selected search.
Close	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 8-24 • Advanced File Search Add dialog

Column/Field	Description
Name	The name of the search. For example, <i>Files not in inventory</i> .
Description	A short description of the search. For example, <i>Files not associated with inventory items</i> .
Criteria	
Add Criteria	Click the dropdown menu and select search criteria. To add more criteria, click Add Criteria and select another item from the dropdown menu. When you select search criteria from the dropdown menu, a boolean operator appears in the center dropdown, and a new dropdown appears from which you must select a criteria value to search the selected field for.
Add Criteria Group	Click to add a group of criteria.
Save	Click to save the new search.
Save and Search	Click to execute the new search without saving the search for future use.
Search without saving	Click to execute the new search without saving the search for future use.
Cancel	Click to close the Search Files dialog without searching.

Inventory Details Pane

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

Table 8-25 • Inventory Details pane

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

Table 8-25 • Inventory Details pane (cont.)

Column/Field	Description
Review Status	<p>The status of the inventory item:</p> <ul style="list-style-type: none"> ● Approved: The item is approved for use in the software project. ● Not Reviewed: The item has not been reviewed. ● Rejected: The item is not approved for use in the software project. Instead, the item needs further review and remediation before being used in the software project.
Alerts	Notifies you whether or not security alerts exist for this item.
Priority	<p>A dropdown list showing the priority level given to this inventory item by the system:</p> <ul style="list-style-type: none"> ● P1--Highest priority ● P2 ● P3 ● P4--Lowest priority <p>You can change the priority for this inventory item by selecting a different priority from the dropdown list and clicking Save. For more information about priorities, see Inventory Priority Calculation.</p>
Vulnerabilities	A count of each vulnerability found and represented by red (high), orange (medium) or yellow (low) depending on the severity. If there are vulnerabilities, click View Details to view vulnerability details.
Created By	The name of the person or process that created the inventory item.
Created On	The date that the inventory item was created.
Updated On	The date that the inventory item was updated. If the item has not been updated since the creation date, the date shown here will be the same as the Created On date.
Name	The name of the inventory item.
Type	<p>The type of finding of this item:</p> <ul style="list-style-type: none"> ● Work in Progress: a set of files with something in common. The work in progress will become a component or license only via manual audit work. ● Component: files from a specific component version with known or unknown license. If this type is selected, the Lookup Component button becomes active. ● License Only: files under a specific license without a known component.

Table 8-25 • Inventory Details pane (cont.)

Column/Field	Description
Component	The name of the component. Click ⓘ to view publicly available information about the component.
License	The name of the license associated with this component. Click ⓘ to view additional information about the license.
Description	A description of the inventory item. You can enter a description in this field.
Url	The URL of the license for this inventory item.
Disclosed	<p>This field is used most often by analysts to denote information about the state of the inventory item. Disclosed items are those that the analyst is aware of before the audit, as opposed to new items that are detected during auto or manual analysis. Specify whether or not this inventory item was detected before or during analysis:</p> <ul style="list-style-type: none">● Yes● No
Modified	<p>Modified items are those that the analyst manually edits at some point during the audit. For example, in an ongoing audit with multiple rescans, it may be necessary to see which items are modified. To denote whether the inventory item has been modified, select one of the following options:</p> <ul style="list-style-type: none">● Yes● No● Unknown
Notes tab	
Detection Notes	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.
Audit Notes	Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis.
As-Found License Text	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.



Table 8-25 • Inventory Details pane (cont.)

Column/Field	Description
Notices Text	The text to be shown in the Notices report for the selected inventory item. For more information about the Notices report, see Generating the Notices Report .
Associated Files tab	Click this tab to view a list of the files that are part of the inventory for this project. Click the X to delete a listed file.

Evidence Details Pane

The **Evidence Details** pane provides details about the inventory, component, and the files in the inventory. The pane has the following fields:

Table 8-26 • Evident Details pane

Column/Field	Description
Expand All/Collapse All	Click to toggle between expanded and collapsed display.
Search field	Enter search criteria.
Tree view 	Click to change the display to a tree view.
List view 	Click to change the display to a list view.
Select Evidence Types	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 8-27 • Project Inventory Review page

Column/Field	Description
Inventory Items (x)	The title of this pane includes the number of inventory items displayed in the list below.

Table 8-27 • Project Inventory Review page (cont.)

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

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 8-28 • Policy page



Column/Field	Description
Policy list	<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">• Edit icon—Click  to edit the selected policy. The Policy Details page is opened, showing the policy details.• Copy icon—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>.

