Code Insight 2021 R2 Release Notes

May 2021

Introduction

These Release Notes provide the following information about the Code Insight 2021 R2 release:

- About Code Insight
- New Features and Enhancements
- Resolved Issues
- Deprecated Functionality
- Known Issues
- Addendum: Enabling Cross-Origin Resource Sharing
- Legal Information

About Code Insight

Code Insight is the next generation Open Source security and compliance management solution. It empowers organizations to take control of and manage their use of open source software (OSS) and third-party components. Code Insight helps development, legal, and security teams use automation to create a formal OSS strategy that balances business benefits and risk management.

New Features and Enhancements

The Code Insight 2021 R2 release provides new features and enhancements in the following areas:

- All-Project Inventory View
- Automated Workflow for Inventory Review/Publication
- Project Administration and Management
- Project Inventory Review
- Project Reporting
- Scanning and Automated Discovery
- Security Vulnerability Reporting
- REST API Enhancements

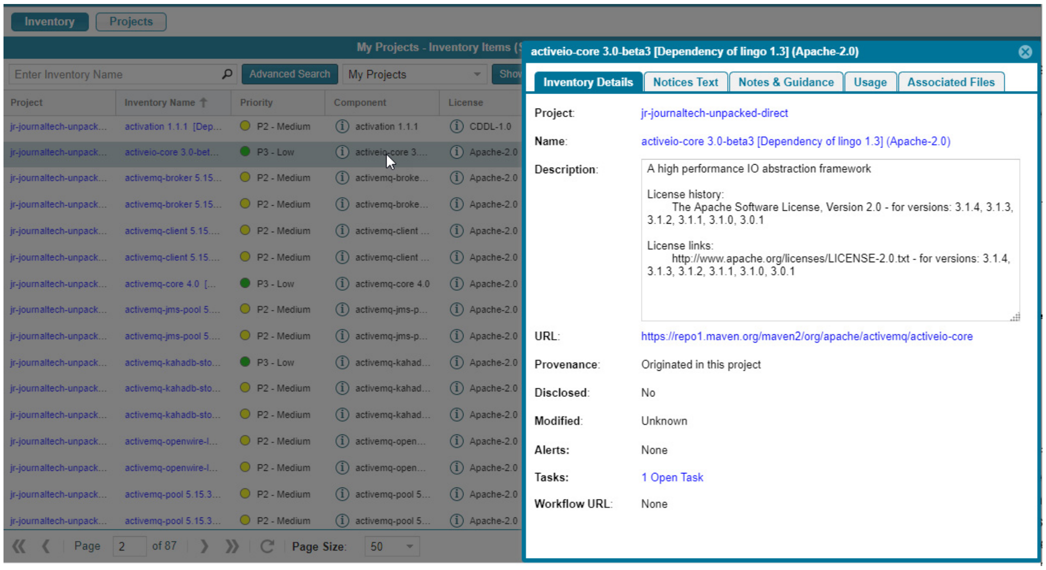
All-Project Inventory View

The following new feature is available for the **Inventory** view, which shows inventory across all Code Insight projects.

New Read-only Inventory Details Slide-out Panel

Users can now examine a read-only version of the details for a given inventory item in the **Inventory** view. These details are displayed on a slide-out panel within the view, providing an easy means of obtaining information about the inventory item without having to open the project.

The slide-out panel is opened by simply clicking within an un-hyperlinked section of the row for the inventory item. The panel shows most of the information available for the inventory item on its **Project Inventory Details** pane in the actual project. (Note, however, that the **Component Details** tab is not available on the slide-out.)



Project	Inventory Name	Priority	Component	License
jr-journaltech-unpack...	activation 1.1.1 [Dep...	● P2 - Medium	ⓘ activation 1.1.1	ⓘ CDDL-1.0
jr-journaltech-unpack...	activeio-core 3.0-bet...	● P3 - Low	ⓘ activeio-core 3....	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-broker 5.15...	● P2 - Medium	ⓘ activemq-broke...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-broker 5.15...	● P2 - Medium	ⓘ activemq-broke...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-client 5.15....	● P2 - Medium	ⓘ activemq-client ...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-client 5.15....	● P2 - Medium	ⓘ activemq-client ...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-core 4.0 [...	● P3 - Low	ⓘ activemq-core 4.0	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-jms-pool 5....	● P2 - Medium	ⓘ activemq-jms-p...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-jms-pool 5....	● P2 - Medium	ⓘ activemq-jms-p...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-kahadb-sto...	● P3 - Low	ⓘ activemq-kahad...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-kahadb-sto...	● P2 - Medium	ⓘ activemq-kahad...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-kahadb-sto...	● P2 - Medium	ⓘ activemq-kahad...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-openwire-l...	● P2 - Medium	ⓘ activemq-open...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-openwire-l...	● P2 - Medium	ⓘ activemq-open...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-pool 5.15.3...	● P2 - Medium	ⓘ activemq-pool 5...	ⓘ Apache-2.0
jr-journaltech-unpack...	activemq-pool 5.15.3...	● P2 - Medium	ⓘ activemq-pool 5...	ⓘ Apache-2.0

Page 2 of 87 Page Size: 50

activeio-core 3.0-beta3 [Dependency of lingo 1.3] (Apache-2.0)

Project: jr-journaltech-unpacked-direct

Name: activeio-core 3.0-beta3 [Dependency of lingo 1.3] (Apache-2.0)

Description: A high performance IO abstraction framework

License history:
The Apache Software License, Version 2.0 - for versions: 3.1.4, 3.1.3, 3.1.2, 3.1.1, 3.1.0, 3.0.1

License links:
http://www.apache.org/licenses/LICENSE-2.0.txt - for versions: 3.1.4, 3.1.3, 3.1.2, 3.1.1, 3.1.0, 3.0.1

URL: https://repo1.maven.org/maven2/org/apache/activemq/activeio-core

Provenance: Originated in this project

Disclosed: No

Modified: Unknown

Alerts: None

Tasks: 1 Open Task

Workflow URL: None

While the slide-out details are read-only, certain values are hyperlinked, enabling you to still explore and maintain the inventory item as your permissions allow. For example, you can click the **Project** name link to open to the **Project Inventory** tab in the actual project, where you can access and edit any inventory in the project. Or you can click the inventory item's **Name** link to open to the item's **Project Inventory Details** pane in project, where you can actually edit the inventory item. Links are also available to open and maintain existing tasks and alerts for the inventory item and to access the item's **Provenance**, **Workflow**, and component **URL** sites.

