Code Insight 2020 R4

Quick Start Guide

Legal Information

Book Name: Code Insight 2020 R4 Quick Start Guide

Part Number: RCI-2020R4-QSG00

Product Release Date: December 2020

Copyright Notice

Intellectual Property

Restricted Rights Legend

Contents

Contents

Code Insight 2020 R4 Quick Start Guide

Code Insight is an end-to-end solution for managing open-source and third-party code in software development projects. Using Code Insight's discovery technology and databases 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 *Code Insight Quick Start Guide* provides basic information that will enable you to quickly start using the product effectively. It contains instructions that walk you through the process of configuring and executing a scan performed by a Scan Server on a codebase that you have uploaded to the server.

Note • Information about alternatives to this type of scan process can be found in the Code Insight User Guide and the Code Insight Plugins Guide.

- Before You Begin
- Code Insight Process Flow
- Launching 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
- Product Support Resources
- Contact Us

Before You Begin

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

Table 1 • Code Insight Configuration Tasks

Task	Description	More Information
Obtain installer and license key	To access the Product and License Center to obtain the installer and key, first sign in to the Revenera Community: https://community.revenera.com In the Community, select **FlexNet Code Insight** from **Find My Product**, and then click **Download Products and Licenses** from the **Product Resources** list on the right on the Community page.	For instructions on downloading the installer and license key, see: https://docs.flexera.com/plc/en/default.htm
Run installer	Install Code Insight on a server that meets system requirements and that has access to a compatible database (such as MySQL 8.0).	See *Installing Code Insight* in the *Code Insight Installation & Configuration Guide*.
Start Tomcat Server	After installation is complete, start the Code Insight Tomcat server.	See *Starting and Stopping Tomcat* in the *Code Insight Installation & Configuration Guide.*
Complete electronic update	After installation is complete and the Tomcat server is started, a full electronic update is automatically performed, which takes approximately 10 hours to complete. You cannot use the application to scan files until the update is completed. *Note • Incremental updates performed between full updates can complete in a shorter amount of time—possibly 4 hours, depending on the amount of data involved.*	
Obtain the Compliance Library	(Optional) The Code Insight Compliance Library (CL), downloaded from the Product and License Center. *Note • The CL is required only if you want to perform a "deep scan" for exact files and source-code fingerprints (snippets) in your codebase that match those found in third-party and open-source software. (This search is additional to the Automated Analysis process basic to all scans.)*	For instructions on installing the CL, see (*Optional) Installing the Compliance Library* in the *Code Insight Installation and Configuration Guide*. Also see *About Code Insight Scans* in the *Code Insight User Guide.*

Table 1 • Code Insight Configuration Tasks (cont.)

Task	Description	More Information
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 (CL) if you want to enable it for use in scans.	See *Adding or Editing Scan Servers or Checking Server Status* in the *Code Insight Installation & Configuration Guide*.
Create user accounts	Create user accounts for all end users and distribute those credentials to the end users.	See *Managing Users* in the *Code Insight Installation & Configuration Guide*.
Set up global project defaults	Define default properties used to set up Code Insight projects, providing a means to standardize the projects at your site and enabling an easier project creation experience for users. (Note that Project Owners can change these defaults as needed at the project level.)	See *Setting Project Defaults* in the *Code Insight Installation & Configuration Guide*.

