FlexNet Code Insight 2018 R3
Quick Start Guide

Legal Information

Book Name: FlexNet Code Insight 2018 R3 Quick Start Guide

Part Number: FNCI-2018R3-QSG00

Product Release Date: October 2018

Copyright Notice

Intellectual Property

Restricted Rights Legend

Contents

Contents

FlexNet Code Insight 2018 R3 Quick Start Guide

FlexNet Code Insight is an end-to-end solution for managing open source and third-party code in software development projects. Using FlexNet Code Insight's large compliance library containing millions of open source components and automated detection rules, you can scan your source code to identify open source/third-party component usage, produce compliance documents, and perform on-going monitoring for vulnerability and intellectual property alerts.

The FlexNet Code Insight Quick Start Guide provides basic information that will enable you to quickly start using the product effectively.

- Before You Begin

- FlexNet Code Insight Process Flow

- Launching FlexNet Code Insight

- Creating a Project and Uploading a Codebase

- Performing a Scan

- Auditing the Scan Results

- Approving/Rejecting Inventory Items

- Performing Remediation

- Releasing the Product with a Notices Report

- Contacting Support

Before You Begin

Before you can start using this guide to become familiar with FlexNet Code Insight, the following configuration tasks must have been completed by your FlexNet Code Insight administrator.

Table 1 • FlexNet Code Insight Configuration Tasks

Task	Description	More Information
Obtain installer and license key	Login to the Flexera Product and License Center and obtain the FlexNet Code Insight installer and license key. https://flexeracommunity.force.com/customer/CCLogin	For instructions on downloading the installer and license key, see: https://resources.flexera.com/instructions/productlicensing/en/FNCI2017.htm
Run installer	Install FlexNet Code Insight on a server that meets system requirements and that has access to a compatible database (such as MySQL 5.7).	See *Installing FlexNet Code Insight* in the *FlexNet Code Insight Installation & Configuration Guide*.
Start Tomcat Server	After installation is complete, start the FlexNet Code Insight Tomcat server.	See *Starting and Stopping Tomcat* in the *FlexNet Code Insight Installation & Configuration Guide*.
Complete electronic update	After installation is complete and the Tomcat server is started, an electronic update is automatically performed, which takes approximately 2 to 4 hours to complete. You cannot use the application to scan files until the update is completed.	
Obtain the Compliance Library	(Optional) The FlexNet Code Insight Compliance Library will be provided on a USB SSD drive. *Note • Using FlexNet Code Insight's automated discovery, you can perform a scan even before obtaining the Compliance Library or setting up a scan server. For more information, see the FlexNet Code Insight User Guide.*	
Set up a scan server	Set up a scan server to perform the scans of source code and binary files. You can also, optionally, provide a path to the location of the Compliance Library.	See *Creating a Scan Server* in the *FlexNet Code Insight Installation Guide*.
Create user accounts	Create user accounts for all end users, and distribute those credentials to the end users.	See *Creating a User* in the *FlexNet Code Insight Installation Guide*.