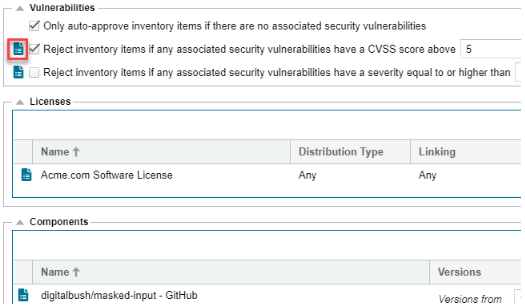
Automated Workflow for Inventory Review/ Publication

The following are enhancements to the automated workflow for inventory review and publication in Code Insight.

Creating Usage Guidance for Any Policy Criterion

Previously, a Policy Manager could add usage guidance information for only license criteria in a policy profile. Now the manager can add usage guidance information to vulnerability and component criteria as well. This information helps users understand what factors were involved in the rejection of inventory, what issues need to be addressed for rejected inventory, or what guidelines or special notes are available for approved inventory.

As with adding usage guidance to a license criterion, the manager simply clicks the **Usage Guidance** icon next to a vulnerability or component criterion to open the **Usage Guidance** pop-up.



Vulnerabilities

☑ Only auto-approve inventory items if there are no associated security vulnerabilities

☑ Reject inventory items if any associated security vulnerabilities have a CVSS score above 5

□ Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than

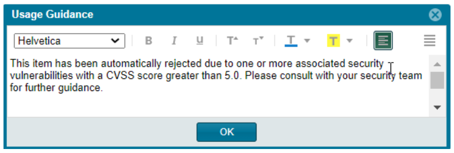
Licenses

Name ↑	Distribution Type	Linking
Acme.com Software License	Any	Any

Components

Name ↑	Versions
digitalbush/masked-input - GitHub	Versions from

From the **Usage Guidance** pop-up, the manager can enter guidance content.

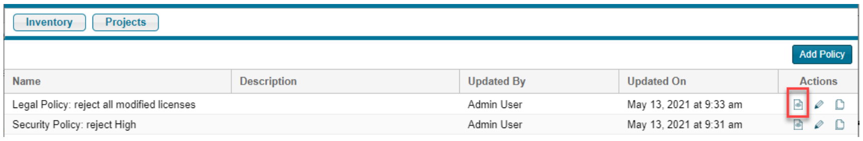


This item has been automatically rejected due to one or more associated security vulnerabilities with a CVSS score greater than 5.0. Please consult with your security team for further guidance.

This usage guidance content is then propagated to those project inventory items that are actually approved or rejected by the policy, providing reviewers with context about the inventory's status.

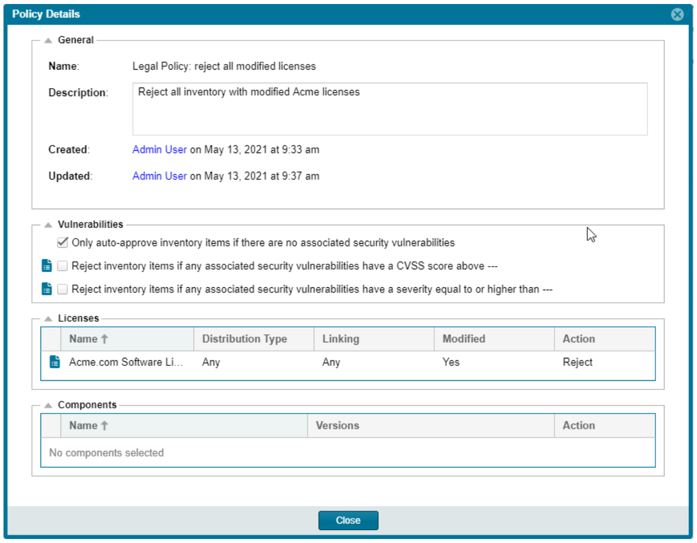
Viewing Policy Details without Opening the Policy

A Policy Manager can now open a read-only view of the details for a given policy directly from the **Policy** page without having to open the policy. The manager simply clicks the **View** icon for the policy listed on the page.



Name	Description	Updated By	Updated On	Actions
Legal Policy: reject all modified licenses		Admin User	May 13, 2021 at 9:33 am	
Security Policy: reject High		Admin User	May 13, 2021 at 9:31 am	

A read-only view of the policy details is displayed.



Policy Details

General

Name: Legal Policy: reject all modified licenses

Description: Reject all inventory with modified Acme licenses

Created: Admin User on May 13, 2021 at 9:33 am

Updated: Admin User on May 13, 2021 at 9:37 am

Vulnerabilities

☑ Only auto-approve inventory items if there are no associated security vulnerabilities

☐ Reject inventory items if any associated security vulnerabilities have a CVSS score above ---

☐ Reject inventory items if any associated security vulnerabilities have a severity equal to or higher than ---

Licenses

Name ↑	Distribution Type	Linking	Modified	Action
Acme.com Software Li...	Any	Any	Yes	Reject

Components

Name ↑	Versions	Action
No components selected		

Project Administration and Management

The following are enhancements to project administration in Code Insight.

