



FlexNet Code Insight 2019 R3

User Guide

Legal Information

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

Copyright Notice

Copyright © 2019 Flexera

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

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

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

Intellectual Property

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

Restricted Rights Legend

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

Contents

- 1 FlexNet Code Insight 2019 R3 User Guide. 11**
 - Intended Audience 12**
 - Contacting Us 12**
- 2 Using FlexNet Code Insight 13**
 - Opening FlexNet Code Insight 14**
 - Viewing Online Help and Online Guides. 15
 - Changing Your Password 15
 - Roles and Permissions in FlexNet Code Insight 15**
 - What is a Code Insight Project? 15**
 - Key Project Elements 16
 - Common Project Configurations 16
 - Creating a Project 17**
 - What Is a FlexNet Code Insight Scan? 18**
 - Applying a Scan Profile to the Project. 18**
 - About Scan Profiles. 19
 - Applying a Scan Profile. 19
 - Selecting Materials to Scan 20**
 - Uploading a Project Codebase 20
 - Uploading the Codebase 20
 - Supported Archive Types for Expansion 21
 - More About Archive Expansion Behavior During Codebase Uploads. 22
 - Scanning the Codebase 24**
 - Overview of Scan Results 25**
 - Inventory 25
 - Review Status of Inventory. 26
 - Inventory Priority 26
 - Inventory Confidence 27

Security Vulnerabilities Associated with Inventory	28
Inventory Usage Information.....	31
Scan Evidence	32
License Information Associated with Inventory	33
License Details from the Code Insight Data Library	33
License Priority	34
Reporting of Detected License Text through the As-Found Text Inventory Field	35
Notices Text.....	36
What Does an Analyst do?	37
Analyzing (Auditing) Scan Results	37
Opening the Analysis Workbench	38
The Analysis Workbench Layout	39
Searching for Codebase Files Based on Name	40
Searching for Codebase Files Based on Search Criteria	41
Creating and Editing File Searches	41
Creating a New File Search.....	41
Editing a File Search.....	43
Copying a File Search	43
Deleting a File Search	44
Using the Filter Legend Options to Filter the Codebase.....	44
Using the Codebase Files Pane Context Menu	46
Marking Files as Reviewed.....	46
Viewing Details for Licenses Associated with Codebase Files.....	46
Using the File Details Tab	48
Viewing the Evidence Summary for a File.....	48
Viewing Binary Strings in a File	49
Viewing Copyright, Email, URL, and License Evidence in a File	49
Viewing Exact Matches	50
Viewing Source Matches	51
More About the “Remote Files” Panels on the Exact or Partial Matches Tabs	52
Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component	53
Using the Evidence Details Tab	54
Using the Inventory Details Tab	54
Using the Inventory Items Context Menu	55
Viewing Security Vulnerabilities for Inventory in Analysis Workbench	55
Viewing or Editing Inventory Usage Information from Analysis Workbench	56
Component Lookup.....	56
Guidelines for Component Lookup	56
Component Lookup Results	57
Performing Component Lookup	57
Creating an Inventory Item from the Analysis Workbench	58
Creating Inventory from the Inventory Items List	58
Creating Inventory from the Codebase Lists.....	60
Editing Inventory from the Analysis Workbench	61
Publishing or Recalling Inventory from Analysis Workbench.....	62

Reviewing Published Inventory	64
Goal of the Reviewer	64
Displaying Project Inventory	65
Searching Published Inventory	65
Viewing Security Vulnerabilities for Project Inventory	66
Viewing Details for the Licenses Associated with Project Inventory	67
Viewing and Updating Notes & Guidance	68
Viewing Usage Information for Project Inventory	68
Viewing Associated Files	69
Creating Inventory from the Project Inventory Tab	69
Editing Inventory from the Project Inventory Tab	71
Approving or Rejecting Inventory Items	72
Creating and Managing Tasks for Project Inventory	72
Note About External Work Items	73
Manually Creating a Task	73
Editing a Task	74
Creating and Viewing External Work Items for a Project Inventory Task	76
Prerequisite	77
Manually Creating a Work Item	77
Viewing a Work Item	78
Recalling a Published Inventory Item	78
Managing Security Vulnerability Alerts	78
Accessing Security Vulnerability Alerts	79
Managing Security Vulnerability Alerts	81
Alert Details	81
Changing the Priority of an Alert	83
Changing the Status of an Alert	83
Creating and Editing Custom Components	83
Creating a Custom Component	84
Step 1: Access the Component Lookup Feature	84
Step 2: Create the Custom Component	84
Create the Custom Component Based on a Keyword in Its Name or Title	85
Create the Custom Component Based on Its Project or Forge URL	86
Create the Custom Component Based on Its Forge	88
Create the Custom Component in Free Form	89
Step 3: Associate an Instance of the Custom Component with the Inventory Item	90
Editing a Custom Component	91
Custom Component Properties	92
Supported Forge-URL Domains for Custom-Component Creation	94
Creating and Editing Custom Licenses	94
Creating a Custom License	94
Step 1: Initiate the Creation of a Custom License	95
When Using Component Lookup to Register a Component Instance for a “component” Inventory Item	95
When Selecting a New License for an Existing Inventory Item	96
When Creating or Editing a “License Only” Inventory Item	97
Step 2: Create the Custom License	97

Editing a Custom License	98
Custom License Properties	99
Managing Custom Detection Rules	100
Creating a Custom Detection Rule	101
Creating a Custom Detection Rule from Inventory of “Component” Type	101
Creating a Custom Detection Rule from Scratch	103
Viewing All Current Custom Detection Rules	103
Editing a Custom Detection Rule	104
Deleting a Custom Detection Rule	104
Rule-Processing Considerations	104
Finalizing the Notices Text for the Notices Report	105
Accessing and Viewing Projects in the System	107
Navigating to the Projects List	107
Using the Project Dashboard	108
Filtering Inventory for a Project from the Project Dashboard	110
Opening a Project	110
Showing Only Your Projects	111
Searching the System	111
Available Filters for Searching Across Projects	112
Searching for Projects by Name	113
Searching All Projects for Inventory Based on a Specific Component and Version	114
Searching All Projects for Inventory Associated with a Specific License	115
Searching All Projects for a Security Vulnerability Advisory	115
Restoring the Full Project List	116
Managing Items in the Project List	117
Managing a Project from the Summary Tab	117
Opening the Project Summary Tab	118
Generating Reports	118
The Project Report	118
The Audit Report	119
The Notices Report	119
Generating the Notices Report	120
Assigning Project Roles to Users	120
Editing the Project Definition and General Settings	121
Updating Scan Settings for a Project	122
Automatically Publishing Inventory	122
Updating Inventory Review and Remediation Settings for a Project	123
Connecting the Project to Remote Data Sources	123
Version Control Settings	123
ALM Settings	124
Changing Project Owners	126
Rescanning Your Codebase	127
Change Events Resulting in Full or Incremental Rescans	127
Effects of Scan-Setting Changes on Rescans	128
Handling of Edited Inventory During Rescans	129
Initiating a Codebase Rescan	130

Exporting Project Data	131
Deleting a Project	132
Creating a Private Project	132
Managing Policy Profiles	133
Understanding Policy Profiles	133
How Policy Profiles Work in the Automated Inventory-Review Process	133
Adding or Editing a Policy Profile	134
Copying a Policy Profile	134
Associating a Policy Profile with a Project	135
Managing Authorization Tokens	135
Accessing the Preferences Page	135
Generating an Authorization Token	136
Copying the Authorization Token to the Clipboard	136
Editing the Token Name	136
Deleting an Authorization Token	137
3 Performing Advanced Searches	139
Advanced Searches	139
Dependencies in Advanced Searches	143
4 Exporting and Importing Project Data	145
About Exporting and Importing	145
Prerequisites When Using the REST Interface	146
REST Client or Command-Line Tool Supporting cURL	146
Authorization Token	146
Project ID	146
Exporting Project Data	148
About an Export	148
Types of Data Exported	149
Prerequisites for Exporting Data	149
Exporting Project Data Using the Web UI	149
Exporting Project Data Using the REST Interface	150
Verifying a Successful Export	151
Importing Project Data	151
About an Import	152
Comparison of Standard and Inventory-Only Imports	152
Prerequisites for Importing Data	154
Import Behavior	155
Default File and Inventory Processing During an Import	155
Available Import Options to Control Import Behavior	155
Other Import Considerations	156
Importing Project Data Using the REST API	157

5	Automated Analysis	159
	What is Automated Analysis?	159
	Supported Development Ecosystems	159
	Supported Ecosystems.....	160
	Notes About Ecosystem Support	161
	Notes about Dependencies Support.....	162
	Supported Archive Formats	162
	Additional Rule-based Detection Capabilities	162
6	Performing Inventory-Only Scanning.....	163
	Inventory-Only Scan	163
	Creating a Project Without Uploading a Codebase	163
	FlexNet Code Insight Plugins	164
7	Configuring Source Code Management	167
	Managing Source Code Management (SCM) Instances	167
	Prerequisites.....	167
	Adding an SCM Instance to the Code Insight Project	168
	Testing an SCM Instance	168
	Synchronizing an SCM Instance	168
	Deleting an SCM Instance	169
	Configuring a Git SCM Instance	169
	Adding a Git SCM Instance to the Code Insight Project.....	169
	Configuring the Git SCM Instance	170
	Configuring a Perforce SCM Instance	170
	Adding a Perforce SCM Instance to the Code Insight Project	170
	Configuring the Perforce SCM Instance	171
	Configuring a TFS SCM Instance.....	172
	Adding a TFS SCM Instance to the Code Insight Project.....	172
	Configuring the TFS SCM Instance.....	173
8	Pages and Panels	175
	The FlexNet Code Insight Dashboard	176
	Users/Permissions Tab	177
	Add User Dialog	178
	Edit User Dialog	179
	Electronic Updates Tab	179
	Overview of Electronic Update Setup	180
	Field Descriptions	181
	Email Server Tab	183
	LDAP Tab	183
	ALM Tab	185
	Scan Servers Tab	187

Scan Server Dialog	189
Scan Profiles Tab	192
Create/Edit Scan Profile Dialog	193
Project Defaults Tab	194
System Settings Tab	200
Projects List Page	200
Project Summary Tab	202
Edit Project: General Tab	205
Edit Project: Scan Settings Tab	206
Edit Project: Review and Remediation Settings Tab	207
Edit (Default) Project Users Page	212
Scan History Dialog	213
Select a New Project Owner Page	214
Analysis Workbench	215
File Search Results Pane	216
Advanced File Search Dialog	217
Advanced File Search Add Dialog	218
Inventory Details Pane	218
Evidence Details Pane	222
Project Inventory Review Page	222
Policy Page	223
Policy Details Page	224
Policy Fields	224
Impact on Policies When CVSS Version Changes on System	228
Custom Detection Rules Tab	228
Custom Detection Rule Dialog	230
Edit Custom Rule Dialog	233
License Details Window	235
Lookup Component Window	236
Add Project Dialog	237
Preferences Page	238
Add Token Dialog	239
Edit Token Dialog	240
Advanced Inventory Search Page	241
Import Project Data Dialog	244
A FlexNet Code Insight User Roles and Permissions	247
System Roles and Permissions	247
Project Roles and Permissions	249
Roles and Permissions to Manage Project Task Flow	251

FlexNet Code Insight 2019 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* describes how to use FlexNet Code Insight to realize these benefits. The guide includes the following sections.

Table 1-1 • FlexNet Code Insight User Guide

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

Intended Audience

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

Contacting Us

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

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

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

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

Using FlexNet Code Insight

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

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

Opening FlexNet Code Insight

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



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



Task

To open FlexNet Code Insight, do the following:

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



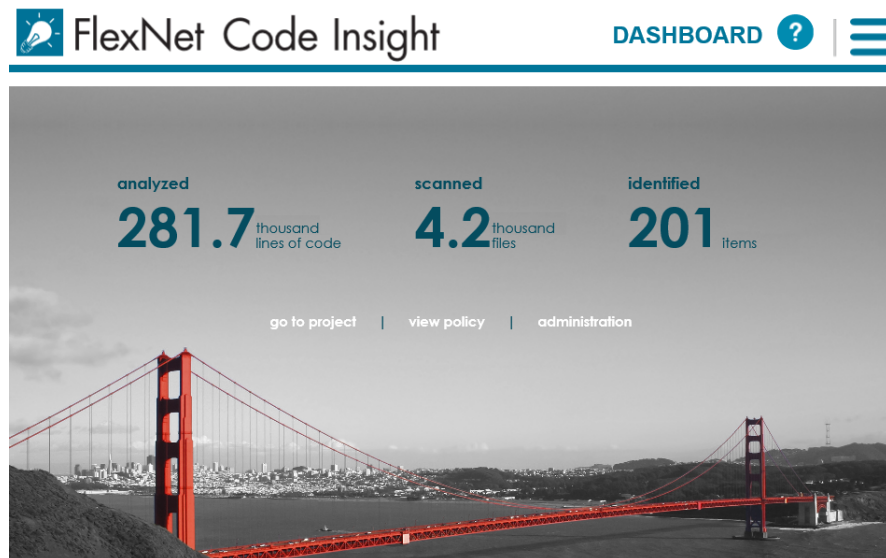
Note • If you are unsure about your server host name, contact your system administrator for guidance.

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



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

3. Click **Login**. The **FlexNet Code Insight Dashboard** appears:



Note • The statistics displayed on the **Dashboard** are from scans that were run on your codebases.



Viewing Online Help and Online Guides

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



Task

To access online help and guides, do the following:

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


Changing Your Password

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



Task

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

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

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

Roles and Permissions in FlexNet Code Insight

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

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

What is a Code Insight Project?

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

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

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

- [Key Project Elements](#)
- [Common Project Configurations](#)



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

Key Project Elements

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

- **Materials to scan or analyze**—Each project has an uploaded codebase or a configured remote scan location (such as on a build server, artifact repository, or version control system).
- **Scan profile**—Each project has an associated scan profile with a set of scan settings that are applied when the project is scanned. (The profile can be one of the default scan profiles or a custom scan profile).
- **Policy profile**—Each project has an associated policy profile with a set of intellectual property or security policies that are applied when project inventory is published to the project (such as during the first scan or when manually published by a project user).
- **Project visibility**—Each project has an associated visibility configuration that specifies which logged-in users have the ability to view or change the project.

Common Project Configurations

These are some examples of common project configurations:

- **Project to scan source code**—The project is configured for a local scan with code that is uploaded to the Scan Server or synchronized to the server through a Version Control System. The selected scan profile performs a full analysis of the source—including searches for exact matches of entire files and for partial source-code matches (fingerprints)—and processes files inside archives.
- **Project to scan build output or binaries**—The project is configured for a remote system scan using one of the scan agent plugins. The selected scan profile performs Automated Analysis and processes dependencies to generate inventory, but does not perform a full analysis of the source.

This scan profile can also be selected for a local scan.

- **Security-focused project**—The policy profile selected for the project triggers an automatic review of project inventory based on the presence of security vulnerabilities, on the CVSS scores and severity of these vulnerabilities, and on other criteria.
- **Project focused on intellectual-property protection**—The policy profile selected for the project triggers an automatic review of project inventory based on the presence of black-listed and white-listed components, version ranges, and licenses.

Creating a Project

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



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



Task

To create a project, do the following:

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



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



Note • The **Project Visibility** setting can also be accessed through the **Edit Project** option on the **Manage Project** menu on the **Summary** tab. For more information, see [Editing the Project Definition and General Settings](#).

- **Policy Profile**—From the dropdown menu, select a policy profile to be used for this project. If you do not select a policy profile, the Default License Policy Profile will be used. For more information about policy profiles, see [Managing Policy Profiles](#).

- **Scan Server**—Select the Scan Server for this project (if **Project Type** is **Standard**). This field is disabled when **Project Type** is **Inventory Only**.
5. Click **Save** to save the new project.
 6. (Optional) Assign roles to users who will interact with the project. For more information, see [Assigning Project Roles to Users](#).

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

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

What Is a FlexNet Code Insight Scan?

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

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

- **Automated Analysis**—The Scan Server uses automated detection rules to identify components, versions, licenses, and security vulnerabilities. In applying these rules, the Scan Server automatically generates inventory items that make up the Bill of Materials. The rules are found in the *Code Insight data library*, which is updated on your Code Insight server through both an internal process and as part of the weekly Electronic Update. For more about Automated Analysis, see the [Automated Analysis](#) chapter.
- **Advanced Analysis**—The Scan Server uses advanced analysis techniques to detect copyrights, emails, URLs, search terms, exact files, and source-code fingerprints (snippets) that match those found in third-party or open-source code.

Advanced Analysis requires the FlexNet Code Insight Compliance Library (CL), downloaded from the Product and License Center. The CL is a database used by the Scan Server to perform exact-file and source-code fingerprint (snippet) matching. Code Insight compares elements of scanned codebase files with information contained in the CL to generate file-level evidence on which you can take action.

Applying a Scan Profile to the Project

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

- [About Scan Profiles](#)
- [Applying a Scan Profile](#)

About Scan Profiles

FlexNet Code Insight includes the following default scan profiles:

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

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

Applying a Scan Profile

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


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



Task

To select a new scan profile, do the following:

1. From the list of projects, select the project for which you want to apply a scan profile.

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

Selecting Materials to Scan

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

- **Traditional scan** where the codebase is uploaded to the Scan Server or synchronized using a source code management system (SCM) such as Git or Perforce. With a traditional scan, you can manually move the code to the Scan Server, upload the code, or configure the project with an SCM. See these locations for instructions:
 - [Uploading a Project Codebase](#)
 - [Configuring Source Code Management](#) chapter
- **Remote scan** using a FlexNet Code Insight scan agent plugin to perform a scan remotely within the context of an Engineering application (such as an IDE, source-management, artifact-repository, CI, build, testing, or installation application). With a remote scan, the FlexNet Code Insight scan agent plugin is configured to scan remotely and send results to FlexNet Code Insight for review and remediation. See the following for more information:
 - [Creating a Project Without Uploading a Codebase](#) in the “Performing Inventory-Only Scanning” chapter
 - *FlexNet Code Insight Plugins Guide* (available for download in the Flexera Customer Community)

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

Uploading a Project Codebase

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

The following topics describe the codebase upload process:

- [Uploading the Codebase](#)
- [Supported Archive Types for Expansion](#)
- [More About Archive Expansion Behavior During Codebase Uploads](#)

Refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix for role requirements to upload the codebase.

Uploading the Codebase

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

The following describes how to upload the project codebase.



Task

To upload a project codebase, do the following:

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



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

5. For **Archive File Expansion Options**, select the level of archive expansion you want to perform on the codebase:
 - **Uploaded file only**—Extract the files from the uploaded archive. Any extracted archives are not expanded.
 - **Uploaded file and first-level archives only**—Extract the files from the uploaded archive and expand all first-level archives in the codebase. Note that the expanded archive itself is retained along with its extracted contents in the parent folder (see [Retention of the Original Archive Files](#)).
 - **Uploaded file and all contained archives**—Extract the files from the uploaded archive and expand archives at all levels (that is, archives with archives within archives and so forth) in the codebase. Note that each expanded archive is retained along with its extracted contents in the parent folder (see [Retention of the Original Archive Files](#)).
6. Click **Upload**. FlexNet Code Insight uploads your codebase file and attaches it to the selected project. You can now scan the uploaded codebase.

Supported Archive Types for Expansion

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

- .zip
- .tar
- .tar.gz
- .7z

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

Table 2-1 • Expandable Archives

• .7z	• .tar.xz
• .cpio	• .tgz
• .tar	• .txz
• .tar.bz2	• .tar.lzma
• .tar.gz	• .zip

More About Archive Expansion Behavior During Codebase Uploads

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

- [Retention of the Original Archive Files](#)
- [Expansion of Archives Containing an Intermediary .tar File](#)
- [Multiple Codebase Uploads to the Same Project](#)

Retention of the Original Archive Files

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

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

Expansion of Archives Containing an Intermediary .tar File

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

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

```
jars.tar.gz
--jar.tar
----file-1.txt
----file-2.txt
----jar.zip
-----\jar
-----abc.jar (color)
```

```
-----xyz.jar
-----classes.zip
-----\classes
-----corporation.class
-----employee.class
```

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

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

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

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

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

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

Multiple Codebase Uploads to the Same Project

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

1. Create project1 and upload the codebase codefiles1.zip, using the **None** option. The contents of codefile1.zip are extracted. Archives in these contents are not expanded.
2. Upload codefile2.zip to the same project (at the same codebase path), this time using the **Uploaded file and all contained archives**. (Keep in mind that codebase1.zip was previously expanded with no further expansion of any archives in its contents.) Now all archives at all levels are expanded within the codefile1 and codefile2 codebases.

3. Upload codefile3.zip to the same project, this time using **Uploaded file and first-level archives only**. Now *only the first-level archives* in all three codebases are expanded.

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

Scanning the Codebase

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

Refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix for role requirements to scan a codebase.



Task

To start the scan, do the following:

1. Navigate to the **Summary** tab, as described previously in [Applying a Scan Profile to the Project](#).
2. Click the **Start Scan** button (or the link in **Scan Status**) to start the scan. If other scans are running, the scan is queued and will automatically run based on queue order. (Click the link in **Past Scans** to view details about the scheduled scan.)



Note • If the **Start Scan** button is disabled, see [Actions to Take When the Start Scan Button is Disabled](#).

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

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

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

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



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

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

3. Do any of the following:

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

Actions to Take When the Start Scan Button is Disabled

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

However, if the server is disabled, you will need to create a new project for the codebase and associate it with an enabled Scan Server.

Overview of Scan Results

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

- [Inventory](#)
- [Scan Evidence](#)
- [License Information Associated with Inventory](#)

Inventory

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

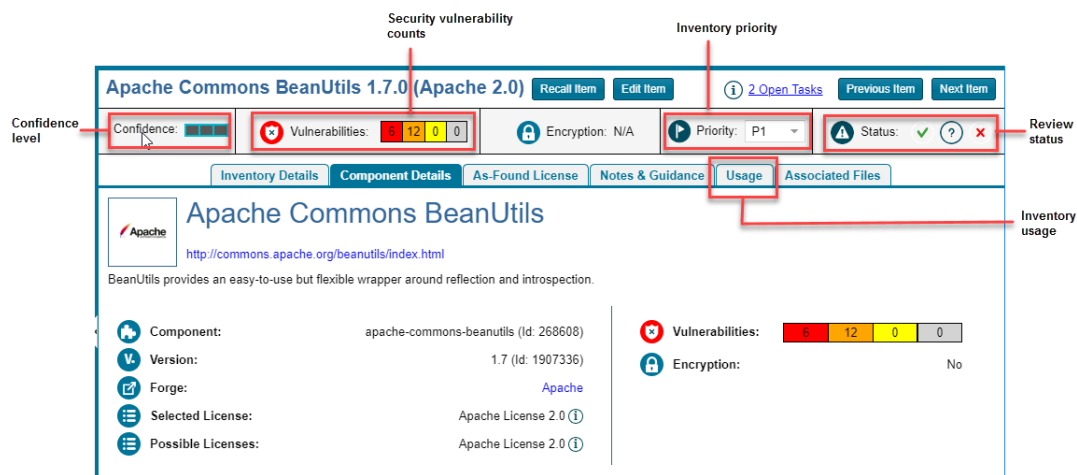
An inventory item typically has an associated component, version, license and list of security vulnerabilities, as well as other details about these elements. See [Inventory Details Pane](#) for a full description of the information collected by the scan.

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

- [Review Status of Inventory](#)
- [Inventory Priority](#)

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

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



Review Status of Inventory

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

For information about setting up policies that automate the inventory review process, see [Managing Policy Profiles](#).



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

Inventory Priority

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

You can manually change the inventory priority by simply selecting a different priority from the **Priority** dropdown either in **Analysis Workbench** or on the **Project Inventory** tab.

For a “Component” Inventory Type

The inventory priority is set to P1 if either of these circumstances exist:

- The inventory item has at least one associated security vulnerability with a severity of High (for CVSS v2) or Critical (for CVSS v3.0).
- The selected license priority is P1 (see [What Does an Analyst do?](#)).

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

For a “License-Only” Inventory Type

When a user selects a license for a license-only inventory item, the inventory priority is set to the license priority (see [What Does an Analyst do?](#)) *unless* that would mean lowering an existing priority.



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

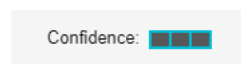
Inventory Confidence

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

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

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

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



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

The following describes the Confidence levels:

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

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

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

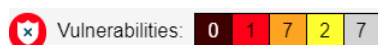
Table 2-2 • Confidences Levels Associated with Various Detection Techniques

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

Security Vulnerabilities Associated with Inventory

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

The **Vulnerabilities** bar graph shows the current security-vulnerability counts by severity level for a given inventory item listed in **Analysis Workbench** or on the **Project Inventory** tab:



Understanding Severity Levels for Security Vulnerabilities

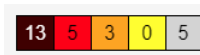
FlexNet Code Insight obtains the severity level of a security vulnerability from the advisory database used to identify the vulnerability. The severity is based on the vulnerability's CVSS (Common Vulnerability Scoring System) score, which can have two different values depending on the scoring system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

CVSS v3.0 Scoring System

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

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

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

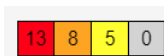


CVSS v2 Scoring System

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

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

The following example **Vulnerabilities** graph reflects vulnerability counts for the same inventory item referenced in the previous section, but in this case CVSS v2 scoring is used. Note that the graph shows the same total number of vulnerabilities as the previous graph shows, but the severity distribution is different. In this case, the graph indicates 13 vulnerabilities of high severity, 8 of medium severity, 5 of low severity, and 0 of unknown severity:



Viewing Security Vulnerabilities

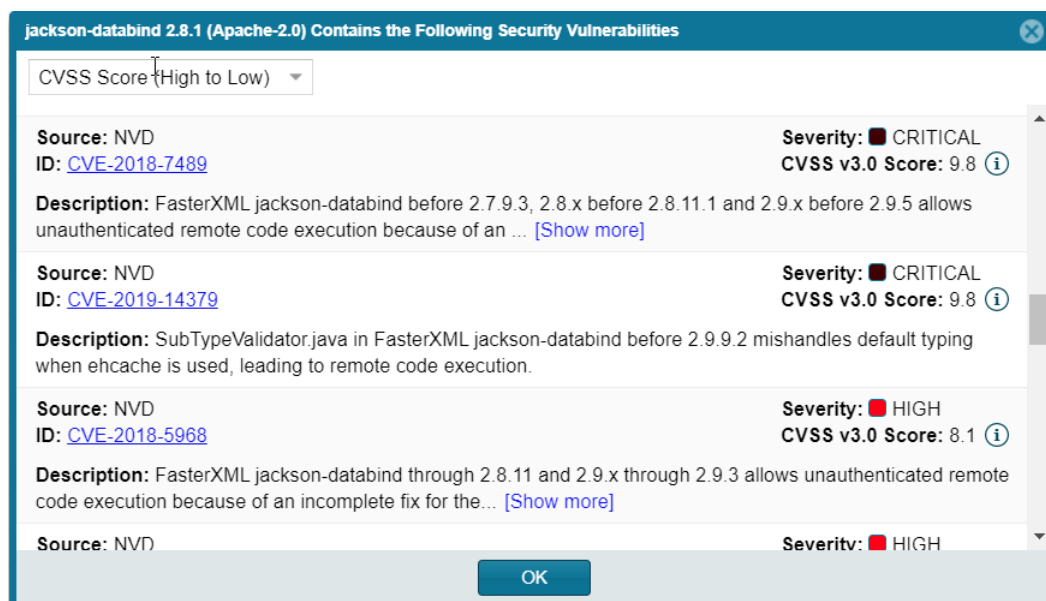
The following procedure explains how to use this graph to obtain details about the security vulnerabilities associated with the inventory item.

**Task**


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

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

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



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

- Each entry identifies a specific security vulnerability associated with the selected inventory item. A vulnerability can be reported by the National Vulnerability Database (NVD) in the form of a CVE (Common Vulnerabilities and Exposures), by Secunia Research in the form an SA (Secunia Advisory), or by other research organizations using their own vulnerability ID formats. In some cases, CVEs will be referenced by one or more advisories. A given entry includes the ID for the vulnerability or advisory, as well as its source (such as NVD or Secunia), severity, CVSS score, and description.
- The CVSS score label for a given entry indicates whether the value is a CVSS v3.0 or CVSS v2 score. If you click the  icon, you can view both CVSS score values.

Severity:  HIGH
CVSS v3.0 Score: 7.5 

- In some cases, the vulnerability or advisory CVSS score is unknown because it has not been scored by the supplier. These vulnerabilities are reported by Code Insight with a CVSS score of **N/A** and a severity of **None** (CVSS v3.0) or **Unknown** (CVSS v2).



Note • Your feedback is welcome in how to handle the severity and scoring of currently unscored vulnerabilities. The FlexNet Code Insight team will do its best to incorporate the results of this feedback into the Code Insight vulnerability database. Contact FlexNet Code Insight Support (see [Contacting Us](#)).

- You can click the vulnerability or advisory ID link (if available) for a given entry to further investigate the vulnerability:

Source: NVD
ID: [CVE-2018-5407](#)

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

Inventory Usage Information

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

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

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

- Distribution Type**—Indicates how you are distributing the item. The distribution type can affect license priority and obligations.

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

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

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

Scan Evidence

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

You can quickly view filter on and view the following evidence for codebase files in **Analysis Workbench**. (For more details about viewing evidence in **Analysis Workbench**, see [Viewing Details for Licenses Associated with Codebase Files](#) and [Using the Evidence Details Tab](#).)


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

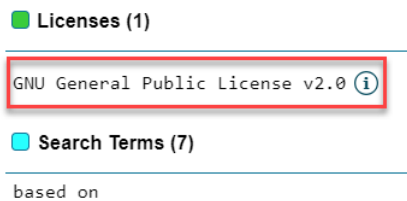
License Information Associated with Inventory

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

- [License Details from the Code Insight Data Library](#)
- [License Priority](#)
- [Reporting of Detected License Text through the As-Found Text Inventory Field](#)
- [Notices Text](#)

License Details from the Code Insight Data Library

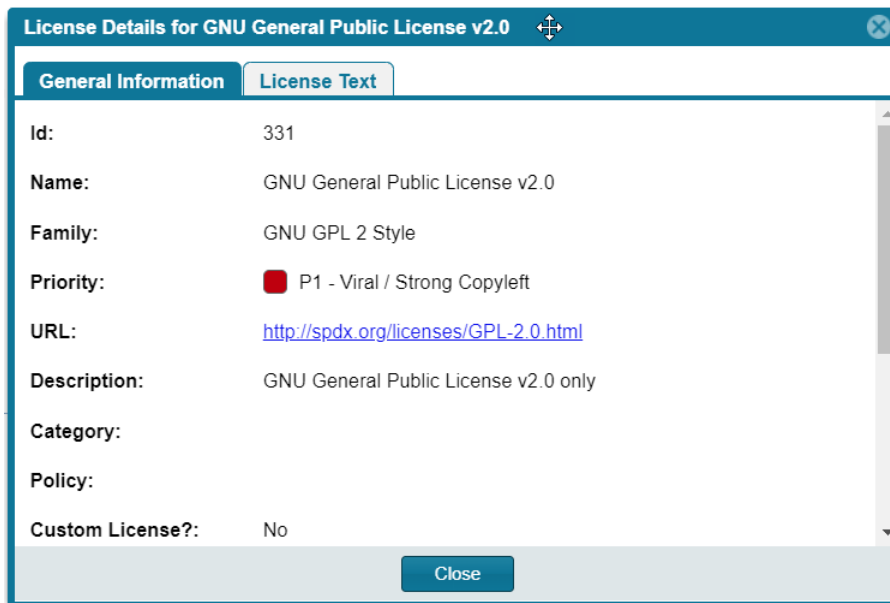
When an inventory item is created by FlexNet Code Insight, it uses information in the FlexNet Code Insight data library to automatically select a license for the component associated with the inventory item. You can view details from the data library for this license by simply clicking  next to any license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



The **License Details** window is displayed containing the following information:

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

For descriptions of these fields in this window, see [License Details Window](#).



The following lists locations in Code Insight user interface where you can access the **License Details** window:

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

License Priority

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

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

Table 2-3 • License Priorities




Priority	Characteristics	Icon	Description
P1	Viral/Strong Copyleft		Usually, P1 licenses require immediate attention due to the possibility of tainting proprietary application code, an issue that can have significant business impact.
P2	Weak Copyleft/ Commercial/Uncommon		The typical P2 license requires legal review and guidance based on corporate policies about the proper use of these types of licenses in your organization.

Table 2-3 • License Priorities (cont.)

Priority	Characteristics	Icon	Description
P3	Permissive/Public Domain		In general, P3 licenses are allowed and have minimal impact to an organization as long as license obligations are satisfied. The most common license obligation is properly attributing the use of an open source component to its author. This is the default priority.

Inventory priority (see [Inventory Priority](#)) is a risk metric for the inventory item that takes license priority into account as one of the contributing factors. Inventory priority is set at scan time when the inventory item is created by the system or during inventory review. You can set or override the inventory priority at any time. License priority, on the other hand, is static and never changes. The license priority is supplied by the Electronic Update.


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



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

Viewing the License Priority

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

License Details for MIT License (also X11)	
General Information	License Text
Id:	7
Name:	MIT License (also X11) (MIT)
Family:	MIT Style
Priority:	 P3 - Permissive / Public Domain

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

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

The following shows the **License & Notices** tab in **Analysis Workbench**:

The screenshot shows the 'License & Notices' tab for the item 'prezeskk-tcpdf (LGPL-3.0)'. The interface includes a 'Recall' button, 'Save', and 'Close' buttons. The 'Review Status' is 'Draft', 'Alerts' are 'None', and 'Priority' is 'P3'. 'Vulnerabilities' are listed as 'No'. The 'Component' is 'prezeskk-tcpdf None Selected'. The 'License' is 'I don't know'. The 'Description' states: 'TCPDF is a PHP class for generating PDF documents and barcodes.' The 'URL' is 'http://www.tcpdf.org/'. The 'Disclosed' status is 'No'. The 'As-Found License Text' field contains the following text: 'The following text is found in file:LICENSE.TXT at /home/qaadmin/scanroot2019r2/1245/moodle-master/lib/tcpdf/LICENSE.TXT'. The 'Licenses & Notices' tab is highlighted with a red box.