FlexNet Code Insight Process Flow

The FlexNet Code Insight process flow consists of a repeatable set of steps that you can perform to manage the open source/third-party components used in your software development projects. The following diagram provides an overview of the steps in this process flow.
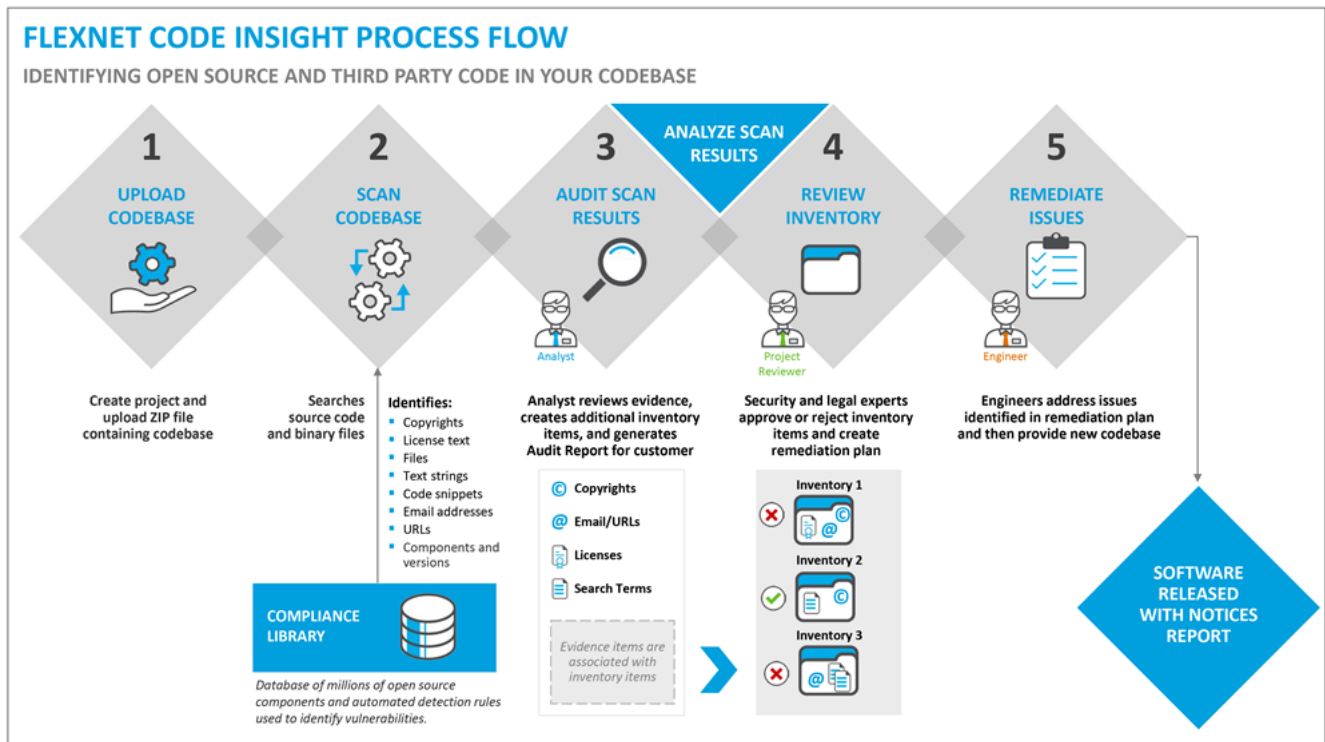
Figure 1: FlexNet Code Insight Process flow

The FlexNet Code Insight process flow consists of the following steps.

Table 2 • FlexNet Code Insight Process Flow

#	Step	Performed By	Description	More Information
1	**Upload Codebase**	Project owner	Create a new project and upload a ZIP file containing the source code and binary files of the codebase you want to scan.	See Creating a Project and Uploading a Codebase.
2	**Scan Codebase**	Project owner	Scan the codebase files to find evidence of open source or third-party components, based on comparison of the codebase with the contents of the **Compliance Library**.	See Performing a Scan.

Table 2 • FlexNet Code Insight Process Flow

#	Step	Performed By	Description	More Information
3	**Audit Scan Results**	Analyst	Use the **Analysis Workbench** tab of the **Projects** view to manually analyze the automatically-generated inventory items and the remaining files that contain evidence of third-party component usage. Create any additional inventory items as required. Generate an Audit Report containing findings and deliver it to the project reviewer, usually in Excel format.	See Auditing the Scan Results and Generating an Audit Report.
4	**Review Inventory**	Project reviewer	Security and legal experts review the findings of the analyst in review meetings, using the **Project Inventory** page to approve or reject each inventory item. These experts develop a remediation plan for any rejected inventory items, making notes in the inventory items or adding additional columns to the Excel version of the Audit Report.	See Approving/Rejecting Inventory Items.
5	**Remediate Issues**	Engineering	Engineering addresses remediation plan to resolve all rejected inventory items, and delivers new version of the codebase. Codebase is rescanned until it is approved for release.	See Performing Remediation.
6	**Release Product with Notices Report**	Release Manager	Product is released with a third-party Notices Report, listing all approved open source/third-party components in the application.	See Releasing the Product with a Notices Report.

Launching FlexNet Code Insight

After you have received a URL address and your login credentials from your FlexNet Code Insight administrator, you are ready to launch the product.