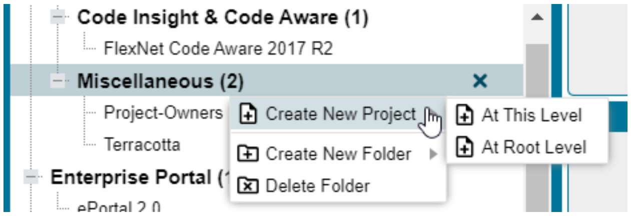
New Project Branching Options

New options in the **Branch Project** wizard enable Project Administrators to retain the following attributes of the source project when branching to a new project so that this information does not need to be manually re-entered in the branch project:

- All project users (including Legal, Security, and Developer contacts)
- Project description
- Project **Visibility**, **Risk**, and **Status** values
- Project hierarchy (child projects only)
- **Usage** field values of project inventory

New Right-Click Options for Projects and Folders in Project Tree

New **At This Level** and **At Root Level** right-click options in the Project tree enable users to easily indicate the location in the tree to which to add a new project and folder:

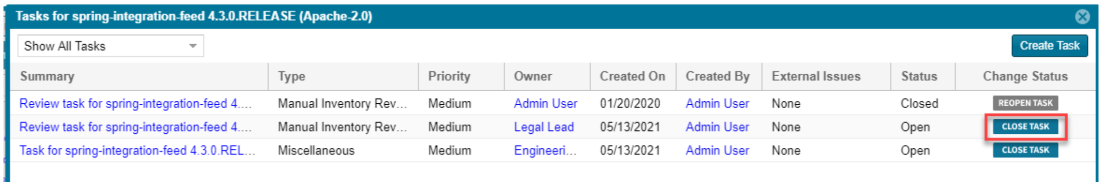


Project Inventory Review

The following new feature is available for reviewing project inventory.

Closing and Reopening Tasks Directly from the Tasks List

A new **Change Status** column on the **Tasks** list enables users to change the status of a given task directly from the list without having to open the task to edit it. Users can close or reopen a task by clicking the button available for the task in the **Change Status** column.



Tasks for spring-integration-feed 4.3.0.RELEASE (Apache-2.0)

Summary	Type	Priority	Owner	Created On	Created By	External Issues	Status	Change Status
Review task for spring-integration-feed 4....	Manual Inventory Rev...	Medium	Admin User	01/20/2020	Admin User	None	Closed	REOPEN TASK
Review task for spring-integration-feed 4....	Manual Inventory Rev...	Medium	Legal Lead	05/13/2021	Admin User	None	Open	CLOSE TASK
Task for spring-integration-feed 4.3.0.REL...	Miscellaneous	Medium	Engineeri...	05/13/2021	Admin User	None	Open	CLOSE TASK

When the **CLOSE TASK** button is clicked for a **Manual Inventory Review** task, the user is also prompted to select a task resolution (**Approved** or **Rejected**) to complete the task closure.

Project Reporting

The following new features are available for generating and viewing project reports.

Project Report Data Now Reflecting License Evidence Discovered by Remote Scan Agents

Data in the Project report now reflects any license evidence found in remote files scanned by a scan agent. This evidence (along with evidence detected by the Scan Server) is captured in the charts and data at the following locations in the report:

- **Additional Evidence** section of the **Summary** sheet
- **Files with License** sheet (with an **Alias** column to identify which files are remote)
- **All Scanned Files** sheet

Ability to Create Fields for Generating Custom Reports in the UI

A new **reportOptions** parameter has been added to the Create Reports and Update Reports REST APIs, enabling you to define custom fields that users complete in order to generate a given custom report. These fields can be used, for example, to filter the report data. For more information, see Updates to Existing APIs.

Scanning and Automated Discovery

This release provides the following enhancement to the Code Insight codebase scan and the Automated and Advanced Analysis techniques used in scans:

Top-Level Inventory Identified for Dependencies in Standalone requirements.txt in a Python Project

In this release, Automated Analysis can now determine the top-level inventory item for dependencies listed in a standalone `requirements.text` file (that is, a `requirements.txt` file residing in a directory that does *not* also contain a `PKG-INFO` or `setup.py` file) in a Python project. Previously, Automated Analysis relied on one of these two files to identify this top-level inventory item.

If `PKG-INFO` or `setup.py` does not exist in the same directory as `requirements.txt`, Automated Analysis determines the top-level inventory item in one of two ways:

- If the Code Insight obtains the codebase through a `git sync` or `git clone` operation, the top-level inventory item to which direct dependencies are mapped is created from the configuration information found in the `.git` file.
- If the codebase has been directly downloaded from a GitHub or PYPI repository and then uploaded to Code Insight for the scan, the top-level inventory item is created using the name of the directory under which `requirements.txt` resides. Direct dependencies identified in `requirements.txt` are then mapped to this inventory item.

  Upon its creation, such an inventory item is considered a “place holder” item because it is created from a directory name, which might or might not be a valid component name. The item is published during the Automated Analysis only if its name matches a valid component in the Code Insight data library, its forge is PyPI or GitHub, and it meets your site’s inventory publication policies. Otherwise, the item remains unpublished for further review. The inventory type for the item is determined as follows:

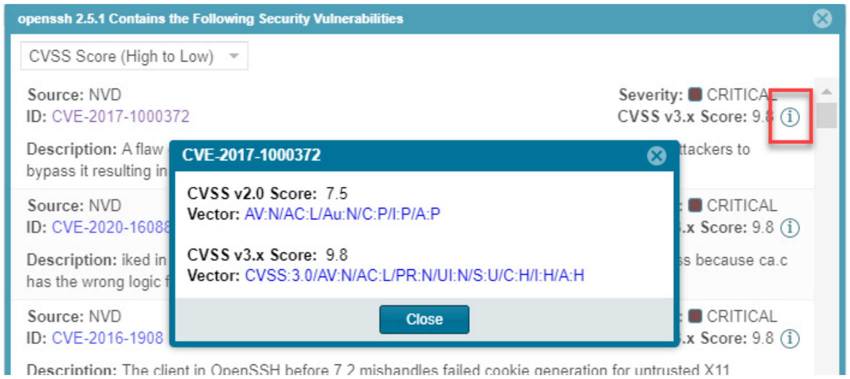
  - If the component name matches a component name in the Code Insight data library, the inventory type is **Component**.
  - If the component is not found in the data library but the inventory’s license matches a license in the data library, the inventory type is **License Only**.
  - If neither the component nor license has a match in the data library, the inventory type is **Work In Progress**.

Security Vulnerability Reporting

This release provides the following enhancement to Code Insight’s reporting of security vulnerabilities found in open-source or third-party components.