This shows the **Licenses & Notices** tab in **Project Inventory**:

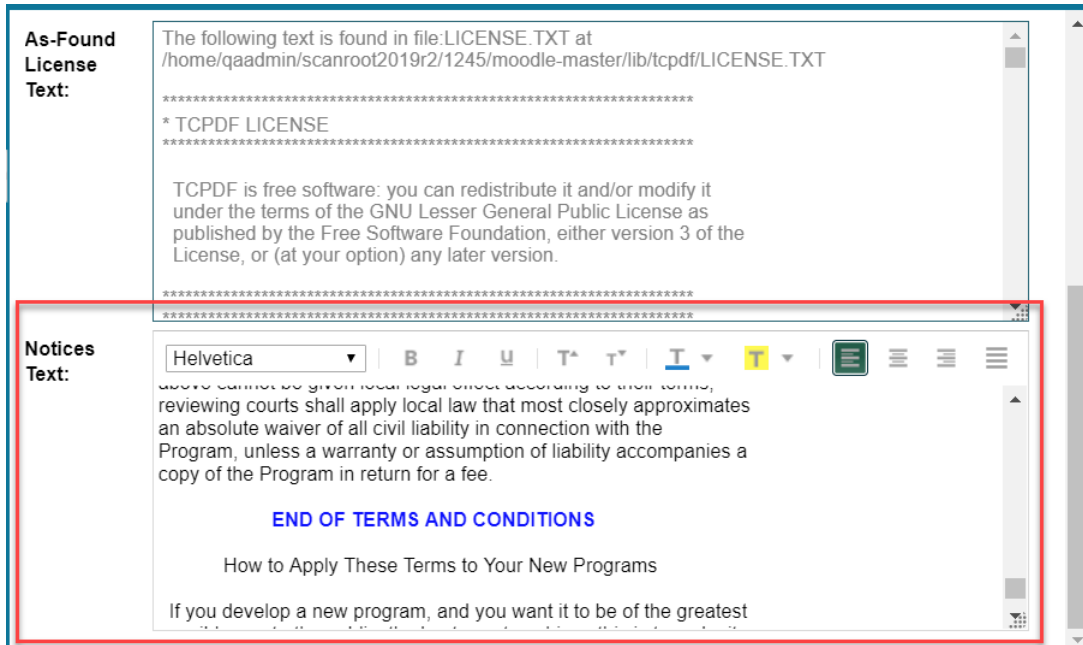
The screenshot shows the 'Licenses & Notices' tab for the item 'prezeskk-tcpdf (LGPL-3.0)' in the 'Project Inventory'. The interface includes 'Recall Item' and 'Edit Item' buttons. The 'Confidence' is shown with a bar chart, 'Vulnerabilities' are 'No', 'Encryption' is 'N/A', and 'Priority' is 'P3'. The 'As-Found License Text' field contains the following text: 'The following text is found in file:LICENSE.TXT at /home/qaadmin/scanroot2019r2/1245/moodle-master/lib/tcpdf/LICENSE.TXT'. The 'Licenses & Notices' tab is highlighted with a red box.

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

For more information about finalizing license text for the Notices report, see [Finalizing the Notices Text for the Notices Report](#).

Notices Text

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



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

For more information about finalizing license text for the Notices report, see [Finalizing the Notices Text for the Notices Report](#).

What Does an Analyst do?

The role of the Analyst is to transform the evidence uncovered by the Scan Server into an inventory item. Analysts create **inventory items** that associate files in your codebase to open source projects. For example, Analysts might evaluate files with a copyright of “Copyright (c) 2015 to 2019 Mark Smith” and a license match to the “zlib” license. Then the Analysts would place these files in a group for the “zlib” open-source project and mark those files as **reviewed** to register progress.

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

Analyzing (Auditing) Scan Results

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

- Discover and remediate code that is under licenses that put your proprietary source code at risk.
- Discover and remediate code with known security vulnerabilities.

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

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

Section Overview

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

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

Opening the Analysis Workbench

Use the following procedure to open the **Analysis Workbench**.



Task

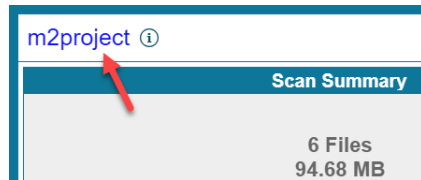
To open the Analysis Workbench, do the following:

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



2. Select **Projects** from the menu. The **Projects** list is displayed.
3. Select a project from the **Projects** list to display its **Project Dashboard** in the right panel.

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

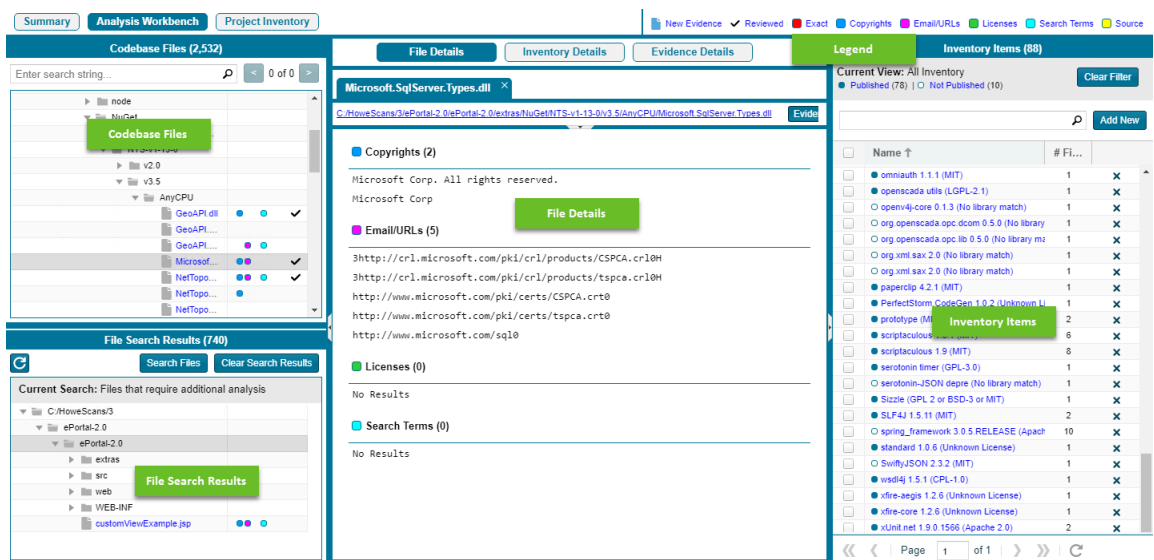


The project opens on either its **Project Inventory** or **Summary** tab (both are displayed). If you have permissions to analyze the scan results, the **Workbench Analysis** tab is displayed.

- Navigate to the **Analysis Workbench** tab to begin the analysis process. See the next section, [The Analysis Workbench Layout](#).

The Analysis Workbench Layout

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



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

- Codebase Files**—Allows you to browse a tree of the scanned files you uploaded for this project.
- File Search Results**—Shows the results of file searches. There are several types of file searches that can be performed. Click a file to see the file's content and evidence in the **File Details** panel.
- File Details**—Shows the actual content of scanned (non-binary) files, including evidence highlighted in color. Here an analyst can research where the code came from to ultimately create an inventory item explaining the scan findings.
- Inventory Items**—Displays a quick view of all the inventory identified in the codebase. Click the name of any item listed in the **Inventory Items** pane to display the inventory details for that item.
- Inventory Details**—Shows information about the selected inventory items identified and used by this codebase.

- **Evidence Details**—Displays evidence that was uncovered by the scan, which is organized and sortable. Click **Evidence Details**, and the middle pane of the **Dashboard** displays details about the evidence. To filter the files in the **File Search Results** to focus attention on a particular finding, select a row or a set of rows and click **Search Files**. For more ways to filter findings, see [Searching for Codebase Files Based on Name](#).
- **Legend**—Provides a key to the colors used in the various panes of the **Dashboard**. The **Legend** is interactive. You can click it to filter what appears in the **File Search Results** pane.



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

Searching for Codebase Files Based on Name

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

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



Task

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

1. In the search text box in the **Codebase Files** pane, enter the partial or full name of the file or folder that you want to search and press **Enter**. You must type at least three characters to initiate the filename search. The text box is highlighted with a red border if you enter fewer than three characters, and an error message is shown in a tooltip.
2. When a match is found, the codebase file tree is expanded as much as necessary to highlight the matching file. The file details are not open until you click on the file in the tree.
3. Select the **Next Match** (>) and **Previous Match** (<) buttons next to the search string box to navigate the results of the search.
 - **Files**—If the Previous or Next match button reaches a file, that file will be highlighted in the codebase tree, and the search term will be highlighted in yellow.
 - **Folders**— If the Previous or Next match button reaches a folder, that folder will be highlighted in the codebase tree and the search term will be highlighted in yellow. The folder will also be automatically expanded one level so that you can see its child items.

The counter between the buttons indicates the total number of matches and the current match number.

4. (Optional) Click the name of a file to display its contents in the **File Details** tab.
5. (Optional) Click the **X** to clear the search string.

Searching for Codebase Files Based on Search Criteria

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



Task

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

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

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

Creating and Editing File Searches

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

- [Creating a New File Search](#)
- [Editing a File Search](#)
- [Copying a File Search](#)
- [Deleting a File Search](#)

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

Creating a New File Search

Use either procedure to create a new file search:

- [Create a File Search from Scratch](#)
- [Create a File Search from a Copy](#)

Create a File Search from Scratch

Use this procedure to create a file search from scratch.



Task

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

1. Navigate to the **Analysis Workbench** tab.
2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.
3. Click **Add New**. The **Create Filter** dialog appears.
4. In the **Name** field, type a name for the search.
5. (Optional) In the **Description** field, type a description of the search. For example, type text that explains what the filter will search for.
6. Enter values in the **Criteria** fields:
 - a. Select a criterion from the drop-down **Select Search Field** menu.
 - b. If applicable, select a search operation (for example, **Contains** or **=**) and provide a search string or value.
 - c. To add another criterion, click **Add Criteria**, select a Boolean value to define how the criteria is applied, and repeat the previous steps to define the criterion. Repeat for each criterion added.
 - d. To add a group of criteria that serves as a criterion, click **Add Criteria Group**, and repeat steps a through c to create the group. The following shows an example of a criteria group:

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



Create a File Search from a Copy

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



Task

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

1. Navigate to the **Analysis Workbench** tab.
2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.
3. Locate the search you want to copy, and click  in its entry. A new file search is created with “Copy of...” in its title.
4. In the entry for the copy, click  to open the filter properties.
5. In the **Name** field, type a new name for the search.
6. Modify the filter criteria as needed and save the changes. See [Create a File Search from Scratch](#) for any additional instructions.


Editing a File Search

Use these instructions to edit an existing file search.



Task

To edit a file search, do the following:

1. Navigate to the **Analysis Workbench** tab.
2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.
3. In the entry for the file search you want to edit, click  to open the filter properties.
4. Modify the filter criteria as needed and save the changes. See [Create a File Search from Scratch](#) for any additional instructions.


Copying a File Search

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



Task

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

1. Navigate to the **Analysis Workbench** tab.
2. In the **File Search Results** pane, click **Advanced Search**. The **Advanced File Search** dialog appears.
3. Locate the search you want to copy, and click  in its entry. A new file search entry is created with “Copy of...” in its title.

Deleting a File Search

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



Task

To delete an existing file search, do the following:

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









Using the Filter Legend Options to Filter the Codebase

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

 New Evidence  Reviewed  Exact  Copyrights  Email/URLs  Licenses  Search Terms  Source

The following describes the filter legend options:

Table 2-4 • Filter Legend

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

The color theme used for evidence types in this legend is also used to indicate the types of evidence found in a given file in the **Codebase Files** and **File Search Results** lists (see the following procedure) and on the **File Details** tab (see [Using the File Details Tab](#)).



Task

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

1. In the **Analysis Workbench**, click the option in the filter legend to identify how you want to filter the codebase files. Results are listed in the **File Search Results** pane.
2. Navigate to the **File Search Results** pane, which now shows a codebase tree containing the files that meet your criterion.
3. Drill down in the codebase tree to view the files.

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

Current Search: Email/URLs		
web		
javascript		
slider.js		
controls.js		
dragdrop.js		
scriptaculous.js		
builder.js		
carpeslider.js		
effects.js		
prototype.js		
lib		

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

Refer to the following sections for different ways to analyze and act on third-party evidence discovered in the files:

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

Using the Codebase Files Pane Context Menu

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

- **Add to inventory**—Select an item listed in the **Codebase Files** list that you want to add to inventory, right-click and choose **Add to inventory** to quickly add your selected items to display the **Add to inventory** dialog. For more information, see [Creating an Inventory Item from the Analysis Workbench](#).
- **Show file inventory**—Select an item listed in the **Codebase Files** list that you want to view in the **Inventory Items** pane, right-click and choose **Show file inventory**. The selected item is listed in the **Inventory Items** pane.
- **Mark as reviewed**—After you have reviewed an item in the **Codebase Files** list, hover over the item, right-click, and then select **Mark as reviewed** to mark the file reviewed and add a checkmark in the **Reviewed** column.
- **Mark as unreviewed**—If you determine that a displayed file has not been reviewed, hover over the item, right-click, and then select **Mark as unreviewed** to mark the file unreviewed and remove the checkmark from the **Reviewed** column.
- **Download File**—Hover your cursor over an item to download, right-click and select **Download File**. The selected item is downloaded to the \temp subdirectory for the open project.

Marking Files as Reviewed

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



Task

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

1. In the **Codebase files** pane of the **Analysis Workbench**, right click on a directory or file you want to mark as reviewed. The **Inventory** popup menu appears.
2. Select **Mark as reviewed**.



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

Viewing Details for Licenses Associated with Codebase Files

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

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



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



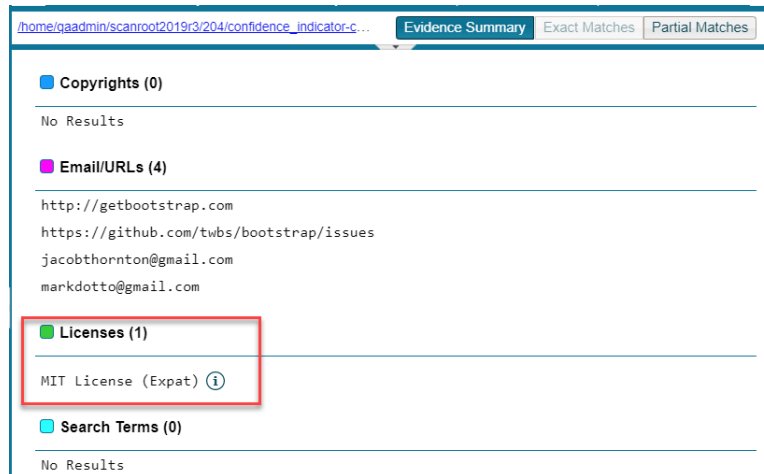
Task

To view details for a license, do the following:

1. (Optional) To make file selection easier, you can filter the codebase files to only those containing license evidence. See [Using the Filter Legend Options to Filter the Codebase](#).
2. In the **Codebase Files** pane or **File Search Results** pane, select the codebase file containing the license evidence you want to review. A file with license evidence will show a green icon in its entry:



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



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

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

For descriptions of these fields on this tab, see [License Details Window](#). Also see [What Does an Analyst do?](#) for background on how the license priority is used.

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

Using the File Details Tab

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

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

Viewing the Evidence Summary for a File

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

- Copyrights
- Emails/URLs
- Licenses
- Search Terms

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



Task

To view the evidence summary, do the following:

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

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

Viewing Binary Strings in a File

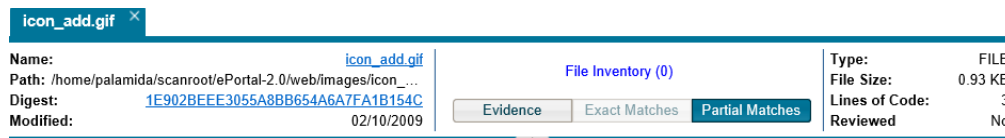
Use this procedure to view the list of strings (each string consisting of at least three consecutive printable characters) found in the content of a binary file. This list enables you to perform a deep search for evidence, such as a copyright or comment snippet, of third-party code in the file.



Task

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

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



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

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

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

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

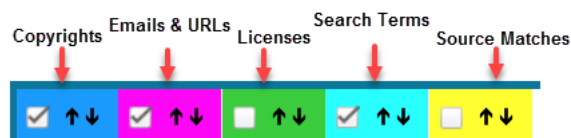


Task


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

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

Color-code selection boxes at the top of the **Partial Matches** tab are used to indicate the type of evidence highlighted in the file. You can hover over a selection box to see a label indicating the type of evidence it highlights. Depending on the types of evidence existing in the file, certain selection boxes might already be selected; others might not be available. (By default, the Licenses selection box is not pre-selected even if license evidence exists in the file; you must manually select it to highlight license evidence.)



4. If necessary, select (or unselect) one or more color-coded selection boxes to highlight the evidence you want to view in the file. For example, the following color-coded selection will highlight (in the same color) each instance of email or URL evidence in the file:



```

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

```

Viewing Exact Matches

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



Task

To review these exact file matches, do the following:

1. Ensure that you have run a scan with **Comprehensive Scan Profile** selected in the project (or a custom scan profile with exact matches enabled). For more information, see “Creating a Scan Profile” in the *FlexNet Code Insight Installation and Configuration Guide*.
2. In the **Analysis Workbench**, click the **Exact** link in the legend at the top right of the page to easily find all files with exact matches (see [Using the Filter Legend Options to Filter the Codebase](#)). Results are listed in the **File Search Results** pane.
3. Click the codebase file from the list in **File Search Results**, and select the **Exact Matches** tab.

The **Remote Files** panels are displayed.

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

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

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

Viewing Source Matches

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



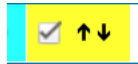
Note • The size limit for a file that you open in the **Partial Matches** tab is 2 MB. If the file you want to inspect is too large, you can download and open it outside of FlexNet Code Insight to inspect it manually for evidence.



Task

To view source matches, do the following:

1. Ensure that you have run a scan with **Comprehensive Scan Profile** selected in the project (or a custom scan profile with source-code matches enabled). For more information, see “Creating a Scan Profile” in the *FlexNet Code Insight Installation and Configuration Guide*.
2. In the **Analysis Workbench**, click the **Source** link in the legend at the top right of the page to filter to all files with source-code matches (see [Using the Filter Legend Options to Filter the Codebase](#)). Results are listed in the **File Search Results** pane.
3. Click a codebase file in the list in **File Search Results**, and select the **Partial Matches** tab.
4. On the **Partial Matches** tab, click the **Source Matches** selection box at the top of the tab to enable *source code fingerprint match* results.



The **Remote Files** panels are displayed.

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

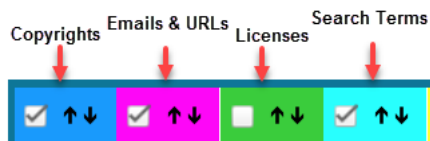
The information in the **Remote Files** panel consists of a set of files from the open source community that contain identical code to the scanned file. This means that the scanned file in the codebase possibly contains content that originated from outside the organization, and its origin needs to be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

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

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

- **CodeRank (CR%)**: A composite heuristic comprised of Coverage, Clustering, and Uniqueness. The higher the number, the stronger the match confidence.
- **Coverage (CV%)**: The percentage of the matching third-party file contained in your scanned file.
- **Clustering (CL%)**: The density or proximity of the source code matches within your scanned file.
- **Uniqueness (U%)**: The uniqueness of the set of discovered source code matches are in the Compliance Library (CL).
- **Matches**: The number of unique matches in the scanned file.

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



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

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

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

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

Note About Filtering in the Panels

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

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

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

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

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

Remote Files Panel




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

The remote files list can be filtered as discussed in [Note About Filtering in the Panels](#).

Components Panel

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

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

- To review the path of a remote file within a component, select the file in the **Remote Files** panel, and then click the **Remote File Paths** icon  in the component row. A remote file is a file found within an open source component release that is either identical to the scanned file, or contains similar partial content as the scanned file. The remote file path is important because similar file structures between the scanned codebase and the remote file content is a potential strong indicator of code reuse from an open source project.
- To view information about the component, click the **Information** icon .
- To add the selected codebase file to an inventory item associated with the component, click the **Add File to Inventory** icon . For more information, see [Adding a Partial or Exact Match Codebase File to an Inventory Item Based on an Associated Component](#).

Licenses Panel

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

You can view information about the license by clicking the **Information** icon  in the license entry.


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

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



Task

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

1. In the **Analysis Workbench**, click the **Exact** or **Source** matches link in the legend at the top right of the workbench to search for codebase files that are exact or partial matches to files in the Compliance Library. Results are listed in the **File Search Results** pane.
2. From the list in **File Search Results**, locate and click the codebase file you want to add to an inventory item based on a specific component version associated with the file.
3. Open the **File Details** tab, and, at the top of the tab, select the **Exact Matches** or **Partial Matches** tab.
Additionally, if you are on the **Partial Matches** tab, select the **Source Matches** checkbox.
4. From the **Remote Files** panel, select the remote file associated with the component on which the inventory item you want to add is based (or will be based if you need to create an inventory item).
5. In the **Components** panel, locate the component version that you believe is the origin of the matching code in the scanned codebase file, and click the **Add File to Inventory** icon  in that component row.

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

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

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

Using the Evidence Details Tab

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

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

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

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

Using the Inventory Details Tab

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

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

- [Editing Inventory from the Analysis Workbench](#)
- [Publishing or Recalling Inventory from Analysis Workbench](#)

Using the Inventory Items Context Menu

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

- **Publish Inventory**—Select inventory items that you would like to publish, right-click, and choose **Publish Inventory** to quickly publish your selected items. Publishing an inventory item makes it visible in the **Project Inventory** view.
- **Recall Inventory**—Select published inventory items that you would like to recall back to an unpublished state, right-click, and choose **Recall Inventory**. The selected items are removed from the **Project Inventory** view and are only visible in the **Analysis Workbench**.



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

- **Show Inventory Files**—To see files associated with the selected inventory items, select the list of inventory items, and right-click and choose **Show Inventory Files**. The associated files will be shown in the **File Search Results** pane.
- **Delete Inventory**—Select inventory items that you want to delete, right-click, and select **Delete Inventory**. The selected items will be deleted from the project.



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

Viewing Security Vulnerabilities for Inventory in Analysis Workbench

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

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



Task

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

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



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

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

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

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

Viewing or Editing Inventory Usage Information from Analysis Workbench

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



Task

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

1. From the **Inventory Details** tab for a selected inventory item in **Analysis Workbench**, select the **Usage** tab.
2. View and, if necessary, edit the usage fields.

For details about the inventory usage fields and how they are used, see [Inventory Usage Information](#).

Component Lookup

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

- [Guidelines for Component Lookup](#)
- [Component Lookup Results](#)
- [Performing Component Lookup](#)

Guidelines for Component Lookup

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

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

- **Apache**— <PROJECT_NAME>, for example “apache-batik”
- **Pypi**—<PACKAGE_NAME>, for example “hash_ring”
- **RubyGems**— <GEM_NAME>, for example “x-editable-rails”
- **Other**— <PROJECT_NAME>, for example “openssl”
- If you cannot locate the component by keyword, select a **Forge** or **URL** search. If you are still unable to locate the component, the component might not exist in the FlexNet Code Insight data library. In this case, you have options to do one of the following:
 - Create your inventory item as **Work in Progress** and name it using the convention <COMPONENT> <VERSION> (<LICENSE>). For example, **myComponent 1.2 (MIT)**. (You can later edit this inventory item to convert it to one of the other inventory types—**Component** or **License**.)
 - Create a custom component. See [Creating and Editing Custom Components](#) for details.

Component Lookup Results

Component Lookup search results are prioritized in the following order:

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

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

Performing Component Lookup



Task

To perform a Component Lookup, do the following:

1. Open a project and navigate to **Analysis Workbench** (or the **Project Inventory** tab).
2. Select an inventory item from the list in the **Inventory Items** pane. The item appears in the **Inventory Details** pane. (For an item selected from the **Project Inventory** tab, you need to also click **Edit Item** to proceed with the next step.)
3. From the **Type** dropdown, select **Component** and click **Lookup Component**. The **Lookup Component** window appears.
4. Select the search type (**Keyword**, **URL**, or **Forge**), and enter the required search criteria. See [Guidelines for Component Lookup](#).

Click **Search** to find components matching your search criteria. For information about the results of the Component Lookup, see [Component Lookup Results](#).

Creating an Inventory Item from the Analysis Workbench

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

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

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

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

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

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

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

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

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

Creating Inventory from the Inventory Items List

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



Task

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

1. If not already on the **Analysis Workbench**, navigate to it.
2. Navigate to the **Inventory Items** list.
3. Click **Add New** at the top of the **Inventory Items** list. A new item, showing default values, opens in its own tab on the **Inventory Details** tab.
4. For the **Name** field, perform the appropriate step, based on the inventory type you intend to select for the **Type** field (see the next step):
 - For inventory of the type **Work in Progress**, specify a name for the inventory item. Best practice is to provide a name in the following conventional syntax used by Code Insight, even if the elements represented in the name are not available in the data library:

<COMPONENT_NAME> <VERSION> (LICENSE_NAME)

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

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

The following are basic steps for using Component Lookup. For details, see [Component Lookup](#).

- a. Click the **Lookup Component** button to locate the component of interest (as described in the next steps) or to create a custom component and instance to associate with the inventory item (see [Creating and Editing Custom Components](#) for continued steps).
- b. In the list of results, navigate to the appropriate component, and click **Show Versions** to display the list of registered instances for that component.
- c. Click **Use This Instance** next to an existing registered instance to associate that instance with the inventory item.

or

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

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

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

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

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

6. Update the remaining fields if appropriate:
 - **Description**—Provide any meaningful information about the inventory item. When the inventory type is **Component**, this field is automatically populated with information about the component, license, or both, but can be edited.
 - **Url**—Enter the website for the third-party code or artifact represented by the inventory item.
 - **Disclosed**—Indicate whether the third-party component or artifact represented by the inventory item was a *known* third-party dependency in your code before it was discovered by the scan or you.
 - For **Distribution Type**, **Part of Product**, **Linking**, **Modified**, or **Encryption**, see [Inventory Usage Information](#).
7. (Recommended) On the **Notes** tab, add content to the **Audit Notes** pane to indicate that this inventory item was manually created. This is helpful information for other auditors and for reviewers.
8. (Optional) Drag and drop one or more files from the **Codebase Files** list (or **File Search Results** list) to the **Associated Files** tab to associate files with the inventory item.
9. When you completed the details for the new inventory item, click **Save**. The name of the inventory item appears in the **Inventory Items** pane.
10. (Optional) To report on newly created or edited inventory items, click **Publish**.

Creating Inventory from the Codebase Lists

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

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



Task

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

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

Add Selected Codebase Files to Existing Inventory

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



Task

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

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

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

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



Task

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

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

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

Editing Inventory from the Analysis Workbench

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



Task

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

1. If not already on the **Analysis Workbench**, navigate to it.
2. Navigate to the **Inventory Items** list in the right pane.
3. Select the inventory item that you want to edit.

A new tab, labeled with the inventory name and showing information about the inventory item, is opened within the **Inventory Details** tab.
4. Make changes to the fields as needed. Refer to [Creating Inventory from the Inventory Items List](#) for field descriptions and additional steps required when updating the inventory type.

Note the following:

- For a **Component** inventory item, you can use the Component Lookup feature to select a different registered instance (or create a new one) or to create a custom component and instance to associate with the inventory item. The **Name**, **Component**, and **License** fields are updated accordingly.
 - You can convert a **Work In Progress** or **License Only** inventory item to a different inventory type, using the **Type** field and performing the additional steps required for the type. The **Name** and other appropriate fields are updated accordingly.
 - If you need to update the component version or associated license only, simply click the Edit (✎) icon next to the **Component** or **License** value, and select a different license or version or both. (This avoids performing a Component Lookup process to edit these elements.)
 - Update any of the other fields as necessary.
5. Click **Save** to change the changes to the inventory item.

Publishing or Recalling Inventory from Analysis Workbench

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

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

- [Publish or Recall an Inventory Item from the Inventory Details Tab](#)
- [Publish or Recall Inventory from the Inventory Items Pane](#)



Note • If you enabled the auto-publish feature in the project scan settings, you do not need to perform the steps below because system-created inventory items are automatically published.

Publish or Recall an Inventory Item from the Inventory Details Tab

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



Task

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

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

or

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

Publish or Recall Inventory from the Inventory Items Pane

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



Task

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

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

or

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



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

Inventory Items (32)		
Current View: All Inventory		
<input checked="" type="radio"/> Published (22) <input type="radio"/> Not Published (10)		
<input type="text"/> <input type="button" value="Add New"/>		
<input type="checkbox"/>	Name ↑	# Files
<input checked="" type="checkbox"/>	cssnormalize-context 0.4.2	1
<input checked="" type="checkbox"/>	dump (BSD or BSD-3-Clause)	1
<input checked="" type="checkbox"/>	file (BSD Style/Attribution or BSD-3-Clause or ...)	1
<input checked="" type="checkbox"/>	jquery (MIT)	3
<input checked="" type="checkbox"/>	jquery 1.10.2 [Found inside complexscorm.zip] ...	1
<input checked="" type="checkbox"/>	jquery 1.2.6 (GPL-2.0 or MIT)	1
<input checked="" type="checkbox"/>	jQuery 3.2.1 (MIT)	2
<input checked="" type="checkbox"/>	jquery-ui.structure 1.12.1	1
<input checked="" type="checkbox"/>	jquery-ui.theme 1.12.1	1
<input checked="" type="checkbox"/>	jqueryui 1.11.0 [Found inside complexscorm.zi...	1

2. Right click to open the context menu, and choose either **Publish Inventory** or **Recall Inventory**.
 - If you selected **Publish Inventory**, the newly published items appear in the **Inventory Items** list with a filled box icon before their names (and are now listed in **Project Inventory**).
 - If you selected **Recall Inventory**, the recalled items appear in the **Inventory Items** list with a clear box icon before their name (and are no longer listed in **Project Inventory**).



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

Reviewing Published Inventory

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

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

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

- [Goal of the Reviewer](#)
- [Displaying Project Inventory](#)
- [Searching Published Inventory](#)
- [Viewing Security Vulnerabilities for Project Inventory](#)
- [Viewing Details for the Licenses Associated with Project Inventory](#)
- [Viewing and Updating Notes & Guidance](#)
- [Viewing Usage Information for Project Inventory](#)
- [Viewing Associated Files](#)
- [Creating Inventory from the Project Inventory Tab](#)
- [Editing Inventory from the Project Inventory Tab](#)
- [Approving or Rejecting Inventory Items](#)
- [Creating and Viewing External Work Items for a Project Inventory Task](#)
- [Recalling a Published Inventory Item](#)
- [Managing Security Vulnerability Alerts](#)

Goal of the Reviewer

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

Displaying Project Inventory

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



Task

To view project inventory, do the following:

1. Open a project and click the **Project Inventory** tab. The **Inventory Items** list pane is displayed on the left.
2. From the list, click the inventory item you want to review. Information about the selected item is displayed in the **Inventory Details** pane on the right.
3. Select any of the tabs to display additional information about the inventory item.
4. To view the published inventory items sequentially:
 - Use the up and down arrows on your keyboard to step through inventory items quickly.
 - Use the **Next Item** and **Previous Item** buttons to move among inventory items.
5. You can view or change various details on the tabs, as well as change priority and status. For more information about the fields on the tabs, see [Inventory Details Pane](#).

Searching Published Inventory

FlexNet Code Insight provides the **Advanced Search** dialog to enable you to quickly filter the list of published inventory items to those of interest based on inventory name, associated security vulnerabilities, and open security vulnerability alerts. In this way, you can easily find the inventory items of interest in the list of published items. The following procedure shows you how to access and use this dialog. Refer also to the [Performing Advanced Searches](#) chapter for practical applications of this search feature.



Task

To filter published inventory, do the following:

1. Open a project, and click the **Project Inventory** tab. The **Inventory Items** pane appears, showing the list of inventory items.
2. Click the **Advanced Search** button at the top of the list to open the **Advanced Inventory Search** dialog.

Advanced Inventory Search

Inventory Items	Security Vulnerabilities	Licenses and Versions
Inventory Name: <input type="text" value="Enter Inventory Name"/>	Security Vulnerability ID: <input type="text" value="Enter Vulnerability ID"/>	License Name: <input type="text" value="Enter License Name"/>
Inventory Priority: <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4	Security Vulnerability Severity: <input type="checkbox"/> Critical (CVSS 9.0 - 10.0) <input type="checkbox"/> High (CVSS 7.0 - 8.9) <input type="checkbox"/> Medium (CVSS 4.0 - 6.9) <input type="checkbox"/> Low (CVSS 0.1 - 3.9) <input type="checkbox"/> None (CVSS = 0)	License Priority: <input type="checkbox"/> P1 - Viral / Strong Copyleft <input type="checkbox"/> P2 - Weak Copyleft / Commercial / Uncommon <input type="checkbox"/> P3 - Permissive / Public Domain <input type="checkbox"/> No License Found
Inventory Review Status: <input type="checkbox"/> Approved <input type="checkbox"/> Rejected <input type="checkbox"/> Not Reviewed	Security Vulnerability Age: <input type="text" value="Any"/>	Version: <input type="checkbox"/> No Associated Version
Dependency Options: <input type="text" value="All Inventory Items"/>		
Inventory Age: <input type="text" value="Any"/>		
Inventory Notifications: <input type="checkbox"/> Inventory with Open Alerts <input type="checkbox"/> Inventory Rejected Due to New Non-Compliant Security Vulnerabilities		
Inventory Tasks Age: <input type="text" value="Any"/>		
Inventory Task Owner: <input type="text"/>		

Apply Or Criteria

Apply Clear Form Close

- From this dialog, select search criteria as needed from the following categories. For a detailed description of the search criteria, see [Advanced Inventory Search Page](#).
 - Inventory Items**—Search for inventory items that have a certain name (or string), priority, review status, or age or that have open vulnerability alerts and work items. (For details on alerts and work items, see [Managing Security Vulnerability Alerts](#) and [Creating and Viewing External Work Items for a Project Inventory Task](#).)
 - Security Vulnerabilities**—Search for inventory items that have vulnerabilities of a certain vulnerability ID, CVSS severity, or age. (Note that list of available severities for **Security Vulnerability Severity** varies depending on the CVSS version being used by Code Insight. The picture above shows the severities for CVSS v3.0. See [Security Vulnerabilities Associated with Inventory](#) for details.)
 - Licenses**—Search for inventory items that have licenses of a certain of a certain name or license priority.
- Select **And** or **Or** from the **Apply Criteria** field.
- Click **Apply** to filter the inventory to display only those inventory items that meet the selected criteria.
- To refresh the list to show all inventory items, click **Show All Items**.