Task **To launch FlexNet Code Insight:**

1. Launch a web browser and navigate to the following URL, entering the server host name provided by your FlexNet Code Insight administrator:

    `http://<your_server_host_name>:PORTNUMBER/codeinsight/`

    The FlexNet Code Insight Login page opens.

2. Enter the `username` and `password` that was provided and click **Login**.

    Note • The default login name is `admin`, and the default password is `Password123`.

3. Click **Login**. The FlexNet Code Insight **Dashboard** opens. It displays statistics from codebase scans that have already been performed, if any.

Navigating Through FlexNet Code Insight

The following are ways to navigate through FlexNet Code Insight from the **Dashboard**:

*   **Links**—Click one of the displayed links: **go to project**, **view policy**, or **administration**.

*   **Menu**—Click the menu icon ( ) at the top right and make a selection from the drop-down.

The main areas of the FlexNet Code Insight interface are:

*   **Projects**—Use to create projects, upload codebases, perform scans, analyze scan results, and generate reports.

*   **Policy**—Use to create and manage policies, which are used by FlexNet Code Insight to automate the review of discovered open source/third-party components in your source code.

*   **Administration**—Use to manage users, set up scan servers and email servers, create and manage scan profiles, and schedule electronic updates.

Creating a Project and Uploading a Codebase

The first step in using FlexNet Code Insight is to create a project and upload the codebase that you want to scan.

- Creating a Project

- Uploading a Codebase

Creating a Project

A project stores the analysis results from a scanned codebase. You must create a project in FlexNet Code Insight before you can scan data and generate reports.

Task   ***To create a new project:***

1. From the **Dashboard** page, click the **go to project** link *or* select **Projects** from the menu. The **Projects** page opens.

2. Click **Add New** and select **Project** from the menu. The **Add Project** dialog box opens.

3. In the **Name** field, enter a name to identify the project.

4. From the **Project Type** field, select **Standard**.

   *Note • The default project type, **Standard**, requires that you upload your codebase to FlexNet Code Insight. You would select **Inventory Only** if you wanted to perform a remote scan (such as on a Jenkins server as part of a build), which would not require you to upload the codebase. For more information, see "Creating a Project Without Uploading a Codebase" in the FlexNet Code Insight User Guide.*

5. From the Project Visibility list, select Public. This selection, the default, allows everyone with access to the FlexNet Code Insight to view the new project.

6. From the **Policy Profile** list, select **Default License Policy Profile**.

   Note • Policies are used by FlexNet Code Insight to automate the review of discovered open source/third-party components in your source code, and a default policy profile is installed with the product. For more information on policies, see the FlexNet Code Insight User Guide.

7. Click **Save**. The project name is now listed in the **Projects** pane. At this point, the **Project Dashboard** area will not contain data. You must upload a codebase and scan it before data and charts appear.

8. Proceed with the steps in Uploading a Codebase.

Uploading a Codebase

Before FlexNet Code Insight can perform a scan, you must upload a ZIP file containing the source code and binary files of a codebase.

Tip • If your codebase changes, you can upload a new version of the codebase file by following the same procedure.

Task   **To upload a codebase to the project:**

1. Perform the steps in Creating a Project

2. In the list of projects in the **Projects** pane, click the **Open project** icon next to the project you want to open. The **Project Summary** page opens.

3. Click **Upload Project Codebase**. The **File Upload** dialog opens.

4. Click **Select Zip File** to browse to a ZIP file containing your codebase.

    *Note • A maximum file size of 2 GB is supported. If you have a ZIP file larger than 2 GB, you can break it up into multiple ZIP files and upload multiple files. If, instead of uploading additional ZIP files to the same project, you want to upload a ZIP file to replace a previously uploaded file, select the **Check to delete existing project codebase files** option; all previously uploaded codebase files will be permanently removed from the scan server along with corresponding scan results.*

5. Click **Upload**. FlexNet Code Insight uploads the codebase file and attaches it to the selected project. You are now ready to scan the codebase.

6. Proceed with the steps in Performing a Scan

Performing a Scan

After you upload a codebase to a project, you are ready to scan the codebase.

-   What is a Codebase Scan?