New Vector Link to the NVD Calculator

The **Vector** value for a given security vulnerability is now a link (see the picture below) that opens to the NVD Common Vulnerability Scoring System Calculator, showing you the environmental and temporal factors that determined the score CVSS score of the vulnerability. You can use the calculator to tweak these factors as necessary to adjust the score for your software product. (Instructions are provided with the calculator.) The adjusted score can help direct your review and remediation processes.


openssh 2.5.1 Contains the Following Security Vulnerabilities
CVSS Score (High to Low)
Close

Source: NVD
ID: CVE-2017-1000372

Description: A flaw … ttackers to
bypass it resulting in …

Severity: 🟥 CRITICAL
CVSS v3.x Score: 9.8 ⓘ

Source: NVD
ID: CVE-2020-16088

Description: iked in … s because ca.c
has the wrong logic f…

🟥 CRITICAL
…x Score: 9.8 ⓘ

Source: NVD
ID: CVE-2016-1908

🟥 CRITICAL
…x Score: 9.8 ⓘ

Description: The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11

CVE-2017-1000372

CVSS v2.0 Score: 7.5
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.x Score: 9.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A value is displayed in the **Vector** field only if the vulnerability is found in the NVD.

REST API Enhancements

The following tables describe the new or updated Code Insight REST APIs:

- CORS Support Now Available for Calling APIs in Cross-Origin Environments
- New APIs
- Updates to Existing APIs

CORS Support Now Available for Calling APIs in Cross-Origin Environments

Code Insight now supports CORS (Cross-Origin Resource Sharing), enabling the invocation of the Code Insight REST APIs from a script or application at a Web location different from that of the Code Insight Core Server. For details, refer to Addendum: Enabling Cross-Origin Resource Sharing for details.

New APIs

The following new REST APIs were added in this release:

Table 1 ▪ New APIs in this Release

Resource	API Endpoint	Method	Description
Files	`/files/{fileId}`	GET	Retrieves details about a given file, including its MD5 digest, path, review status, and associated project and any evidence discovered. The **fileId** and **Authorization** fields are required to invoke this API. To view details for a remote file ID, you must also set **isRemote** to **true**. Only an Analyst for the project to which the file belongs can successfully invoke this API.

Table 1 ▪ New APIs in this Release

Resource	API Endpoint	Method	Description
Project	/projects/{projectId}/contact	GET	Retrieves the Project Contact of a project. Any user can invoke this API.
		PUT	Updates a project contact. A user with a System Administrator or Project Administrator role can invoke this API.
	/projects/{projectId}/scanNodes	GET	Retrieves data about all scan nodes—Scan Server and remote systems—for a project. The **projectId** and **Authorization** fields are required to invoke this API. Any user can successfully invoke this API as long as the project is public. If the project is private, only those users assigned to a role in the project can call this API.

Updates to Existing APIs

The following updates to existing APIs have occurred in this release.

Table 2 ▪ Updates to Existing APIs

Resource	API Endpoint	Method	Description
Inventory	/inventories/search	GET	The response now includes the inventory associated with any remote file and folder IDs specified, provided these files and folders are in the same project.
	/inventories/{inventoryId}/files	PUT	Remotes files that match the paths specified in the request are now associated (in addition to any Scan Server files) with the given inventory item. If a specified file path is the found at the remote location and on the Scan Server, both files are associated with inventory item.

Table 2 ▪ Updates to Existing APIs

Resource	API Endpoint	Method	Description
Project	`/projects/{projectId}/allscannedfiles`	GET	Two new fields—**remote** and **FileId**—are added to each file listed in the response to show its file ID and whether the file is remote.
	`/projects/{projectId}/evidences`	GET	The response now shows remote files and any evidence associated with a given remote file.
	`/projects/{projectId}/files`	GET	Two new fields—**remoteFolderIds** and **remoteFileIds**—are added to the response to list the IDs of files and folders scanned on a remote system by a scan agent. The new fields distinguish the IDs of the remote files and folders from the IDs of files and folders on the Scan Server that have identical paths. (The IDs for the Scan Server files and folders are listed in the existing **folderId** and **fileId** fields).
Reports	`/reports`	GET	(Custom reports only) The response now includes the definitions for any custom fields configured for a report.
		POST PUT	A new **reportOptions** parameter enables you to define one or more fields in a custom report. If a custom report currently requires a second project, you will need to make changes to the report script to accommodate this new parameter. See the following link: https://community.flexera.com/t5/FlexNet-Code-Insight-Customer/Custom-Reports-Framework-in-FlexNet-Code-Insight/ta-p/132702
	`/reports/{reportId}`	GET	(Custom reports only) The response now includes the definitions for any custom fields configured for the report.

Resolved Issues

The following issues are resolved in this release.

Table 3 ▪ Resolved Issues

Issue	Resolution Notes
SCA-25942	Large Debian (.deb or .dsc) files no longer causing scans to hang.
SCA-28812	Scan of a Python tar.gz file no longer reporting false positive Python dependencies.
SCA-29031	X-Content-Type-Options, X-XSS-Protection, and Strict-Transport-Security response headers now used in all requests, including static resource requests. (The Strict-Transport-Security response header is used for only HTTPS-enabled requests.)
SCA-29934	Scans no longer failing due to recursive symlinks.
SCA-30142 **SCA-34243**	Documentation added to describe how to configure SSL for Azure DevOps, Bamboo, and Jenkins scan-agent plugins. See the *Code Insight 2021 R2 Plugins Guide*.
SCA-30728	Scan no longer reporting false positive dependencies when configured for transitive-dependency detection.
SCA-30936	Scan no longer failing due to broken symlinks. (The broken links are skipped.)
SCA-30990	Synchronization failure with Git repository (due to checkout error) resolved by setting a minimum requirement of Git client version 2.17.
SCA-31054	Documentation added to describe how to configure HTTPS along with SHH for synchronization with a Git repository using Code Insight's SCM (Source Code Management System) connector. See the *Code Insight 2021 R2 Installation & Configuration Guide*.
SCA-31513	Policy page no longer changing the format of a license name after it has been added to the policy.
SCA-31757	Errors in attempting to call REST functionality from a Web site different from that of the Code Insight Core Server. These errors have been addressed with Code Insight's support for CORS. See Addendum: Enabling Cross-Origin Resource Sharing.
SCA-31833	Log now reporting the deletion of the correct root file when a project is deleted.
SCA-32069	False positive security vulnerabilities no longer reported for the "delegate" component.
SCA-32381	Previously missing Cache-Control response header now included in .png and .json requests to prevent caching.