Viewing Security Vulnerabilities for Project Inventory

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

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



Task

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

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



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

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

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

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

Viewing Details for the Licenses Associated with Project Inventory

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

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

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



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



Task

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

1. If you are not there already, navigate to the **Project Inventory** tab.
2. Click a published inventory item from the **Inventory Items** list.
3. Select the **Component Details** tab. The license selected for this component is listed as the selected license.

4. Click the information icon (i) next to the **Selected License** value (the license currently associated with the inventory item) or the **Possible Licenses** (other valid license candidates with which you could associate the inventory item). The **License Details** window appears with the **General Information** tab in focus.

For descriptions of these fields on this tab, see [License Details Window](#). Also see [What Does an Analyst do?](#) for background on how the license priority is used.

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

Viewing and Updating Notes & Guidance

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



Task

To view notes and guidance, do the following:

1. If you are not there already, navigate to the **Project Inventory** tab.
2. Select an inventory item from list.
3. Select the **Notes & Guidance** tab to view or edit notes that can help in reviewing or remediating the inventory item. For example, if the inventory item was manually created, you might include a note that specifies this.
4. Review or update content in the panes as needed.

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

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

Viewing Usage Information for Project Inventory

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



Task

To view inventory usage information, do the following:

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

Viewing Associated Files

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



Task

To view associated files, do the following:

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

Creating Inventory from the Project Inventory Tab

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

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

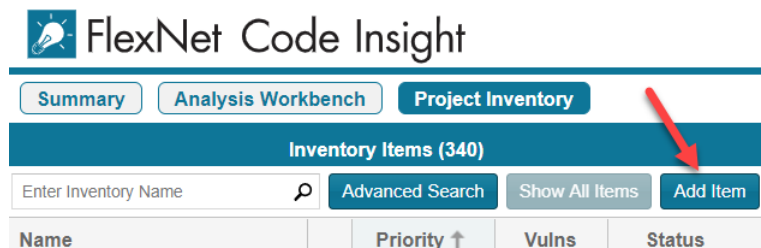
- When you save the inventory item, it is automatically published.
- No files can be associated with an inventory item when it is created from the **Project Inventory** tab.
- If you register a new component instance (a unique component-version-license combination) when creating inventory, the registered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



Task

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

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



The **New Inventory** dialog opens.

3. For the **Name** field, perform the appropriate step, based on the inventory type you intend to select for the **Type** field (see the next step):
 - For inventory of the type **Work in Progress**, specify a name for the inventory item. Best practice is to provide a name in the following conventional syntax used by Code Insight, even if the elements represented in the name are not available in the data library:
`<COMPONENT_NAME> <VERSION> (LICENSE_NAME)`
 - For inventory of the type **Component** or **License only**, leave the **Name** field blank. The field will be automatically populated based on the registered component or license instance.
4. From the **Type** dropdown, select the type of inventory item you want to create and perform the related step or steps:
 - **Work in Progress**—Create this type of inventory item if you want to quickly represent third-party code or an artifact without having to select an associated component, version, or license from the data library. (You can later edit this inventory item to convert it to one of the other inventory types.) This option is typically used if you need a placeholder or cannot find the associated element in the data library. Items of type **Work in Progress** are not affected by policies and do not receive vulnerability updates or alerts.
 - **Component**—Create this type of inventory item if you know the component, version, and license for the third-party code or artifact *and* you either are able to locate it in the Code Insight data library using the Component Lookup feature or you need to create it as a custom component because it is not in the library. This type of inventory is associated with a registered component instance—that is, a unique component-version-license combination—and is affected by policies and receives vulnerability updates and alerts.

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

The following are basic steps for using Component Lookup. For more details, see [Component Lookup](#).

- a. Click the **Lookup Component** button to locate the component of interest (as described in the next steps) or to create a custom component and instance to associate with the inventory item (see [Creating and Editing Custom Components](#) for continued steps).
- b. In the list of results, navigate to the appropriate component, and click **Show Versions** to display the list of registered instances for that component.
- c. Click **Use This Instance** next to an existing registered instance to associate that instance with the inventory item.

or

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

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

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

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

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

5. Update the remaining fields if appropriate:
 - **Description**—Any meaningful information about the inventory item. When the inventory type is **Component**, this field is automatically populated with information about the component, license, or both, but can be edited.
 - **Url**—The website for the third-party code or artifact represented by the inventory item.
 - **Disclosed**—Indicates whether the third-party component or artifact represented by the inventory item was a *known* third-party dependency in your code before it was discovered by the scan or you.
 - For **Distribution Type**, **Part of Product**, **Linking**, **Modified**, or **Encryption**, see [Inventory Usage Information](#).
6. Click **Save**. The name of the inventory item is added to the **Inventory Items** list.

Editing Inventory from the Project Inventory Tab

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



Task

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

1. Navigate to the **Project Inventory** tab.
2. In the **Inventory Items** list, select the inventory item that you want to edit. Information about the inventory item is displayed in the right pane.
3. In the header on the right pane, click the **Edit Item** button next to the component name.



The **Edit Inventory** dialog opens.

4. Make changes to the fields as needed. Refer to [Creating Inventory from the Project Inventory Tab](#) for field descriptions and additional steps required when updating the inventory type. Note the following:
 - For a **Component** inventory item, you can use the Component Lookup feature to select a different registered instance (or create a new one) or to create a custom component and instance to associate with the inventory item. The **Name**, **Component**, and **License** fields are updated accordingly.
 - You can convert a **Work In Progress** or **License Only** inventory item to a different inventory type, using the **Type** field and performing the additional steps required for the type. The **Name** and other appropriate fields are updated accordingly.
 - If you need to update the component version or associated license only, simply click the Edit (✎) icon next to the **Component** or **License** value, and select a different license or version or both. (This avoids performing the longer Component Lookup process to edit these elements.)

- Update any of the other fields as necessary.
 - No additional files can be associated with an inventory item from **Project Inventory** tab.
5. Click **Save** to change the changes to the inventory item.

Approving or Rejecting Inventory Items

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



Task

To approve or reject inventory items, do the following:

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

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

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

Creating and Managing Tasks for Project Inventory

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

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

The following topics are described in this section:

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

Note About External Work Items

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

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

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

Manually Creating a Task

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

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



Task

To create a task manually, do the following:

1. Navigate to the **Project Inventory** page.
2. Select the inventory item to which you want to add a task. Alternatively, to help you locate the inventory item, click the **Advanced Search** button to open the **Advanced Inventory Search** dialog. From here you can filter inventory items accordingly.

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

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

4. Select the type of task you want to create—**Manual Inventory Review**, **Remediate Inventory**, or **Miscellaneous**. (Refer to the descriptions of task types earlier in this section.)
5. Complete the following fields as needed:
 - In the **Summary** field, provide a summary or title for the task.
 - In the **Details** field, provide instructions or requirements for completing this task (or provide any information that will be useful to the reviewer).
 - Keep the **Status** as **Open** for a new task.
6. By default, the new task is assigned to the default point of contact (defined for the project), as listed in the **Owner** field. To change the task owner, click the **Assign** button under the **Owner** field, and select a new owner.
7. To create an external work item associated with the task, click the **Create Work Item** button. (See [Creating and Viewing External Work Items for a Project Inventory Task](#) for details.)

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

You can repeat this step to create another work task.

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

Editing a Task

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



Task

To edit a task, do the following:

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

2. Select the inventory item to which the task you want to edit is associated. Alternatively, click the **Advanced Search** button to open the **Advanced Inventory Search** dialog, where you can select filters that help you pinpoint the inventory item. For example, you can select to filter on those inventory items associated with tasks that are assigned to a specific user or created within a certain date range.

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

3. In the **Tasks** section, click the **x Open Tasks** or **x Closed Tasks** link to view the **Tasks** list for the inventory item. (Use the search filter at the top of the dialog to show **All**, **Open**, or **Closed** tasks.
4. Locate the appropriate task from the **Tasks** list, and click the link in the **Summary** column to show the **Task Details** dialog.

The screenshot shows a 'Create Task' dialog box. It has a title bar with 'Create Task' and a close button. The main area contains several fields: 'Type' is set to 'Miscellaneous', 'Summary' is 'Task for apache 2.4.6 (Artistic-1.0)', 'Details' is 'Helvetica', 'Status' is 'Open', 'Priority' is 'Medium', 'Owner' is 'Admin User', and 'Work Items' is 'None'. There are buttons for 'Assign', 'Create Work Item', 'Save', and 'Close'.

5. Use the information in [Manually Creating a Task](#) for updating the task fields or adding an external work item. To change the status of the task, see either [Closing or Reopening a Review Task](#) or [Closing or Reopening a Remediation or Miscellaneous Task](#).
6. Click **Save** to save the updates.

Closing or Reopening a Review Task

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

- If the inventory item has only one review task associated with it, the **Approve** or **Reject** status of the task sets the inventory item status to **Approve** or **Reject** accordingly.
- If the inventory item has two or more review tasks associated with it, the **Reject** status of a single review task automatically sets the inventory item status to **Reject**. All review tasks are closed but can be reopened for further investigation.
- If an inventory item has two or more review tasks associated with it and these tasks are a combination of open tasks and tasks with an **Approve** status, the inventory item retains its **Not Reviewed** status.

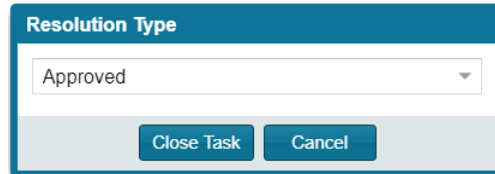
Note that, depending on the inventory review and remediation options defined for the project, the **Reject** status that is automatically set when you close a **Manual Inventory Review** task can automatically create a **Remediate Inventory** task. For more information about these options, see [Updating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



Task

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

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



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

Closing or Reopening a Remediation or Miscellaneous Task

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

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



Task

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

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

Creating and Viewing External Work Items for a Project Inventory Task

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

The following topics are described in this section:

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

Prerequisite

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

Manually Creating a Work Item

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

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



Task

To create a work item manually, do the following:

1. Navigate to the **Project Inventory** page.
2. Select the inventory item associated with the task to which you want to add a work item. Alternatively, click the **Advanced Search** button to open the **Advanced Inventory Search** dialog, where you can select filters that help you pinpoint the inventory item. For example, you can select to filter on those inventory items associated with tasks that are assigned to a specific user or created within a certain date range.

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

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



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

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

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

7. Click **Create Work Item**.

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

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

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

Viewing a Work Item

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



Task

To view a work item, do the following:

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

Recalling a Published Inventory Item

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

Managing Security Vulnerability Alerts

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

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

Refer to these topics for more information:

- [Accessing Security Vulnerability Alerts](#)
- [Managing Security Vulnerability Alerts](#)

Accessing Security Vulnerability Alerts

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

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

From Email Notifications

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

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

From Analysis Workbench

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

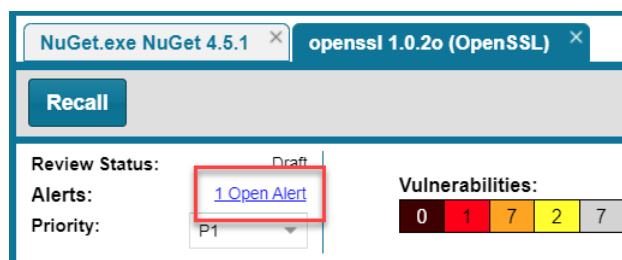


Task

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

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

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



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

From Project Inventory

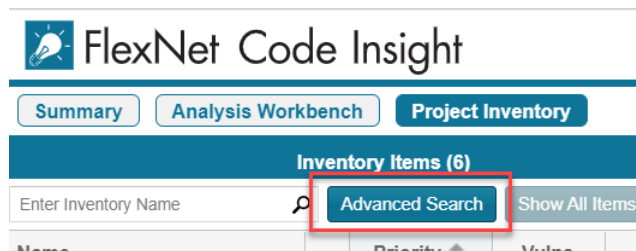
This procedure describes how to access the security vulnerability alerts for a specific inventory item from the **Project Inventory** tab for a project.




Task

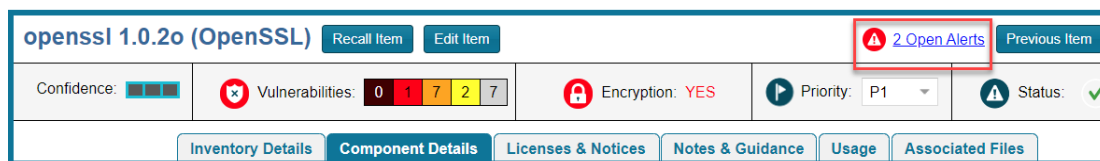
To view security vulnerability alerts from Project Inventory, do the following:

1. Open the **Project Inventory** tab for a project. The **Inventory Items** list is displayed in the left pane.
2. (Optional) To filter the **Inventory Items** list to show only inventory that have alerts, click **Advanced Search**, select the **Inventory with Open Alerts** option, and click **Apply**.



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

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



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



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

Managing Security Vulnerability Alerts

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

- [Alert Details](#)
- [Changing the Priority of an Alert](#)
- [Changing the Status of an Alert](#)

Alert Details

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

Table 2-5 • Information on the Alerts dialog

Column	Description
Type	The alert type. Currently, only New Vulnerability alerts are available.
Date	The date that the alert was generated.
Priority	<p>The priority of the alert, which, by default, is based on the official severity level of the security vulnerability associated with the alert, as described here:</p> <ul style="list-style-type: none"> • High—The default when the vulnerability severity level is Critical, High, or None in the CVSS v3.0 scoring system or, in the CVSS v2 scoring system, High or Unknown. • Medium—The default when the severity level is Medium in either scoring system. • Low—The default when the severity level is Low in either scoring system. <p>You can change this value as needed. See Changing the Priority of an Alert.</p> <p>For more information about the severity levels for security vulnerabilities, see Viewing Security Vulnerabilities for Project Inventory.</p>
Status	<p>The status of the alert in FlexNet Code Insight:</p> <ul style="list-style-type: none"> • Open—The alert needs to be addressed. • Closed—The alert has been addressed (usually because remediation was performed or it was determined to be a false positive for your code). The ⓘ icon is shown to identify who closed the alert and when. <p>Change this value as needed. See Changing the Status of an Alert.</p>

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

Column	Description
Details	<p>Details about the security vulnerability:</p> <ul style="list-style-type: none">● Source—The advisory database in which the Code Insight located the vulnerability, such as NVD (National Vulnerability Database), Secunia (Secunia Advisories), Debian Advisories, or others.● ID—The identification number of the vulnerability associated with the Common Vulnerabilities and Exposures (CVE). If this is a hyperlinked value, click it to go to the actual entry for the vulnerability on the advisory website.● CVSS Score—The score of the vulnerability based on the Common Vulnerability Scoring System (CVSS). The values of the CVSS score range from 0.1 to 10, with 10 being the most serious. If the vulnerability has no score, the value is N/A.● Description—The description of the vulnerability as found in the advisory database. <p>Also see Security Vulnerabilities Associated with Inventory.</p>

Filtering Alerts

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



Task

To filter the list of alerts, do the following:

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

Type	Date ↓	Priority	Status
New Vulnerability	9-20-2019	Medium	Open

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

Changing the Priority of an Alert

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



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



Task

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

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

Changing the Status of an Alert

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

For more information about the **Open** and **Closed** statuses, see [Alert Details](#).



Task

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

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

Creating and Editing Custom Components

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

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

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

- [Creating a Custom Component](#)
- [Editing a Custom Component](#)
- [Custom Component Properties](#)
- [Supported Forge-URL Domains for Custom-Component Creation](#)

Creating a Custom Component

Use the following steps to create a custom component:

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

Step 1: Access the Component Lookup Feature

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



Task

To access the Component Lookup feature, do the following:

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

The screenshot shows a 'New Inventory' window with a title bar. Below the title bar is a section titled 'Inventory Details'. It contains three fields: 'Name' with a text input, 'Type' with a dropdown menu showing 'Component', and 'Description' with a text area. A blue button labeled 'Lookup Component' is positioned to the right of the 'Type' dropdown.

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

Step 2: Create the Custom Component

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

- [Create the Custom Component Based on a Keyword in Its Name or Title](#)
- [Create the Custom Component Based on Its Project or Forge URL](#)
- [Create the Custom Component Based on Its Forge](#)
- [Create the Custom Component in Free Form](#)

Create the Custom Component Based on a Keyword in Its Name or Title

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



Task

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

1. On the **Lookup Component** window, select the **Keyword** option.
2. In the **Keywords** field, enter a keyword used in the name of the component you are creating.

3. (Optional) Click **Search** to see the list of existing components whose names contain the keyword. If the component you intend to create already exists, you can select an instance of the already existing component to associate with the inventory item, or you can continue to create a custom component with different name and title (continue with the next step).

Keep in mind that the name and title of a component you create must be unique in the FlexNet Code Insight data library.

4. Click **Create New Component** to open the **New Custom Component** window, showing the **Name** and **Title** fields automatically populated with the keyword you entered.

Note that window opens in the Free Form format, enabling you to add missing values and edit pre-populated values for the component as needed.

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

6. Click **Save**.

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

Create the Custom Component Based on Its Project or Forge URL

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



Task

To create a custom component based on its URL:

1. On the **Lookup Component** window, select the **URL** option.
2. In the **URL** field, enter URL for the component. As you enter the URL, it is checked for an acceptable format (such as <http://example.com>), but not for validity.

3. (Optional) Click **Search** to see the list of existing components that use the entered URL. If the component you intend to create already exists in the FlexNet Code Insight data library, you can select an instance of the already-existing component to associate with the inventory item; or you can continue to create a custom component with a different name and title (continue with the next step)
4. Click **Create New Component**.
 - If Code Insight recognizes the URL you entered as belonging to one of the forge-URL domains currently supported for custom component creation, the **New Custom Component** window opens, showing component fields—including **Name**, **Title**, **URL**, and **Forge**—automatically populated with values based on domain conventions. (For the list of supported domains, see [Supported Forge-URL Domains for Custom-Component Creation](#).)

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

5. Update the component fields as necessary, noting that the **Name**, **Title**, and **URL** fields are required. For more information about these fields, see [Custom Component Properties](#).
 - If the URL you initially entered (at the top of the window) belongs to a supported domain and you edit that URL, click **Get Details** to update the remaining field values according to forge-URL domain conventions.
 - If you must manually provide field values because the URL you initially entered does not belong to a supported domain, click **?** in the upper part of the window for examples of the standard name, title, and URL conventions used by the **Forge** value you select.
6. Click **Save**.
 - If the required information has been properly entered, the component is saved to the Code Insight data library and listed in **Lookup Component** window. Continue with [Step 3: Associate an Instance of the Custom Component with the Inventory Item](#).
 - If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

Create the Custom Component Based on Its Forge

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



Task


To create a custom component based on its forge:

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

3. (Optional) Click **Search** to see the list of existing components that use the entered forge specifications. If the component you intend to create already exists in the FlexNet Code Insight data library, you can select an instance of the already-existing component to associate with the inventory item; or you can continue to create a custom component with a different name and title (continue with the next step).
4. Click **Create New Component**.
 - If the forge you entered is one of the forge-URL domains currently supported for custom component creation, the **New Custom Component** window opens, showing component fields—including **Name**, **Title**, and **Forge**—automatically populated with values based on domain conventions. (For the list of supported domains, see [Supported Forge-URL Domains for Custom-Component Creation](#).)

- If the forge you entered is not one of the supported domains, the **New Custom Component** window opens, showing the **Forge** field automatically populated with the forge type you selected.

Note that **New Custom Component** window opens in the **Free Form** mode, enabling you to add missing values and edit pre-populated values for the component as needed.

5. Update the component fields as necessary, noting that the **Name**, **Title**, and **URL** fields are required. (Click  in the upper part of the window for examples of the standard name, title, and URL conventions used by the **Forge** value you selected.) If you do not know the URL, enter **NA**. For more information about these fields, see [Custom Component Properties](#).
6. Click **Save**.
 - If the component information has been properly entered, the component is saved to the Code Insight data library and listed in **Lookup Component** window. Continue with [Step 3: Associate an Instance of the Custom Component with the Inventory Item](#).
 - If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

Create the Custom Component in Free Form

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




Task

To create a custom component in Free Form mode:

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

The window opens in the **Free Form** form, enabling you to provide your own values for the component fields. (No field values are automatically populated.)

Optionally, you can switch to the **URL** form on the **New Custom Component** window, enabling you to enter a project or forge URL by which to create the component. Once you enter the URL, you must click **Get Details** to continue:

- If the URL belongs to a supported forge-URL domain, component fields are automatically populated with values based on domain conventions, as described in [Create the Custom Component Based on Its Project or Forge URL](#).
 - If the URL does not belong to a supported domain (that is, Code Insight is unable to parse the URL), you must click **OK** on the resulting “Unable to parse URL...” message box to proceed to manually complete component fields in **Free Form** mode (continue with the next step 2).
2. Update the component fields, noting that the **Name**, **Title**, and **URL** fields are required. (Click  in the upper part of the window for examples of the standard name, title, and URL conventions used by the **Forge** value you select.) If you do not know the URL, enter **NA**. For more information about these fields, see [Custom Component Properties](#).
 3. Click **Save**.
 - If the component information has been properly entered, the component is saved to the Code Insight data library and listed in **Lookup Component** window. Continue with [Step 3: Associate an Instance of the Custom Component with the Inventory Item](#).
 - If the component name and title combination already exists in the data library, an error message is displayed. You can either select the already-existing component from the **Lookup Component** window to associate it with the inventory item or edit the custom component details to provide a different name or title.

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

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

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



Task

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

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

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

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

Editing a Custom Component

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



Task To edit a custom component, do the following:

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

The screenshot shows a 'New Inventory' form with a blue header. Under 'Inventory Details', there are three fields: 'Name' (a text input), 'Type' (a dropdown menu currently showing 'Component'), and 'Description' (a text area). A blue button labeled 'Lookup Component' is positioned to the right of the 'Type' dropdown.

2. Click **Lookup Component** to open the **Lookup Component** window.
3. Search for the custom component by keyword, URL, or forge.
4. Locate the component in the search results, and update the component in any of these ways:
 - Click **Edit Custom Component** to update the component properties. See [Custom Component Properties](#) for field descriptions.
 - Click **Show Versions** to create one or more component-version-license instances for the component.

The screenshot shows the 'Lookup Component' window. On the left is the GitHub logo. To its right is the text 'abc20js/abc20 - GitHub' and the URL 'https://github.com/abcjs/abc'. On the right side, there are three icons with labels: a plus icon for 'Component:', a list icon for 'Possible Licenses:', and a plus icon for 'Custom Component:'. At the bottom, there is a blue button labeled 'Edit Custom Component' and a link labeled 'Show Versions'. Two red arrows point to the 'Edit Custom Component' button and the 'Show Versions' link.

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

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




Custom Component Properties

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

Table 2-6 • Fields to Define a Custom Component

Component Field	Description
Create Using	<p>(Available during component creation) The “form” mode used to create the custom component. The information you entered on the Lookup Component window initially determines the mode used, but you can switch modes here.</p> <ul style="list-style-type: none">● URL—Mode used when creating the component based on the URL for its project or forge (see Create the Custom Component Based on Its Project or Forge URL). This form includes the actual URL value, located beneath the Create Using section, which is either pre-populated from the Component Lookup window or manually entered here. If necessary, click Get Details to view component fields to complete or update them. <p>If the URL is recognized as belonging to a supported forge-URL domain supported for custom component creation, required component fields are automatically populated on the Component Lookup window. See the URL field description next in this table for more information.</p> <ul style="list-style-type: none">● Free Form—Mode used to define or update component fields manually when creating the custom component using any other method (see Create the Custom Component Based on a Keyword in Its Name or Title, Create the Custom Component Based on Its Forge, Create the Custom Component in Free Form). Certain fields might be automatically populated based on the information entered previously on the Lookup Component window.
URL	<p>(Available under Create Using during component creation when the URL form is selected) The project or forge URL for which you are creating the custom component.</p> <p>If the URL is recognized as belonging to a supported forge-URL domain supported for custom component creation, required component fields are automatically populated according to domain conventions. Any change made to this URL is automatically updated to the other field values when you click Get Details.</p> <p>If the URL does not belong to a supported domain, you must manually provide all remaining necessary component details. (Click Get details to display the fields.)</p> <p>For information about supported forge-URL domains, see Supported Forge-URL Domains for Custom-Component Creation.</p>

Table 2-6 • Fields to Define a Custom Component (cont.)


Component Field	Description
Name	<p>(Required) The name of the custom component. During component creation, this field might be automatically populated based on information entered on the Lookup Component window.</p> <p>To help you provide this value in an appropriate format, click  in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains.</p>
Title	<p>(Required) The component title. During component creation, this field might be automatically populated based on information entered on the Lookup Component window.</p> <p>To help you provide this value in an appropriate format, click  in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains.</p>
Description	A description of the custom component to provide any additional meaningful information about the component.
URL	<p>(Required) The URL for the project or forge of the custom component. During component creation, this field is pre-populated with the same URL value provided in the URL form (see the Create Using field) when that URL is recognized as belonging to a supported forge-URL domain.</p> <p>Otherwise, to help you provide this value in an appropriate format, click  in the upper part of the window for examples of the standard name, title, and URL conventions used by different forge-URL domains.</p> <p>If you do not know the URL for the component, enter NA.</p>
Forge	<p>The type of project repository used by the custom component. During component creation, this field is automatically populated with an appropriate value when you are creating the component based on either of the following:</p> <ul style="list-style-type: none"> • Its forge (see Create the Custom Component Based on Its Forge). • The URL for its project or forge <i>and</i> the URL belongs to a forge-URL domain supported by the custom-component creation process. For more information, see Create the Custom Component Based on Its Project or Forge URL and Supported Forge-URL Domains for Custom-Component Creation. <p>Otherwise, the default Other is displayed. However, you can select any other forge from the dropdown.</p>
Encryption	Yes or No value depicting whether this component supports encryption. The default is No .

Supported Forge-URL Domains for Custom-Component Creation

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

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

- GitHub
- NuGet Gallery
- npm
- SourceForge
- RubyGems

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

Creating and Editing Custom Licenses

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

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

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

- [Creating a Custom License](#)
- [Editing a Custom License](#)
- [Custom License Properties](#)

Creating a Custom License

Use the following steps to create a custom license:

- [Step 1: Initiate the Creation of a Custom License](#)
- [Step 2: Create the Custom License](#)

Step 1: Initiate the Creation of a Custom License

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

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

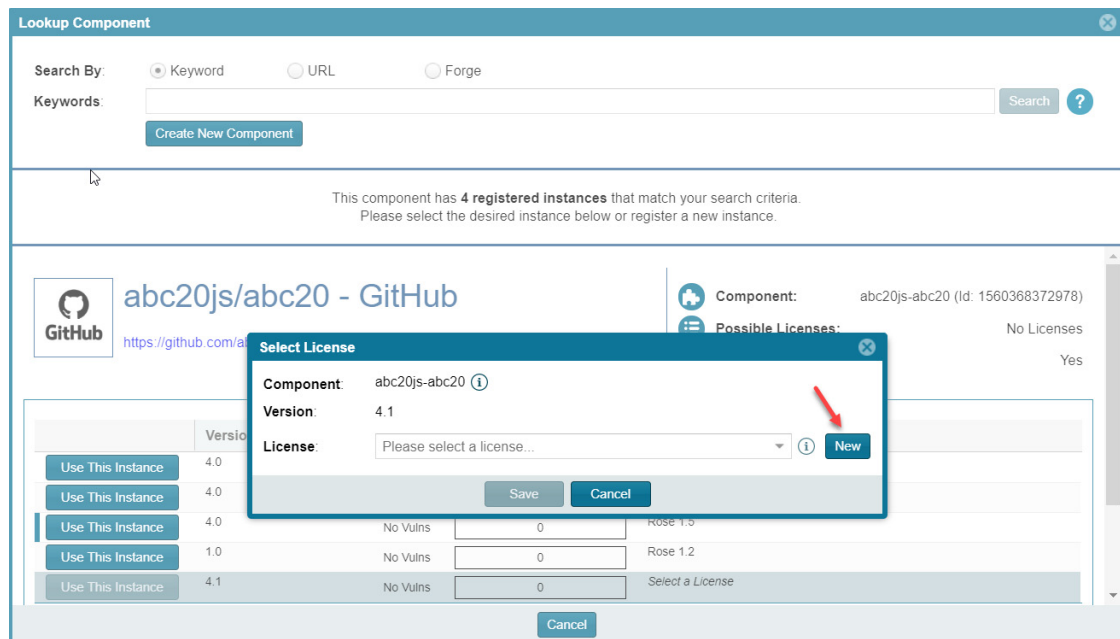
When Using Component Lookup to Register a Component Instance for a “component” Inventory Item

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



Task To create a custom license when registering a component instance for a “component” inventory item, do the following:

1. For an inventory item that you are creating or editing in **Analysis Workbench** or from the **Project Inventory** tab, access the **Lookup Component** window (see [Performing Component Lookup](#)).
2. Locate the component for which you want to register a new component-version-license instance to associate with the inventory item, and click **Show Instances** (or **Versions**) to list its registered instances.
3. Click **Register New Instance** to set up a new instance with which to associate the custom license you are creating.
4. After selecting a component version in the new instance entry, click the **Select a License** dropdown and choose **Select Another License**. The **Select License** dialog is displayed.



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

6. Continue with [Step 2: Create the Custom License](#).

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


When Selecting a New License for an Existing Inventory Item

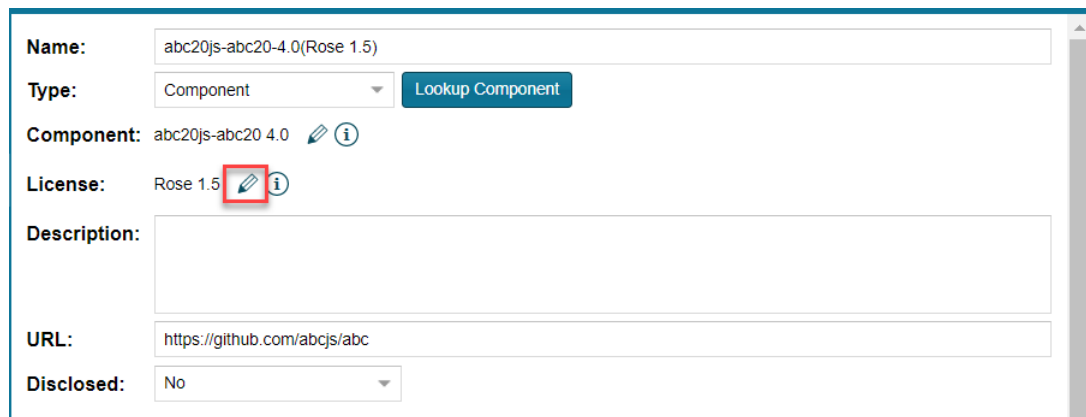
You can create a custom license when updating an existing inventory item of the type **Component** in Analysis Workbench or from the Project Inventory tab.



Task

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

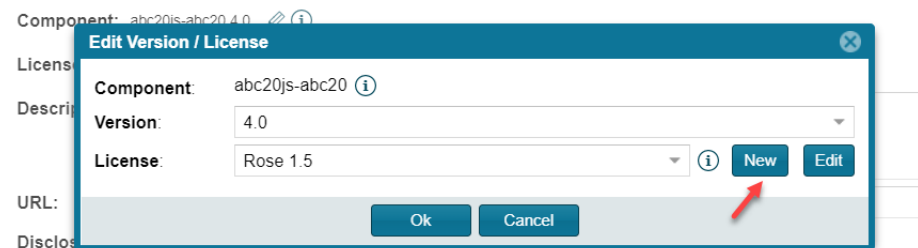
1. When editing an existing inventory item of the type **Component** in **Analysis Workbench** or from the **Project Inventory** tab, click  next to the **License** or **Component** field.



The screenshot shows a form for editing a component. The fields are: Name (abc20js-abc20-4.0(Rose 1.5)), Type (Component), Component (abc20js-abc20 4.0), License (Rose 1.5), Description, URL (https://github.com/abcjs/abc), and Disclosed (No). The License field has a red box around the pencil icon next to it.

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

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



The screenshot shows the 'Edit Version / License' dialog box. It has fields for Component (abc20js-abc20), Version (4.0), and License (Rose 1.5). There are 'New' and 'Edit' buttons next to the License field, and 'Ok' and 'Cancel' buttons at the bottom. A red arrow points to the 'New' button.

3. Continue with [Step 2: Create the Custom License](#).

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

When Creating or Editing a “License Only” Inventory Item

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



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



Task

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

1. When creating or editing inventory in **Analysis Workbench** or from the **Project Inventory** tab, select **License Only** in the **Type** field for the inventory item.
2. Next to the **License** dropdown, click **New** to display the **Create Custom License** window.

The screenshot shows a form for creating a custom license. The 'Name' field is populated with 'New Inventory Item 2019.06.20.21.13.11'. The 'Type' dropdown menu is set to 'License Only' and is highlighted with a red rectangular box. The 'License' dropdown menu shows 'Select a License...' with an information icon and a 'New' button next to it. A red arrow points to the 'New' button. The 'Description' field is empty. The 'URL' field is empty. The 'Disclosed' dropdown menu is set to 'No'.