-   Selecting a Scan Profile

-   Scanning a Codebase

What is a Codebase Scan?

During a scan, FlexNet Code Insight performs a static analysis of files of any type (source or binary) in the codebase and finds evidence of open source or third-party components. Detection of these components is based on comparison of the target codebase with the contents of the **Compliance Library**, a large database of open source projects, which includes component, version, license, and security vulnerability information.

The evidence that FlexNet Code Insight discovers during a scan includes:

- Third-party copyright statements

- Open source license text matches

- File name matches to files collected in the Compliance Library

- Code-snippet matches to code collected in the Compliance Library

- Search terms (text string) matches

- Email addresses and URLs

The scanner will also automatically generate inventory based on various automated discovery techniques:

- Automated Discovery from Package Analysis (such as .jar, NuGet)

- AutoWriteUp Rules from Flexera's Compliance Library

- MID Rules from Flexera's Compliance Library

FlexNet Code Insight continually updates the Compliance Library with new open source releases and newly reported security vulnerabilities.

Selecting a Scan Profile

The level of comprehensiveness of a scan is determined by the **Scan Profile** that is selected for a project. FlexNet Code Insight comes with a **Standard**, a **Basic (without CL)**, and a **Comprehensive** scan profile. The major differences among these scan profiles is that the **Comprehensive** scan only performs source code matches, the **Standard** scan does not, and the Basic (without CL) scan only searches the codebase for a set of strings that may indicate third-party code. While searching the source code for snippets of third-party content takes more time, it results in a deeper scan of the code base and provides a more in-depth analysis.

Note • You can also create your own customized scan profiles. For more information, see "Creating a Scan Profile" in the FlexNet Code Insight Installation and Configuration Guide.

You select a scan profile for your project on the **Edit Project** dialog box.

Task   **To select a scan profile for a project:**

1. Open the **Project Summary** page for your project.

2. At the bottom of the screen, click **Manage Project** and select **Edit Project** from the popup. The **Edit Project** dialog opens.

3. Select the **Scan Settings** tab. The **Scan Settings** tab opens.

4. From the **Scan Profile** list, select **Standard Scan Profile** (the default), **Basic Scan Profile (Without CL)**, or **Comprehensive Scan Profile**.

5. Click **Save**.

Scanning a Codebase

After you create a project and upload a codebase, you are ready to perform a scan.

Task   ***To scan a codebase:***

1. Perform the steps in Creating a Project and Uploading a Codebase.

2. On the **Project Summary page**, click **Start Scan**. Information about the scan's progress appears in the **Scan Status** area of the **Project Summary** page.

   When the scan is complete, one of the following messages will be displayed in the **Last Scan** field:

   - **Completed**—This message, displayed in green, indicates that the scan succeeded with no warnings during the scan or analysis.

   - **Completed with warnings**—This message indicates that the scan succeeded, but warnings were generated during the analysis.

   - **Failed**—This message, displayed in red, indicates that the scan failed.

3. Proceed with the steps in Auditing the Scan Results.

Auditing the Scan Results

After the codebase has been scanned, the analyst uses the **Analysis Workbench** tab to manually analyze the automatically-generated inventory items and the remaining files that contain evidence of third-party indicators. The analyst then creates any additional inventory items that are required.
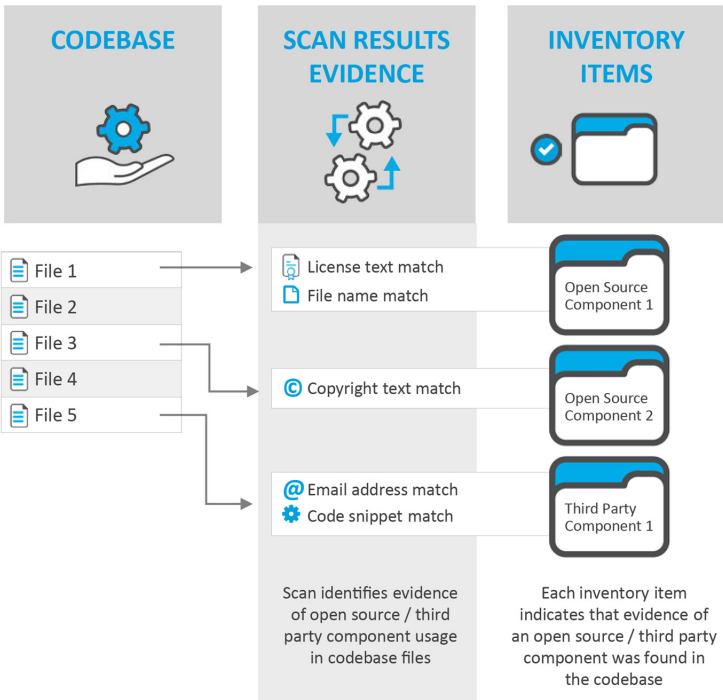
- Overview of Scan Results