Table 3 • Resolved Issues (cont.)

Issue	Resolution Notes
SCA-32391	Previously missing Content-Security-Policy HTTP response header now included in all requests.
SCA-32413	System Administrators unable to change a Project Contact/Owner using the Update Project or the Users REST API. This issue is addressed with the introduction of the Update Contact REST API. See New APIs.
SCA-32572	False positive security vulnerabilities no longer reported for modularized “lodash” components.
SCA-32623	The DOC Software license no longer being reported instead of the BSD 3-Clause license. The BSD 3-Clause license is now being reported.
SCA-32666	Dashboard now reflecting counts of remote files marked as reviewed.
SCA-32996	The Intel Open Source license no longer being reported instead of the BSD 3-Clause license. The BSD 3-Clause license is now being reported.
SCA-33038	False positive security vulnerabilities no longer reported for the “wrappy - npm” component.
SCA-33063	False positive security vulnerabilities no longer reported for the “@types/lodash” component.
SCA-33306	The response for the Fetch Evidences REST API no longer showing evidence merged from two projects whose scans are running simultaneously. Now evidence for only the specified project is returned.
SCA-33552	False positive security vulnerabilities no longer reported for the “generex” component.
SCA-33553	False positive security vulnerabilities no longer reported for the “jandex” component.

Deprecated Functionality

The following Code Insight and related functionality has been deprecated.

CVE-Feed APIs (1.0) Deprecated/Discontinued by NVD

Code Insight relies on feeds from the National Vulnerability Database (NVD) to obtain the latest CVE information. Recently, NVD switched the feed version from 1.0 to 2.0. In Code Insight 2020 R4, updates were made to accommodate the schema changes incurred by the switch.

To ensure your Code Insight instance obtains the latest security vulnerability information, you must migrate to Code Insight 2020 R4 or later.

Known Issues

The following are current known issues in Code Insight. The issues are organized as follows:

- All-Project Inventory View
- Automated Workflow for Inventory Review/Publication
- Export and Import
- Installation and Configuration
- Manual Codebase Analysis
- Performance
- Project Administration and Management
- Project Inventory Review
- Project Reporting
- REST APIs
- Scan Agent Plugins
- Scanning and Automated Discovery
- Source Control Management (SCM) Support
- Web UI

All-Project Inventory View

The following are known issues in the **Inventory** view, which shows inventory across all Code Insight projects.

SCA-34403: Inventory details slide-out panel opening twice

When a user clicks an inventory item in the **Inventory** view, the panel showing the inventory's read-only details appears briefly on the right side of the view and then properly slides out from the right.

Workaround: None exists.

Automated Workflow for Inventory Review/Publication

The following are known issues with the automated workflow for inventory review and publication in Code Insight.

SCA-11193: Incorrect URL(s) in email notifications

In cases where Code Insight is running on a server that uses multiple IP addresses (for example, a server that has both a wired and wireless active network connection), the Core Server address cannot be accurately resolved. As a consequence, users can encounter an incorrect URL in the email notification received from Code Insight. This issue is most often seen if the Code Insight core server is configured as “localhost” instead of a full IP address.

Workaround: None exists.

Export and Import

The following are known issues with the Code Insight project export and import functionality.

SCA-3222: Import overrides inventory details

Importing the same inventory into a project that already contains inventory can cause some details to be overwritten or blanked out. If duplicate inventory (by associated repository item ID) is encountered during the import process, inventory details are overwritten with data from the export data file.

Recommended: Perform an export of the project prior to importing into the project in case you need to return to the original project state.

SCA-21295: Import of Detection Notes over 16 MB generates an error

When Code Insight uses a MySQL database, an error can occur during a project import if the source project’s **Detection Notes** content exceeds 16 MB. The import process generates an error message and continues processing the inventory but does not import the notes.

Workaround: Ensure that only a single network interface controller is enabled on the core server running Code Insight. As an added measure, configure the core server using a numerical IP address instead of a “localhost”.

Installation and Configuration

The following are known issues with Code Insight installation and configuration.

SCA-15952: Installer unable to install embedded JRE on some Windows 10 instances

Running the installer on some (but not all) Windows 10 systems results in an “Installation: Successful null” message and does not completely populate the `<INSTALL_ROOT>\jre` directory.

Workaround: Should you encounter the above error, install the JRE manually. Download JRE 8u192 here. Configure the JAVA_HOME and JRE_HOME variables in `catalina.*` to point to the newly installed JRE.

SCA-1652 / SCA-5812: Deleted or disabled users are still visible in the Web UI

Users who are deleted from the LDAP server or disabled in LDAP still appear on the **Users** page in the Code Insight Web UI and in some selection lists, such as for projects.

Workaround: None exists. However, deleted or disabled users are blocked from logging into the application and attempting to add one of these users will results in an error.

If this workaround is not sufficient or doable, contact Revenera Support for information about executing a database SQL script that can help to complete the index process within the expected time. The script must be run *before* the Electronic Update is started. (To contact Revenera Support, access the **Get Support** menu in the Revenera Community at https://community.revenera.com.)

Manual Codebase Analysis

The following are known issues with manual codebase analysis in the **Analysis Workbench** in Code Insight.

SCA-27011: Advanced Search based on low confidence inventory not working

In the **Analysis Workbench**, an **Advanced Search** for files associated with inventory that has a low confidence level is returning incorrect or no results.

Workaround: None exists.

SCA-22398: Licenses not highlighted even though evidence exists

Cases can occur during a scan when a license is discovered in the scan results and listed on the **Evidence Summary** tab, but no associated license text is highlighted on the **Partial Matches** tab. The lack of highlighting occurs because the scanner is unable to calculate the offsets for license text in the file.