3. Continue with [Step 2: Create the Custom License](#).

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

Step 2: Create the Custom License

Once you performed one of the procedures in [Step 1: Initiate the Creation of a Custom License](#) to open the **Create Custom License** window, use these steps to create the custom license.



Task

To create the custom license, follow these steps:

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

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

Editing a Custom License

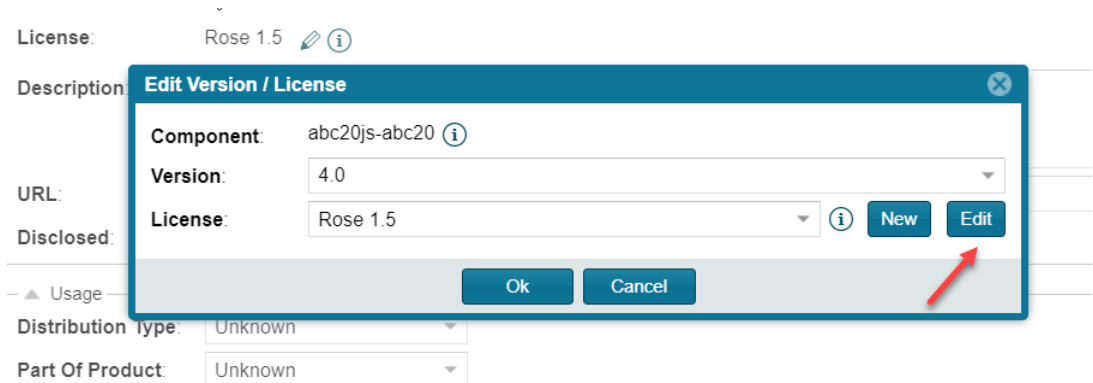
You can edit only custom licenses. When a custom license is selected in any **License** dropdown, the **Edit** button is displayed next to the **New** button, enabling you to update properties for the license. The updates you make to the license at the inventory-item level are saved to the license in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



Task

To edit a custom license, follow these steps:

1. Using any of the procedures described in [Step 1: Initiate the Creation of a Custom License](#), access the License dropdown used to associate a license with the given inventory item.
2. If the custom license you want to update is not already selected for the inventory item, select it from the **License** dropdown.



3. Click **Edit** next to the **License** dropdown to open the **Edit Custom License** window.

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

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

Custom License Properties

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

Table 2-7 • Fields to Define a Custom License

Component Field	Description
Name	The full name of the license (for example, The Rose License 1.5).
Short Name	A unique shorthand representation of the license. This is usually the license SPDX short identifier (for example, Rose-1.5).

Table 2-7 • Fields to Define a Custom License (cont.)

Component Field	Description
Family	A license category that spans multiple license instances (for example, MIT, Public Domain, BSD-3 Clause, and others). The family designation is helpful to a legal reviewer to understand the “type” of license prior to investing the time to analyze the complete license text.
URL	The URL used to access the license on the Internet. This value should start with http:// or https:// .
Priority	<p>The level of importance in investigating this license in terms of its possible business impact on your organization. The higher the level, the greater need to investigate the license:</p> <ul style="list-style-type: none">● P1—Viral, strong copyleft license (requires immediate attention).● P2—Weak copyleft or commercial or uncommon license (requires legal review).● P3—Permissive or public domain license (generally allowed because of its minimal business impact). This is the default if no priority is specified. <p>For details about each priority level, see What Does an Analyst do?.</p>
Description	Meaningful information about the license for your reference.
License Text	The complete text of the license. Be sure to encode any HTML characters.

Managing Custom Detection Rules

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

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

- [Creating a Custom Detection Rule](#)
- [Viewing All Current Custom Detection Rules](#)
- [Editing a Custom Detection Rule](#)
- [Deleting a Custom Detection Rule](#)
- [Rule-Processing Considerations](#)

Creating a Custom Detection Rule

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

- [Creating a Custom Detection Rule from Inventory of “Component” Type](#)
- [Creating a Custom Detection Rule from Scratch](#)

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

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



Task

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

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

2. Click the **Create Custom Rule** button to open the **Custom Detection Rule** dialog. For a description of the fields on this dialog, refer to [Custom Detection Rule Dialog](#).

Note that the **Component**, **License**, **Description**, and **URL** values are pre-populated from the inventory item on which you are basing the rule and are not editable.

Custom Detection Rule

Component: gitjava 2.0

License: General Public License

Description: New github component

URL: https://www.github.com

As-Found License Text:

Notices Text:

Audit Notes:

3. Add or edit **As-Found License Text**, **Notices Text**, and **Audit Notes** content as needed for the rule. (These fields are pre-populated with any content currently defined in the inventory item on which you are basing the rule.) This information is displayed in the future inventory items created automatically by the rule.
4. Scroll down to the **File MD5** pane, which is pre-populated with the list of codebase files associated with the inventory item you created. The MD5 value for each file is provided.
5. Select one or more files to add to the rule.

File MD5:

<input checked="" type="checkbox"/>	/home/qaadmin/scanroot2019r3/716/Email-Refund-...	bb755f126da1308eba83347c5a3b8ce5
<input checked="" type="checkbox"/>	/home/qaadmin/scanroot2019r3/716/License.txt	6a4ac0e19b9329fa4208791b6bc9b393
<input type="checkbox"/>	/home/qaadmin/scanroot2019r3/716/message.html	60dcf306ae6189a0bfdd83927b205c95

« < | Page 1 of 1 | > » | ↺

Displaying 1 - 3 of 3

Save **Cancel**

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

Creating a Custom Detection Rule from Scratch

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

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

1. Open the **Custom Detection Rules** tab, using the procedure in [Viewing All Current Custom Detection Rules](#).
2. Click **Create Custom Rule** to open the **Custom Detection Rule** dialog. For a description of the fields on this dialog, refer to [Custom Detection Rule Dialog](#). Note the following:
 - Once you use **Lookup Component** to select or create a component for the rule, the component information is populated on the dialog. However, you can edit this information as needed.
 - You can add **As-Found License Text**, **Notices Text**, and **Audit Notes** content as needed for the rule. This information is displayed in the future inventory items created automatically by the rule.
3. Scroll down to the **File MD5** pane.
4. For each codebase file you want to add to the rule, click the **Add File** button and provide the file’s name and MD5 value.

Name	MD5
message.jar	60DCF306AE6189A0BFDD83927B205C95
trial.lib	100FDC9000F4510BBDD0F17111D778E58

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

Viewing All Current Custom Detection Rules

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



Task

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

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



2. Select **Custom Data** from the menu to open the **Custom Detection Rules** tab, showing the list of current custom detection rules. From this tab, you can do the following:
 - View the component information (name, version, license, and forge URL) on which each rule is based.

- Create a custom detection from scratch (see [Creating a Custom Detection Rule](#)).
- Edit a custom detection rule or remove it from the Code Insight system.



Editing a Custom Detection Rule

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



Task

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

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


Deleting a Custom Detection Rule

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



Task

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

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

Rule-Processing Considerations

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

- If the custom detection rule is associated with more than one file, the scan uses OR logic when processing the files against the target codebase. Consequently, only one file match between codebase and the rule is required to automatically create an inventory item.
- If two rules are created with identical details and codebase files, a single inventory item is generated during a scan when both rules are applied.

- If two rules are created using the same component, version, and license details and the same codebase files, but have different **Description**, **URL**, **Audit Notes**, **As-Found License Text**, or **Notices Text** content, a single inventory item is generated during a scan when both rules are applied. In the inventory item, values that differ between the rules for a given field are separated (shown on separate lines or with a separator) within the field.
- If two rules with are created with the same codebase files but use a different component, two inventory items are generated during the scan.

Finalizing the Notices Text for the Notices Report

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

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

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



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



Task

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

1. Navigate to one of these locations:

In **Analysis Workbench**, on the **Inventory Details** tab for a specific inventory item, open the **Licenses & Notices** tab.

prezeskk-tcpdf (LGPL-3.0)

Recall Save Close

Review Status: Draft
Alerts: None
Priority: P3

Vulnerabilities: No

Created By: Automated Finding
Confidence: [Red Bar]
Created On: May 30, 2019 at 16:16
Updated On: May 30, 2019 at 16:16

Component: prezskk-tcpdf None Selected

License: I don't know

Description: TCPDF is a PHP class for generating PDF documents and barcodes.

URL: http://www.tcpdf.org/

Disclosed: No

Usage Notes Associated Files (1) **Licenses & Notices**

As-Found License Text: The following text is found in file:LICENSE.TXT at /home/qaadmin/scanroot2019r2/1245/moodle-master/lib/tcpdf/LICENSE.TXT

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

Project Inventory

Items (22)

Advanced Search Show All Items Add Item

Priority ↑	Vulns	Status
P1	0	✓ ? (X)
P1	0	✓ ? (X)
P1	0	✓ ? (X)
P2	1	✓ ? (X)
P2	2	✓ ? (X)

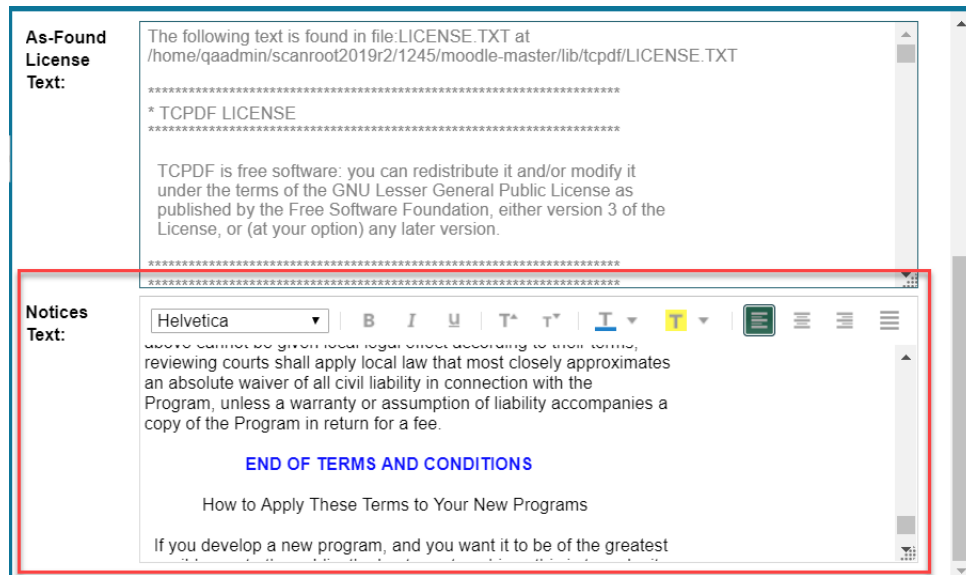
prezeskk-tcpdf (LGPL-3.0) Recall Item Edit Item

Confidence: [Red Bar] Vulnerabilities: No Encryption: N/A Priority: [Play Icon]

Inventory Details Component Details **Licenses & Notices** Notes & Guidance Us

As-Found License Text: The following text is found in file:LICENSE.TXT at /home/qaadmin/scanroot2019r2/1245/moodle-master/lib/tcpdf/LICENSE.TXT

- In the **Notices Text** field, enter (or paste from a source such as the content in the **As-Found License Text** field) the license content for the inventory item.
- Modify and format the text exactly as you want it to appear in the Notices report.



4. Select **Save** to save your changes.

When the Notices report is run, the content from the **Notices Text** pane is used as the “notices” information for the inventory item in the report.

Accessing and Viewing Projects in the System

This section describes the various ways you can access projects in your FlexNet Code Insight system in order to view their details and manage them:

- [Navigating to the Projects List](#)
- [Using the Project Dashboard](#)
- [Opening a Project](#)
- [Showing Only Your Projects](#)
- [Searching the System](#)
- [Managing Items in the Project List](#)

Navigating to the Projects List

You access projects in the FlexNet Code Insight system from the **Projects** list, a manageable display of the projects available in the system. (The projects can be grouped in folders for easier accessibility.)

Use the following procedure to open the **Projects** list. The procedure assumes that you have logged into FlexNet Code Insight.



Task

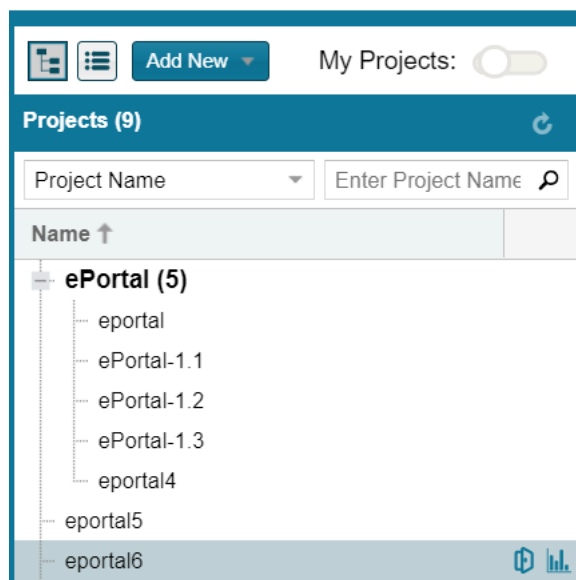
To open the Projects list, do the following:

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

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



The **Projects** list is displayed.

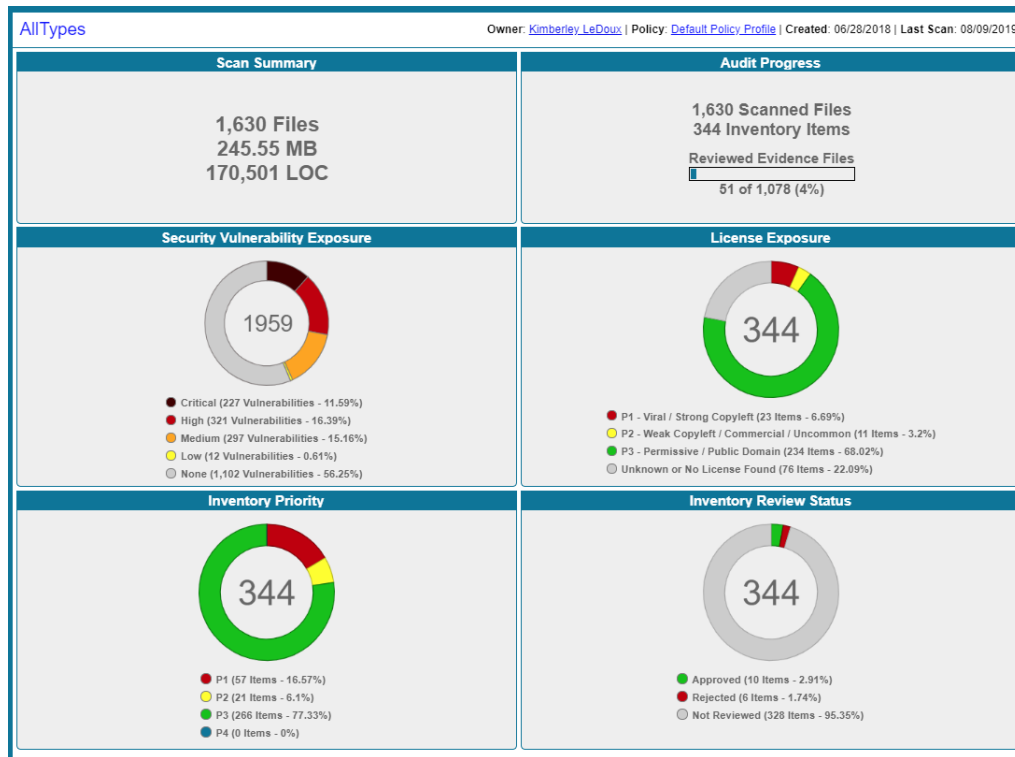


2. (Optional) Click the **My Projects** toggle at the top of the list to show only those projects with which you are associated as Project Owner or through a project role. (For details, see [Showing Only Your Projects](#).) You can also search projects by name, inventory, or security vulnerability as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

Using the Project Dashboard

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


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



Task

To use the Project Dashboard, do the following:

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

(Alternatively, hover over the project entry, and click its **Load Project Dashboard** icon  in the project entry to display the dashboard.)

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

- **Scan Summary**—A summary of your most recent scan, including number of files scanned, the size of the codebase/files, and the number lines of code.
- **Audit Progress**—A snapshot of the audit progress of the selected project.
- **Security Vulnerability Exposure**—An interactive color-coded chart and legend that provide an overview of the security vulnerabilities by severity across all the project inventory. The number in the center of the chart is the total number of security vulnerabilities found across all inventory items. (The colors in this chart can vary depending on the CVSS version Code Insight is using. See [Security Vulnerabilities Associated with Inventory](#) for details.)
- **License Exposure**—An interactive color-coded chart and legend that provide an overview of the licenses identified by priority across all of the project inventory. The number in the center of the chart is the total number of inventory items identified for the current project.
- **Inventory Priority**—An interactive color-coded chart and legend that provide an overview of the priority of inventory in the selected project. For more information about inventory priority, see [Inventory Priority](#).

- **Inventory Review Status**—An interactive color-coded chart and legend that show you the review status (**Approved**, **Rejected**, **Not Reviewed**) of the inventory for the selected project.
3. (Optional) Hover your mouse cursor over the color-coded segments in the charts to view details related to a given segment. If you want, click a color-coded segment to open the project to view the inventory items associated with the segment. See [Filtering Inventory for a Project from the Project Dashboard](#) for details.

Alternatively, you can open the project to view all its inventory (see [Opening a Project](#)), or select another project from the **Projects** list to view its dashboard.

Filtering Inventory for a Project from the Project Dashboard

After you create a project, and upload and scan a codebase, you can quickly filter the project's inventory to view potential problems and take steps to eliminate issues, such as high exposure items (shown in red), from your project inventory.



Task

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

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

Opening a Project

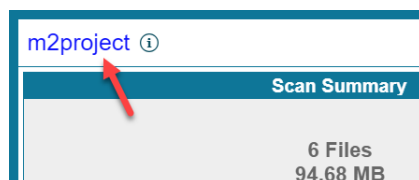
Use this basic procedure to open a project.



Task

To open a project, do the following:

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. Select a project in the **Projects** list. Its **Project Dashboard** is displayed on the right.
3. To open the project, either click the **Open Project** icon (🔗) next to the project entry in the **Projects** list, or click the project's name link in the upper left corner of the dashboard (shown below):



The project is opened on either of the following tabs for the project:

- If the project contains published inventory items, the **Project Inventory** tab. For more information about the **Project Inventory** tab, see [Reviewing Published Inventory](#).

- If the project does not contain published inventory items, the project's **Summary** tab. For more information about the **Summary** tab, see [Managing a Project from the Summary Tab](#). For information about publishing inventory, see [Publishing or Recalling Inventory from Analysis Workbench](#).

Note that the **Analysis Workbench** tab is also available for users with the proper permissions (although you have to navigate to open it). The Analysis Workbench enables a user to perform a deep analysis of the scan results. For more information, see [The Analysis Workbench Layout](#).

Showing Only Your Projects

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

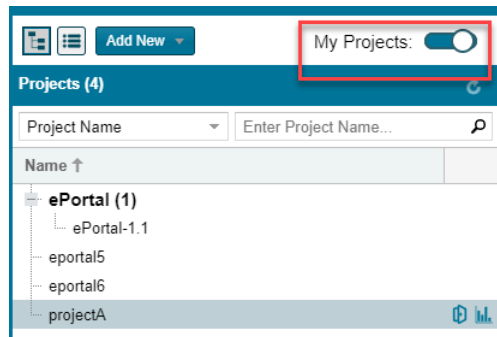
Additionally, this filter can work in conjunction with the system filters described in [Searching the System](#) to display only your projects that have specific project or inventory attributes.



Task

To show your projects only, do the following:

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



3. Select a project from the filtered list to open its dashboard. See [Using the Project Dashboard](#) for details.
Alternatively, open the project to view its inventory on the **Project Inventory** tab. See [Opening a Project](#) for details.
4. (Optional) To turn off this filter, click the **My Projects** toggle again.

Searching the System

FlexNet Code Insight enables you to search both globally across all projects, as well as locally for a given project. At the global level, you can use the filters available in the **Projects** list quickly search for projects and inventory of interest in the system, as described in this section.

At the project-level on the **Project Inventory** tab, you can further narrow your search results to specific inventory items.

To search globally, use the filters available in the Projects list. specify criteria to quickly search for and find projects and inventory of interest in the system. Using the search filters available for the **Projects** list, you can search projects by name, inventory, components and versions, licenses, and security vulnerabilities. You can perform multiple search types, each one further filtering the current search results. Then, at the project level on the **Project Inventory** tab, you can continue to narrow your search results to specific inventory items.

The following topics describe these search methods:

- [Available Filters for Searching Across Projects](#)
- [Searching for Projects by Name](#)
- [Searching All Projects for Inventory Based on a Specific Component and Version](#)
- [Searching All Projects for Inventory Associated with a Specific License](#)
- [Searching All Projects for a Security Vulnerability Advisory](#)
- [Restoring the Full Project List](#)

Available Filters for Searching Across Projects

The following filters are available from the **Projects** list to perform searches across all projects in your FlexNet Code Insight system.

Table 2-8 • Available Filters for Searching Across Projects

To search across all projects for...	...use this filter	Filter criterion	Criterion example	Refer to...
Projects with a name containing a specific string	Project Name	Project name	MyProject	Searching for Projects by Name
Inventory based on a specific component and version	Project Inventory	Component and version as it appears in the Inventory Name value	Apache Struts 2.3.14.3	Searching All Projects for Inventory Based on a Specific Component and Version
		Component name as it appears on the Component Details tab for the inventory item	struts2-core	
Inventory associated with a specific license	Project Inventory	The Selected License value as it appears on the Component Details tab for the inventory item	GNU General Public License v2.0	Searching All Projects for Inventory Associated with a Specific License
		The license name as it appears in the Inventory Name value	GNU General Public License or GPL-2.0+	
		The SPDX short identifier for the license	GPL-2.0+	

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

To search across all projects for...	...use this filter	Filter criterion	Criterion example	Refer to...
Inventory impacted by a specific security vulnerability	Security Vulnerability	The complete ID of the security vulnerability	<p>CVE-2018-11776 for an NVD vulnerability</p> <p>SA40575 for a Secunia advisory</p> <p>DSA-4315 for a Debian advisory</p>	Searching All Projects for a Security Vulnerability Advisory

Searching for Projects by Name

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

Search Rules

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

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

Searching for Projects by Name

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



Task

To search projects by name, do the following:

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Project Name** from search dropdown on the left.
3. Enter the project name (or a partial string in the name) in the **Enter Project Name** field. The list of projects changes to reflect the search results, and a filtered count (for example, “(19 of 123)”) is provided in the **Projects** list header to show the number of projects returned by the search.

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

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

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

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

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

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

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

Search Rules

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

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

Searching All Projects by Component and Version

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



Task

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

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. At the top of the list, select **Project Inventory** from search dropdown on the left.
3. In the **Enter Search Criteria** field, specify the complete name or a partial string for one of the following:
 - The name of the component as it appears on the **Component Details** tab (for example, [struts2-core](#)) for an inventory item
 - The name of the component and version as it appears in the **Inventory Name** value (for example, [Apache Struts 2.3.14.3](#))

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

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

Searching All Projects for Inventory Associated with a Specific License

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

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

Search Rules

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

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

Searching All Projects by License

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



Task

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

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

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

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

Searching All Projects for a Security Vulnerability Advisory

You might find it sometimes necessary to quickly see how a specific security vulnerability impacts your organization. You can search the system for a security vulnerability or advisory in one of the following ways:

- **If you know the exact ID of the security vulnerability or advisory**—Use the **Security Vulnerability** search filter with the *exact* security vulnerability ID as the search criterion, as described in this section.

- If you do not know the ID of the security vulnerability or advisory (for example, in the case of a zero-day vulnerability for which an ID has not been published)—Use the **Project Inventory** search filter to provide the name of the vulnerable component as the search criterion. See [Searching All Projects for Inventory Based on a Specific Component and Version](#) for details.

Search Rules

When you use the **Security Vulnerability** search filter to search projects associated with a specific security vulnerability, the following rules apply:

- Only one vulnerability ID can be specified as a search criterion.
- Only exact matches of the full vulnerability ID string are supported. Partial strings are not supported.
- The string you enter does not support spaces.
- Only published inventory items are searched.
- The search does not validate the vulnerability ID you enter. If you enter an invalid ID, no results are returned in the **Projects** list.

Searching for a Security Vulnerability

Use this procedure to locate projects by the *exact* security vulnerability ID you specify.



Task

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

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

If no inventory items meet the specified criterion, the **Projects** list shows “No Projects”.
5. Open one of the projects to see a filtered list of inventory items that are impacted by the security vulnerability. (See [Opening a Project](#) for details.)

Restoring the Full Project List

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

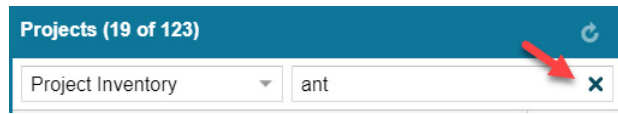


Task

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

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.

2. At the top of the list, Click the **X** icon in the criterion field to remove the current **Projects** list filter:



The full list of projects is restored.

Managing Items in the Project List

As Project Owner, you can rename any of your projects in the **Projects** list or move your projects to different project folders in the list. Additionally, if you have Create Project permissions, you can create new folders in the **Projects** list.



Task

To rename or move your projects in the Projects list, do the following:

1. Navigate to the **Projects** list. See [Navigating to the Projects List](#) for instructions.
2. Do one or both of the following:
 - To rename one of your projects, double-click the project name, and overwrite the current name with the name.
 - To move one of your projects to a different folder, drag and drop the project to the desired folder.
 - To create a new folder, click the **Add New** button and select **Folder**.

Managing a Project from the Summary Tab

The following topics describe how to use features on the **Summary** tab to manage the currently opened project.

Refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix for the various user roles required manage projects.

- [Opening the Project Summary Tab](#)
- [Generating Reports](#)
- [Assigning Project Roles to Users](#)
- [Editing the Project Definition and General Settings](#)
- [Automatically Publishing Inventory](#)
- [Updating Scan Settings for a Project](#)
- [Updating Inventory Review and Remediation Settings for a Project](#)
- [Connecting the Project to Remote Data Sources](#)
- [Changing Project Owners](#)
- [Rescanning Your Codebase](#)
- [Exporting Project Data](#)
- [Deleting a Project](#)


Opening the Project Summary Tab

When you open a project from the **Project List** page, the **Summary** tab shows you information about the project. On this page, you can view project details, scan settings, scan status, and report information. You can also change Project Owners, manage project settings, start and stop scans, generate reports, and upload project codebases.



Task

To open the Summary tab, do the following:

1. From the list of projects, click the project you want to open. The name of the project appears at the top of the right panel.
2. Do one of the following to open the project:
 - Click the project name (in the example, *New Project*) in the title bar of the right panel.
 - Click the **Open Project** icon (.

The project is opened to its **Project Inventory** page.

3. Click the **Summary** button at the top of the window to open the **Summary** tab for the project.

Generating Reports

On the **Summary** tab, you can generate the following reports that describe your aspects of the project:

- [The Project Report](#)
- [The Audit Report](#)
- [The Notices Report](#)

The Project Report

The Project report summarizes the inventory, vulnerabilities, remaining scan evidence, and review and remediation tasks for a selected project. It produces output in JSON and Excel format. This report is useful in understanding the existing project's legal and security risks based on identified inventory items, as well as the additional potential risk based on the file-based scan results known as third-party indicators.



Task

To generate the Project report, do the following:

1. Navigate to the **Summary** tab for the project (see [Opening the Project Summary Tab](#)).
2. Click the **Generate Report** menu and select **Project Report**. A prompt will appear, explaining that the report is being generated in the background. When the report has been generated, the **Download** hyperlink appears in the **Project Report:** field.
3. Click the **Download** hyperlink and respond to the prompts to save the report. The report is saved in a .zip file in both JSON and Excel formats:
 - **JSON**—Can be processed programmatically to integrate with other applications.

- **XLSX**—Can be viewed in Microsoft Excel.
4. Navigate to the folder where you saved the report .zip file, and unzip the file.
 5. When the files have been unzipped, double-click one of the files to open it.
 6. (Optional) Select the tabs (**Summary**, **Priority Legend**, **Inventory Items**, **Tasks**, and so forth) at the bottom of the sheet to view additional report information.

The Audit Report

Audit reports provide another way to distribute your research and findings to others in your organization. Only published inventory items appear in Audit reports.



Task

To generate an Audit report, do the following:

1. Navigate to the **Summary** tab for the project (see [Opening the Project Summary Tab](#)).
2. Click the **Generate Report** menu and select **Audit Report**. A prompt will appear, explaining that the report is being generated in the background. When the report has been generated, the **View | Download** hyperlink appears in the **Audit Report** field.
3. Determine if you want to view or download the report:
 - To view the report in your browser, click **View**.
 - To download the report, click **Download**. You will be prompted to save the report, which will be saved in the following formats in a .zip file:
 - **HTML**—Can be viewed in any browser.
 - **JSON**—Can be processed programmatically to integrate with other applications.
 - **XLSX**—Can be viewed in Microsoft Excel.
4. Navigate to the folder where you saved the report .zip file, and unzip the file.
5. When the files have been unzipped, double-click one of the files to open it.
6. (Optional) Select the tabs (**Summary**, **Priority Legend**, and so forth) at the bottom of the sheet to view additional report information.

The Notices Report

FlexNet Code Insight provides the ability to produce a Notices report to satisfy the attribution requirements of most open source licenses. The report is created in text format.

After Engineering has completed the remediation plan, resolving all rejected inventory items, the codebase is rescanned until it is approved for release. When the codebase is approved for release, you need to generate a Notices report to accompany the software application. This report is a compilation of all the open source/third-party components contained in the product and their license content (notices).

The Notices report shows only published inventory. The inventory can be system-generated or custom and of any type—**Work in Progress**, **Component**, or **License**.

The following items can appear in the Notices report for each inventory item:

- **Inventory name**—The entry in this field is based on naming conventions, which is usually the component name, version, and governing license name.
- **Inventory URL**—If the inventory URL is not available, FlexNet Code Insight uses the associated component URL. If both are unavailable, no URL will appear in the report.
- **Inventory Notices Text**—The final “notices” text associated with the inventory item. It is pulled from the **Notices Text** field on the **License & Notices** tab for a selected inventory item in **Analysis Workbench** or in **Project Inventory**. If this field is empty, FlexNet Code Insight uses the content in the **As-Found License Text** field (also on the **License & Notices** tab), which shows the verbatim text license text found in the codebase by the system. If no **As-Found License Text** or **Notices Text** information is available, the text pulled from the FlexNet Code Insight data library for the selected license is used in the Notices report. For more information, see [Finalizing the Notices Text for the Notices Report](#)

Generating the Notices Report



Task

To generate a Notices Report, do the following:

1. Navigate to the **Summary** tab for the project (see [Opening the Project Summary Tab](#)).
2. Select **Notices Report** from the **Generate Report** dropdown. A prompt appears explaining that the report will be generated in the background while you continue to work in FlexNet Code Insight.
3. Click **OK**. When the report has been generated. When the report has been generated, the **View | Download** hyperlink appears in the **Basic Report:** field.
4. Determine if you want to view or download the report:
 - To view the report in your browser, click **View**.
 - To download the report, click **Download**. On the prompt that appears, choose the next action for the report download:
 - **Open**—The report opens in your default text editor.
 - **Save**—The report is saved in the specified directory.
 - **Cancel**—The report is not downloaded.

Assigning Project Roles to Users

The Project Owner assigns roles to users, enabling them to analyze the codebase and manage and publish inventory, review published inventory, or view private projects. The following are the available roles that users can have in a project:

- **Analysts** have the ability to manage the codebase and inventory using the Analysis Workbench. They can create new inventory, edit existing inventory, and publish inventory. They can also review files and add files to inventory.
- **Reviewers** have the ability to approve and reject inventory and manage inventory using the **Project Inventory** tab. They can create new inventory and edit existing inventory.

- **Observers** have the ability to view inventory in a private project. They have read-only access to project inventory and can run reports. Development managers and executives are usually assigned this role.



Note • The Observer role is available for private projects only.

For public-view projects, users who are not directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project. For additional information about private projects, see [Creating a Private Project](#).

For a reference to the various user roles and their permissions, refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix.

The following procedure can be used to assign users and roles to public-view and private projects.



Task

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

1. As the Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click the **Manage Project** menu at the bottom of the page and select **Edit Project Users**. The **Edit project users** page appears.
3. To assign users to a given role, drag and drop one or more user names from the **Select Users** list to the desired “role” pane (**Analysts**, **Reviewers**, or **Observers**).



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

4. Repeat this step as necessary to assign users to roles. (A user can be assigned to multiple roles.)
5. To remove a user from a role, simply click **X** next to the user’s name in the appropriate “role” pane.
6. Click **Close** when you have finished managing the reviewer, analyst, and observer role assignments.

Editing the Project Definition and General Settings

The Project Owner can edit the project’s definition and general settings.



Task

To update project settings, do the following:

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

Updating Scan Settings for a Project

You can switch the project to a different scan profile, update which sub-folders to scan, and change settings for automatically publishing inventory during the scan (see [Automatically Publishing Inventory](#)).



Task

To update scan settings for the project, do the following:

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

Automatically Publishing Inventory

FlexNet Code Insight provides the ability to automatically publish inventory without the need for an analyst to be involved. This feature supports a fully automated end-to-end process where there is no human analyst involvement. (For example, the auto-publish feature works in conjunction with workflow policies that automatically review inventory items as they are published, as described in [Managing Policy Profiles](#).) If there is a human analyst involved, the auto-publish feature can be turned off, allowing the analyst to publish the inventory manually after analysis.

When the auto-publish feature is enabled, additional options are made available to set the minimum inventory confidence level for publishing inventory and to automatically mark files associated with an auto-published inventory as “reviewed”.



Task

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

1. As the Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Edit Project** from the popup menu. The **Edit Project** page opens.
3. Select the **Scan Settings** tab.
4. Enable or disable **Automatically publish system-created inventory items**. When you enable this option, the associated options, **Mark associated file as reviewed** and **Minimum inventory confidence level**, are made available for updating. See [Edit Project: Scan Settings Tab](#) for a description these options.
5. When you have set the auto-publish feature, click **Save**. The **Summary** tab is opened.