- Reviewing the Project Dashboard

- Overview of the Analysis Workbench

- Reviewing Codebase Files and Creating Inventory Items

- Generating an Audit Report

Overview of Scan Results

When FlexNet Code Insight performs a scan of a codebase, it identifies evidence of open source/third-party component usage, and associates that evidence with inventory items. The following diagram illustrates the relationship between codebase files, evidence, and inventory items.

SCAN RESULTS

EVIDENCE AND INVENTORY ITEMS

CODEBASE

SCAN RESULTS EVIDENCE

INVENTORY ITEMS

File 1
File 2
File 3
File 4
File 5

License text match
File name match

Copyright text match

Email address match
Code snippet match

Open Source Component 1

Open Source Component 2

Third Party Component 1

Scan identifies evidence of open source / third party component usage in codebase files

Each inventory item indicates that evidence of an open source / third party component was found in the codebase

Figure 2: Scan Results: Evidence and Inventory Items

In the scan results, codebase files that contain evidence of open source/third-party components are associated with inventory items.

Evidence

Evidence consists of text string matches, file name matches, or code snippet matches that have been found in your codebase that identify the use of open source/third-party components in your codebase, based upon information found in the Compliance Library. The use of these components may expose your applications to compliance issues and security vulnerabilities.

Inventory Items

Inventory items associate open source/third-party components with the files in your code base that contain the detected evidence. During the scan, many inventory items are automatically created based upon defined rules, and are automatically published. Published inventory items appear in **Audit Reports** and are listed on the **Project Inventory** review page. During the audit, if the analyst finds partial matches of evidence in a file not already associated with an inventory item, the analyst can create a new inventory item to associate that evidence with an open source/third-party component.

Process Flow

After the analyst performs a review of the detected evidence and inventory items, as described in Reviewing Codebase Files and Creating Inventory Items, security and legal experts in the organization need to review each published inventory item (and the discovered evidence) to approve or reject the inclusion of the associated open source/third-party component in the software project, as described in Approving/Rejecting Inventory Items.

Reviewing the Project Dashboard

After you have scanned your codebase, a summary of the scan results is displayed in the **Project Dashboard**. To open the