Table 8-28 • Policy page (cont.)

Column/Field	Description
Add Policy button	Click the Add Policy button to create a new policy. The Policy Details 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. 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 8-29 • Policy Details page

Column/Field	Description
General	
Name	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.
Description	The policy description, if it exists. You can edit or add a description.
Created	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.
Updated	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.
Security Vulnerabilities	
Only auto-approve inventory items if there are no associated security vulnerabilities	Select this checkbox to have Code Insight skip any matching license-based or component policies if the inventory item has any associated security vulnerabilities.

Table 8-29 • Policy Details page (cont.)

Column/Field	Description
Reject inventory items if any associated security vulnerabilities have a CVSS score above...	<p>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.</p> <p>This policy takes precedence over any other automated approval policy.</p>
Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than ...	<p>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.</p> <p>This policy takes precedence over any other automated approval policy.</p>
Licenses	
Select a License 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 Add License to add it to the policy.</p>
Add License button	Click the Add License button to add the selected license as a criterion for the policy.
License 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"> • Name—The name of the license. • Usage Guidance icon—Click  to display the Usage Guidance dialog, in which you can add or edit text that will help reviewers in reviewing this license. • License Details icon—Click  to display the License Details dialog for the selected license. • Action—Select one of the following to indicate what status is automatically assigned based on the license: <ul style="list-style-type: none"> • Approve • Reject • No Action (same as the “Not Reviewed” inventory status, thus requiring a manual review) • Delete icon—Click  to delete the license from the policy.
Components	

Table 8-29 • Policy Details page (cont.)


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

Table 8-29 • Policy Details page (cont.)

Column/Field	Description
Close	Click to close the Policy Details page. If you have made changes the policy, be sure that you have clicked Save 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 8-30 • License Details dialog

Column/Field	Description
General Information Tab	
Id	The identification number of the license in the database.
Name	The name of the license. For example, <i>Academic Free License v1.1</i> .
Priority	The priority ranking as determined by FlexNet Code Insight. For more information, see Understanding License Priorities .
URL	The URL where the license is available on the internet.
Description	A short description of the license.
Category	A license attribute that supports arbitrary classification of a license.
Custom License?	Tells you if this license is a custom license.
Commercial	A designation of whether the licenses is classified as commercial.
Copyleft	A designation of whether the licenses is considered a copyleft license.
Free Software License	A designation of whether the licenses is a free software license.
GPL V2 Compatible	A designation of whether a license is compatible with GPL-2.0.
License Text Tab	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 8-31 • Lookup Component dialog

Column/Field	Description
Search by	Select the type of search you want to perform: <ul style="list-style-type: none">• Keyword• URL• Forge
Keywords	Enter a search term to look it up in the CL.
Select this Component	Click this button to select the displayed component to add to an existing inventory item or to create a new one.
Show Instances	Select this hyperlink to display all instances that match your search criteria. By default, FlexNet Code Insight shows only one matching instance.
Register New Instance	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 8-32 • Add Project dialog

Column/Field	Description
Name	Enter a name for the new project.
Project Type	From the dropdown menu, select the type of scan that will be run on this project: <ul style="list-style-type: none">• Standard: This is the default scan type. It requires that you upload your codebase to FlexNet Code Insight.• Inventory Only: 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.

Table 8-32 • Add Project dialog (cont.)

Column/Field	Description
Project Visibility	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 Private , 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> .
Policy Profile	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 8-33 • Preferences page

Column/Field	Description
Change Password	
New Password	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.
New Password Confirm	Reenter the password you entered in the New Password field.
Update Password	After entering the password in both fields, click Update Password to save your changes.
Authorization Tokens	
Add Token	Click this button to display the Add Token dialog.
Name	A list of the names of previously created tokens.
Token	Displays the system-generated token associated with the name.
Create Date	The date on which the token was created.

Table 8-33 • Preferences page (cont.)

Column/Field	Description
Actions	A group of icons that indicate actions you can take on each token: <ul style="list-style-type: none">• Edit (): Click to open the Edit Token dialog.• Delete (): Click to delete the selected token. The token will be deleted immediately.• Copy to clipboard (): Click to copy the selected token to the clipboard. You can use this option to copy tokens for Jenkins Plugin configurations.