Code Insight Process Flow

The 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.
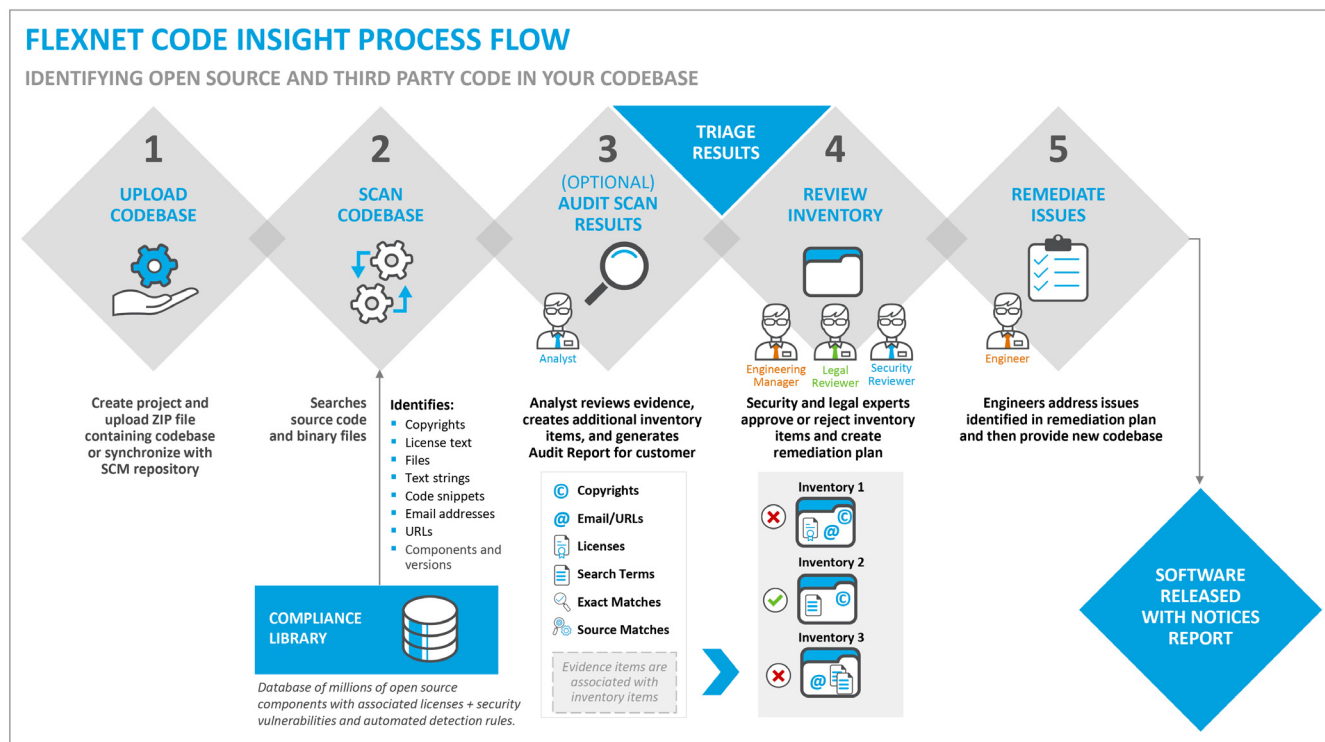
Figure 1: Code Insight Process flow

The Code Insight process flow consists of the following steps.

Table 2 • 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. The codebase is uploaded to the Scan Server.	See Creating a Project and Uploading a Codebase and Other Methods for Accessing a Codebase to Scan.
2	**Scan Codebase**	Project owner	Scan the codebase files to find evidence of open-source or third-party components, based on Automated Analysis and on a comparison of the codebase with the contents of the Compliance Library (CL) (if it is installed). The scan translates these findings into an inventory of third-party components for the project.	See Performing a Scan.
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. Publish inventory items to the **Project Inventory** page for stakeholder review. Additionally, 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, assigning review or remediation tasks, or adding additional columns to the Excel version of the Audit Report.	See Approving/Rejecting Inventory Items.

Table 2 • Code Insight Process Flow (cont.)

#	Step	Performed By	Description	More Information
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 Code Insight

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

Task   ***To launch Code Insight:***

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

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

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

Navigating Through Code Insight

The following are ways to navigate through 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 Code Insight interface are:

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

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

- **All-inventory view**—Use to review and access inventory items across all projects.

- **Administration**—Use to manage users, schedule electronic updates, set up email servers and scan servers, configure LDAP and integration with Application Lifecycle Management (ALM) systems, create and manage scan profiles, and define global project defaults.

Creating a Project and Uploading a Codebase

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

- Creating a Project

- Uploading a Codebase

- Other Methods for Accessing a Codebase to Scan

Creating a Project

A project stores the analysis results from a scanned codebase. You must create a project in 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 Visibility** list, select **Public**. This selection, the default, allows everyone with access to the Code Insight to view the new project.

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

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

6. From the **Scan Server** list, select the scan server to be used for scanning the codebase for this project.

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 Code Insight can perform a scan, you must upload the archive file containing the source code and binary files of a codebase to the Scan Server. This archive can be a `.zip`, `.7z`, `.tar`, or `.tar.gz` file.