Updating Inventory Review and Remediation Settings for a Project

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

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



Task

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

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

Connecting the Project to Remote Data Sources

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

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

Version Control Settings

Use the **Version Control Settings** tab on the **Edit Project** page to connect to one or more Source Code Management (SCM) repositories directly from FlexNet Code Insight so you can scan and audit code without manually moving that data to the Scan Server. For information about connecting to a remote data sources, see the [Configuring Source Code Management](#) chapter.

ALM Settings

FlexNet Code Insight integrates with application lifecycle management (ALM) systems, enabling Code Insight users to create and manage external work items associated with inventory directly from Code Insight. In this way, inventory requiring further review and remediation can be tracked externally as part of the user's existing issue-tracking system.

For example, a Code Insight scan might uncover security vulnerabilities or “copyleft” licenses requiring further review by the Security and Legal teams. With an ALM integration, these issues can be quickly converted into work items that point to corresponding issues in the ALM instance.

Integration with a specific ALM system is enabled through a corresponding Code Insight connector that supports pre-populated data (in the form of one or more *instances*) used to connect to the ALM system and to set up work items. Additionally, a given ALM instance controls the synchronization of data between Code Insight and the server based on a configured synchronization frequency.

To configure an ALM connector, the system or application administrator defines one or more of these instances in Code Insight, a process described in the “Integrating with Application Life Cycle Management” chapter in the *FlexNet Code Insight Installation and Configuration Guide*.

Then, in order to create and manage work items for a given project, you must associate the project with a specific ALM instance. The following sections describe how to associate (and unassociate) a project with an ALM instance. Currently, Code Insight is installed with a Jira connector. Future releases will provide additional support for other ALM systems.

- [Associating a Jira Instance to a Project](#)
- [Using Code Insight Variables](#)
- [Unassociating an ALM Instance from a Project](#)

Associating a Jira Instance to a Project

Use the following instructions to associate a Code Insight project with a Jira instance.



Task

To associate a Jira instance to a project, do the following:

1. As the Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Edit Project** from the popup menu. The **Edit Project** page opens.
3. Select the **ALM Settings** tab.
4. From the **ALM Instance** dropdown, select the Jira instance to associate to this project. The current settings for the Jira instance are displayed on **ALM Settings** tab.

If no instances are available in the dropdown, ensure that at least one instance is configured at the application level. Instructions for configuring a Jira instance are found in the *FlexNet Code Insight Installation and Configuration Guide*.

5. Complete the fields on the **ALM Settings** tab. See the inline help for explanations of the fields.
 - Certain fields might already contain a value based on the global application defaults set when the Jira instance was created (as described in the *FlexNet Code Insight Installation and Configuration Guide*.) However, you can override any global defaults with the information you enter here. For example, if you change the **Default Issue Type** from **Task** to **Bug**, the value **Bug** becomes the new default for this project. See [ALM Tab](#) for field details.

- You can include (or override) Code Insight variables in the **Default Summary** and **Default Description** fields. These variables will be replaced by actual values in descriptive text that displays for a newly created Jira issue and work item. For more information, see the next section, [Using Code Insight Variables](#).
6. When you have completed the settings, click **Save** to associate the Jira instance to the project.
- Validation for these field values takes place during work item creation. If the information entered here is invalid (for example, the **Assignee** value does not exist in the Jira system), the information will still be saved, but users will not be able to create the work item in the future.
- Once you have associated the Jira instance with the project, all work items created in this project will have a corresponding Jira issue on the provided instance.

Using Code Insight Variables

The **Default Summary Text** and **Default Description Text** fields support Code Insight variables that communicate details about the Code Insight project, inventory item, and other relevant information in the work item and associated Jira issue.

Supported Variables

The following table lists the available variables for use in the text entered in the **Default Summary Text** and **Default Description Text** fields:

Table 2-9 • 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, do the following:

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

Changing Project Owners

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



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



Task

To change the Project Owner, do the following:

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



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

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



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

Rescanning Your Codebase

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

Both analysis types run separate scans. When you run the initial scan on your codebase, they each perform a *full* scan (that is, a scan on all codebase files). For any subsequent codebase rescan that a user initiates, each analysis type performs either a full rescan, an *incremental* rescan (that is, a scan on only changed codebase files), or no rescan. The type of rescan executed for an analysis type depends on changes that might have occurred in your codebase or with your Code Insight configuration or version prior to the rescan. A full rescan can be costly.

The following topics provide information you should know about the rescan process and includes instructions on initiating a rescan:

- [Change Events Resulting in Full or Incremental Rescans](#)
- [Effects of Scan-Setting Changes on Rescans](#)
- [Handling of Edited Inventory During Rescans](#)
- [Initiating a Codebase Rescan](#)

Change Events Resulting in Full or Incremental Rescans

The following table shows the types of change events that result in a full or an incremental rescan for Automated Analysis and Advanced Analysis should you initiate a rescan on your codebase:

Table 2-10 • Change Events Resulting in Full or Incremental Rescans

Changes to...	Automated Analysis	Advanced Analysis	Details
Codebase files	Incremental rescan	Incremental rescan	Changes in codebase files are determined by the MD5 hash digest of the files.
Automated Analysis rule set	Full rescan	No rescan	Rules are automatically pushed to your Code Insight server through both an internal process and the weekly Electronic Update.

Table 2-10 • Change Events Resulting in Full or Incremental Rescans (cont.)

Changes to...	Automated Analysis	Advanced Analysis	Details
FlexNet Code Insight version	Full rescan	No rescan	This change is usually an upgrade in the Code Insight version.
Scan profile settings	Full rescan	Full rescan	<p>Depending on the scan profile settings that were changed, one or both analysis types will perform a full rescan. Note that changes to settings that apply to source-code matching result in an <i>expensive</i> Advanced Analysis full rescan. See Effects of Scan-Setting Changes on Rescans for more information.</p> <p>Scan profiles are configured by the Administrator as described in the <i>FlexNet Code Insight Installation and Configuration Guide</i>.</p>
CL version	No rescan	Full rescan	This change is associated with a change to the CL Path value identified in the Scan Server setup. (This setup is handled by the Administrator, as described in the <i>FlexNet Code Insight Installation and Configuration Guide</i> .)

Effects of Scan-Setting Changes on Rescans

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



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

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

Table 2-11 • Types of Full Rescan to Expect Should Scan Profile Settings Change

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

Handling of Edited Inventory During Rescans

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

- The component version string or the associated license
- Codebase-file associations (only in **Analysis Workbench**)
- Inventory properties and notes

However, normal Code Insight rescan behavior can result in actions that impact your inventory changes. For example, an updated Automated Analysis rule set might associate codebase files to an inventory item different from the one to which you have *manually* associated these files. Logically, the rescan would remove the associations you defined and re-apply them to the inventory item identified in the rule set.

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

- [Rescan Rules to Preserve Your Inventory Edits](#)
- [Rescan Scenario: Handling of Files Manually Disassociated from Inventory Before Rescan](#)

Rescan Rules to Preserve Your Inventory Edits

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

- All the user-created inventory, its file associations, and edits are considered *not* system-updatable and therefore are preserved.
- Any change to a system-generated inventory item (including the component) results in the inventory item being classified as user-created and therefore not system-updatable (see the previous rule.) However, the rescan can add additional files to the inventory item if the component, version, and license match.
- If one or more files were disassociated from a system-generated inventory item before the rescan, rescan logic assumes that these files were erroneously associated with the component initially. Therefore, the rescan does not attempt to re-associate these files to the inventory item; nor does it associate the files with another inventory item that uses the same component name (with a different version or license). The following example scenario illustrates this rule.

Rescan Scenario: Handling of Files Manually Disassociated from Inventory Before Rescan

The following scenario demonstrates how the rescan process handles files that you manually disassociated from a system-generated inventory item before the rescan.

In this scenario, the initial scan on your codebase generated the inventory item **log4j 2.6** and associated the files **file1.jar** and **file2.jar** with the item.

However, after analyzing the inventory, you realize that **file2.jar** should be associated instead with **log4j 2.11**, an inventory item that does not exist in your current inventory. To remedy this, you perform the following steps:

1. Create an inventory item named **log4j 2.11**.
2. Disassociate the **file2.jar** from **log4j 2.6**.
3. Associate **file2.jar** with the inventory item **log4j 2.11** that you just you created.

On rescan, your edits remain intact:

- The file **file1.jar** remains associated with the inventory item **log4j 2.6**.
- The inventory item **log4j 2.11** that you created is preserved along with its association with the file **file2.jar**.

The rescan also results in the creation of a new system-generated inventory item, **log4j 2.10**. However, the rescan does not associate the file **file2.jar** with the new inventory item.

Initiating a Codebase Rescan

Use the following procedure to rescan your codebase.

Refer to the [FlexNet Code Insight User Roles and Permissions](#) appendix for role requirements to scan a codebase.



Task

To start the rescan, do the following:

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

2. Perform either step:

- Click the **Start Scan** button. If a scan is currently running or the Scan Server is currently not active, this button is disabled. You can use the second option (see next bullet) to schedule a scan.
- Click the link in **Scan Status** to schedule a scan. If other scans are running, the scan is queued and will automatically run based on queue order. If the Scan Server is inactive, the scan will automatically start based on queue order once the server is running again. (Click the link in **Past Scans** to view details about the scheduled scan.)

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

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

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

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



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

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

Exporting Project Data

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



Task

To export project data, do the following:

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



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

Deleting a Project

Project Owners can use this procedure to delete any of their projects.



Task

To delete a project, follow these steps:

1. As Project Owner, navigate to the **Summary** tab (see [Opening the Project Summary Tab](#)).
2. Click **Manage Project** and select **Delete Project** from the dropdown menu.
3. When prompted, select **Yes** to proceed with the deletion. If the Scan Server associated with the project is temporarily inactive or is disabled, a pop-up is displayed to inform you that the server is down.

Creating a Private Project

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



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



Task

To create a private project, do the following:

1. If you are not viewing the **Project** list, navigate to it.
2. Click **Add New**. The **Add Project** dialog appears with default values appearing in all the fields but **Name**.
3. In the **Name** field, enter a name for the new private project.
4. From the **Project Visibility** dropdown, select **Private**.
5. Complete the other fields as described in [Creating a Project](#).
6. Click **Save** to save the new private project.

If the user is not a **Project Owner**, **Project Analyst**, **Project Reviewer**, or **Project Observer** for this **Private** project, the project will not be visible on the **Project Folders** page; and the project and vulnerability ID searches will not return private projects unless the user has the rights to see these projects.

7. (Optional) Assign roles to users who will interact with the private project. For more information, see [Assigning Project Roles to Users](#).

Managing Policy Profiles

This section describes the purpose of policies in FlexNet Code Insight and provides procedures for adding, editing, copying, and deleting policies. The following topics are included:

- [Understanding Policy Profiles](#)
- [Adding or Editing a Policy Profile](#)
- [Copying a Policy Profile](#)

Understanding Policy Profiles

Policy profiles are used by FlexNet Code Insight to automate the inventory review process—that is, automatically mark published inventory items as approved, rejected, or requiring a manual review—without the need for a manual review. Policy profiles can be defined up-front or revised during the manual inventory review process. The Code Insight Administrator grants the **Manage Policy** role to users who have rights to manage policy profiles. Typically, these would be legal or security users.

Code Insight provides a default policy profile (called *Default License Policy Profile*) that can be used as is, modified, or copied to fit your need. This policy profile contains typical settings for a team who is distributing software. You can also create policies from scratch.

The topics covered in this section include:

- [How Policy Profiles Work in the Automated Inventory-Review Process](#)
- [Adding or Editing a Policy Profile](#)
- [Copying a Policy Profile](#)
- [Associating a Policy Profile with a Project](#)

How Policy Profiles Work in the Automated Inventory-Review Process

A policy profile is defined with a set of policy criteria based on components, licenses, or security vulnerabilities. Any conflicting criteria are resolved in favor of an automated rejection of the inventory item. In other words, rejections will always take precedence over approvals. A criterion in the policy profile can also optionally include usage guidance text as a way to communicate with the developer any obligations or best-practices related to a given inventory item. The policy criteria are evaluated when an inventory item is published. If none of the criteria in the profile applies to a given inventory item, the system leaves the inventory item in a **Not Reviewed** (requiring a manual review) state.

You can further automate the inventory review process by setting policies that define what action Code Insight takes once an item is rejected or assigned a **Not Reviewed** status. See [Updating Inventory Review and Remediation Settings for a Project](#) for details.

Adding or Editing a Policy Profile

The following procedure describes how to add a new policy profile or edit an existing one.



Note • If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, policies you defined in this profile might have changed. For more information, see [Impact on Policies When CVSS Version Changes on System](#) for details.



Task

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

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



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

3. To edit an existing policy profile, select it from the list, and click the **Edit** icon .

or

To add a new policy profile, click **Add Policy**.

The **Policy Details** page is displayed.

4. Refer to the associated help (or to [Policy Details Page](#)) for details about the fields used to define the policy profile.
5. Click **Save** to save the updates or to add the new policy profile.

Copying a Policy Profile

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




Task

To copy an existing policy, do the following:

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



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

3. Select the policy profile to copy from the policy list, and click **Copy** icon .

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

Associating a Policy Profile with a Project

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

Managing Authorization Tokens

FlexNet Code Insight uses a JSON Web Token (JWT) to authorize user access to the Code Insight public REST interface. You might be required to explicitly enter an authorization token for certain functionality that uses this REST interface directly (that is, not through Code Insight web UI), such as the following:

- Project import and export processes (see the [Exporting and Importing Project Data](#) chapter)
- The execution of remote scan agents (see [Performing Inventory-Only Scanning](#))

Code Insight enables you to generate and manage one or more of these authorization tokens.

An authorization token is for use by the Code Insight user account that creates it. Thus, an authorization token that your user account generates will give you REST access to only the Code Insight functionality for which your account has permissions. Additionally, you can view and manage only those authorization tokens for the user account under which you are logged in.

Authorization tokens are created and managed from **Preferences** page, as described in the following procedures:

- [Accessing the Preferences Page](#)
- [Generating an Authorization Token](#)
- [Copying the Authorization Token to the Clipboard](#)
- [Editing the Token Name](#)
- [Deleting an Authorization Token](#)

Accessing the Preferences Page

Use these steps to open the **Preferences** page.



Task

To open the Preference page, use these steps:

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



3. Select **Preferences** to open the **Preferences** page.

Generating an Authorization Token

Use the following procedure to generate an authorization token.



Task

To generate an authorization token, do the following:

1. Access the **Preferences** page (see [Accessing the Preferences Page](#)).
2. From the **AUTH Tokens** pane, click **Add Token**.
3. Enter a name for the new token and specify an expiration date (or choose **Never Expires**).
4. Click **Save**.

Copying the Authorization Token to the Clipboard

Use the following procedure to copy an authorization token to the clipboard so that you can paste it in your REST API interface.



Task

To copy an authorization token to the Clipboard, do the following:

1. Access the **Preferences** page (see [Accessing the Preferences Page](#)).
2. From the **AUTH Tokens** pane, locate the token you want to copy, and click the **Copy to clipboard** icon (📋) in the **Actions** column.
3. Click **Select Token Text** to select the entire token value, and then press Ctrl + C to copy it.
4. Paste token in the appropriate location for use by the REST interface.

Editing the Token Name

You can edit only the name of an authorization token, not its expiration date or value.



Task

To edit the token name, do the following:

1. Access the **Preferences** page (see [Accessing the Preferences Page](#)).
2. From the **AUTH Tokens** pane, locate the token you want to edit, and click the Edit icon (✎).
3. Update the token name as needed.
4. (Optional) To copy the token value to the Clipboard for pasting into the REST interface, click **Select Token Text** to select the entire token value, and then press Ctrl + C to copy it.

Deleting an Authorization Token

Use the following procedure to delete an authorization token.



Task

To delete an authorization token, do the following:

1. Access the **Preferences** page (see [Accessing the Preferences Page](#)).
2. From the **AUTH Tokens** pane, locate the token you want to edit, and click the Edit icon (✕).

Performing Advanced Searches

This chapter discusses FlexNet Code Insight's advanced inventory searching capabilities:

- [Advanced Searches](#)
- [Dependencies in Advanced Searches](#)

Advanced Searches

Although you could use the simple search on the **Project Inventory** tab to find inventory items that match text strings, FlexNet Code Insight provides the ability to use additional criteria to display only the items that are of interest. (Simply click the **Advanced Search** button on this tab to access the **Advanced Search** dialog.) Many combinations of search criteria are available, depending upon the type of inventory you want to find. The following table, which is arranged by persona (job function or department), presents a number of advanced searches and their typical results.

For details about using the Advanced Search dialog and all its available search fields, see [Searching Published Inventory](#) and [Advanced Inventory Search Page](#)

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
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</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 transitive dependencies), only top-level inventory items (excluding all dependency inventory items), or all inventory items.</p> <p>Useful for focusing on or filtering out dependency inventory items.</p>	<p>Dependency Options = <i>All Inventory Items</i></p> <p>Dependency Options = <i>Only Top-Level Inventory Items</i></p> <p>Only Dependency Inventory Items = <i>Only Dependency Inventory Items</i></p>
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> <i>From: 09/05/2018 To: 10/31/2018</i></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>
Analyst, Reviewer	By Confidence Level	<p>Inventory generated with a specific level of confidence (High, Medium, or Low). The level is based on the measure of the strength of the discovery technique used to generate the item. (See Inventory Confidence in the “Using FlexNet Code Insight” chapter.)</p> <p>Useful for determining whether the item should be triaged or reviewed to validate or further refine the finding.</p>	<p>Inventory Confidence Level = <i>High</i> (or <i>Medium</i> or <i>Low</i>)</p>

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
Security Analyst	By Vulnerability ID	Inventory with a specific vulnerability (NVD CVE or Secunia Advisory). Useful when you are looking for inventory exposing you to a specific security issue, typically a newsworthy event.	Security Vulnerability ID = <i>SA71946</i>
Security Analyst	By Security Risk Exposure	Inventory containing security vulnerabilities of a specified severity. Useful to filter to inventory items that require immediate attention based on your corporate security policy. For example, we must address all high-severity security issues in the current release.	Security Vulnerability Severity = <i>High</i>
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</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>

Table 3-1 • Sample Advanced Searches

Persona	Search Type	Finds...	Example
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.	<i>Review Status = Approved and Security Vulnerability Age = 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.	<i>License Priority = P1 - Viral/Strong Copyleft</i>
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.	<i>Inventory Review Status = Approved and License Priority = 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.	<i>Inventory Review Status = Approved or License Priority = P1 - Viral/Strong Copyleft or Security Vulnerability Severity = High</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 and Importing Project Data

The following sections describe the project export and import functionality in FlexNet Code Insight:

- [About Exporting and Importing](#)
- [Prerequisites When Using the REST Interface](#)
- [Exporting Project Data](#)
- [Importing Project Data](#)

About Exporting and Importing

FlexNet Code Insight provides export and import functionality for project data. The export-import process can be performed on the same server or across servers. Project data can be quickly imported into an empty project to create inventory or imported into a scanned project to create inventory with file associations. The imported inventory in both cases is “live”—that is, ready to be reviewed and edited.

Export and import functionality is useful in any of these following scenarios:

- **Backup of project and audit data**—Use export to create a full backup of a Code Insight project. The backup data file includes project and scan details, all inventory (with inventory details, field values, file associations, and inventory status), the review status of files, and any custom data. The project data can be restored to a new project for an archived view or for ongoing scanning and auditing.
- **Copying or branching a project**—Use the export-import process to create an exact copy of a project for future scanning and audit work. To do this, export the data from the source project, scan the target project (pointed to the same codebase), and import the data into the target project. The target project can be used for continued scanning and analysis work while the source project remains unchanged.
- **Versioning a project**—Use the export-import process to apply analysis work performed on one product version to the next product version. For example, you can apply the analysis work performed on project “foo-v1” to project “foo-v2”. To do this, export the data from “foo-v1”, scan “foo-v2”, and import the data into “foo-v2”.

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

- **Audit work reuse**—As in the versioning example above, you can use the export-import process to apply analysis work performed on one project to another project containing a subset of similar files. Export data from “project1”, scan “project2” (pointed to “project2” codebase), and import the data into “project2”. Likewise, this process can be used to apply analysis work from several different projects to the current project.

- **Sharing of live audit results between teams**—Use the export-import process to share live audit results between teams or with Flexera Professional Services. For example, you can export data from “project 1” on “instance 1” and import the data into “project 2” on “instance 2”. Results are imported either into an empty project for a live view of inventory or into a scanned project for a live view of inventory with file associations and access to the codebase file tree. To ensure that all inventory is processed, use the `createEmptyInventory=true` flag during the import (see [Available Import Options to Control Import Behavior](#) for details).
- **Migrating audited projects from FlexNet Code Insight v6 to v7**—Use import to create live project inventory in Code Insight v7 from exported v6 project or workspace data. After exporting data from a v6 project, run the Audit Data Migration Tool (available for download in the Flexera Product and License Center) to map inventory fields from Code Insight v6 to v7 and to convert the exported data to the proper JSON data format required for import into v7. Then perform an import into a Code Insight v7 project. Import into an empty project for a live view of inventory only or into a scanned project for a live view of inventory with file associations.
- **Creating inventory from an external system**—Use import to create project inventory in Code Insight from a data file containing legacy or external data. This type of import requires the conversion of the legacy data to the JSON format used by imported data prior to importing into the new project.

Prerequisites When Using the REST Interface

The following are prerequisites when using the FlexNet Code Insight REST interface to execute an export or import:

- [REST Client or Command-Line Tool Supporting cURL](#)
- [Authorization Token](#)
- [Project ID](#)

These prerequisites are not needed if you are performing an export using the FlexNet Code Insight Web UI.

REST Client or Command-Line Tool Supporting cURL

A REST client or command-line interface with cURL support is required to execute the cURL commands that call the REST API to export or import project data.

To download cURL, go to <https://curl.haxx.se/download.html>. Once cURL is installed, ensure that it is added to your PATH environment variable so that you can use it with batch or PowerShell scripts and call it from the command prompt of any working directory.

Authorization Token

Using the REST interface requires a valid JSON Web Token (JWT) for the owner of the project from which data is to be exported or to which data is to be imported. For instructions on obtaining the JWT, see [Managing Authorization Tokens](#) in the “Using FlexNet Code Insight” chapter. The token is not required if using the Web UI.

Project ID

When using the REST interface to execute an import or export, you need to provide the ID of the project from which you are exporting data or the project to which you are importing data.

You can obtain the project ID visually through the FlexNet Code Insight Web UI or programmatically through the REST interface.

Obtaining the Project ID from the FlexNet Code Insight Web UI

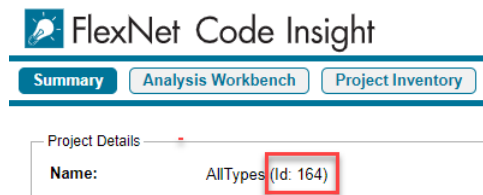
The following are just a few options you can use to obtain the project ID from the Web UI.



Task

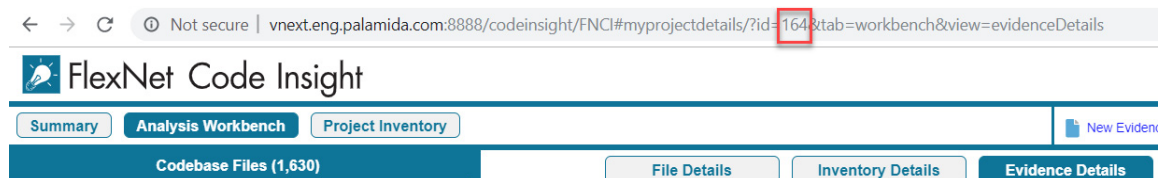
To obtain the project ID through the Web UI, do either of the following:

- Locate the **Name** value on the **Project Summary** page for the project. The ID is displayed in parentheses:



Or

- Locate the project ID included in the URL on any of the project pages, as shown in this example:



Obtaining the Product ID Through the REST Interface

Obtain the product ID by issuing a cURL command that calls the **Get Project Id** REST API.



Important • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.



Task

To obtain the project ID by calling the Get Project Id REST API, do the following:

Execute the following cURL command that invokes the **Get Project Id** REST API using the GET method. Replace the highlighted variables with your server host ID (hostname or IP address) and port, project name, and authorization token.

```
curl -X GET "HOST:PORT/codeinsight/api/project/id?projectName=PROJECT_NAME" -H "accept: application/json" -H "Authorization: Bearer JWT_TOKEN"
```

The following is an example:

```
curl -X GET "http://localhost:8888/codeinsight/api/project/id?projectName=AllTypes" -H "accept: application/json" -H "Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pb2IsInVzZXJJZCI6MSwiaWF0IjoxNTY2ODU5NTg2fQ.qV2j8ZLgNGNjST80dPRwvE0-0y1x7w-0zr5h7Jz2d9uqY8tvACsV68posEU09tD-YX1gXznX-IGnrnopDU7G3w"
```



Note • If the project name contains a space or special character, replace the character with its encoded version. For example, use `project%20foo` for a project named `project foo`.

The response contains the project ID (in this example, 164):

```
{"Content": "164"}
```

Exporting Project Data

The following sections provide the details about exporting project data:

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



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

About an Export

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

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

Project data export is accessible through either of these options:

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



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

Types of Data Exported

The export always processes project data in full—that is, there is no way to limit the exported data. Thus, the data file containing the exported data for a given project includes the following content:

- **Export information**—The project owner, the FlexNet Code Insight version from which data is being exported, the most recent Compliance Library and Electronic Update versions used by the project, the date and time of the export, and more.
- **Project details and scan settings**—The name, description, scan profile, policy profile, and scanroot path of the project from which data is being exported.
- **Inventory**—All data for the project's inventory, including inventory fields, publication and review statuses, associated codebase files, and associated repository items.
- **Reviewed files**—The absolute file path and MD5 for each codebase file marked as reviewed.
- **Custom data**—Custom versions, licenses, and custom mappings between these entities.



Note • Some data contained in the exported data file is for informational purpose only and is not necessarily processed during an import.

Prerequisites for Exporting Data

To export data, ensure that the following prerequisites are met:

- A FlexNet Code Insight v7 instance that is currently running.
- An existing, non-empty project (containing at least one inventory item) on that instance.
- Items listed in [Prerequisites When Using the REST Interface](#) (if performing the export using REST API).

Exporting Project Data Using the Web UI

Use the following instructions to export project data using the FlexNet Code Insight Web UI.



Task

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

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

Depending on your browser configuration for downloads, either process can happen:

- You are prompted to enter a new name used for both the .zip archive and the data file (or keep the default name, which includes the project ID and export timestamp) and to select a download location for the archive. When you save the information, Code Insight creates the .zip archive with the name and in the location you specified.

- The .zip archive is created with the default name and saved to the download location configured for your browser.

The following shows an example export archive generated on a Windows system. In this case, the archive uses the default name:

C:\Users\kdr\Downloads\55-export-12-22-2020_10-42.zip

The archive content would include the following data file:

55-export-12-22-2020_10-42.json



Note • If an archive with the same name exists in the export data directory, the archive is overwritten with the new data.

5. Verify that the export process completed successfully. See [Verifying a Successful Export](#).

Exporting Project Data Using the REST Interface

Use the following information to export project data by using a cURL command that calls the **exportProjectData** REST API.



Important • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.



Task

To export project data by calling the exportProjectData REST API, do the following:

1. Ensure that all requirements in [Prerequisites for Exporting Data](#) and [Prerequisites When Using the REST Interface](#) are met.
2. To initiate the export process, execute the following cURL command to invoke the **exportProjectData** REST API using the GET method. Replace the highlighted variables with your server host name and port, the project ID, and the authorization token. Also, replace PROJECT_DATA_FILE with the name that you want to give to both the JSON file containing the exported data and the .zip file in which the data file will be compressed.

```
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.eyJzdWIiOiJhZG1pbGlzInVzZXJJZCI6MSwiaWF0IjoxNTY2ODU5NTg2fQ.qV2j8ZLgNGNJsT8
OdPRwE0-0y1x7w-0zr5h7Jz2d9uqY8tvACsV68posEU09tD-YXlgXznX-IGrnpODU7G3w" > ProjectKDR.zip
```

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

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

When the export completes, Code Insight generates a .zip archive containing the project data in JSON format and saves it to the directory from which the statement was executed. The archive file name and data file name are the same (except for their extensions). For example, if the export command is executed from the C:/fnci/project_export directory and the output redirect value is [ProjectKDR-export-12-22-2020_10-42.zip](#), the path and file name for the archive would be this:

C:/fnci/project_export/[ProjectKDR-export-12-22-2020_10-42.zip](#)

The data file within the archive would be this:

[ProjectKDR-export-12-22-2020_10-42.json](#)



Note • If an archive with the same name exists in the export data directory, the archive is overwritten with the new data.

3. Verify that the export process completed successfully. See [Verifying a Successful Export](#).

Verifying a Successful Export

Use this procedure to verify that the export process completed successfully.



Task

To verify a successful completion of the export process, do the following:

1. Unzip the archive.

If the export process was not successful, the .zip archive includes a file containing the appropriate status code and error message.

2. (Optional) Open the JSON data file with a utility that supports JSON, such as Textpad or Notepad++, to determine noticeable errors.
3. If errors exist, resolve them, delete the invalid archive file, and run the export script again.

Otherwise, the contents of the .zip file are ready to be imported into a target project or used for backup purposes.

Importing Project Data

The following sections provide the details about importing project data:

- [About an Import](#)
- [Comparison of Standard and Inventory-Only Imports](#)
- [Prerequisites for Importing Data](#)
- [Import Behavior](#)
- [Importing Project Data Using the REST API](#)



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

About an Import

Project data import is available through the FlexNet Code Insight REST interface, as described in [Importing Project Data](#). The following sections provide overview information about the import process.

Input Used in the Import Process

The input to the API is an archived JSON data file containing project data. The archive is first decompressed and the included data file is then applied to the specified target project (that is, the project to which the data is imported).

You can create the JSON data file for input by performing an export from a FlexNet Code Insight v7 project (according to the instructions in [Exporting Project Data](#)) or by performing an export from a Code Insight v6 project and then using the Audit Migration Tool to convert the data into the required format. You can also create the JSON file manually from data exported from an external system. In all cases, the input to the API must be a data file of the expected JSON data format.

Target Project Types

Import is typically performed on a target project that was created as a “standard” project and is associated with an already-scanned codebase. A scan of the target project codebase is required prior to the import in order to build the codebase file tree and to prepare the project for storing file information. This type of import creates inventory with file associations and provides access to the codebase files through **Analysis Workbench**. The inventory is live—that is, ready to be edited and reviewed.

Alternatively, an import can be performed on a project that was created as an “inventory only” project and that does not require a scanned codebase. This type of import creates live inventory without any file associations and does not provide access to the codebase files through **Analysis Workbench**.

For more information about the import types and the data imported for each, see the next section, [Comparison of Standard and Inventory-Only Imports](#).

Comparison of Standard and Inventory-Only Imports

The data that is imported is controlled by the **Type** of the *target project* (that is, the project to which data is imported). For example, if the project was created as a standard project (that is, its **Type** attribute is **Standard**), then the import will be a standard import. If the project was created as an inventory-only project (that is, its **Type** attribute is **Inventory Only**), then the import will be an inventory-only import.

The following table highlights the basic differences between the two import types.

Table 4-1 • Comparison of Standard and Inventory-Only Imports

Import Behaviors and Usage	Standard Import	Inventory-only Import
Import scope	<p>Performs a full import (that is, both inventory and codebase files are processed):</p> <ul style="list-style-type: none"> Processes all inventory items (published and unpublished). Per inventory item, provides inventory details, status, and associated repository item (component-version-license). Lists associated file paths for inventory. 	<p>Performs a partial import:</p> <ul style="list-style-type: none"> Processes inventory only. Does <i>not</i> process codebase files (reviewed or unreviewed).
File processing	<p>Does the following:</p> <ul style="list-style-type: none"> Processes all files marked as reviewed in the data file to be imported. Provides absolute file paths and MD5s for processed files. Does <i>not</i> import unreviewed files. 	<p>Does <i>not</i> process files (reviewed or unreviewed).</p>
Custom-data processing	Imports custom versions, custom licenses, and custom mappings.*	Imports custom versions, custom licenses, and custom mappings.*
Required type for target project	Requires a project created with the Standard attribute.	Requires a project created with the Inventory Only attribute.
Target project codebase requirement	Requires a codebase that is uploaded (or synchronized) to the target project <i>and scanned</i> .	Requires <i>no</i> codebase.
Access to imported inventory and codebase files	<p>Provides direct access to the following:</p> <ul style="list-style-type: none"> Imported inventory through Project Inventory and Analysis Workbench. Imported codebase files through Analysis Workbench. 	<p>Provides direct access to imported inventory through Project Inventory. (Access to inventory and codebase files through Analysis Workbench is <i>not</i> available.)</p>

Table 4-1 • Comparison of Standard and Inventory-Only Imports (cont.)

Import Behaviors and Usage	Standard Import	Inventory-only Import
Usage	<p>Produces a full project copy that can be used for the following (for ongoing scanning and analysis):</p> <ul style="list-style-type: none">• Full project backups.• Application of analysis work from one product version to another (branching).• Application of analysis work from one project version to another.	<p>Provides a means to create inventory from the following:</p> <ul style="list-style-type: none">• An external system.• A Code Insight inventory-only project that is configured to scan remotely using a Jenkins or other scan agent plugin.

* The import does not process custom components. Instead, FlexNet Code Insight creates target inventory of the work-in-progress (WIP) type or license-only type to represent inventory with custom components.

Prerequisites for Importing Data

To import data, ensure that the following prerequisites are met:

- A FlexNet Code Insight v7 instance that is currently running.
- An existing Code Insight project to which data will be imported. The type of import you want to perform determines the type of project needed (and vice versa):
 - To perform a standard import, you need a standard project with an uploaded and scanned codebase. The scanned codebase can be the same or similar to the one whose project data you intend to import.
 - To perform an inventory-only import, you need an inventory-only project with no scanned codebase. You are most likely to have an inventory-only project if the project was created as part of a remote scan on an external system using the FlexNet Code Insight Jenkins plugin or another Code Insight scan agent plugin.