Workaround: None exists.

SCA-22308: “Email/URLs” evidence truncated

In some cases after running a scan, the **Email/URLs** evidence on the **Evidence Details** tab in **Analysis Workbench** is truncated.

Workaround: None exists.

SCA-10414: Associated files not displayed when user adds more than 37K files to inventory

When more than 37K files are added to an inventory item, the associated files are not displayed on the **Associated Files** tab.

Workaround: Right-click the inventory item and select **Show Inventory Files**. The content on the **File Search Results** pane in **Analysis Workbench** is filtered to the associated files for the inventory item.

Performance

The following are known issues with Code Insight performance.

Performance slower with MySQL 8 than with MySQL 7

Codebase scans and updates to the Code Insight data library are slower when Code Insight uses the MySQL 8 (5.8) database compared to when it uses MySQL 7 (5.7).

Project Administration and Management

The following are known issues with project administration in Code Insight.

SCA-20012: File filters in Chrome and Edge browsers not showing supported upload archive types correctly

When selecting a codebase archive to upload from File Upload dialog, the file filter on the browser you are using might list the supported archive types properly:

- On the Chrome browser, the file filter list incorrectly shows “Custom Files” instead of “Supported Files” and does not allow you to filter on the individual supported archive types.
- On the Edge browser, the file filter list shows unsupported archive types.

Workaround: None exists.

Project Inventory Review

The following are known issues with Code Insight project inventory.

SCA-11520: Policies not applied on rescan of a project

The triggering event for applying policy to project inventory is “Publish” (not scan). Policies are applied during the initial scan if the default setting **Automatically publish system-created inventory items** is enabled and not applied during a rescan because inventory is not re-published. This behavior is in place to avoid inadvertent overriding of inventory status due to a change in policy by another user.

Workaround: To apply policy, first recall all inventory and rescan with **Automatically publish system-created inventory items** enabled.

Project Reporting

The following are known issues with Code Insight reporting.

SCA-22054: Project Report not showing URLs for custom vulnerabilities

The Project report is not showing the NVD (National Vulnerability Database) URLs for custom vulnerabilities until they are updated to the Data Library.

Workaround: Use the Web UI to view all vulnerabilities associated with inventory.

SCA-11263: Project Report hyperlink on tasks worksheet for inventory does not work

Clicking on an inventory link in the Project Report takes the user to the login page even if user is currently logged in. This is a bug in Excel.

Workaround: Log into the application. Go back to the Excel report output and click on the hyperlink again. This is an issue only for inactive sessions.

REST APIs

The following are known issues with the Code Insight REST interface.

SCA-16508: Swagger page hangs when required API parameters are missing

Instead of producing an appropriate error message, a Swagger page can hang when you attempt to execute an API without providing required parameters.

Workaround: None exists.

SCA-7950: Page and size parameters are not working with some REST APIs

Limiting the result set returned by some REST APIs is not currently supported. Using the page and size parameters with the Component Lookup and Get Project Inventory APIs (and possibly others) returns the full result set.

Workaround: None exists. However, the issue will be addressed in an upcoming release.

Scan Agent Plugins

The following are known issues with Code Insight scan-agent plugins.

SCA-28141: Maven, Ant, and Gradle scan-agent rescans might fail in dynamic host environments

Rescans performed by Maven, Ant, and Gradle scan-agent plugins v2.0 (introduced in Code Insight 2020 R3) might fail in dynamic host environments. This is due to a v2.0 requirement that rescans use the same scan-agent alias and hostname used in the previous scan. This will be addressed in a future release.

Workaround: Use the Jenkins scan-agent or the scan-agent for another CI tool that supports the “host” property. This property enables you to provide a user-defined hostname that does not change between scans.

SCA-27678: Possible deadlocks with parallel agent scans on same project

Deadlocks might occur when at least one scan-agent scan and one or more other scans (agent or server) run simultaneously on the same project.

Workaround: Scans can be scheduled in sequence to avoid deadlock exceptions.

SCA-27431: Dependencies currently not reported for Maven and Gradle scan agents

Previous versions (1.*x*) of the Maven and Gradle scan-agent plugins scanned both the dependencies section *and* the project build directory of the Maven or Gradle application project. However, version 2 of the plugins, introduced in Code Insight 2020 R3, scans the project build directory, but not the dependencies section. Thus, dependencies are currently not reported for scans performed by the two plugins.

Workaround for Maven: Refer to the Maven documentation for instructions on how to include dependencies as a part of build directory. An example install command for including dependencies might be:

```
maven-dependency-plugin install copy-dependencies ${project.build.directory}/project-dependencies
```

Workaround for Gradle: Refer to the Gradle documentation for instructions on how to include dependencies as a part of build directory. An example install command for including dependencies might be:

```
task copyToLib(type: Copy) { into "$buildDir/output/lib" from configurations.runtime }
```

You would then use the following command to run the scan agent from the Gradle application project:

```
gradle build copyToLib code-insight-scan
```

SCA-3378: Jenkins scan-agent plugin – downgrade not supported

After a Jenkins plugin upgrade, a downgrade button option is available in the Web UI. Clicking on the option results in a 404 error.

Workaround: None exists.

Scanning and Automated Discovery

The following are known issues with Code Insight codebase scans and the detection techniques used by scans.

SCA-33465: Scan agent inventory results impacted when CODEINSIGHT_ROOT variable set to wrong path

A scan agent can produce different inventory count results when the CODEINSIGHT_ROOT variable is set as environment variable and defined with an incorrect path compared to when the variable is set to the correct path or simply not used as an environment variable. (The scan agent does not require CODEINSIGHT_ROOT to be set as an environment variable.)

Workaround: If you are running the scan agent on the same machine as Code Insight Core Server, determine whether CODEINSIGHT_ROOT has been set as environment variable. If it has, ensure that it points to the correct path. Otherwise, do not set CODEINSIGHT_ROOT as an environment variable.