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 Archive File** to browse to for the archive file (`.zip`, `.7z`, `.tar`, or `.tar.gz`) containing your codebase.

5.   (Optional) Select **Delete existing project codebase files** to have Code Insight delete previously uploaded codebase files associated with this project.

Note • *If you select this option, 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.*

6.   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.

   ● **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.

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

8.   Proceed with the steps in Performing a Scan.

Other Methods for Accessing a Codebase to Scan

Uploading a codebase is not the only method available for accessing a codebase to scan in Code Insight. However, for the purpose of keeping the getting-started process streamlined, this document focuses on the upload process only. The other methods you can use to access a codebase for a project are briefly described here:

- **Synchronize with your Source Control Management system**—An alternative to uploading a codebase to the Scan Server is to synchronize a codebase repository from a Source Control Management application (such Perforce, Git, Subversion, or TFS) to the Scan Server for scanning. For more information, refer to "Configuring Source Code Management" in the *Code Insight User Guide*.

- **Scan a codebase on a remote server**—Instead of uploading or synchronizing codebases to the Scan Server, you can install a Code Insight scan-agent plugin on a remote system to directly scan a codebase on that system. The results of the remote scan are sent to an existing project on the Code Insight Core Server. For more information, refer to the *Code Insight Plugins Guide*.

Whether your project's codebase is uploaded or synchronized to the Scan Server or resides on a remote system on which a plugin is installed (or is a combination of code files from two or more of these methods), the results of all scans on the complete codebase will be available in your Code Insight project. Within the project, you can then perform further analyses of the codebase files and review, remediate, and finalize the inventory of the open-source and third-party software findings.

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, Code Insight performs a static analysis of files of any type (source or binary) in the target codebase, using automated detection rules to identify open-source or third-party components and their versions, licenses, and security vulnerabilities. The scan generates inventory items based on the component information it identifies.

Additionally, the scan can identify components by searching for files and source code in the codebase that match files (exact-content matching) or source-code snippets found in open-source and third-party software. Detection of file and source-code snippet matches is based on the comparison of the scanned codebase with the contents of the Compliance Library (CL), a large library containing the information needed to perform content matching.

The evidence that Code Insight discovers during a scan includes:

- Third-party copyright statements
- Open-source license text matches
- File name matches to files collected in the CL
- Code-snippet matches to code collected in the CL
- Search terms (text string) matches

- Email addresses and URLs

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

- Automated Analysis of packages (such as .jar, NuGet)

- Automated Analysis based on search terms, file names, and other heuristics

- AutoWriteUp Rules from the Code Insight CL

Code Insight continually updates the CL 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. 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 performs file and 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 codebase 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 Code Insight Installation & 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 Server 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. If the scan completed successfully, 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

- Analyzing Codebase Files and Creating Inventory Items

- Generating an Audit Report

Overview of Scan Results

When 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.
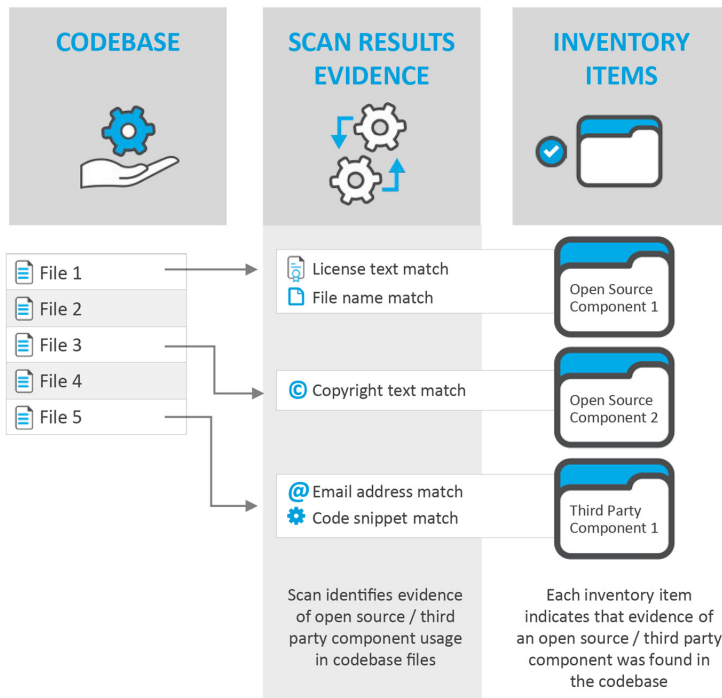

Figure 2: Scan Results: Evidence and Inventory Items

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, exact file-content 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 (CL). 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. 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. The analyst can then manually publish the inventory item for stakeholder.