See Also

[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 8-34 • Add Token dialog

Column/Field	Description
Name	Enter a name for the token you are creating.
Token Validity	Select one of the validity periods: <ul style="list-style-type: none">• Never Expires: The authorization token never expires.• Expires On: The authorization token is valid until the date you pick on the Validity Calendar.
Validity Calendar	If you check the Expires On 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 8-35 • Edit Token dialog

Column/Field	Description
Name	Enter a name for the token you are creating.
Token	Displays the actual characters of the system-generated token.
Select Token Text	Click this button to highlight the token characters displayed in the Token field. To copy the token to the clipboard, press CTRL-C .
Expiration	A read-only field that displays the expiration date of the token, or the text, "Token has no expiration date."
Save	Click this button to save your edits.
Cancel	Click this button to exit the Edit Token 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 8-36 • Advanced Inventory Search page

Column/Field	Description
Inventory Items	
Inventory Name	Enter the whole or partial name of an item for which to search. For example, if you enter <i>apache</i> in this field, FlexNet Code Insight will find all inventory items that have the word <i>apache</i> in their name.

Table 8-36 • Advanced Inventory Search page (cont.)


Column/Field	Description
Inventory Priority	<p>Select one or more of these checkboxes to use the inventory priority in your advanced search:</p> <ul style="list-style-type: none"> ● P1: ● P2: ● P3: ● P4:
Inventory Review Status	<p>Select one or more of the following checkboxes to use the review status in your advanced search:</p> <ul style="list-style-type: none"> ● Approved: The item has been reviewed and approved by the reviewer. ● Rejected: The item has been reviewed and rejected by the reviewer. ● Not Reviewed: The item has not yet been reviewed.
Dependency Options	<p>Select one of the following options to determine the level of dependency of inventory items in your advanced search:</p> <ul style="list-style-type: none"> ● All Inventory Items: Searches for all inventory items regardless of dependency. ● Only Top-Level Inventory Items: Searches only for top-level inventory items but does not include dependencies if any. ● Only Dependency Inventory Items: Searches only for inventory items with dependencies.
Inventory Age	<p>Search by inventory publication date. This dropdown field has the following choices:</p> <ul style="list-style-type: none"> ● Last 1 day: If today is Feb 6th, search from Feb 5th 12 AM. ● Last 7 days: If today is Feb 6th, search from Jan 30th 12 AM. ● Last 30 days: If today is Feb 6th, search from Jan 7th 12 AM. ● Custom Date Range: Select a beginning and ending date from the popup calendar. <div>  <p>Note • To appear in search results based on inventory age, an inventory item must have been published. The search will not find items that were created but not published.</p> </div>
Inventory Notifications	<p>Select either or both options to search for inventory items with security vulnerability alerts or those items that have been rejected due to new security alerts that are non-compliant with policy.</p>

Table 8-36 • Advanced Inventory Search page (cont.)

Column/Field	Description
Security Vulnerabilities	
Security Vulnerability ID	Enter a valid vulnerability ID to search for.
Security Vulnerability Severity	<p>Select one or more of the following severities to include in your search:</p> <ul style="list-style-type: none"> ● High Severity (CVSS 7.0 - 10.0) ● Medium Severity (CVSS 4.0 - 6.9) ● Low Severity (CVSS 0.0 - 3.9)
Security Vulnerability Age	<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"> ● Last 1 day: If today is Feb 6th, search from Feb 5th 12 AM. ● Last 7 days: If today is Feb 6th, search from Jan 30th 12 AM. ● Last 30 days: If today is Feb 6th, search from Jan 7th 12 AM. ● Custom Date Range: Select a beginning and ending date from the popup calendar.
Licenses	
License Name	The full or partial name of the license to search for.
License Priority	<p>Select one or more of the following license priorities to limit your search:</p> <ul style="list-style-type: none"> ● P1: Viral/Strong Copyleft ● P2: Weak Copyleft/Commercial/Uncommon ● P3: Permissive/Public Domain ● No License Found
Apply And/Or Criteria	<p>Select one of the boolean criteria to apply to the search selections:</p> <ul style="list-style-type: none"> ● Or: The item may contain any one or more of the chosen criteria to be displayed. This is the default boolean operator. ● And: The item must meet all chosen criteria to be displayed.
Apply	Click this button to apply the selected search criteria and return to the Inventory Items page to view the results. The title bar of the Inventory Items page denotes that the display shows only filtered results.
Clear Form	Click this button to remove any previously specified search criteria.


Table 8-36 • Advanced Inventory Search page (cont.)

Column/Field	Description
Close	Click this button to close this page and return to the Inventory Items 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 Project Summary page. It lets you set options that FlexNet Code Insight uses to import data. The dialog has the following fields:

Table 8-37 • Import Project Data dialog

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