SCA-31486: Scan status not immediately in effect after “Stop Scan” issued

Currently, when a user forces a currently running scan to stop (for example, by clicking **Stop Scan** from the project **Summary** tab or the global **Scan Queue** dialog), the stopped status for the scan might not take effect immediately, even after a screen refresh.

Workaround: None exists.

SCA-30756: Increased scan times for some codebases when NG-bridge data update facility is enabled

In cases where the instance on which the Code Insight Scan Server is running has the NG-bridge data update facility enabled, the scan is able to identify more exact-file matches. However, increased matching can also cause the scan and rescan times to increase for certain codebases. This increased time can be a problem for some sites.

Workaround: Disable the NG-bridge data update facility. (Note that this facility is initially disabled by default.)

SCA-30423: Scans with large number of source-code matches resulting in longer scan times

When project is scanned with the Comprehensive scan profile or a custom scan profile, either of which has source-code matching enabled, the scan takes longer than usual if it encounters a large number of matches.

Workaround: None exists.

SCA-30205: Re-uploading codebase causing scan issues

When you re-upload a codebase that contains a folder with the same name and path as a previously uploaded and scanned file, the already scanned file is not deleted. When you rescan the codebase, the number of scanned files seems to include the folder as a file.

Workaround: Rename the folder to a name different from the name of the already uploaded and scanned file.

Inventory automatically published during previous scan now unpublished after rescan

To address issues, Code Insight now assigns a confidence level of **Low** to those inventory items that are identified by a file-name analyzer technique (a part of automated analysis) during a scan. If your project is configured to publish inventory with **Medium** or **High** confidence, inventory detected by this technique will now have an automatic unpublished status. This change is applicable only for new scans.

Workaround: The previously published inventory items are still available. In the **Analysis Workbench**, simply filter inventory by **Not Published** to view the unpublished inventory, and then publish inventory as needed.

SCA-26486: Conda first-level dependencies with Semantic versions not resolved

Semantic versions for Conda first-level dependencies are not being resolved.

Workaround: None exists.

SCA-7820: Some NPM version patterns are not supported

When scanning an NPM project, certain versions might not be detected through automated analysis. The following are not supported: URLs as dependencies, versions containing a hyphen (for example, `"crypto-js": "3.1.9-1"`), and versions of the format X.X.X (for example, `"through": "X.X.X"`).

Workaround: None exists.

SCA-3000: Scan agent plugins might generate inventory with no selected license

In this release, using the scan agent plugin, you might end up with inventory that has no license associated with it if the scan agent is not able to identify a specific license in the scanned files. In this case, the inventory item is created using Compliance Library data. You might see the inventory item with one or more possible licenses and potentially no selected license.

Workaround: Recall the inventory item to prevent it from showing up in the published inventory items list.

Source Control Management (SCM) Support

The following are known issues with Code Insight SCM support.

SCA-30568: Significant space consumed by Perforce synchronization logs in Code Insight

When a user synchronizes a Code Insight project with a Perforce codebase by clicking **Sync Now** from any SCM instance tab, the synchronization automatically adds Perforce log data to the Tomcat logs in Code Insight. This behavior can result in large Tomcat log files.

Workaround: Synchronize Code Insight with the Perforce codebase directly through the Perforce command-line client installed on the Scan Server instance.

SCA-27751: Failure of Perforce SCM instance to synchronize Unicode files to Scan Server

Perforce SCM instances can fail to synchronize Unicode-formatted files to the Scan Server if the instance is running in Windows and configured for SSL.

Workaround: None exists.

SCA-27674: Synchronization with Team Foundation Server Failing (Linux only)

Codebase synchronization with a Team Foundation Server (TFS) instance on Linux fails when character spaces or certain special characters exist in attributes used to set up the synchronization on the **Version Control Settings** tab for a project.

The following issue has been logged with TFS:

https://github.com/microsoft/team-explorer-everywhere/issues/321

Workaround: None exists.

Web UI

The following are known issues with the Code Insight Web UI.

SCA-27892: Project Dashboard showing incorrect format after report generation for agent scans

If only a scan agent has performed a remote scan for a project and a report is subsequently generated for the project, the project Dashboard is showing a split **Scan Summary** pane with scan statistics for both the scan agent and the scanner (which shows statistics of 0 since it has run no scan). The **Scan Summary** should not be split; the full pane should list statistics for the remote scan only.

SCA-21917: Last Server Scan field on dashboard showing date of report generation

The **Last Server Scan** value on the **Project Dashboard** should show the date of the last scan. However, when a report is generated, this date changes to the report-generation date.

Workaround: Obtain the last scan date from the scan history link (in the **Past Server Scans** field) on the project **Summary** tab.

SCA-20683: Project details not automatically updating after scan

Project details are not automatically updating after a scan in the Web UI.

Workaround: Refresh the screen.

Addendum: Enabling Cross-Origin Resource Sharing

Note ▪ *The following content describing functionality introduced in Code Insight 2021 R2 was not included in the 2021 R2 user documentation. However, it will be made a available as part of the user documentation at a future date.*

CORS (Cross-Origin Resource Sharing) is an HTTP-header-based tool that allows secure cross-origin requests and data transfers between browsers and servers. Cross-origin situations occur when the Web location from which a request originates is different from the Web location of the server to which the request is sent. Cross-origin locations can differ in scheme (HTTP or HTTPS), domain (such as `mylocation.com` versus `yourlocation.com`), or port.

For example, if you have created a script or application that makes Code Insight REST API calls, these calls will most likely result in errors if the script resides at a Web location different from Code Insight Core Server web location.

To enable a secure, successful exchange of requests and responses in a cross-origin scenario, you need to set up a CORS filter on the Code Insight Core Server. This filter identifies the origins (clients) from which the Core Server (server) will accept requests and specifies the types of headers and HTTPS methods that the server will support in the requests.

The following sections describe how to configure the CORS filter:

- Configuring the CORS Filter
- CORS Initialization Parameters
- Identifying Origins for the cors.allowed.origins Initialization Parameter
- About HTTP Headers

Configuring the CORS Filter

By default, the CORS filter is not configured on the Code Insight Core Server. To configure the filter, you must add the following code snippet to the `Built-in Filter Mappings` section in the `<codeInsightInstallation>/tomcat/conf/web.xml` file. See CORS Initialization Parameters for more information about the filter parameters.