Project Dashboard, click the **Load Project Dashboard** button ( ) on the **Projects** page. The **Project Dashboard** lists statistics and charts that summarize the scan results for the selected project.
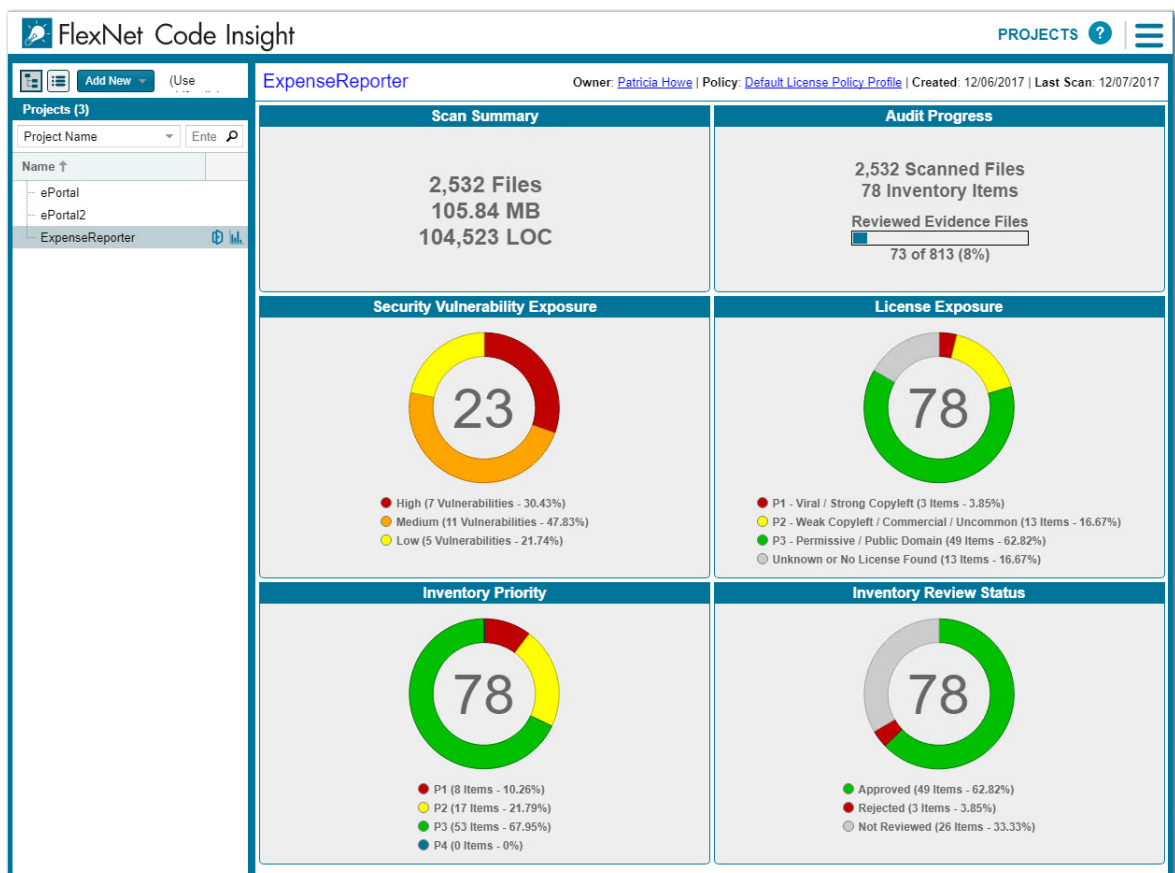
Figure 3: Project Dashboard

The **Project Dashboard** includes the following information:

● **Scan Summary**—Lists the total number of files in the scanned codebase, the size of the codebase/files, and the number of lines of code that were scanned.

● **Audit Progress**—Lists the number of scanned files and inventory items, and percentage of evidence files that have been reviewed.

- **Security Vulnerability Exposure**—an interactive color-coded chart and legend that provide an overview of the security vulnerabilities by severity across all the project inventory. The number in the center of the chart is the total number of security vulnerabilities found across all inventory items.

- **License Exposure**: an interactive color-coded chart and legend that provide an overview of the licenses identified by priority across all of the project inventory. The number in the center of the chart is the total number of inventory items identified for the current project.

- **Inventory Priority**: an interactive color-coded chart and legend that provide an overview of the priority of inventory in the selected project.

- **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.

Quickly Viewing Project Inventory

FlexNet Code Insight's interactive charts and legends allow you to jump quickly to the inventory of interest from the **Project Dashboard**.

Task   ***To jump to the inventory of interest from the Project Dashboard:***

1. Look for an area of interest in one of the charts or legends in the **Project Dashboard**.

2. Point to a color on a graph or legend and click your mouse. The **Project Inventory** tab appears, displaying only those inventory items that match the status of the color you clicked on.

Overview of the Analysis Workbench

You can view the detailed results of a FlexNet Code Insight codebase scan on the **Analysis Workbench** of the **Projects** view. The **Analysis Workbench** tab consists of multiple panes and tabs that list the evidence of open source/third-party components that were discovered during the scan.

Table 3 • Analysis Workbench

Pane/Tab	Description
Codebase Files Pane	Lists all of the files in the codebase. If you click on a file, evidence summary details on that file are displayed in the File Details Tab. Before a software application can be approved for release, every file in the codebase needs to be reviewed.
File Search Results Pane	Use the **Search Files** button in this pane to filter the list of codebase files by a predefined filter (such as **Files that require additional analysis**) or a new filter that you create.