For more information about import types and project types, see [Comparison of Standard and Inventory-Only Imports](#). For instructions on creating a standard or inventory-only project, refer to [Creating a Project](#).



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

- A valid .zip archive containing the JSON data file with the project data to be imported.
- A completed Electronic Update.
- Items listed in [Prerequisites When Using the REST Interface](#) (if performing the export using REST API).

Import Behavior

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

- [Default File and Inventory Processing During an Import](#)
- [Available Import Options to Control Import Behavior](#)
- [Other Import Considerations](#)

Default File and Inventory Processing During an Import

The following information describes the default behavior for processing files and inventory during an import. (You can modify this default behavior as needed by reconfiguring options, as described in the next section, [Available Import Options to Control Import Behavior](#).)

During an import, the file path (and optionally the MD5) is the key for matching data in the data file with the codebase files for the target project. File paths are matched between the data file to be imported and target codebase files by subtracting the root path from the absolute path, as demonstrated in this example:

- **Absolute file path**—/home/fnci/scanRoot/1/ePortal-1.3/src/gettext.c
- **Root path**—/home/fnci/scanRoot/1/
- **File path**—ePortal-1.3/src/gettext.c

The following default logic applies during the import process:

- Only those codebase files that have file paths that match in both the data file to be imported and the scanned target codebase based are processed for inventory-to-file association in the target project. See [checkInventory \(default: false\)](#) for more information.
- Only those codebase files that have file paths and MD5s that match in both the data file to be imported and the scanned target codebase are processed when marking files as reviewed in the target project. See [checkReviewed \(default: true\)](#) for more information.
- Only those inventory items whose associated files have file paths that match in both the data file to be imported and the scanned target codebase are processed into the target project. See [createEmptyInventory \(default: false\)](#) for more information.

Available Import Options to Control Import Behavior

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

If these options are not set, the default values apply.

checkInventory (default: false)

This option specifies whether file MD5 should be used as criteria (in instead of file path) when associating files to inventory in the target project during the import process. By default, this option is disabled, so that only files that match based on file path between the data file to be imported and the target project codebase are associated with inventory in the target project. For example, the file “/ePortal-1.3/src/gettext.c” listed in the data file as belonging to inventory “Item 1” will be considered for association to this inventory item in the target project only if the scanned target project codebase contains the file “/ePortal-1.3/src/gettext.c” with the same file path. However, if the file or the directory containing the file has been renamed in the target project codebase, but the file contents have not changed, you can use the file MD5 as criteria for associating files to inventory instead of using the file path.

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

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

checkReviewed (default: true)

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

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

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

createEmptyInventory (default: false)

This option determines whether “empty” inventory items are still processed in the target project during the import. Empty inventory items either have no file associations in the data file to be imported or do have associated files in the data file but no matching file paths for these files in the scanned target codebase.

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

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

Other Import Considerations

Consider the following additional behavior during import processing.

Duplicate Inventory

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

Manually Unreviewed Files

A codebase file that is manually “unreviewed” in the source project does not retain its unreviewed status in the target project if the target codebase scan has marked the corresponding target file as “reviewed”. This occurs because the data file to be imported stores information about only those codebase files that have been marked as reviewed in the source project. Hence, no information about the unreviewed file exists in the import data to overwrite information for this same file in the target project.

If, during a standard import, you want to retain the reviewed and unreviewed status of codebase files as defined in the source project, manually mark all of the codebase files in the target project as unreviewed before importing the data file.

Importing Project Data Using the REST API

Use the following information to export project data by using a cURL command that calls the **importProjectData** REST API.



Note • If copying the cURL command directly from the following instructions for your own use, copy it to a text editor first to remove formatting and any line breaks or extra spaces.



Task

To run an import, do the following:

1. Ensure that all prerequisites in [Prerequisites for Importing Data](#) and [Prerequisites When Using the REST Interface](#) are met.
2. To initiate the import process, execute the following cURL command to invoke the **importProjectData** REST API using the POST method. Replace the highlighted variables with your server host ID (hostname or IP address) and port, the project ID, and the authorization token. Also, replace PROJECT_DATA_FILE with the name of .zip archive containing the JSON data file you are importing.

```
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 eyJzdWIiOiJqcnViaW4iLCJ1c2VySWQiOiJEWLCjYpYXQiOiJMTA5NjM2NzZ9" -H "cache-control: no-cache" -H "Content-Type: application/octet-stream"
```



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

When the import is complete, a status message with **OK** will appear in the command prompt window. If the import is not successful, a status code and error message is displayed.

3. To verify that the import has completed successfully, follow these steps:
 - a. Open the target project in FlexNet Code Insight and navigate to the **Inventory** page (see [Searching the System](#)).
 - b. Confirm that the total number of inventory items includes the newly imported items. (Keep in mind that, by default, only inventory with matching associated files in the target codebase are imported.)
 - c. Confirm that the inventory items contain accurate inventory details and file path associations.

Automated Analysis

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

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

What is Automated Analysis?

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

Automated Analysis is used in both scanning scenarios outlined below:

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

Supported Development Ecosystems

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

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

Supported Ecosystems

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


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

Table 5-1 • Supported Ecosystems




























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

Table 5-1 • Supported Ecosystems (cont.)

Language/ File Type	Package	Registry	Manifest File	Top-level Inv.	Direct Dep.	Trans. Dep.	Notes
PHP	Composer	https://packagist.org/	composer.json	✓	✓	—	—
			composer.lock	✓	✓	—	—
RPM	RPM Header	N/A	.rpm	✓	N/A	N/A	—
Ruby	Gem	https://rubygems.org/api/v1/	.gem	✓	✓	—	See Notes for Supported Ruby Ecosystems .
			Gemfile	✓	✓	—	
			.gemspec	✓	✓	—	
Swift, Obj-C	CocoaPods	N/A	Podfile.lock	✓	—	—	—
			.podspec	✓	—	—	—
Various	Git Repo	https://github.com	config	✓	—	—	See Notes for Supported Git Ecosystems .

Notes About Ecosystem Support

The following sections provide additional information (such as limitations, requirements, and clarifications) to consider for the various ecosystems supported in the Code Insight Automated Analysis process.

Notes for Supported Go Ecosystems

Note the following for Go ecosystems:

- A go-lang project configured with a supported package manager must include a license file to enable Code Insight to discover it as top-level inventory.
- Currently, Code Insight supports the discovery of top-level inventory only in scans of pre-build Artifact source code.
- If the codebase is uploaded from the release section of the VCS repository, Code Insight must use the version in the name of the project's parent folder as the version in the top-level inventory name. Any changes to the version in the parent folder name can result in the wrong version being reported in the inventory.

Notes for Supported Ruby Ecosystems

Note the following for Ruby ecosystems:

- For RubyGem projects, Code Insight shows all platform-related dependencies and those dependencies that are not part of a “test” or “dev” group as inventory. Any gems identified as “dev” or “test” are not considered for inventory.
- Only SemVer expressions in the *major.minor.patch* format are supported to resolve dependencies listed in the manifest file.

Notes for Yocto Ecosystems

Code Insight parses a .bb file only if it contains an SCR_URI property value that starts with [git://](#) or [https://](#). If the SCR_URI property contains more than one URI, only the first supported URI is considered.

Notes for Supported Git Ecosystems

FlexNet Code Insight scans configuration files inside .git folders encountered in a project codebase and uses identified information to create inventory items.

Notes about Dependencies Support

FlexNet Code Insight supports scanning for top-level inventory items, direct dependencies, and transitive dependencies. The scan profile, managed by the Code Insight administrator, is used to configure of the desired depth of scan with respect to dependencies. See [About Scan Profiles](#) for information about scan profiles.

Note the following additional information about dependency scanning:

- Dependencies represent open-source packages that are referenced by the scanned codebase, but not necessarily present in the codebase.
- Dependency scanning is designed to be used when scanning pre-build artifacts, typically found in source-code bundles. Since this scenario relies on package-management configuration files, it is not 100% precise in the resolution of the declared dependencies. In many cases, dependencies will be resolved to the latest available version within the declared range. However, this version can differ from the actual package version pulled down as part of the build.
- Dependency scanning is not designed for scanning post-build artifacts when using the scan agent plugins to scan on the build servers as part of the build process. In such scenarios, all dependencies have already been resolved by the build system and are present in the scanned codebase.

Supported Archive Formats

The Automated Analysis process in FlexNet Code Insight uses 7-Zip to read archive files. Use the following link to view the archive formats supported by 7-Zip:

<https://sevenzip.osdn.jp/chm/general/formats.htm>

Additional Rule-based Detection Capabilities

Automated detection used in the Automated Analysis process can also generate findings based on other rule-based techniques that include the following:

- Search term analysis
- File name analysis
- CDN analysis

Performing Inventory-Only Scanning

This section discusses FlexNet Code Insight inventory-only scanning. The following topics are covered in this section:

- [Inventory-Only Scan](#)
- [Creating a Project Without Uploading a Codebase](#)
- [FlexNet Code Insight Plugins](#)

Inventory-Only Scan

FlexNet Code Insight has the ability to scan files on a remote system and manage the inventory items created from the remote server. This type of scan is referred to as an inventory-only scan. It allows you to integrate automatic package-level scanning into your build process using the scan agent plugins such as Jenkins. This integration includes automated package discovery and targeted components. For additional information about automated analysis, see [Automated Analysis](#).



Note • *FlexNet Code Insight does not generate email notifications for remote scan events.*

Creating a Project Without Uploading a Codebase

Organizations may be reluctant to upload their codebase into FlexNet Code Insight. Instead, they want to keep their codebase in its existing development system due to security, consistency, or other concerns. To address this requirement, FlexNet Code Insight provides scan agents that can scan a codebase wherever it resides and send the results as inventory to the Code Insight server for review and remediation by users. This process requires an inventory-only project on Code Insight server for handling the returned results, but requires no codebase upload to Code Insight.

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

Phase 1—Create an inventory-only project in FlexNet Code Insight. See [Creating a Project](#).

Phase 2—Create a valid JSON Web Token (JWT) for the user whose account will be used to connect to FlexNet Code Insight. For instructions on generating the JWT, see [Managing Authorization Tokens](#) in the “Using FlexNet Code Insight” chapter.

Phase 3—Install and configure the appropriate scan agent plugin. (For information how to install and configure the plugin, see the *FlexNet Code Insight Plugins Guide*.) As part of the configuration process, you will need to provide the name of the inventory-only project that you created, the URL of the FlexNet Code Insight core server, and the JWT.

When the plugin is invoked (for example, by a build in Jenkins) the remote codebase will be scanned, and identified inventory items will be created on the FlexNet Code Insight server. The resulting inventory can be managed in FlexNet Code Insight.



Note • In the case of an inventory-only project, the **Analysis Workbench** will not be available. However, all other inventory management functionality is supported.

FlexNet Code Insight Plugins

FlexNet Code Insight offers the following standard scan agent plugins:

Table 6-1 • Overview of the Standard Plugins

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

Additionally, a generic scan agent plugin is available with Code Insight that enables you to scan arbitrary file systems of your choice. It also easily integrates with certain Engineering systems, such as TeamCity and GitLab, to perform scans as part of a build process or can serve as an example for developing your own scan agent plugin (as described in *FlexNet Code Insight Plugins Guide*).

Requirement Considerations

Refer to the *FlexNet Code Insight Plugins Guide* for a list of requirements for each scan agent plugin.

Configuring Source Code Management

FlexNet Code Insight provides a connector that allows you to use Source Code Management systems (SCM) as a source for codebase data. This section discusses the following topic:

- [Managing Source Code Management \(SCM\) Instances](#)
- [Configuring a Git SCM Instance](#)
- [Configuring a Perforce SCM Instance](#)
- [Configuring a TFS SCM Instance](#)

Managing Source Code Management (SCM) Instances

FlexNet Code Insight provides the ability to scan data obtained from synchronization with a remote data source. The following sections provide information on adding and managing SCM instances.

- [Adding an SCM Instance to the Code Insight Project](#)
- [Testing an SCM Instance](#)
- [Synchronizing an SCM Instance](#)
- [Deleting an SCM Instance](#)

Prerequisites

Before performing the procedures in this section, ensure that an SCM command-line client is properly installed on the FlexNet Code Insight Scan Server and that connectivity between the SCM client and the SCM server is properly configured. Refer to the “Integrating with Source Code Management” chapter in the *FlexNet Code Insight Installation and Configuration Guide* for details.

If Code Insight is running as a service, make sure that the user context under which the service runs has appropriate permissions to run the SCM client.

Adding an SCM Instance to the Code Insight Project

You can specify configuration information about your remote data source when you edit your Code Insight project.



Task

To add an SCM instance, do the following, do the following:

1. Navigate to the **Summary** tab for the project to which you are synchronizing codebase files.
2. Open the **Manage Project** menu and select **Edit Project**. The **Edit Project** page opens.
3. Select the **Version Control Settings** tab.
4. Select the desired connector (remote data source) from the **Application** dropdown menu.
5. Click **Add Instance**. The available fields for the selected application will appear on a new **Instance** tab. See the inline help for explanations of the fields on this tab.
6. After editing the fields for your specific instance, click **Save**. You should now test and synchronize the instance.

Testing an SCM Instance

If you add an instance or edit any of the fields associated with your SCM instance, you should test the connection to ensure the repository is responsive.



Task

To test your connection, do the following:

1. If you are not already on the **Version Control Settings** tab on the **Edit Project** page, navigate to it.
2. Select the **Instance** tab for the connection you want to test.
3. Click **Test Connection** to confirm that the repository is reachable. After a moment, FlexNet Code Insight displays a success message dialog if the connection is successful. If the connection is not successful, ensure that your entries on the **Instance** tab are correct and click **Test Connection** again.

Synchronizing an SCM Instance

After testing your SCM connection, you can synchronize the instance to get the codebase files from the selected repository.



Task

To sync an SCM instance, do the following:

1. If you are not already on the **Version Control Settings** tab on the **Edit Project** page, navigate to it.
2. Click **Sync Now** to synchronize files from the repository to the root directory of the Code Insight Scan Server associated with your project. The root directory contains directories identified by project IDs. Under each project ID directory, subdirectories with names such as `git.0` or `git.1` are generated, one for SCM instance created for your project. (The number of subdirectories under the directory for your project ID is equal to the number of instances created for your FlexNet Code Insight project.)

Note the following:

- If multiple instances have been added, clicking **Sync Now** will synchronize all instances. If the sync fails for one instance, the overall sync will fail as well.
- If the Scan Server assigned to the project to which you are synchronizing codebase files is disabled, the **Sync Now** button is also disabled. Consider reassigning the project to an enabled Scan Server. (If necessary, see your FlexNet Code Insight administrator for information about which servers are enabled).

Deleting an SCM Instance

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



Task

To delete an SCM instance, do the following:

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

Configuring a Git SCM Instance

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

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

Adding a Git SCM Instance to the Code Insight Project

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



Task

To configure a Git SCM instance, do the following:

1. Use the instructions in [Adding an SCM Instance to the Code Insight Project](#) to navigate to the **Version Control Settings** tab and add a Git SCM instance, selecting **Git** from the **Application** dropdown.
2. See [Configuring the Git SCM Instance](#) for a description of the settings used to define a Git SCM instance, or use the inline help provided for each setting on the tab.
3. Once you save the Git SCM instance, test the Code Insight connection with Git SCM instance, as described in [Testing an SCM Instance](#).

Configuring the Git SCM Instance

The following settings are used to configure a Git SCM instance.

Table 7-1 • Setting Used to Configure a Git SCM Instance

Git SCM Instance Setting	Description
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, do the following:

1. Use the instructions in [Adding an SCM Instance to the Code Insight Project](#) to navigate to the **Version Control Settings** tab and add a Perforce SCM instance, selecting **Perforce** from the **Application** dropdown.
2. See [Configuring the Perforce SCM Instance](#) for a description of the settings used to define a Perforce SCM instance, or use the inline help provided for each setting on the tab.
3. If SSL has been configured for communication between the Perforce server and the Perforce client on Code Insight, execute the following command in p4 to establish the trust between the server and client. Unless this trust is established, connections between the Perforce server and client will fail.

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

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

When prompted to establish trust, enter **yes**.

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

Configuring the Perforce SCM Instance

The following settings are used to configure a Perforce SCM instance.

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

Perforce SCM Instance Setting	Description
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> <pre>tcp:<p4ServerHostID>:<p4Port></pre> <p>For an SSL connection</p> <pre>ssl:<p4ServerHostID>:<p4Port></pre> <p>p4ServerHostID and p4Port identify the hostID (hostname or IP address) and port of the Perforce server</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.

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

Perforce SCM Instance Setting	Description
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 Performer SCM instance, do the following:

1. Use the instructions in [Adding an SCM Instance to the Code Insight Project](#) to navigate to the **Version Control Settings** tab and add a TFS SCM instance, selecting **TFS** from the **Application** dropdown.
2. See [Configuring the TFS SCM Instance](#) for a description of the settings used to define a TFS SCM instance, or use the inline help provided for each setting on the tab.
3. Once you save the TFS SCM instance, test the Code Insight connection with the TFS SCM instance, as described in [Testing an SCM Instance](#).

Configuring the TFS SCM Instance

The following settings are used to configure a TFS SCM instance for the Code Insight project.

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

Perforce SCM Instance Setting	Description
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> <pre><protocol>:<tfs_host>:<port>/<collection>/<project></pre> <p>For earlier versions of TFS:</p> <pre><protocol>:<tfs_host>:<port>/<collection>/<tfsroot>/<project></pre>
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/Permissions Tab](#)
- [Add User Dialog](#)
- [Edit User Dialog](#)
- [Electronic Updates Tab](#)
- [Email Server Tab](#)
- [LDAP Tab](#)
- [ALM Tab](#)
- [Scan Servers Tab](#)
- [Scan Server Dialog](#)
- [Scan Profiles Tab](#)
- [Create/Edit Scan Profile Dialog](#)
- [Project Defaults Tab](#)
- [Projects List Page](#)
- [Project Summary Tab](#)
- [Edit Project: General Tab](#)
- [Edit Project: Scan Settings Tab](#)
- [Edit Project: Review and Remediation Settings Tab](#)
- [Edit \(Default\) Project Users Page](#)
- [Scan History Dialog](#)

- [Select a New Project Owner Page](#)
- [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](#)
- [Policy Page](#)
- [Policy Details Page](#)
- [Custom Detection Rules Tab](#)
- [Custom Detection Rule Dialog](#)
- [Edit Custom Rule Dialog](#)
- [License Details Window](#)
- [Lookup Component Window](#)
- [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.

Table 8-1 • FlexNet Code Insight Dashboard (cont.)

Column/Field	Description
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](#)[Policy Page](#)[Users/Permissions Tab](#)[Electronic Updates Tab](#)[Email Server Tab](#)[LDAP Tab](#)[ALM Tab](#)[Scan Servers Tab](#)[Scan Profiles Tab](#)


Users/Permissions Tab

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

Table 8-2 • Users tab

Column/Field	Description
Add User	Click to display the Add User dialog.
Manage Permissions	Click to display the Manage Permissions dialog used to assign the following permissions to users: Administrator, Manage Policy, and Create Projects.
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.

Table 8-2 • Users tab (cont.)

Column/Field	Description
Enter Search Criteria	Enter a string by which to filter the list of users. A full or partial match to any of the user details is allowed. Click  to remove the filter.

See Also

[Add User Dialog](#)

[Edit User Dialog](#)

“Configuring FlexNet Code Insight” in the *FlexNet Code Insight Installation & Configuration Guide*

Add User Dialog

The **Add User** dialog on the **Administration** page allows you to add new users to the FlexNet Code Insight system. The dialog contains the following columns and fields:

Table 8-3 • Add User dialog

Column/Field	Description
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.
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/Permissions Tab](#)

Edit User Dialog

The **Edit Users** dialog is where you can edit users who are already in the FlexNet Code Insight system. The dialog contains the following columns and fields:

Table 8-4 • Edit User dialog

Column/Field	Description
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.
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/Permissions Tab](#)

Electronic Updates Tab

An initial full Electronic Update is run automatically after your initial startup of FlexNet Code Insight. It provides the basis of a local data library used by FlexNet Code Insight to identify OSS and third-party code in your codebase. The **Electronic Updates** tab on the **Administration** page enables you to configure how and when subsequent Electronic Updates are run to keep this library up to date. Refer to the following topics for more information:

- [Overview of Electronic Update Setup](#)
- [Field Descriptions](#)

For detailed instructions on how to schedule and run Electronic Updates, see “Configuring FlexNet Code Insight” in the *FlexNet Code Insight Installation & Configuration Guide*.

Overview of Electronic Update Setup

The following describes the basics for configuring electronic updates:

- [Specifying an Update as Server or Local](#)
- [Scheduling Electronic Updates](#)

Specifying an Update as Server or Local

The **Electronic Update Type** field (see [Field Descriptions](#) below) on the **Electronics Update** tab enables you to configure the Electronic Update to run as either a server or local update. The difference between the two methods is the means by which the FlexNet Code Insight server obtains the files required to run the update:

- During a **server** Electronic Update, the most recent Electronic Update files are automatically downloaded from Flexera to the FlexNet Code Insight server prior to processing the update.
- For a **local** Electronic Update, you must manually download the Electronic Update files from Flexera to a location that is locally accessible to the Code Insight server, such as a shared drive or a local USB drive. Then, when an update is triggered, the Code Insight server automatically uploads the files and proceeds with the update. This type of Electronic Update is useful when the Code Insight server has no external Internet access or when a specific Electronic Update version is needed for testing or demo purposes.

Scheduling Electronic Updates

The remaining fields (see [Field Descriptions](#) below) on the **Electronic Updates** tab allow you either to schedule an Electronic Update to run automatically at regular intervals or to manually request an update as needed. By default, an update is *incremental* (that is, the update applies on changes from the previous update). However, you have the option force a *full* Electronic Update, which replaces all data from the previous update. (A full update might be necessary, for example, if the most recent update did not complete properly.)

In summary, you can schedule the following:

- An incremental Electronic Update (server type only) that runs automatically at a regular frequency that you define.
- An incremental Electronic Update (server or local type) that you manually run as needed.
- A full Electronic Update (server or local type) that you manually run when necessary. Use this option with caution as forcing a full update to run will take several hours to complete, similar to the initial update run when FlexNet Code Insight was first installed.



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

Field Descriptions

The tab contains the following columns and fields:

Table 8-5 • Electronic Updates tab

Column/Field	Description
General	<p>The initial step in running an Electronic Update is to determine whether you are running it as a local or server update. For more information about these two types of updates, see Specifying an Update as Server or Local.</p>
Electronic Update Type	<p>Select the type of Electronic Update to run based how the FlexNet Code Insight server obtains the Update Manifest and Update Data files required to perform the update:</p> <ul style="list-style-type: none"> ● Local—As part of the Electronic Update process, the Code Insight server uploads each of these files from a locally accessible location (to which you have manually downloaded the appropriate files from Flexera prior to the update). Use the Update Manifest File and Update Data File fields to identify the locations from which Code Insight server will upload the files. ● Server—The most recent Electronic Update files are automatically downloaded from Flexera to the Code Insight server as part of the Electronic Update process.
Local Electronic Update configuration	<p>If you intend to run a <i>local</i> Electronic Update, you must specify the location of the two required “update” files that you manually downloaded from Flexera. The location of each file must be locally accessible. To run the update, use the Run Update Now option.</p>
Update Manifest File	<p>Click Select File to search for and select the Update Manifest file (update_manifest.txt) to upload to the Code Insight server. The manifest file contains the following:</p> <ul style="list-style-type: none"> ● Information that Code Insight uses to determine whether to perform the update. ● The expected hash value for each data file stored in the update.zip file (see the Update Data File field description). This information will be compared with the hash values of actual files in the archive to ensure that the files have not changed or been tampered with.
Update Data File	<p>Click Select File to search for and select the data archive (update.zip) file to upload to the Code Insight server. This archive contains data files that provide the CVSS information used by Code Insight to perform update.</p> <p>Code Insight uses the hash information in the manifest file (see the Update Manifest File field description) to ensure that the data files are the expected ones and have not changed or been tampered with.</p>

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

Column/Field	Description
Configuration for automatic Electronic Updates (server update only)	FlexNet Code Insight enables you to configure <i>server</i> incremental updates to run automatically at a frequency you define, as described below.
	Note that you can always manually force an incremental or full update between the scheduled updates, or you can disable scheduled automatic updates altogether and manually run updates as needed. In either case, you would need to use the Run Update Now option to run an Electronic Update.
	<p>Update Frequency</p> <p>Select from one of the available frequencies for running an incremental Electronic Update automatically:</p> <ul style="list-style-type: none"> • Never—If you select Never, Electronic Updates will not be run automatically. (Selection of this option hides any further dropdowns.) You can always manually schedule an incremental or full update as needed using the Run Update Now option. • Daily—If you select Daily, a second dropdown is displayed to choose the time of day when you want the Electronic Update to occur. • Weekly—If you select Weekly, both the “time of day” dropdown and the Select a day... dropdown are displayed. Select both the time of day and the day of the week when you want the Electronic Update to occur.
	<p>Save Schedule</p> <p>Click this button to save the schedule. Your future incremental updates will run automatically according to the frequency you defined.</p>
Configuration for manually running an Electronic Update	You can manually run an Electronic Update at any time. The update is run immediately or placed in queue and initiated once all pending scans have completed. Currently, this is the only way to schedule a local update. If automatic server updates are also configured, a manually-run update is in addition to the automatic updates.
	<p>Run Update Now</p> <p>Select the scope of the manually-run update:</p> <ul style="list-style-type: none"> • Incremental Update—Schedule an incremental Electronic Update. However, if no changes have occurred in the Electronic Update data since it was last run, the update is not executed. • Full Update—Force a full Electronic Update to run whether or not changes have occurred in the Electronic Update data since it was last run. Use this option judiciously as a full Electronic Update takes several hours to complete, similar to the time required to run the initial update when FlexNet Code Insight was installed.
	<p>Update</p> <p>Click this button to initiate the Electronic Update immediately or once pending scans are completed.</p>

See Also

“Configuring FlexNet Code Insight” chapter in the *FlexNet Code Insight Installation & Configuration Guide*

Email Server Tab

The **Email Server** tab on the **Administration** page allows you to enable email notifications and set email options. The tab contains the following columns and fields:

Table 8-6 • Email Server tab

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

Table 8-7 • LDAP tab

Column/Field	Description
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	<p>Specify the URL of your LDAP server in this format:</p> <p><code>ldap://<ldap_server_host>:<ldap_port></code></p> <p>The following is an example LDAP server URL:</p> <p><code>ldap://ad.mycompany.com:389</code></p>

Table 8-7 • LDAP tab (cont.)

Column/Field	Description
Authentication Type	<p>Select the type of LDAP authentication that will be used:</p> <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	<p>Enter the LDAP user name used for authentication, providing the user's full Distinguished Name (DN). Note that the user must have permissions to query the LDAP server.</p> <p>This field is disabled if anonymous authentication is selected.</p>
LDAP Password	<p>Enter the password for the user name specified in the previous field. This field is disabled if anonymous authentication is selected.</p>
LDAP Query Details	
LDAP Base	<p>Specify the base node of the LDAP server.</p>
LDAP Search Base	<p>Specify the Search Base, which, along with the Search Query, is used to query a list of users for synchronizing with FlexNet Code Insight.</p>
LDAP Search Query	<p>Specify the search query for your LDAP server. The following is an example search query:</p> <p><code>(&(objectClass=person)(memberOf=CN=SCAGroup,CN=Users,DC=ad,DC=mycompany,DC=com))</code></p>
Use Paging	<p>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.</p>
LDAP Page Size	<p>Indicate the page size. The default page size is 1000 elements.</p>
LDAP User Sync Frequency	<p>Specify the frequency at which FlexNet Code Insight will synchronize user data with the LDAP server:</p> <ul style="list-style-type: none"> • Never—Select this option to disable the automatic user sync. A user sync will occur only if the user clicks the Sync Now button. For all other values, automatic user sync is enabled per the configured frequency. (This is the default value.) • 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.

Table 8-7 • LDAP tab (cont.)

Column/Field	Description
Search Sub-tree	Select this checkbox to enable deep searches through the subtree of the path defined by LDAP Base + LDAP Search Base . Note that, while helpful in locating users in certain cases, a deep search can negatively affect performance (and therefore, by default, is not enabled).
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, the value <code>(uid={0})</code> , when used with the LDAP Search Base and LDAP Search Query specified above, searches for an entry where the uid is equal to the user name.
[actions]	
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.




ALM Tab

The **ALM** tab on the **Administration** page allows you to configure Jira and other ALM (Application Lifecycle Management) instances for integration with Code Insight for the purpose of creating work items in external workflow systems. The tab contains the following columns and fields:

Table 8-8 • ALM tab

Column/Field	Description
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.

Table 8-8 • ALM tab (cont.)

Column/Field	Description
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.
Default Assignee	The default user to whom to assign work items created for this instance.
Default Summary Text	Default text to display as a summary for the issue on the ALM server. The text supports the following Code Insight variables: \$PROJECT_NAME, \$INVENTORY_ITEM_NAME, \$COMPONENT_NAME, \$VERSION_NAME, \$LICENSE_NAME, \$NUMBER_VULNERABILITIES, \$NUMBER_FILES, or \$INVENTORY_URL.
Default Description Text	Default text to display as a description for the issue on the ALM server. The text supports the following Code Insight variables: \$PROJECT_NAME, \$INVENTORY_ITEM_NAME, \$COMPONENT_NAME, \$VERSION_NAME, \$LICENSE_NAME, \$NUMBER_VULNERABILITIES, \$NUMBER_FILES, or \$INVENTORY_URL.

Scan Servers Tab

The **Scan Servers** tab on the **Administration** page lists the Scan Servers that you have identified to your FlexNet Code Insight system. Each entry in the list shows basic information about the given Scan Server including its status. From a given entry, you can access a separate dialog to edit server properties as well as refresh the entry itself to see the latest server status. The tab also lets you define a new Scan Server. The tab contains the following columns and buttons to identify and

manage Scan Servers:

Table 8-9 • Scan Servers tab






Category	Field
[Scan Server entry]	The following columns for each entry in the Scan Server list provide information about the given Scan Server, as well as a means to refresh the Scan Server status and edit server properties.
	<p>Alias</p> <p>The user-defined name for the Scan Server, as well as the server's current status. The following icons represent the server status:</p>
	<p> The green icon indicates that the Scan Server is “enabled” for scanning and is currently running (turned on). Scans are run in queue order.</p>
	<p> The red icon indicates that the Scan Server is “enabled” for scanning but is currently not running (that is, it is turned off). Any attempts to associate a project with the Scan Server or upload a codebase to the server generates an error. Additionally, any attempt to initiate a scan will result in the scan's being queued. However, once the server is active, the scan will start based on queue order. (Users can click the Past Scans link on the project Summary page to view details about the scheduled scan.)</p>
	<p> The gray icon indicates that the Scan Server is “disabled” (that is, cannot be used for scanning). Whether or not the server is running has no effect on this status. If an enabled server is needed for scans on a project assigned to a disabled Scan Server, you must create a new project.</p>
	<p>Host</p> <p>The localhost value is used if the Scan Server is on the same instance as the Core Server.</p>
	<p>Port</p> <p>The port used by the Scan Server on the host instance. By default, the port is 8888.</p>
	<p>CL Path</p> <p>The path for the FlexNet Code Insight Compliance Library (CL). If the path is specified, the CL is accessed as part of the scan to perform exact-file and source-code fingerprint (snippet) matching. Elements of scanned codebase files are compared with information contained in the CL to generate file-level evidence on which you can take action.</p> <p>If the path is not specified, the codebase is scanned without using the CL. This type of scan generates inventory from Code Insight's Automated Analysis feature but has limitations. For more information about the Compliance Library, see What Is a FlexNet Code Insight Scan?.</p>
	<p>Codebase Path</p> <p>The path on the Scan Server where FlexNet Code Insight will store and manage all uploaded code for projects that use this Scan Server. Once the Scan Server is added to the Code Insight system, this field cannot be edited.</p>

Table 8-9 • Scan Servers tab (cont.)

Category	Field
[actions for scan server entry]	<p>Select the appropriate icon for the desired action:</p> <ul style="list-style-type: none"> The  (Edit) icon to edit the configuration for the given Scan Server. The Scan Server dialog is opened, enabling you to make edits. The  Refresh icon (visible when you hover over the Scan Server entry) to refresh the Scan Server entry, including its status.
[action]	<p>Use the following button to add a new Scan Server to the Code Insight system—that is, that is, identify the server to the FlexNet Code Insight Core Server to make it available for scanning purposes. To add a Scan Server, ensure that it has been installed and is running. See the <i>FlexNet Code Insight Installation and Configuration Guide</i> for instructions for installing and starting a Scan Server.</p>
	<p>Add Scan Server Click this button to add a new Scan Server. The Scan Server dialog is displayed.</p>

See Also
[Scan Server Dialog](#)

Scan Server Dialog

Before a user can assign project codebases to a Scan Server in order to scan them, the Scan Server must first be installed either on the same instance as the Code Insight Core Server or on a separate instance, as described in the *FlexNet Code Insight Installation and Configuration Guide*. (The Scan Server must have the same version as the Core Server.) As administrator, you must then use the **Scan Server** dialog to “add”—that is, identify—the server to the FlexNet Code Insight system to make it available for scanning purposes.

In addition to adding a new Scan Server, you use the **Scan Server** dialog to edit an existing Scan Server’s properties. For detailed instructions on adding or editing a Scan Server, see “Adding or Editing Scan Servers” in the *FlexNet Code Insight Installation and Configuration Guide*.

Multiple Scan Servers

If multiple Scan Servers have been installed, you can identify more than one of these servers to the system, thus enabling users to distribute codebase scans. Keep in mind that, when multiple Scan Servers are installed, each should be installed on a different instance with a unique host ID and port. The codebase for a given project can be assigned to only one of the Scan Servers (but multiple project codebases can be assigned to a single Scan Server). All codebases assigned to a given Scan Server are stored on that server in a location that you specify.

Prerequisite for Adding or Editing a Scan Server

Ensure that the Scan Server that you are adding or editing is currently running and that the Scan Server you are adding has the same version as the Core Server.