Once you have configured the CORS filter, you must restart the Core Server.

```
<filter>
        <filter-name>CorsFilter</filter-name>
        <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
        <init-param>
            <param-name>cors.allowed.origins</param-name>
            <param-value>*</param-value>
        </init-param>
        <init-param>
            <param-name>cors.allowed.methods</param-name>
            <param-value>GET,POST,HEAD,PUT,DELETE,OPTIONS,PATCH</param-value>
        </init-param>
        <init-param>
            <param-name>cors.allowed.headers</param-name>
            <param-value>Access-Control-Allow-Origin,Access-Control-Request-
Method,Authorization,Content-Type</param-value>
        </init-param>
        <init-param>
            <param-name>cors.preflight.maxage</param-name>
            <param-value>86400</param-value>
        </init-param>
    </filter>
    <filter-mapping>
        <filter-name>CorsFilter</filter-name>
        <url-pattern>/api/*</url-pattern>
    </filter-mapping>
```

CORS Initialization Parameters

The following provides more information about the initialization parameters used to define in the CORS filter set up for use by Code Insight. These parameters can be adjusted for Code Insight installed at your site.

Table -1 ▪ CORS Initialization Parameters

Initialization Parameter	Definition

`<filter>`
`<filter-name>CorsFilter</filter-name>`
`<filter-class>`
`   org.apache.catalina.filters.CorsFilter`
` </filter-class>`
` </filter>`
` ...`
` <filter-mapping>`
` <filter-name>CorsFilter</filter-name>`
` <url-pattern>/*</url-pattern>`
` </filter-mapping>`
	The basic code that enables the CORS filter. The filter adds the appropriate `Access-Control-*` headers to responses and issues the 403 return code when a request is invalid or not permitted.

`cors.allowed.origins`	The origins (clients) whose requests the server will accept. For security purposes, you should replace the asterisk * value (shown for this parameter in the code snippet provided in Configuring the CORS Filter) with the URL for each specific origin accepted by the server. For details, see Identifying Origins for the cors.allowed.origins Initialization Parameter.
`cors.allowed.methods`	The HTTP methods that are allowed in cross-origin requests to access Code Insight data. The value in the provided code snippet (see Configuring the CORS Filter) permits all methods, but you can adjust this list according to your site's requirements. (The default methods include GET, POST, and HEAD.) ***Note** ▪ The HEAD method is used to retrieve only headers from the server, similar to a GET but with no message body returned.* The listed methods are included as part of the `Access-Control-Allow-Methods` header in the pre-flight response so that the client knows which methods are allowed.

Table -1 ▪ CORS Initialization Parameters (cont.)

Initialization Parameter	Definition
`cors.allowed.headers`	The HTTP request headers allowed in actual requests. Be sure to include the `Authorization` header, which is required for Code Insight REST API calls. Additionally, for POST or PUT requests, the `Content-Type` header needs to be passed along with `Authorization` header. The headers specified here are returned as part of the `Access-Control-Allowed-Headers` header in the server's response to a pre-flight request, informing the client which headers are allowed in requests.
`cors.exposed.headers`	(Not shown in the code snippet) The specific headers that can be exposed to the client as part of the response, enabling the client to then use these headers. These headers are returned as part of the `Access-Control-Expose-Headers` header in the Core Server's response to a pre-flight request.
`cors.preflight.maxage`	The maximum number of seconds that the results of the pre-flight request can be cached. (The results include the information contained in the `Access-Control-Allow-Methods` and `Access-Control-Allow-Headers` headers.) The provided code snippet (see Configuring the CORS Filter) uses the value 86400, representing 24 hours, but you can adjust this value as needed. The CORS default value is 1800.

Identifying Origins for the cors.allowed.origins Initialization Parameter

The `cors.allowed.origin` parameter, used to configure the CORS filter, identifies the clients (origins) that are allowed to issue requests to the server. The code snippet provided in Configuring the CORS Filter shows an asterisk * as the value for this parameter, indicating that a request can come from any origin. For security purposes, this value should be set to the one or more specific request origins that the server supports.

Defining an Origin

Use the following format for each origin added:

```
Origin: <scheme> "://" <hostname> [ ":" <port> ]
```

Note the following:

- Use all lower case in the URL. The value is case-sensitive.
- Be sure to include the port number, as it is required. However, you do not have to include the port number if it is known to be configured as part of host name.

- The host name can be the fully qualified domain name (FQDN).
- When specifying multiple origins, separate them with commas, as in this example:

  `Origin: http://www.machine123.org:8080, http://www.machine1000.smc.com:8080`

Example Origin Formats

The following are examples of origin formats:

- `http://www.w3.org` (port known to be configured with hostname)
- `https://www.apache.org` (port known to be configured with hostname)
- `http://www.abc.domain.com` (port known to be configured with hostname)
- `http://<origin_Machine_hostName>:8080`
- `https://<FQDN(fully_qualified_domain_name)>:8080`
- `http://<origin_host_IP_address>:8080`

About HTTP Headers

The following table provides information about some of the HTTP headers used in requests and responses.

Table -2 ▪ HTTP Headers

Header	Type	Definition
`Access-Control-Request-Method`	Request	Used by browsers when issuing a pre-flight request inform the server which HTTP method will be used when the actual request is made.
`Origin`	Request	Identifies the URL from which the request originated.
`Access-Control-Request-Headers`	Request	Used by browsers when issuing a pre-flight request to inform the server which HTTP headers the client intends to send in the actual request. The server's response to this header is the `Access-Control-Allowed-Headers` header, informing the client which headers are allowed in the request.
`Access-Control-Allow-Origin`	Response	Indicates that the origin of the request can access the response. If the origin is not permitted to send the request, a 403 code is returned for a pre-flight request, while an actual request fails with a CORS error.

Legal Information

Copyright Notice

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 Software, see https://www.revenera.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera Software 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.