Process Flow

After the analyst performs a review of the detected evidence and inventory items, as described in Analyzing 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.

*Note • The following **Project Dashboard** example shows the results for a scan performed by a Scan Server. If one or more remote scans were run for the project, the **Project Dashboard** would reflect the results of the remote scans. If both remote scans and a Scan Server scan were run for the project, the dashboard would show a compilation of statistics for both scan types. For more information about remote scans, see Other Methods for Accessing a Codebase to Scan.*
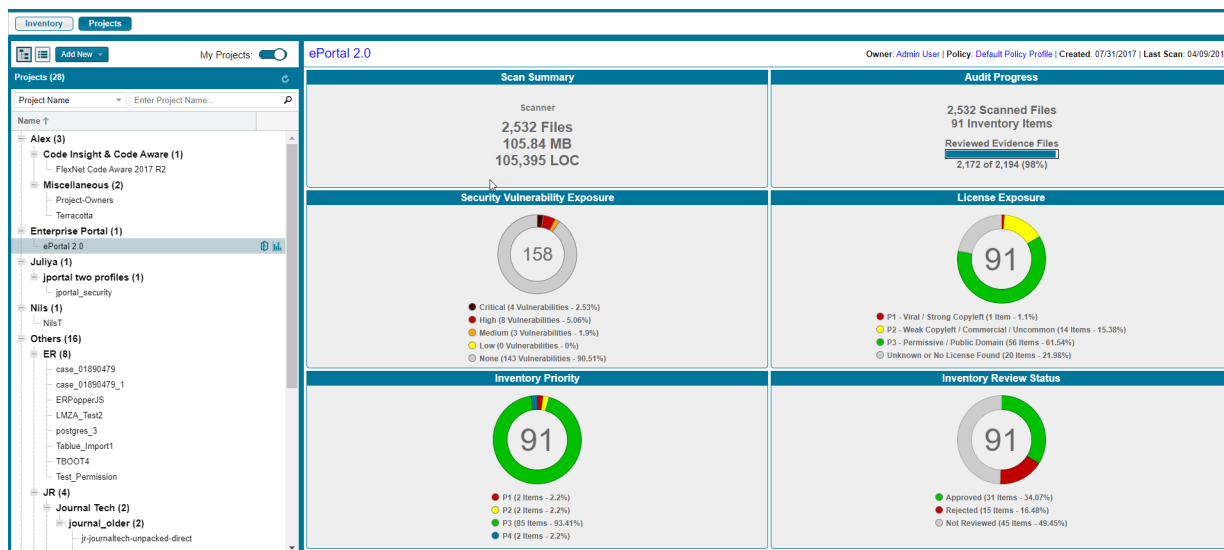
Figure 3: Project Dashboard

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

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 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 **Advanced Search** 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. This pane also shows the results of the filters selected on the **Analysis Workbench** legend (see Using the Legend to Identify/Filter Evidence Types).
File Details Tab	If you click on a file in the **Codebase Files** or **File Search Results** panes, summary details of evidence for 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.

Table 3 • Analysis Workbench (cont.)

Pane/Tab	Description
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.

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.

Analyzing 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 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 *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 severity.

    - **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.

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

Approving/Rejecting Inventory Items

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

Note that **Project Inventory** page can include inventory items that were automatically approved or rejected. This automatic review occurs when policies defined for the project are applied at the time an inventory item is published. The policies are based on the component version range, licenses, and security vulnerabilities. If a matching policy does not exist for a given inventory item at publication time, the item shows as **Not Reviewed**. However, the project can be configured to automatically assign review tasks to default legal and security contacts to conduct manual reviews on the non-reviewed items. These reviewers then check for intellectual property (IP) and security compliance. For more information, see *Managing Policy Profiles* and *Updating Review and Remediation Settings for a Project* in the *Code Insight User Guide*.