Dialog Fields

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

Table 8-10 • Scan Server dialog

Column/Field	Description
Alias	Enter a common name for the Scan Server.
Host	<p>Provide the hostname (such as kr1.eng.companyA.com) or IP address of the instance hosting the Scan Server. If the Scan Server is on the same instance as the Core Server, enter localhost.</p> <p>The same host-and-port combination must be unique among the <i>enabled</i> Scan Servers. (See Status is this table for a description of enabled Scan Servers.)</p>
Port	<p>Specify the port used by the Scan Server on the host instance. By default, the port is 8888.</p> <p>The same host-and-port combination must be unique among the <i>enabled</i> Scan Servers. (See Status is this table for a description of enabled Scan Servers.)</p>
CL Path	<p>Provide the path for the FlexNet Code Insight Compliance Library (CL), downloaded from the Flexera Product and License Center. The CL is a database used by the Scan Server to perform exact-file and source-code fingerprint (snippet) matching. Code Insight compares elements of scanned codebase files with information contained in the CL to generate file-level evidence on which you can take action.</p> <p>The validity of the entered path is checked when you click Save.</p> <p>Alternatively, leave this field blank to scan your codebase without using the CL. (Code Insight provides the scan profile “Basic Scan Profile (without CL)” to perform the scan.) This type of scan generates inventory from Code Insight’s Automated Analysis feature but has limitations, as described in “About Scanning without the Compliance Library” in the <i>FlexNet Code Insight Installation and Configuration Guide</i>. Keep in mind that, when you run a scan using the CL (that is, by specifying a valid CL path), you obtain a deeper, more comprehensive scan on your codebase.</p> <p>For additional information, see the following:</p> <ul style="list-style-type: none"> • “Managing Scan Profiles” in the <i>FlexNet Code Insight Installation and Configuration Guide</i> for more information about the “Basic Scan Profile (without CL)” and about creating and managing scan profiles in general. • Applying a Scan Profile in the “Using FlexNet Code Insight” chapter in this book for instructions on associating a scan profile with a project. • What Is a FlexNet Code Insight Scan? in the “Using FlexNet Code Insight” chapter in this book for information about Code Insight scans in general.

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

Column/Field	Description
Codebase Path	<p>Provide the path on the Scan Server where FlexNet Code Insight will store and manage all uploaded code for projects that use this Scan Server. Ensure you have adequate disk space to store the codebases. The recommended starting size for this directory is 500GB.</p> <p>The directory must already exist. The validity of the entered path is checked when you click Save.</p> <p>Once the Scan Server is added to the Code Insight system, this field cannot be edited.</p>
Status	<p>By default, the Scan Server is enabled for scanning.</p> <p>However, if necessary for an existing Scan Server, select Disabled to make the Scan Server unavailable for further scans. Once disabled, the server is no longer displayed in the Scan Server dropdown during project creation or when setting global project defaults. Additionally, this field becomes read-only on the Edit Project dialog.</p> <p>Note the following about disabling a Scan Server:</p> <ul style="list-style-type: none">● If this Scan Server is the system default Scan Server (as defined on the Project Defaults tab), you must change this default to another server before you can disable the current server. See Project Defaults Tab for instructions on updating the default Scan Server.● If this Scan Server is associated with one or more projects, a warning is displayed before you can disable the server. Once you click Yes, the Start Scan and Upload Project Codebase options are disabled on the Summary page for each project associated with the server. <p>If you attempt to re-enable a disabled Scan Server when another currently <i>enabled</i> Scan Server has the same host-and-port combination or alias, you receive an error when you click Save.</p>
Save	<p>Click this button to save any changes you made to the Scan Server properties. Errors are generated when the following conditions exist:</p> <ul style="list-style-type: none">● The Scan Server you are adding or editing is not running.● The version of the Scan Server you are adding is different from the Core Server version.● The codebase path or CL path is invalid.
Cancel	<p>Click this button to cancel any changes you made to the fields on the Scan Server dialog.</p>


See Also

[Project Defaults Tab](#)
[Edit Project: Scan Settings Tab](#)
[Scan Servers Tab](#)
[What Is a FlexNet Code Insight Scan?](#)

Scan Profiles Tab

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

Table 8-11 • Scan Profiles tab

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 Scan Server 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 Scan Server.• Exact Matches—Whether Scan Server is to identify those codebase files that exactly match file information in the CL (Compliance Library).• Source Code Matches—Whether the Scan Server is to identify code strings in the scanned codebase files that exactly match strings in the CL (Compliance Library).• 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](#)
[What Is a FlexNet Code Insight Scan?](#)
[Applying a Scan Profile to the Project](#)

Create/Edit Scan Profile Dialog

Both the **Create Scan Profile** dialog and the **Edit Scan Profile** dialog contain the following fields to define a scan profile:

Table 8-12 • Create/Edit Scan Profile dialog

Field	Description
Perform Package/License Discovery in Archives	Select this option to have the Scan Server recursively perform package discovery and license detection within all archive files encountered in the project codebase. By default, this option is selected.
Dependency Support	<p>Determine the level of dependency scanning to be performed by the Scan Server. 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 Scan Server calls out to the relevant package management repository to obtain transitive dependency information. <p>For a description of Code Insight dependency support for supported ecosystems, see the Automated Analysis chapter.</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.
Exact Matches	Select this option to have the Scan Server record exact matches for scanned files based on data from the Compliance Library (CL).
Source Code Matches	Select this option to have the Scan Server 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 Scan Server to perform source-code matching for files that have already been associated with one or more inventory items through automated analysis.
Include Files with Exact Matches	(Available only when Source Code Matches is selected) Select this option if you want the Scan Server to perform source-code matching for files that have already been identified as having exact matches.
Search Terms	Provide a list of search terms to be used in the scan. Use the + button to add a term and the - button to remove a term.
Scan Exclusions	Provide a list of file extensions to be excluded from the scan. Use the + button to add an exclusion term and the - button to remove an exclusion.

See Also

[Scan Profiles Tab](#)

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

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

Project Defaults Tab

The settings on **Project Defaults** tab on the **Administration** page work provide a convenient way to default fields used to configure new projects to ensure consistency and enable an easier project creation experience for users. Although the settings you define here are global across all projects, they can be overridden at the project level as needed.

See the following field descriptions for more information.

Table 8-13 • Project Defaults tab

Category	Field
General Options	<p>These options set defaults for project creation and assign default users to project roles. Users can change these defaults when creating a project or when editing a project or its users using Manage Project Edit Project General or Manage Project Edit Project Edit Project Users on the project Summary tab.</p>
Project Type	<p>Select the default project type based on scan requirements:</p> <ul style="list-style-type: none"> ● Standard—A project whose scans require that its codebase be uploaded to FlexNet Code Insight or be synchronized pre-scan using an SCM plugin (such as Bitbucket, Git, Perforce, or TFS). This is the initial system default. This is the initial system default. ● Inventory Only—A project whose scans are performed through a remote scan agent, thus eliminating the need to upload the codebase to FlexNet Code Insight. These scans generate project inventory only. Consequently, the Analysis Workbench is <i>not</i> available for codebase analysis. For details about inventory-only projects, see Performing Inventory-Only Scanning.
Project Visibility	<p>Select the default for visibility status—Public or Private—for projects. (The initial system default is Public.)</p> <p>For public projects, users who are not the Project Owner nor directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project.</p>
Project Risk	<p>Select the default risk value (Low, Medium, or High) for projects. To edit, select another value from the dropdown. The initial system default is Medium.</p>
Project Users	<p>Click the Edit Project Users link to open the Edit Default Project Users page. From here you assign project roles—Analysts, Reviewers, and Observers—that will default for any new project created (but which can then be edited at the project level). See Edit (Default) Project Users Page for details.</p>

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

Category	Field
Scan Settings	These options identify the default Scan Server and scan profile for projects. Users can change these settings at the project level by navigating to Manage Project Edit Project Scan Settings from the project Summary tab.
	Scan Profile Select the scan profile to default for projects. Click ⓘ to view the details of the scan profile.
	Scan Server Select the Scan Server to default for projects. Note that only those Scan Servers in an “enabled” state are available for selection. If only one Scan Server has been identified to the system, this server is automatically selected as the default.
Automated Inventory Publish Options	These options configure defaults for automatically publishing project inventory once a scan completes. Users can change these settings at the project level by navigating to Manage Project Edit Project Scan Settings from the project Summary tab.
	Automatically publish system-created inventory items Select this option to automatically publish inventory items that Code Insight creates as part of the scan (that is, system-generated inventory items). If you select this option, the Minimum inventory confidence label and Mark associated files as reviewed fields are enabled.
	Minimum inventory confidence level for auto-publish Select the default minimum Inventory Confidence level required to automatically publish a system-generated inventory item: <ul style="list-style-type: none"> ● Low—Automatically publish all system-generated inventory. ● Medium—Automatically publish only those system-generated inventory items with Medium and High confidence levels. ● High—Automatically publish only those system-generated inventory items with a High confidence level. For a description of the Confidence levels and how they are used, see Inventory Confidence .
	Mark associated file as reviewed Select this option if you want Code Insight to automatically mark the files associated with each automatically published inventory item as “reviewed”.

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


Category	Field
Automated Review Options	<p>These options configure defaults for enabling policies that automatically accept or reject inventory when it is published. Users can change these settings at the project level by navigating to Manage Project Edit Project Review and Remediation Settings from the project Summary tab.</p>
	<p>Policy Profile</p> <p>Select the default policy profile to associate with all new projects. (The system default is Default License Policy Profile.)</p> <p>The policy profile contains a set of policies that use components, versions, licenses, and vulnerability scores and severities as criteria to automatically reject or approve inventory items during a codebase scan (or post-scan).</p> <p>For more information about policy profiles in general, see Managing Policy Profiles.</p>
	<p>automatically reject inventory items impacted by a new vulnerability that violates your policy</p> <p>Indicate the default action to take for published inventory affected by a new security vulnerability downloaded as part of an Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the Project Inventory tab.</p> <ul style="list-style-type: none"> <p>Select this checkbox to automatically reject those project inventory items impacted by a new security vulnerability only if this vulnerability has a CVSS score or severity <i>greater than</i> the thresholds configured as policy for the Code Insight project. For each inventory item rejected due to a new security vulnerability, the  icon and a tip are added to indicate the status change and its reason.</p> <p>If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.</p> <p>Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability.</p> <p>For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see Policy Page and Policy Details Page. For information about associating these policies with a project, see Managing Policy Profiles.</p>

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

Category	Field
Manual Review Options	<p>These options configure defaults for project inventory not automatically reviewed by policy. Users can change these settings at the project level by navigating to Manage Project Edit Project Review and Remediation Settings from the project Summary tab.</p> <hr/> <p>What should happen if inventory items are not reviewed by policy? Indicate the default action to trigger for those inventory items that are <i>not</i> affected by policy (and therefore have a Not Reviewed status) during the publication of inventory either as part of a scan or manually by a user:</p> <ul style="list-style-type: none"> ● do nothing—Simply show the status of the inventory item as Not Reviewed on the Project Inventory tab. ● send an email notification to the project owner—Automatically send an email to the Project Owner, stating the need for a manual review of the item. The value for Select the minimum priority... (described in the next table entry) affects this option. ● automatically create a manual review task—Automatically create a manual review task assigned to the default legal or security reviewer (or both reviewers), and send an email, notifying the reviewer(s) about assigned task. <p>Information about managing such a task to track the progress of a manual review is found in Creating and Managing Tasks for Project Inventory.</p> <p>The value for Select the minimum priority... (described in the next table entry) affects this option.</p> <hr/> <p>Select the minimum priority to perform the action selected above (Enabled when an option other than do nothing is selected for the previous field.) Select the default minimum inventory priority (P1, P2, P3, or P4) to which the value for the previous field applies.</p> <p>For example, if the previous field is set to send an email notification to the project owner and minimum priority is set to P3, then the email notification will be sent for only those non-reviewed inventory items with a P1, P2, or P3 priority. No email notification will be sent for P4 inventory items.</p> <div data-bbox="716 1434 751 1478" data-label="Image"> </div> <p>Note • This option has no effect when the do nothing value is selected.</p>

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

Category	Field
Manual Review Options	<p>What type of manual reviews will be performed on this project?</p> <p>Set the default type of manual review tasks to be generated:</p> <ul style="list-style-type: none"> • Legal Only—Review tasks are generated for those non-reviewed inventory items that so not meet legal policy criteria. The tasks are automatically assigned to the default Legal reviewer. • Security Only—Review tasks are generated for only those non-reviewed inventory items that have security vulnerabilities. The tasks are automatically assigned to the default Security reviewer. • both Legal and Security—Review tasks are generated for all non-reviewed inventory items that do <i>not</i> meet legal policy criteria; these are assigned to the default Legal reviewer. Additionally, review tasks are generated for those non-reviewed inventory tasks associated with security vulnerabilities and are assigned to the default Security reviewer. <p>With this value, a single inventory item might have both a legal review task and security review task generated. However, if the default reviewers are the same user, a single task is created, describing the requirement for both a legal and security manual review.</p>
	<p>Select reviewers for this project</p> <p>If desired, designate a new default Legal reviewer or Security reviewer (or both) to which to assign manual review tasks. (The Project Owner is the designated as the initial system default for both reviewers.)</p> <p>Then, depending on the type of manual review selected for the project (see the What type of manual reviews will be performed... option described previously), Code Insight determines which reviewer (Legal or Security or both) is assigned the task and then notified of the task by email. The reviewer(s) can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory.</p> <p>To select a new default reviewer, click Change User next to the name of the current Legal reviewer or Security reviewer assignee, then select a user from the Select new...contact dialog, and click Apply. (To reset the reviewer to the Project Owner, click Reset.)</p> <p>When a new default reviewer is selected, that user is automatically given the role of project “reviewer” should the user not currently have this role. However, should the current reviewer reassign a specific task to another user, the “reviewer” role is not automatically assigned to that user.</p> <p>If the Project Owner is specified as a default reviewer, the owner’s actual name is displayed for the reviewer at the project level.</p>

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

Category	Field
Remediation Options	<p>These options configure defaults for rejected project inventory. Users can change these settings at the project level by navigating to Manage Project Edit Project Review and Remediation Settings from the project Summary tab.</p>
What should happen if inventory items are rejected?	<p>Indicate the default action to trigger for those inventory items that are automatically rejected by policy during the publication of inventory either as part of a scan or manually by a user:</p> <ul style="list-style-type: none"> ● do nothing—Simply show the status of the inventory item as Reject on the Project Inventory tab. ● send an email notification to the project owner—Automatically send an email to the Project Owner, stating the need for remediation work on the inventory item. ● automatically create a remediation task—Automatically create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. ● automatically create a remediation task and an external work item—Automatically do the following: <ul style="list-style-type: none"> ● Create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (See the previous bulleted item for more information.) ● Associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). The work item is created and assigned using the settings defined for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings.
Assignee for remediation work	<p>If desired, designate a new default development contact—for example, an engineering manager—to which to assign remediation tasks. (The Project Owner is the initial system default.) This contact can then manage the task accordingly—for example, reassigning it to another user or manually creating an external work item and assigning it to someone on the development team. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory.</p> <p>To select a new contact, click Change User next to the name of the current assignee, select a user from the Select new...contact dialog, and click Apply. (To reset the reviewer to the Project Owner, click Reset.)</p> <p>If the Project Owner is specified as the default, the owner's actual name is displayed as the remediation assignee at the project level.</p>

See Also

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

System Settings Tab

The **System Settings** tab is used to define settings that configure your FlexNet Code Insight system. The tab provides the following configuration settings:

Table 8-14 • System Settings Tab

Column/Field	Description
Security Vulnerability Options	Select the CVSS (Common Vulnerability Scoring System) version— CVSS v3.0 or CVSS v2 in which to display security vulnerability scores and severities in the Code Insight Web UI. Initially, CVSS v 2.0 is the default. If you switch versions, the CVSS scores and severity values displayed for vulnerabilities will be impacted, as will policies based on these values. For more information, see Security Vulnerabilities Associated with Inventory and Managing Policy Profiles .

See Also

[Security Vulnerabilities Associated with Inventory](#)
[Managing Policy Profiles](#)
[Policy Details Page](#)
“Setting the Common Vulnerability Scoring System” in the *FlexNet Code Insight Installation and Configuration Guide*

Projects List Page

The **Project List** page enables you to search for, view, and add FlexNet Code Insight projects. The page contains the following fields:

Table 8-15 • Projects List page


Column/Field	Description
Tree view	Click to change the display to a tree view.
	

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



Column/Field	Description
List view 	Click to change the display to a list view.
Add New	Click to add a new folder or project to the list. (This button is displayed only if you have permission to create projects.)
My Projects	Click to show only those projects with which you are associated, either as Project Owner or with a project role (Analyst, Reviewer, or Observer).
Projects (x)	Lists the number of projects in the system. If the list is filtered, the filtered count is shown in relation to the full count (for example, “(19 of 123)”).
Project Search fields	<p>From the search filters on the left, select the filter based on the type of search you want to perform (Project Name, Project Inventory, or Security Vulnerability).</p> <p>In the field on the right, enter the string criterion for the search:</p> <ul style="list-style-type: none"> • When searching for a project name, enter a partial string or full project name. • When searching for project inventory, enter the inventory name, component name, license name, or SPDX short identifier of the inventory item. The characters must be consecutive in the search string. A partial string is supported. • When searching for a security vulnerability, enter the exact vulnerability ID. <p>Press Enter to view the filtered list. If no inventory items meet the specified criterion, the Projects list shows “No Projects”.</p> <p>To clear the search filter and restore the full project list, click  in the criterion field.</p> <p>See for Searching the System for full details.</p>
Name	A hyperlinked list of the names of all projects in the system. When you select a project from the list, information about the project appears in the panes of the Summary tab. Click the arrow to toggle the list from A to Z or from Z to A.
Selected Project Name	When you select a project from the list, the name of the selected project appears in this field. You can click the selected project name to open the project.
Owner	The hyperlinked name of the person who owns the project. Click the name to open your default email program to send an email to the Project Owner.
Profile	Displays the name of the profile attached to the selected project. If no profile is attached to the project, “No profile selected” appears.
Created	Displays the data that the project was created.
Last Scan	Displays the date that the codebase was last scanned.

Table 8-15 • 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 Tab](#)

[Using the Project Dashboard](#)

[Searching the System](#)

Project Summary Tab

The **Summary** tab for the project allows you to add and edit users who can work in FlexNet Code Insight, view scan settings and status, generate reports, and manage projects. The page contains the following fields:

Table 8-16 • Project Summary tab

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.
Legal Contact	<p>The hyperlinked name of the default legal contact assigned to tasks created to review legal issues in the project inventory. Click the name to open your default email program to send an email to the contact.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</p>
Security Contact	<p>The hyperlinked name of the default security contact assigned to tasks created to review security issues in the project inventory. Click the name to open your default email program to send an email to the contact.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</p>

Table 8-16 • Project Summary tab

Column/Field	Description
Developer Contact	<p>The hyperlinked name of the default development contact assigned to remediation tasks created to take action on code-related issues in the project inventory. Click the name to open your default email program to send an email to the contact.</p> <p>Initially, this default contact is the Project Owner. This field appears only if a new default legal contact is assigned. See Updating Inventory Review and Remediation Settings for a Project for details.</p>
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 this project. Users assigned to roles in the project can perform various maintenance functions based on permissions. ● Private: Only users assigned to roles in this project have access to it.
Project Risk	The project vulnerability risk value (Low , Medium , or High).
Scan Settings	
Policy Profile	The name of the profile associated with 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	<p>Notifies you when the scan is scheduled and waiting in queue. Click the hyperlinked term here to schedule a scan. If other events are scheduled, the scan is placed in a queue. Otherwise, it is run immediately.</p> <p>If the Scan Server is disabled, the link is also disabled.</p>

Table 8-16 • Project Summary tab

Column/Field	Description
Last Scan	The final status of the last scan and provides a statistical summary of what was scanned.
Past Scans	Click the hyperlinked term here to view the scan history for the selected project. A dialog appears with a list of scans performed on the project. If a scan has not yet been performed for the project, the list will be empty.
Reports	
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 start your codebase scan. If the Scan Server is disabled, this option is disabled.
Generate Report	Click to generate a Project, Audit, or Notices report in the background to display later.
Upload Project Codebase	Click to upload the codebase that will be scanned for the selected project. You can also use this option to overwrite the current codebase with the most recent version. If the current project is not associated with a Scan Server or the Scan Server is disabled, this button is disabled.
Manage Project	A dropdown menu that allows you to 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 Uploading a Project Codebase	

Edit Project: General Tab

The **General** tab on the **Edit Project** dialog displays information about the selected project that you can edit. The tab contains the following fields:

Table 8-17 • Edit Project: General tab

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	<p>The visibility status—Public or Private—of the project.</p> <p>For public projects, users who are not the Project Owner nor directly assigned the Reviewer or Analyst role have read-only access to the project inventory. However, private projects are hidden from all users except the Project Owner and those users assigned as Analysts, Reviewers, and Observers of the project.</p>
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 the Projects list under which the project is currently grouped. To edit the project location in the list, select one of the following:</p> <ul style="list-style-type: none"> ● Clear Project Folder button—Click this button to remove the project from the current folder in the Projects list and place it in the root folder. ● Select a New Folder dropdown—Click the down arrow to locate and select an available folder to which to move the project.

Edit Project: Scan Settings Tab

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

Table 8-18 • Edit Project: Scan Settings tab



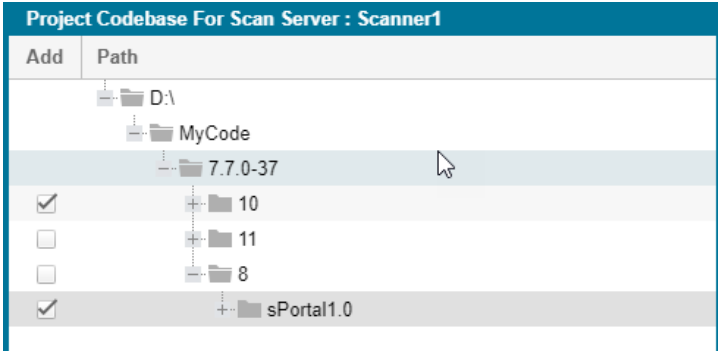
Column/Field	Description
General	These fields identify the Scan Server and profile used to run a project scan.
Scan Profile	The scan profile associated with the project. You can select a different scan profile from the dropdown list. Click  to view the properties of the currently selected scan profile.
Scan Server	The Scan Server assigned to this project. This field is not editable. Click  to view the properties of the currently selected Scan Server.
Auto-Publish	These options configure the automatic publication of project inventory once a scan completes.
Automatically publish system-created inventory items	Select this option to auto-publish inventory items that Code Insight automatically creates based on internal system policies. If you select this option, the Minimum inventory confidence label and Mark associated files as reviewed fields are enabled.
Minimum confidence level for auto-publish	Select the minimum Inventory Confidence level required to auto-publish a system-generated inventory item: <ul style="list-style-type: none"> ● Low—Auto-publish all system-generated inventory. ● Medium—Auto-publish only those system-generated inventory items with Medium and High confidence levels. ● High—Auto-publish only those system-generated inventory items with a High confidence level. For a description of the Confidence levels and how they are used, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.
Mark associated files as reviewed	Select this option to automatically mark the files associated with each auto-published inventory item as “reviewed”.

Table 8-18 • Edit Project: Scan Settings tab (cont.)

	Column/Field	Description
Project Codebase for Scan Server	Path	<p>These settings enable you to limit which directories are scanned in your codebase.</p> <p>From the interactive directory tree representing the project's codebase on the Scan Server, select the checkbox next to one or more top-level directories that you want to scan. To scan only specific subdirectories in a top-level directory, drill down in that directory and select the desired subdirectories.</p> 
	Selected Paths	<p>If the Scan Server is down, no project tree is displayed.</p> <p>The pane showing the path for each directory currently selected for the scan. As a quick method for removing a given directory from the scan without having to drill down in the tree to locate it, simply click the X next to the directory in this pane. If the Scan Server is down, this pane is blank.</p>
Actions		These buttons control whether you save your updates to scan settings.
	Save	Click this button to save your edits to the scan settings and return to the Summary tab.
	Cancel	Click this button to return to the Summary tab without saving your edits.

See also

[Updating Scan Settings for a Project Automatically Publishing Inventory](#)

Edit Project: Review and Remediation Settings Tab

The **Review and Remediation Settings** tab on the **Edit Project** dialog enables you to overwrite default settings that configure the automation of the review, remediation, and status notification processes for published inventory in your project. These settings, which work in conjunction with the set of policies in the project's policy profile, are used to set up the following in your project:

- The policy profile to associate with the project. The policies in the selected profile work in conjunction with the review, remediation, and notification configuration defined on this tab.

- Automatic creation of manual review tasks for inventory items not reviewed by policy during publication performed as part of a scan.
- Automatic assignment of review tasks to the default legal or security contact that you specify.
- Automatic creation of remediation tasks and associated external work items for inventory that is rejected either automatically by policy or during manual publication by an analyst.
- Automatic assignment of remediation tasks to the default engineering contact that you specify.
- Automatic rejection of published inventory impacted by new vulnerabilities detected in the latest scan or Electronic Update.
- The automatic generation of email notifications that alert the Project Owner of rejected or non-reviewed published inventory items that need attention.

See the following field descriptions for more information.

Table 8-19 • Edit Project: Review and Remediation Settings tab


Section/Field	Description
Automated Review Options	
Policy Profile	<p>Select policy profile you want to associate with your project.</p> <p>The policy profile contains a set of policies that use vulnerability scores and severities, license types, and component versions as criteria to automatically reject or approve inventory items during a codebase scan (or post-scan).</p> <p>For more information about policy profiles in general, see Managing Policy Profiles in the “Using FlexNet Code Insight” chapter.</p>
automatically reject inventory items impacted by a new vulnerability that violates your policy	<p>Determine what action the system should take for published inventory affected by a new security vulnerability discovered during a post-publication scan or an Electronic Update. The selected action applies to both non-reviewed and previously approved inventory items on the Project Inventory tab.</p> <ul style="list-style-type: none"> ● Select this checkbox to automatically reject those project inventory items impacted by a new security vulnerability only if this vulnerability has a CVSS score or severity <i>greater than</i> the thresholds configured as policy for the Code Insight project. For each inventory item rejected due to a new security vulnerability, the  icon and a tip are added to indicate the status change and its reason. <p>If a new vulnerability does not exceed policy thresholds, the current status of the inventory item is not affected.</p> <ul style="list-style-type: none"> ● Leave the checkbox unselected to retain the current status of inventory items impacted by the new vulnerability. <p>For information about setting policies that define CVSS-score and severity thresholds used to reject or approve inventory items automatically, see Policy Page and Policy Details Page. For information about associating these policies with a project, see Managing Policy Profiles.</p>

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


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

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

Section/Field	Description
What type of manual reviews will be performed on this project?	<p>Determine the type of manual review tasks to be generated:</p> <ul style="list-style-type: none"> ● Legal Only—Review tasks are generated for those non-reviewed inventory items that meet no policy criteria. The tasks are automatically assigned to the default Legal reviewer. ● Security Only—Review tasks are generated for only those non-reviewed inventory items that have security vulnerabilities. The tasks are automatically assigned to the default Security reviewer. ● both Legal and Security—Review tasks are generated for all non-reviewed inventory items meeting no policy criteria and are assigned to the default Legal reviewer. Additionally, review tasks are generated for those non-reviewed inventory tasks associated with security vulnerabilities and are assigned to the default Security reviewer. <p>With this value, a single inventory item might have both a legal review task and security review task generated. However, if the default reviewers are the same user, a single task is created, describing the requirement for both a legal and security manual review.</p>
Select reviewers for this project	<p>If desired, designate a new default Legal reviewer or Security reviewer to which to assign manual review tasks.</p> <p>Then, depending on the type of manual review selected for the project (see the What type of manual reviews will be performed... option described previously), Code Insight determines which reviewer (Legal or Security) is assigned the task and then notified of the task by email. The reviewer can then manage the task accordingly, possibly reassigning it to another user. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.</p> <p>To select a new reviewer, click Change User next to the name of the current Legal reviewer or Security reviewer assignee, select a user from the Select new...contact dialog, and click Apply.</p> <p>When a new default reviewer is selected, that user is automatically given the role of project “reviewer” should the user not currently have this role. However, if the current reviewer reassigns a specific task to another user, the “reviewer” role is not automatically assigned to that user.</p>

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

Section/Field	Description
What should happen if inventory items are rejected?	<p>Determine what action should be triggered for those inventory items that are automatically rejected by policy during the publication of inventory either as part of a scan or manually by a user:</p> <ul style="list-style-type: none"> ● do nothing—Simply show the status of the inventory item as Reject on the Project Inventory tab. ● send an email notification to the project owner—Automatically send an email to the Project Owner, stating the need for remediation work on the inventory item. ● automatically create a remediation task—Automatically create a remediation task assigned to the default development contact (see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (Information about managing such a task to track the remediation progress is found in Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) ● automatically create a remediation task and an external work item—Automatically do the following: <ul style="list-style-type: none"> ● Create a remediation task assigned to the default development contact ((see the Assignee for remediation work option) and send an email, notifying the contact about the assigned task. (Information about managing such a task to track the remediation progress is found in Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.) ● Associate a work item with the task, creating the work item in an Application Lifecycle Management (ALM) system (such as an issue in Jira). The work item is created and assigned using the settings defined for the ALM instance to which the Code Insight project is associated. For more information about configuring an ALM instance for the project, see ALM Settings in the “Using FlexNet Code Insight” chapter.
Assignee for remediation work	<p>If desired, designate a new default development contact to which to assign remediation tasks.</p> <p>This contact can then manage the task accordingly—for example, reassigning it to another user or manually creating an external work item and assigning it to someone on the development team. For details about managing and reassigning tasks, see Creating and Managing Tasks for Project Inventory in the “Using FlexNet Code Insight” chapter.</p> <p>To select a new contact, click Change User next to the name of the current assignee, select a user from the Select new...contact dialog, and click Apply.</p>

See also

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

Edit (Default) Project Users Page

The **Edit Project Users** page, accessed from the **Manage Project** menu on the **Summary** tab for a specific project, is used to assign Code Insight users to various roles for the project.

The **Edit Default Project Users** page, available from the **Project Defaults** tab on the **Administration** page, is used to set project role assignments that default for any new project created (but which can then be edited at the project level on the **Edit Project Users** page).


For a description of the project roles and more information about the procedures used to manage them on the **Edit Project Users** page, see [Assigning Project Roles to Users](#). (These same procedures basically apply to the **Edit Default Project Users** page.) Additionally, for a description of the permissions enabled for each project role, see the appendix [FlexNet Code Insight User Roles and Permissions](#).

The following describes the fields on the **Edit Project Users** and **Edit Default Project Users** page:

Table 8-20 • Edit (Default) Project Users page

Column/Field	Description
Select Users	The list of all users defined for your FlexNet Code Insight system. From this list, you select the users to which you want to assign project roles.
Add User	Select one or more users in the Select Users pane, and then select the appropriate option— Add to Analysts , Add to Reviewers , or Add to Observers —from the Add User dropdown to add the users to the desired “role” pane. This procedure is an alternative to dragging and dropping users to the appropriate “role” pane.
Search	Enter a full or partial user name to search for a user in the system.
Analysts	<p>The pane listing users who are currently assigned to the Analyst role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Analysts from the Add User dropdown to add the selected users to the pane.)</p> <p>To remove a user from this role, click ✕ next to the user name in the pane.</p>

Table 8-20 • Edit (Default) Project Users page (cont.)

Column/Field	Description
Reviewers	<p>The pane listing users who are currently assigned to the Reviewer role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Reviewers from the Add User dropdown to add the selected users to the pane.)</p> <p>To remove a user from this role, click X next to the user name in the pane.</p>
Observers	<p>The pane listing users who are currently assigned to the Observer role. To assign additional users to this role, drag and drop one or more users from the Select Users list to this pane. (Alternatively, select Add to Observers from the Add User dropdown to add the selected users to the pane.)</p> <p>To remove a user from this role, click X next to the user name in the pane.</p> <p></p> <p>Note • On the Edit Project Users page, the Observers pane is visible only for private projects. On the Edit Default Project Users page, this pane is always visible, enabling you to assign observers that will default for any private project that might be created. For more information, see Creating a Private Project.</p>
Close	Click this button to save your changes.

See Also
[Assigning Project Roles to Users](#)

Scan History Dialog

The **Scan History** dialog displays a list of previous scans that have been performed on the selected project. The dialog contains the following fields:

Table 8-21 • Scan History dialog


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.

Table 8-21 • Scan History dialog (cont.)

Column/Field	Description
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 Page

The **Select a new project owner** page is where you can change the owner of a selected project. The page contains the following fields:

Table 8-22 • Select a New Project Owner page

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 8-23 • 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 copyright text.● 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 8-23 • Analysis Workbench (cont.)

Column/Field	Description
Copyrights	Lists the copyright text 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

[Reviewing Published Inventory](#)


File Search Results Pane

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



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


Table 8-24 • 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 8-25 • 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 8-26 • 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 in the **Analysis Workbench** or on the **Project Inventory** tab provides details about the inventory, component, and files in the inventory. The pane has the following fields:

Table 8-27 • Inventory Details pane

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 8-27 • 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	<p>Notifies you whether or not security alerts exist for this item. If alerts exist, click the x Open Alerts or x Closed Alerts link to view their details. If no alerts exist, None is displayed. For more information about alerts, see Managing Security Vulnerability Alerts.</p>
Priority	<p>A dropdown list showing the priority level given to this inventory item by the system, with P1 as the highest priority and P4 as the lowest.</p> <p>You can change the priority for this inventory item by selecting a different priority from the dropdown list and clicking Save. For more information about priorities, see Inventory Priority.</p>
Vulnerabilities	<p>A bar graph showing the count of known vulnerabilities by severity color for the inventory item. Click the graph to view the list of vulnerabilities and their details. For details about the graph and vulnerabilities in general, see Security Vulnerabilities Associated with Inventory.</p> <p>If no vulnerabilities have been found for the inventory item, the value No is displayed in place of the graph. (In Analysis Workbench, if the Type value for the inventory item is Work in Progress or License Only, the value N/A is displayed.)</p>
Created By	<p>The name of the person or process that created the inventory item.</p>
Confidence	<p>A simple three-segment graph representing the Confidence level (High, Medium, or Low) of the inventory item. The Confidence level is the measure of the strength of the discovery technique used to generate the inventory item. The graph shows three shaded segments for High confidence, two for Medium, and one for Low.</p> <p>For more information about the Confidence levels, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.</p>
Created On	<p>The date that the inventory item was created.</p>
Updated On	<p>The date that the inventory item was updated. If the item has not been updated since the creation date, the date shown here will be the same as the Created On date.</p>
Name	<p>The name of the inventory item.</p>

Table 8-27 • Inventory Details pane (cont.)