Table 3 • Analysis Workbench (cont.)

Pane/Tab	Description
File Details Tab	If you click on a file in the **Codebase Files** or **File Search Results** panes, evidence summary details of that individual codebase file are displayed in this tab, which has several subtabs: • **Evidence Summary**—Lists a summary of the evidence detected for that file. • **Exact Matches and Partial Matches subtabs**—Displays the actual content of scanned (non-binary) files, with evidence highlighted using color-coding to indicate its type, such as green for licenses, blue for copyrights, etc.
Evidence Details Tab	Displays a summary of all evidence discovered in the codebase, which is organized and sortable.
Inventory Items Pane and Inventory Details Tab	Lists all existing open source/third-party components for which evidence was discovered. For more information, see Viewing Inventory Items and Inventory Details.
Legend	Provides a key to the colors used in the various panes on this tab to identify the type of evidence detected in a file. For more information, see Using the Legend to Identify/Filter Evidence Types.

Viewing Inventory Items and Inventory Details

The **Inventory Items** pane of the **Analysis Workbench** tab lists all existing open source/third-party components for which evidence was discovered. Inventory items with a blue dot have already been automatically published (based on rules), while inventory items with a hollow dot need to be reviewed by the analyst and published, if necessary.

If you double-click on an inventory item in the **Inventory Items** pane, details on the item are listed on the **Inventory Details** tab in the middle pane of the **Analysis Workbench** tab.

Using the Legend to Identify/Filter Evidence Types

The legend area of the **Analysis Workbench** tab provides a key to the colors used in the various panes to identify the type of evidence detected in a file.

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

Figure 4: Legend on Analysis Workbench Tab

This legend is interactive. To filter the codebase file listing by evidence type or review status, click on one of the items in the legend. For example, if you click on **Copyrights**, the **File Search Results** list is filtered by the **Copyrights** evidence category.

Reviewing Codebase Files and Creating Inventory Items

After the codebase is scanned, the results of the scan should be reviewed and evaluated by an analyst. 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 a product. During an audit, the analyst needs to discover all code that:

- Is under licenses that put your proprietary source code at risk.

- Has known security vulnerabilities.

- Has no license or is under business unfriendly licenses from competitors or malicious sources.

The analyst needs to review all listed files in the codebase and mark them as reviewed. In some cases, the analyst may need to associate discovered evidence with existing inventory items or new inventory items that they create. The analyst's final step it to publish all reviewed inventory items, making them available for reporting and review by security and legal experts. For detailed information on how to perform these tasks, see the *FlexNet Code Insight User Guide*.

Generating an Audit Report

Audit reports provide way for the analyst to distribute their research and findings to others, such as the security and legal experts who need to approve or reject each inventory item.

Task   **To generate an Audit Report:**

1. Open the **Project Summary** page for your project.

2. At the bottom of the screen, click **Generate Report** and select **Audit Report** from the popup menu. A dialog box opens stating that the report will be generated as a background process.

3. Click **OK**. When the report has been generated, **View** and **Download** are displayed next to **Audit Report**.

4. To view the HTML version of the report in a web browser, click **View**. The report opens in a web browser with the following information displayed for each published inventory item:

    - **Name**—Name of inventory item. Click on the name to view detailed information on that item.

    - **Component**—Name of open source/third-party component associated with this inventory item.

    - **License**—Name of license applicable to this component.

    - **Vulnerabilities**—Number of vulnerabilities identified in the inventory item by priority.

    - **Files**—Number of codebase files associated with this inventory item.

5. Click **Download** to download a ZIP file containing the report in the following formats:

    - **HTML**—Can be viewed in any browser.

    - **JSON**—Can be processed programmatically to integrate with other applications.

    - **XLSX**—Can be viewed in Microsoft Excel.

Approving/Rejecting Inventory Items

The next step in the FlexNet Code Insight process flow is to have security and legal experts review all published inventory and categorize them as either **approved** or **rejected** for use in the software project.