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** bar graph provides a count of each vulnerability found categorized by severity. Click the bar to see details on the vulnerabilities.

4. Review the following additional information:

Area	Description
Confidence	Indicates the confidence level (High, Medium, or Low) of an inventory item. This level is the measure of the strength of the discovery technique used to generate the inventory item. The confidence level is represented by a graph with three segments—three shaded segments indicate High confidence, two indicate Medium, and one indicates Low. For more information, see *Inventory Confidence* in the *Code Insight User Guide*.
Encryption	Indicates whether the inventory item contains encryption technology.
Priority	Specifies the priority of the inventory item in terms of its importance within the scope of the inventory review process, with **P1** as the highest priority. You can change the priority for this inventory item by selecting a different value from the list. For more information, see *Inventory Priority* in the *Code Insight User Guide*.
Status	Shows the status of the inventory item as being Approved, Rejected, or Not Reviewed.
Inventory Details Tab	Shows details about the inventory item including usage information and links to any open or closed tasks for the item. If your Code Insight installation is integrated with an external workflow system that tracks the tasks, links to this system and to details about your workflow request might be available.
Component Details Tab	Lists additional details about the inventory item.
Notices Text Tab	Displays the **As-Found License Text** found in the codebase during the scan. Depending on the detection technique, this field can show actual license text for one or more licenses or be a reference to a license. The **As-Found License Text** content cannot be edited, but you can copy it to the **Notices Text** field (also on this tab) if you need to modify it. Any text in the **Notices Text** field is considered final and is included in the Notices report. 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 Notices report. If both fields are empty, the report uses the license content from Code Insight data library.

Area	Description
Notes & Guidance Tab	On this tab, the following information is listed: ● **Detection Notes**—Notes generated by 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.*
Usage	Lists details such as how the item is being distributed with your product, how the item's libraries are linked to your product, whether the item provides encryption technology, whether you have modified its code, and so forth. Usage details are important 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 can also 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.
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, assign remediation tasks to the Engineering department (and provide remediation notes) to address the legal or security issues. For details, see *Creating and Managing Tasks for Project Inventory* in the *Code Insight User Guide*.

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 Code Insight analyst to rescan and begin the 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, select **Notices Report** from the **Select Report** dropdown.

3. Click **Generate Report**. A dialog box opens stating that the report will be generated as a background process.

4. Click **OK**. When the report has been generated, the **View | Download** links appear next to the **Select Report** field.

5. Select either option:

   - To view the report in your browser, click **View**.

   - To download the report, click **Download**. A `.zip` file is downloaded, containing the report data as a `.txt` file. (The text format enables you to reformat the report data as you want.)

The Notices Report can 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 the final text to include in the Notices Report by entering it on the **Notices Text** tab for the inventory item in **Analysis Workbench** or **Project Inventory**. See "Finalizing the Notices Text for the Notices Report" in the Code Insight User Guide.

Next Steps

Refer to this documentation for more information about Code Insight:

- _Code Insight User Guide_ for additional information about accessing and using Code Insight features and functionality.

- _Code Insight Installation & Configuration Guide_ to learn about configuring advanced features such as remote scanning of the product.

- _Code Insight Plugins Guide_ for information about running remote agent scans on codebases that you do not upload to the Code Insight server.

Product Support Resources

The following resources are available to assist you with using this product:

- Revenera Product Documentation

- Revenera Community

- Revenera Learning Center

- Revenera Support

Revenera Product Documentation

You can find documentation for all Revenera products on the Revenera Product Documentation site:

https://docs.revenera.com

Revenera Community

On the Revenera Community site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Revenera's product solutions, you can access forums, blog posts, and knowledge base articles.

https://community.revenera.com

Revenera Learning Center

The Revenera Learning Center offers free, self-guided, online videos to help you quickly get the most out of your Revenera products. You can find a complete list of these training videos on the Learning Center site:

https://learning.revenera.com

Revenera Support

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the Revenera Community.

https://community.revenera.com

Contact Us

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

http://www.revenera.com

You can also follow us on social media:

- Twitter

- Facebook

- LinkedIn

- YouTube

- Instagram