Column/Field	Description
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, enabling you to select a new component instance for the inventory item. • License Only—Files under a specific license without a known component.
Component	<p>The name of the component. Click ⓘ to view publicly available information about the component; or click ✎ to select a new version (or license) for the inventory item.</p>
License	<p>The name of the license associated with this component. Click ⓘ to view additional information about the license; or click ✎ to select a new license (or version) for the inventory item.</p>
Description	<p>A description of the inventory item. You can update the description as needed.</p>
Url	<p>The URL of the license for this inventory item. You can update the URL as needed.</p>
Disclosed	<p>The Yes or No option indicating whether the third-party component or artifact represented by the inventory item known third-party dependency in your code before it was discovered by the scan or you.</p> <p>This field is used most often by analysts to denote information about the state of the inventory item.</p>
Usage tab	
Distribution Type	<p>The option indicating how the inventory item is distributed:</p> <ul style="list-style-type: none"> • Internal—Internally only (such as test framework that might be included in the codebase but is not distributed with the product). • External—Externally with the product, shipped to customers (outside of your organization, including a private cloud deployment at the customer's site) • Hosted—Hosted in your company's data center (such as a SAAS application). • Unknown—Unknown distribution type.
Part of Product	<p>The Yes, No, or unknown option indicating whether the item is part of the core product or an infrastructure piece such as a build or test tool. This can affect whether third-party notices are required for this item.</p>



Table 8-27 • Inventory Details pane (cont.)

Column/Field	Description
Linking	<p>The option indicating whether the libraries are statically linked (included in the materials), dynamically linked (brought in at runtime), or not linked at all. The Unknown value indicates that linking status is not known.</p> <p>Linking can affect license priority and obligations.</p>
Modified	<p>The Yes, No, or Unknown option indicating whether a project contributor, such as a developer, has modified the software from its original form. Modification can be an important factor for determining license obligations and distribution requirements that are governed by a specific license.</p>
Encryption	<p>The Yes, No, or Unknown option indicating whether the component provides the encryption capabilities used in the product. Encryption can affect export controls.</p>
Notes tab	
Detection Notes	<p>System notes that specify the automated detection technique that was used to locate the component; license information in the case that the license has changed from one version to another or if the component has multiple licenses; attributes extracted from a POM or manifest file containing project and configuration details.</p>
Audit Notes	<p>Any notes added to the inventory item by the auditor or reviewer, based on findings during the analysis.</p>
As-Found License Text	<p>The actual license text for the license associated with the inventory item; this text is manually added by the analyst during the audit or, in some cases, automatically added by the system based on a high-confidence detection rule. You can enter text in this field for future reference.</p>
Notices Text	<p>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.</p>
Associated Files tab	<p>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.</p>

Evidence Details Pane

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

Table 8-28 • 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 8-29 • 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.
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

Table 8-29 • Project Inventory Review page (cont.)



Column/Field	Description
Search criteria	<p>The prompt for this field changes based upon your selection in the Search type field:</p> <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.

Policy Page

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

The page has the following fields:

Table 8-30 • Policy page

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

See Also

[Policy Details Page](#)

[License Details Window](#)

[Managing Policy Profiles](#)

Policy Details Page

The **Policy Details** page lets you define or edit a policy profile that can be used to automatically review inventory items when they are published. Inventory items that meet any of the component, license, or security vulnerability criteria in the policy profile can be automatically approved or rejected (or flagged for a manual review) based on the policy definition. The following topics describe this page:

- [Field Descriptions](#)
- [Impact on Policies When CVSS Version Changes on System](#)

Policy Fields

The page has the following fields:

Table 8-31 • Policy Details page

Column/Field	Description
General	These fields identify the policy profile you are creating or editing.
Name	The name of the policy profile that you are editing or copying. If you are copying a profile, the name will read Copy of <i>selected_policyProfile</i> , where <i>selected_policyProfile</i> is the name of the profile you selected to copy. To change the name of the profile, type a new name in this field.
Description	The policy profile description, if it exists. You can edit or add a description.
Created	(Edit view only) The name of the user who created the policy profile, and the date and time the profile was created. You can click the hyperlinked name to send an email to the user who created the profile.
Updated	(Edit view only) The name of the user who last updated the policy profile, and the date and time the profile was updated. You can click the hyperlinked name to send an email to the user who updated the profile.

Table 8-31 • Policy Details page (cont.)



Column/Field	Description
Vulnerabilities	The following criteria automatically approve or reject inventory items with security vulnerabilities during publication.
Only auto-approve inventory items if there are no associated security vulnerabilities	Select this checkbox to have Code Insight skip any matching license-based or component policies if the inventory item has any associated security vulnerabilities.
Reject inventory items if any associated security vulnerabilities have a CVSS score above <score>	<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 value you enter.</p> <p>This policy takes precedence over any other automated approval policy.</p>  <p>Note • If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, the value you selected for this field might change. See Impact on Policies When CVSS Version Changes on System for details.</p>
Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than <severity level>	<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 severity you select. (For information about vulnerability severities, see Security Vulnerabilities Associated with Inventory.)</p> <p>This policy takes precedence over any other automated approval policy.</p>  <p>Note • If the FlexNet Code Insight administrator changes the CVSS version for Code Insight, the value you selected for this field might change. See Impact on Policies When CVSS Version Changes on System for details.</p>
Licenses	The following fields create policies that automatically approve or reject inventory associated with a given license.
Select a License... (dropdown)	<p>The dropdown of available licenses on which you can create policies.</p> <p>Select a license, and click Add License to add it to the Licenses policy list.</p>

Table 8-31 • Policy Details page (cont.)




Column/Field	Description
Licenses (list)	<p>The list of license policies (in a grid format) currently used by this profile 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 window for the selected license.● Action—Select one of the following to indicate what status to automatically assign to any inventory item associated with this license:<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.

Table 8-31 • Policy Details page (cont.)


Column/Field	Description
Components	The following fields create a policies that automatically approve or reject inventory based the component associated with the inventory.
Add Component button	Click this button to select a component on which to create the policy, or create a new component from the Lookup Component window. (See Lookup Component Window for information about how to use this window.) Once you select a component, its entry is added to the Components policy list.
Components (list)	<p>The list of current components and version (in a grid format) currently used by this profile for automatically reviewing inventory items.</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 Version from field and the maximum version in the to field. ● To specify any version after a specific version, select the specific version in the Versions from field and the wild card * in the to field. <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 to automatically assign to inventory items associated with this 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.

Table 8-31 • Policy Details page (cont.)

Column/Field	Description
[actions]	These actions to manage the policy profile.
Save	Click to save the changes you have made to this policy profile.
Close	Click to close the Policy Details page. If you have made changes the profile, be sure that you have clicked Save before closing the page; otherwise, changes are lost.

Impact on Policies When CVSS Version Changes on System

If the FlexNet administrator changes the CVSS version for FlexNet Code Insight, the following describes the impact on policies related to vulnerabilities.

When CVSS v2 is switched to CVSS v3.0

Code Insight makes the following changes:

- If the severity level for the **Reject inventory items if any associated securities vulnerabilities have a severity level equal to or higher than...** field was **Unknown** previously, it is now **None**.
- An additional severity, **Critical**, is available for this same field.

When CVSS v3.0 is switched to CVSS v2

Code Insight makes the following changes:

- If the severity level for the **Reject inventory items if any associated securities vulnerabilities have a severity level equal to or higher than...** field was previously **None**, it is now **Unknown**.
- If the severity level for this same field was previously **Critical**, note that this severity is no longer available. To handle the conversion, Code Insight checks to see if a score was previously entered in the **Reject inventory items if any associated security vulnerabilities have a CVSS score above...** field. If a score less than **9** was entered, that value is retained in the field (since the previous **Critical** severity started with the score **9**). If a value greater than **9** or no value was entered, the value for this field is now **9**.

See Also

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

Custom Detection Rules Tab



The **Custom Detection Rules** tab on the **Custom Data** page lists the custom detection rules currently available for use in codebase scans in your FlexNet Code Insight system. Custom detection rules are user-defined when needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. These custom rules are saved to the FlexNet Code Insight data library for global use across projects.

From this page, you can also select to edit a rule or remove a rule from your Code Insight system.

For complete details about custom detection rules, see [Managing Custom Detection Rules](#).

The following describes the columns and actions you can perform from the **Custom Detection Rules** tab.

Table 8-32 • Custom Detection Rules tab

	Column/Field	Description
[actions]	Enter Component Name search string	To locate specific custom detection rules, enter a component-name string by which to filter the list of detection rules. The search results show only those rules whose component name contains the search string you provided. (This filter applies to only those custom rules visible in the UI; no call is made to the data library.)
	Create Custom Rule	Click to open the Custom Detection Rule dialog to create a new custom detection rule.
[Custom rule entry]	The following columns provide details about each custom detection rule and give you access to actions you can take on the rule.	
	Component	The name of the component on which the custom detection rule is based.
	Version	The component version.
	License	The license found in the FlexNet Code Insight data library and associated with the component.
	URL	The forge URL for the component.
	[actions for custom rule entry]	Actions you can perform on the currently selected rule: <ul style="list-style-type: none">Click  to edit the custom detection rule. The Edit Custom Rule dialog is opened.Click  to delete the custom detection rule from your FlexNet Code Insight system. The rule will no longer be applied during project scans.

See Also

[Managing Custom Detection Rules](#)

[Custom Detection Rule Dialog](#)

[Edit Custom Rule Dialog](#)

Custom Detection Rule Dialog

The **Custom Detection Rule** dialog enables you to create a custom detection rule. You can define custom rules as needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. The custom detection rules are saved to the FlexNet Code Insight data library for global use across projects. For complete details about custom detection rules, see [Managing Custom Detection Rules](#).

This dialog is accessed from two locations:

- From the **Inventory Details** tab in **Analysis Workbench** for an inventory item of the “component” type—whether system-generated or manually created—to which codebase files have been manually associated (as described in [Creating a Custom Detection Rule from Inventory of “Component” Type](#)).
- From **Custom Detection Rules** tab accessed from the **Custom Data** tab on the FlexNet Code Insight main menu (as described in [Creating a Custom Detection Rule from Scratch](#)).

The ability to edit certain fields depends on how you accessed the dialog. To help explain these differences, the following table designates the two access locations as “**Inventory Details** tab” and “**Custom Detection Rules** tab”.

The following describes the columns and actions you can perform from the **Custom Detection Rule** dialog.

Table 8-33 • Custom Detection Rule dialog



Column/Field	Description
[component selection]	<p>The following fields describe the component on which the custom detection rule is based. If you have accessed this dialog from the Inventory Details tab for an inventory item in Analysis Workbench, these fields are auto-populated with component information from the inventory item and are <i>not</i> editable. If you have accessed this dialog from the Custom Detection Rules tab, these fields are populated once you select the component and <i>are</i> editable as described below.</p>
Component	<p>The name of the component on which this detection rule is based.</p> <p>If you accessed this dialog from the Custom Detection Rules tab, click Lookup Component to select the component and its version, license, and forge URL. The License and URL fields are populated accordingly.</p> <p>If you accessed this dialog from the Inventory Details tab, this field is not editable.</p>
License	<p>The license associated with the component.</p> <p>If you accessed this dialog from the Custom Detection Rules tab, you cannot edit the field directly once it is populated from the component selection, but you can select a different license. To do so, click  to switch to another license and, optionally, change the component version. Additionally, click  to view the details and text of the selected license as stored in the FlexNet Code Insight data library.</p> <p>If you accessed this dialog from the Inventory Details tab, this field is not editable.</p>
Description	<p>A description of the component.</p> <p>If you accessed this dialog from the Custom Detection Rules tab, this field is editable. It is not editable if you accessed the dialog from the Inventory Details tab.</p>
URL	<p>The forge URL for the component.</p> <p>If you accessed this dialog from the Custom Detection Rules tab, this field is editable. It is not editable if you accessed the dialog from the Inventory Details tab.</p>

Table 8-33 • Custom Detection Rule dialog (cont.)

Column/Field	Description
[license, notices, and note content]	<p>The following fields are used to provide license or notice content and any audit notes for the inventory item generated from this rule. These field are editable.</p> <p>If you accessed this dialog from the Inventory Details tab, these fields might be pre-populated with information from the manually created inventory. However, you can edit this information as needed.</p>
	<p>As-Found License Text</p> <p>The license content you want to associate with the inventory item. If no Notices Text content is provided, the Notices report uses the information in this field as the license text for the third-party component. For more information, see Finalizing the Notices Text for the Notices Report.</p>
	<p>Notices Text</p> <p>The exact content to include in the Notices report. This is usually a modification of the content in As-Found License Text. (You can copy the As-Found License Text content to the Notices Text pane and edit it.)</p> <p>If content exists in this field, the Notices report uses it as the license text for the third-party component and ignores any information in the As-Found License Text pane. For more information, see Finalizing the Notices Text for the Notices Report.</p>
	<p>Audit Notes</p> <p>Any notes you want to add to the inventory item based on your findings during the analysis.</p>
[associated codebase files]	<p>This pane identifies the codebase files (by file name and MD5 value) on which to base the rule. You must identify at least one file.</p> <p>If you have accessed this dialog from the Inventory Details tab, the files associated with the inventory item are automatically listed and available for selection. If you have accessed this dialog from the Custom Detection Rules tab, you must manually provide file name and MD5 value for each file.</p> <p>Keep in mind that, if the custom detection rule is associated with multiple files, the scan uses OR logic when processing the files against the target codebase. Consequently, only one file match between codebase and the rule is required to automatically create an inventory item.</p>
	<p>File MD5</p> <p>If you accessed this dialog from the Inventory Details tab:</p> <ul style="list-style-type: none"> ● To add one or more files, click the check-box next to each desired file. ● To remove a from the rule, click its check-box to deselect it. <p>If you accessed this dialog from the Custom Detection Rules tab:</p> <ul style="list-style-type: none"> ● To add a file, click Add File and enter the exact file name and MD5 value for the file. ● To remove a file from the rule, click X in the file entry.

Table 8-33 • Custom Detection Rule dialog (cont.)

	Column/Field	Description
Actions		The following are actions conclude the rule-creation session.
	Save	Click Save to save the new custom detection rule to the Code Insight data library. You will be asked for confirmation to proceed with the creation.
	Cancel	Click Cancel to cancel the rule creation process. You will be asked for confirmation to proceed with the cancellation.

See Also[Managing Custom Detection Rules](#)[Creating a Custom Detection Rule from Inventory of “Component” Type](#)[Creating a Custom Detection Rule from Scratch](#)[Finalizing the Notices Text for the Notices Report](#)

Edit Custom Rule Dialog

The **Edit Custom Rule** dialog enables you to edit an existing custom detection rule. Custom detection rules are user-defined when needed to supplement the internal detection rules used by Automated Analysis to automatically create inventory during a scan. These custom rules are saved to the FlexNet Code Insight library for global use across projects. For complete details about custom detection rules, see [Managing Custom Detection Rules](#).

The following table describes the fields, buttons, and icons on the **Edit Custom Rule** dialog. You can edit any of the fields, using the methods described in the table.

Table 8-34 • Edit Custom Rule dialog



	Column/Field	Description
Component selection		The following fields describe the component on which the custom detection rule is based. These fields are editable.
	Component	The name of the component on which this detection rule is based. You cannot edit this value directly, but you can switch to another component. To do so, click Lookup Component to select another component, along with its version, license, and forge URL.
	License	<p>The license associated with the component. You cannot edit this value directly, but you can select a different license. Click  to switch to another license and, optionally, change the component version.</p> <p>Additionally, you can click  to view the details and text of the selected license as stored in the FlexNet Code Insight data library.</p>
	Description	A description of the component.
	URL	The forge URL for the component.
License, notices, and note content		The following fields are used to provide license or notice content and any audit notes for the inventory item generated from this rule. These fields are editable.
	As-Found License Text	The license content you want to associate with the inventory item. If no Notices Text content is provided, the Notices report uses the information in this field as the license text for the third-party component. For more information, see Finalizing the Notices Text for the Notices Report .
	Notices Text	<p>The content to include in the Notices report. This is usually a modification of the content in As-Found License Text pane. (You can copy the As-Found License Text content to the Notices Text pane and edit it.)</p> <p>If content exists in this field, the Notices report uses it as the license text for the third-party component and ignores any information in the As-Found License Text pane. For more information, see Finalizing the Notices Text for the Notices Report.</p>
	Audit Notes	Any notes you want to add to the inventory item based on your findings during the analysis.

Table 8-34 • Edit Custom Rule dialog (cont.)

Column/Field	Description
Associated codebase files	<p>This pane lists the codebase files (by file name and MD5 value) on which the rule is based. You can add or delete files as needed within this list. When adding a file, you are required to manually enter the its MD5 value.</p> <p>At least one file must be associated with the rule.</p> <p>Keep in mind that, if the custom detection rule is associated with multiple files, the scan uses “OR” logic when processing the files against the target codebase. Consequently, only one file match between codebase and the rule is required to automatically create an inventory item.</p>
File MD5	<p>To add a file, click Add File and enter the exact file name and MD5 value for the file.</p> <p>To remove a file from the rule, click X in the file entry.</p>
Actions	The following are actions conclude your update session.
Save	Click Save to save the rule updates to the Code Insight data library. You will be asked for confirmation to proceed with the creation.
Cancel	Click Cancel to cancel your updates. You will be asked for confirmation to proceed with the cancellation.

See Also[Managing Custom Detection Rules](#)[Finalizing the Notices Text for the Notices Report](#)

License Details Window

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

Table 8-35 • License Details window

Column/Field	Description
General Information Tab	
Id	The identification number of the license in the data library.
Name	The name of the license (for example, <i>Academic Free License v1.1</i>).
Priority	The priority ranking of the license as determined by FlexNet Code Insight. For more information, see What Does an Analyst do?
URL	The URL where the license is available on the internet.

Table 8-35 • License Details window (cont.)

Column/Field	Description
Description	A short description of the license.
Category	A license category that spans multiple license instances (for example, MIT, Public Domain, BSD-3 Clause, and others). The family designation is helpful to a legal reviewer to understand the “type” of license prior to investing the time to analyze the complete license text.
Custom License	A designation of whether this license is a custom license.
Commercial	A designation of whether the licenses is classified as commercial.
Copyleft	A designation of whether the licenses is considered a copyleft license.
Free Software License	A designation of whether the license is a free software license.
GPL V2 Compatible	A designation of whether a license is compatible with GPL-2.0.
License Text Tab	The complete text of the selected license as stored in the FlexNet Code Insight data library. This text represents the external forge license text.

Lookup Component Window

The **Lookup Component** window lets you search for a component in the FlexNet Code Insight data library and display additional information about the component, such as vulnerabilities and license issues. The window has the following fields:

Table 8-36 • Lookup Component window

Column/Field	Description
Search by	Select the type of search you want to perform or the method you want to use to create a custom component: <ul style="list-style-type: none">● Keyword—Search for a component or create a custom component that uses a specific keyword in its name.● URL—Search for a component or create a custom component that uses a specific project or forge URL.● Forge—Search for a component or create a custom component that is based on a specific forge.
Keywords	Enter the name or title keyword by which to search components or to create a custom component.
URL	Enter the project or forge URL by which to search components or to create a custom component.

Table 8-36 • Lookup Component window (cont.)

Column/Field	Description
Forge	Select the forge (project repository) by which to search components or to create a custom component.
Create New Component	Click this button to open the New Custom Component window. This window is populated with any criteria you entered on the Lookup Component window. For information on creating a custom component, see Creating and Editing Custom Components .
Select this Component	Click this button to return to your original screen, now populated with information about this component.
Show Instances	<p>Click to display all version-license instances registered for the component. From this list, you have the option to select an instance for the component; or you can register a new instance.</p> <p>If security vulnerabilities exist for a given instance, a bar graph is displayed, showing the current security-vulnerability counts by severity level for a given inventory item. See Security Vulnerabilities Associated with Inventory for details.</p>
Register New Instance	Click this button to add a new component-version-license instance using information in the Code Insight data library.
Use This Instance	Click this button to associate the version-license instance to the component that you are associating with the inventory item.
Edit Custom Component	(Available if the component is custom) Click this button to open the Edit Custom Component window to update the component properties.

Add Project Dialog

The **Add Project** dialog appears when you select **Project** from the **Add New** dropdown menu. It lets you provide a name and select options for a new project. The dialog has the following fields:

Table 8-37 • Add Project dialog

Column/Field	Description
Name	Enter a name for the new project.

Table 8-37 • Add Project dialog (cont.)

Column/Field	Description
Project Type	<p>Select the project type based on its scan requirements:</p> <ul style="list-style-type: none"> • Standard—A project whose scans require that your codebase be uploaded to FlexNet Code Insight or be synchronized pre-scan using an SCM plugin (such as Bitbucket, Git, Perforce, or TFS). • Inventory Only—A project whose scans require a scan agent to run within the project's development environment, thus eliminating the need to upload the codebase to FlexNet Code Insight. These scans generate a project inventory only; no Analysis Workbench is available for codebase analysis. For details about inventory-only projects, see the Performing Inventory-Only Scanning chapter.
Project Visibility	Select the default for visibility status— Public or Private —for projects. When private, only the Project Owner and users assigned to project roles have access to the project to view and manage it.
Policy Profile	From the dropdown menu, select a policy profile to be used for this project.
Scan Server	<p>Select the scan server for this project. Once the initial scan for this project is run, the scan server cannot be changed.</p> <p>If Project Type is Inventory Only, this field is disabled.</p>




Preferences Page

The **Preferences** page appears when you select **Preferences** from the main menu. From this page, you can change your FlexNet Code Insight user account password. In addition, you can view and add authorization tokens—that is, JSON Web Tokens known as JWTs—for use with Code Insight REST APIs. (The authorization token are associated with the current user account.) The page has the following fields:

Table 8-38 • Preferences page

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 in upper case. 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.
AUTH Tokens	

Table 8-38 • Preferences page (cont.)

Column/Field	Description
Add Token	Click this button to display the Add Token dialog.
Name	A list of the names of previously created tokens.
Token	The system-generated token associated with the name.
Create Date	The date on which the token was created.
Actions	<p>A group of icons that indicate actions you can take on each token:</p> <ul style="list-style-type: none">● Edit (): Click to open the Edit Token dialog.● Delete (): Click to delete the selected token. The token is deleted immediately.● Copy to clipboard (): Click to copy the selected token to the clipboard. You can use this option to copy tokens so that you paste them whenever needed for Code Insight REST access (for example, when configuring the Code Insight plugins, importing or exporting project data, or running REST API directly).

See Also[Add Token Dialog](#)[Edit Token Dialog](#)[Exporting and Importing Project Data](#)[Performing Inventory-Only Scanning](#)

Add Token Dialog

The **Add Token** dialog appears when you click the **Add Token** button on the **Preferences** page. It lets you create an authorization token (that is, a JSON Web Token known as a JWT) to be used to authenticate calls to FlexNet Code Insight REST APIs. The token is associated with the user account under which you are logged in or whose password you have changed in the **Change Password** fields on the **Preferences** page. The dialog has the following fields:

Table 8-39 • Add Token dialog

Column/Field	Description
Name	Enter a name for the token you are creating.
Token Validity	<p>Select one of the validity periods:</p> <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.

Table 8-39 • Add Token dialog (cont.)

Column/Field	Description
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 select a date.
Save	Click this button to save the token.
Cancel	Click this button to exit the Add Token dialog without saving the token.

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 edit an authorization token (that is, a JSON Web Token known as a JWT) used to authenticate calls to FlexNet Code Insight REST APIs. The token is associated with the user account under which you are logged in or whose password you have changed in the **Change Password** fields on the **Preferences** page.

This dialog also allows you to copy the token value to the Clipboard so that you paste it whenever needed for Code Insight REST access (for example, when configuring the Code Insight plugins, importing or exporting project data, or running REST API directly).

The dialog has the following fields:

Table 8-40 • Edit Token dialog

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](#)
[Exporting and Importing Project Data](#)
[Performing Inventory-Only Scanning](#)

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 8-41 • 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 apache in this field, FlexNet Code Insight will find all inventory items that have the word <i>apache</i> in their name.
Inventory Priority	<p>Select one or more of these checkboxes (P1, P2, P3, or P4) to search the inventory by inventory priority.</p> <p>For more information about inventory priority, see Inventory Priority in the “Using FlexNet Code Insight” chapter.</p>
Inventory Review Status	<p>Select one or more of the following checkboxes to filter the inventory display based on the review status of inventory items:</p> <ul style="list-style-type: none"> ● Approved—Show only inventory that has been reviewed and approved, either manually by a reviewer or automatically during the auto-publish process. ● Rejected—Show only inventory that has been reviewed and rejected, either manually by a reviewer or automatically during the auto-publish process. ● Not Reviewed—Show only items that have not yet been reviewed. <p>For more information about the review status, see Review Status of Inventory in the “Using FlexNet Code Insight” chapter.</p>
Dependency Options	<p>Select one of the following options to filter the inventory display based on dependency level:</p> <ul style="list-style-type: none"> ● All Inventory Items—Display all inventory items—top-level inventory and first-level and transitive dependencies. ● Only Top-Level Inventory Items—Display only top-level inventory items only. No first-level or transitive dependencies are listed. ● Only Dependency Inventory Items—Display only first-level and transitive dependencies.

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


Column/Field	Description
Inventory Age	<p>Search by inventory publication date. This dropdown field has the following choices:</p> <ul style="list-style-type: none"> • Any—Show any published inventory. • Last 1 day—If today is Feb 6th, search from Feb 5th 12 AM. • Last 7 days—If today is Feb 6th, search from Jan 30th 12 AM. • Last month—If today is Feb 6th, search from Jan 7th 12 AM (30 days). • Custom Date Range—Select a beginning (From) and ending (To) date from the popup calendar. <p></p> <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>
Inventory Notifications	<p>Select one or more of the following checkboxes to filter the inventory display based on security vulnerabilities:</p> <ul style="list-style-type: none"> • Inventory with Open Alerts—Display only inventory items that have open vulnerability alerts (that is, alerts for vulnerabilities that were discovered post-publication and have not been closed). • Inventory Rejected Due to New Non-Compliant Security Vulnerabilities—Inventory items that have been rejected due to new security alerts that are non-compliant with policy.
Inventory Tasks Age	<p>Search for published inventory items with tasks of a certain age (based on creation date). This dropdown field has the following choices:</p> <ul style="list-style-type: none"> • Any—Show any published inventory. • Last day—If today is Feb 6th, search from Feb 5th 12 AM. • Last 7 days—If today is Feb 6th, search from Jan 30th 12 AM. • Last month—If today is Feb 6th, search from Jan 7th 12 AM (30 days). • Custom Date Range—Select a beginning (From) and ending (To) date from the popup calendar.
Inventory Task Owner	<p>Search for published inventory items with tasks assigned to a specific user (or any user):</p> <ul style="list-style-type: none"> • Any—Inventory with tasks assigned to any user. • Only Mine—Inventory with tasks assigned to you (current user). • Specific User—Inventory with tasks assigned to a specific user. (A Select user pop-up enables you to select the user.)

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

Column/Field	Description
Inventory Confidence Level	<p>Search for system-generated published inventory items that have a Confidence level of either High, Medium, or Low.</p> <p>The Confidence level is the measure of the strength of the discovery technique used to generate the inventory item. For a description of the Confidence levels and how they are used, see Inventory Confidence in the “Using FlexNet Code Insight” chapter.</p>
Security Vulnerabilities	
Security Vulnerability ID	Enter a valid vulnerability ID for which to search.
Security Vulnerability Severity	<p>Search for inventory associated with vulnerabilities having the severity levels you specify here. The severity list differs depending on the CVSS version used by FlexNet Code Insight.</p> <p>If CVSS v3.0 is used, the following severities are listed:</p> <ul style="list-style-type: none"> ● Critical (9.0 - 10.0) ● High (CVSS 7.0 - 8.9) ● Medium (CVSS 4.0 - 6.9) ● Low (CVSS 0.1 - 3.9) ● None (CVSS = 0) <p>If CVSS v2 is used, these severities are listed:</p> <ul style="list-style-type: none"> ● High (CVSS 7.0 - 10.0) ● Medium (CVSS 4.0 - 6.9) ● Low (CVSS 0.1 - 3.9) ● Unknown (N/A) <p>For more information about vulnerability severities, see Security Vulnerabilities Associated with Inventory in the “Using FlexNet Code Insight” chapter.</p>
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 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.

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

Column/Field	Description
Licenses	
License Name	The full or partial name of the license for which to search.
License Priority	Select one or more of the following license priorities to limit your search: <ul style="list-style-type: none">● P1—Viral/Strong Copyleft● P2—Weak Copyleft/Commercial/Uncommon● P3—Permissive/Public Domain● No License Found For more information about license priority, see What Does an Analyst do? in the “Using FlexNet Code Insight” chapter.
Apply And/Or Criteria	Select one of the boolean criteria to apply to the search selections: <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.
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 **Summary** tab. It lets you set options that FlexNet Code Insight uses to import data. The dialog has the following fields:

Table 8-42 • 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 (Default)
Import File Location	Select this option to browse for the project data file you want to import.

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

Column/Field	Description
Create inventory with no matching files	<p>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.</p>  <p>Note • <i>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.</i></p>
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.



FlexNet Code Insight User Roles and Permissions

This appendix serves as a reference to the various user roles and permissions that Code Insight offers as a means to control user access to its functionality at your site:

- [System Roles and Permissions](#)
- [Project Roles and Permissions](#)
- [Roles and Permissions to Manage Project Task Flow](#)

System Roles and Permissions

The following table lists the system roles and associated permissions used to manage the FlexNet Code Insight system. The initial FlexNet Code Administrator (and any subsequent administrators) assigns these roles to other FlexNet Code Insight users by using the **Manage Permissions** dialog accessed from the Administration **Users/Permissions** tab. (For details, see “Managing User Permissions for System Activities” in the “Configuring FlexNet Code Insight” chapter in the *FlexNet Code Insight Installation and Configuration Guide*.)

One user can be assigned multiple roles.

For Information on creating and managing FlexNet Code Insight users in general, see “Managing Users” in the “Configuring FlexNet Code Insight” chapter in the *FlexNet Code Insight Installation and Configuration Guide*.

Table A-1 • System Roles and Permissions

		Roles		
		Administrators	Manage Policy	Create Project
Permissions	Notes			
Administer Code Insight:		✓	—	—
<ul style="list-style-type: none"> Set system settings Manage users and permissions Schedule or run Electronic Updates Configure an email server Configure LDAP users Configure Application Lifecycle (ALM) instances Configure a Scan Server Configure scan profiles Define global project defaults 				
Manage policies:		—	✓	—
<ul style="list-style-type: none"> Create and edit policy profiles 				
Create projects:	The Project Creation role is controlled by the Allow All Users to Create Projects option on the Manage Permissions dialog. If Yes (default), any user has this role. If No , only users assigned this role can create projects. (For details, see “Managing User Permissions for System Activities” in the “Configuring FlexNet Code Insight” chapter in the <i>FlexNet Code Insight Installation and Configuration Guide</i> .) Users who have this role can also create project folders in the Projects list.	—	—	✓
<ul style="list-style-type: none"> Create projects (and thereby automatically become Project Owner for each) Create project folders (in Projects list) 				

Project Roles and Permissions

The following table lists the various roles and associated permissions used to manage a given project in Code Insight. The Project Owner assigns the Analyst, Reviewer, and Observer roles to FlexNet Code Insight user and can reassign project ownership. For details about these roles and the procedure for assigning them, see [Assigning Project Roles to Users](#).

Table A-2 • Project Roles and Permissions

		Roles			
		Project Owner	Analyst	Reviewer	Observer
Permissions	Notes				
Manage a project: <ul style="list-style-type: none"> Reassign project ownership Manage project users Rename project Move projects in Project Folder Tree Manage scan settings Manage inventory review/remediation settings Manage Source Control Management (SCM) and Application Lifecycle (ALM) instances 	<p>The project creator automatically becomes Project Owner, who can then reassign ownership to another user.</p> <p>See the previous section, System Roles and Permissions, for information about the Create Project role needed to create projects.</p>	✓	—	—	—
View project inventory	Any user (not just one with a project role) can view the Project Inventory tab and the associated inventory details.	✓	✓	✓	✓*

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

		Roles			
		Project Owner	Analyst	Reviewer	Observer
Edit, create, and recall project inventory	<p>On the Project Inventory tab, only Reviewers and the Project Owner can perform inventory review functions:</p> <ul style="list-style-type: none"> Recall inventory Edit inventory priority, review status, and alerts Update Notices Text (on the Licenses & Notices tab) and Notes & Guidance text (except Detection Notes) for inventory Approve or reject inventory <p>However, on this same tab, only Analysts and the Project Owner have access to the Add Item button to create inventory and to the Edit Item button to edit inventory definition properties (such as component, version, selected license, URL, and usage).</p>	✓	✓	✓	—
Access and use Analysis Workbench	<ul style="list-style-type: none"> View codebase file tree Create, edit, and recall inventory and manage custom detection rules. Edit Notices Text on the Licenses & Notices tab Edit Audit Notes on the Notes tab 	✓	✓	—	—
Invoke a scan		✓	✓	—	—
Upload codebase		✓	✓	—	—
Import/export project data		✓	✓	—	—

* The Observer role is available for only projects defined as “Private”. Only Observers, the Project Owner, Analysts, and Reviewers have access to the “Private” project to which they are assigned. The Observer is considered a regular user, restricted to viewing project inventory and generating reports for the “Private Project”.

Roles and Permissions to Manage Project Task Flow

The following table lists the project roles and permissions used to manage tasks to review or remediate inventory items in a project.

Table A-3 • Project Task-Flow Roles and Permissions

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