Task   **To approve or reject an inventory item:**

1. Open the **Project Inventory** page. The **Inventory Items** pane lists all published inventory items.

2. Click on one of the inventory items. In the right pane, the **Inventory Details** tab opens for the selected item.

3. The **Vulnerabilities** area provides a count of each vulnerability found categorized by severity. Click **View Details** to see details on the vulnerabilities.

4. Review the following additional information:

Area	Description
Encryption	Indicates whether the inventory item contains encryption technology.
Priority	Specifies the priority of the inventory item, with **P1** as the highest priority. You can change the priority for this inventory item by selecting a different value from the list.
Status	Shows the status of the inventory item as being Approved, Rejected, or Not Reviewed.
Component Details Tab	Lists additional details about the inventory item.
As-Found License Tab	Lists license text for the license associated to 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.
Notes & Guidance Tab	On this tab, the following information is listed: • **Detection Notes**—Notes generated by FlexNet Code Insight that specify the automated detection technique that was used to locate the component, license information in the case that the license has changed from one version to another or if the component has multiple licenses, attributes extracted from a POM or Manifest file containing project, and configuration details. • **Audit Notes**—Notes entered by the analyst based on findings during the analysis. • **Usage Guidance**—Notes entered by the analyst that indicate how the component should or should not be used in accordance with the company policy. • **Remediation Notes**—Notes entered by the security or legal experts related to remediation actions required for the given inventory item. *Important • For inventory items that are rejected, it is important that the security and legal experts record remediation steps that the Engineering team has to take in the **Remediation Notes** field or in a new column of the Excel version of the Audit Report.*

Area	Description
Associated Files Tab	Lists the codebase files associated with the inventory item.

5. After you review the inventory item's information, mark it **Approved** (✔) or **Rejected** (✖) by clicking the appropriate icon in the **Status** column of the **Inventory Items** pane. A circle will appear around the selected status icon. Until the item has been approved or rejected, the item will remain in **Not Reviewed** status (?).

You can also approve or reject an inventory item by clicking the appropriate icon in the **Status** area of the **Inventory Details** pane.

6. For inventory items that are rejected, provide remediation notes to the Engineering department.

Performing Remediation

Before a software product can be released, all published inventory items need to be approved. If any inventory items are rejected, Engineering personnel needs to implement the suggested remediation steps for each inventory item.

After those remediation steps have been completed by Engineering, a new version of the codebase needs to be provided to the FlexNet Code Insight analyst to rescan and begin the FlexNet Code Insight process flow again.

When security and legal experts are able to perform the steps in Approving/Rejecting Inventory Items without having to reject a single inventory item, the software product is ready for release.

Releasing the Product with a Notices Report

After Engineering has completed the remediation plan, resolving all rejected inventory items, the codebase is rescanned until it is approved for release. When the codebase is approved for release, you need to generate a **Notices Report** to accompany the software application that identifies all open source/third-party components that it contains.

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

Task   ***To generate a Notices Report:***

1. Open the **Project Summary** page for your project.

2. At the bottom of the screen, click **Generate Report** and select **Notices Report**. A dialog box opens stating that the report will be generated as a background process.

3. Click **OK**. When the report has been generated, click **View** or **Download** next to **Notices Report**. The Notices Report appears and may include the following information:

    • **Inventory name**—The component name, version, and governing license name is listed.

    • **Inventory URL**—The associated component's URL is listed, if available.

    • **Inventory notices text**—The associated component's license text is listed, if available.

    This Notices Report will satisfy the attribution requirements of most open source licenses.

*Note • You can manually add additional text to include in the Notices Report by entering it in the **Notices Text** field on the Inventory Details tab. See Viewing Inventory Items and Inventory Details.*

Next Steps

Refer to this documentation for more information about Code Insight:

• *FlexNet Code Insight User guide* for additional information about accessing and using Code Insight features and functionality.

• *FlexNet Code Insight Installation and Configuration Guide* to learn about configuring advanced features such as remote scanning of the product.

Contacting Support

If you need further support, please submit your questions through our online **Customer Community** portal:

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

• If you do not have a login to the Customer Community, you can request one on the **Login Request** page of our site:

https://flexeracommunity.force.com/customer/CCLoginRequest

• If you are unable to use the steps above, please visit the following site for other options to reach out to Flexera Support:

https://flexeracommunity.force.com/customer/CCContactSupport