

Code Insight 2024 R1 Release Notes

February 2024

Introduction	2
About Code Insight	2
Revenera Resources	2
New Features and Enhancements	3
Advanced Inventory Searches	3
Automated Workflow for Inventory Publication and Review	3
Components and Licenses	4
Data Library, Library Refreshes, and Electronic Updates	5
Jobs Queue	6
Installation, Upgrades, and Configuration	7
Project Inventory	7
Project Management	10
Scanning and Automated Discovery	11
REST API Enhancements	11
New APIs	11
Updates to Existing APIs	11
Resolved Issues	14
Migration and Installation Notes	15
Known Issues	16
All-Project Inventory View	17
Automated Workflow for Inventory Publication and Review	17
Custom Detection Rules	18
Data Library, Library Refreshes, and Electronic Updates	18
Export and Import	21
Installation, Upgrades, and Configuration	21
Inventory History	23
Manual Codebase Analysis	23
Performance	25
Project Inventory	25
Project Management	25
Project Reporting	27
REST APIs	27
Scan Agent Plugins	28
Scanning and Automated Discovery	32
Source Code Management (SCM) Support	35

Vulnerability Suppression/Unsuppression	37
Web UI	38
Code Insight Security Issues	38
Legal Information	39

Introduction

These Release Notes provide the following information about the Code Insight 2024 R1 release:

- [About Code Insight](#)
- [Reverera Resources](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Migration and Installation Notes](#)
- [Known Issues](#)
- [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.

Reverera Resources

The following resources can help you stay up to date with Code Insight news and product knowledge:

- In addition to providing case management, the [Reverera Community](#) site can help you 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 Reverera's product solutions, you can access forums, blog posts, and knowledge base articles.
- You can find documentation for Code Insight and all other Reverera products on the [Reverera Product Documentation](#) site.
- The [Reverera Learning Center](#) offers free, self-guided online videos to help you quickly get the most out of your Reverera products. You can find a complete list of these training videos in the Learning Center.
- 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 [Reverera Community](#).

New Features and Enhancements

The Code Insight 2024 R1 release and its subsequent service packs offer new features and enhancements in the following areas:

- [Advanced Inventory Searches](#)
- [Automated Workflow for Inventory Publication and Review](#)
- [Components and Licenses](#)
- [Data Library, Library Refreshes, and Electronic Updates](#)
- [Jobs Queue](#)
- [Installation, Upgrades, and Configuration](#)
- [Project Inventory](#)
- [Scanning and Automated Discovery](#)
- [REST API Enhancements](#)

Advanced Inventory Searches

The following enhancements to the Advanced Inventory Search feature are now available. This feature is available on the **Project Inventory** tab, in the **Analysis Workbench**, and in the **Inventory View**. (For complete information refer to “Advanced Inventory Search Dialog” in the *Code Insight User Guide*.)

New “Created by” Filter

The new **Created By** criterion on the **Advanced Inventory Search** dialog enables users to filter inventory by the type of value entered in the inventory item’s **Created By** field. The user can select one of three options to define the filter:

- **Any**—Show all inventory no matter the value of an inventory item’s **Created By** field.
- **Users**—Show only inventory that has been manually created by users.
- **System**—Show only inventory generated automatically by Code Insight.

The new filter is available for an Advanced Inventory Search from the **Project Inventory** tab, **Analysis Workbench**, and the global **Inventory** view.

For complete information, refer “Advanced Inventory Search Dialog” in the *Code Insight User Guide*.

Automated Workflow for Inventory Publication and Review

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

Automatic Inventory Review by Policy

Code Insight offers a set of policy criteria that automatically review an inventory item to determine an **Approved**, **Rejected**, or **Not Reviewed** status for the item. Previously, this automatic review took place whenever an inventory item was published manually or automatically by the system. Starting in this release, automatic reviews of published inventory also take place when any of these events occur:


- The component version, license, or any usage properties for an inventory item are updated and saved. See [Automatic Review by Policy After Editing Published Inventory](#) in this document.
- An inventory item is created on the **Project Inventory** tab. See [Automatic Review by Policy When Saving New Inventory on the Project Inventory Tab](#) in this document.
- A Code Insight project reviewer runs an **Apply Policy - Project** job across inventory in the project. See [Forced Automatic Review by Policy Across All Published Inventory in a Project](#) in this document.
- A Code Insight policy manager runs an **Apply - Global** job across inventory in all projects associated with a given policy in the Code Insight instance. See [Forced Automatic Review by Policy Across Published Inventory in All Projects](#) in this document.

Components and Licenses

The following enhancements to component and license information in the Code Insight database and Data Library are now available.

Ability to Edit Custom Components in Global Component & License Lookup

Users can now edit custom components when searching components from the Global Component & License Lookup feature. A user simply locates the custom component in the Lookup list, and clicks the associated **Edit** button (shown below) to update the component from a pop-up window. (Only custom components are associated with an **Edit** button.)

Global Component & License Lookup				
<div>Components Licensess</div>				
Search By: <input checked="" type="radio"/> Keyword <input type="radio"/> URL <input type="radio"/> Forge <input type="radio"/> Component ID				
Keyword: componentOne			Search	Create New Component
Component Name ↑	Forge	URL	Possible License(s)	Actions
① a259937-componentone	GitHub	https://github.com/a259937/ComponentOne		📄
① componentone_studio_enterprise_2012_v2_...	npm	https://www.npmjs.com/package/componentone_...		📄
① componentone_studio_for_activex_2010_v3_...	npm	https://www.npmjs.com/package/componentone_...		📄
① componentone_studio_for_activex_2010_v3_...	npm	https://www.npmjs.com/package/componentone_...		📄
① componentone_studio_for_winforms_2010_v...	npm	https://www.npmjs.com/package/componentone_...		📄
① componentone-webmarket-appl	Other	http://c1webmarket.componentone.com/c1webm...		📄
① impossibleCustomComponentOne	Other	NA		📄 
① react-native-test-componentonetwothree	npm	https://www.npmjs.com/package/react-native-test...	① ISC License	📄



Note - In previous releases, a **Versions** column was displayed on the **Components** tab in Global Component & License Lookup. This column has now been replaced with the **Actions** column (show in the above screenshot), which includes icons that enable users to view component versions and edit the component.

Once you successfully save the edits to the custom component, the search is automatically filtered to the component for your convenience. For complete information, refer to “Editing a Custom Component” in the *Code Insight User Guide*.

New Property Indicating “custom” Licenses in License Lookup APIs

The License Lookup APIs now include a new **custom** property indicating whether the license was manually created (**true**) or not (**false**). See [Updates to Existing APIs](#).

Data Library, Library Refreshes, and Electronic Updates

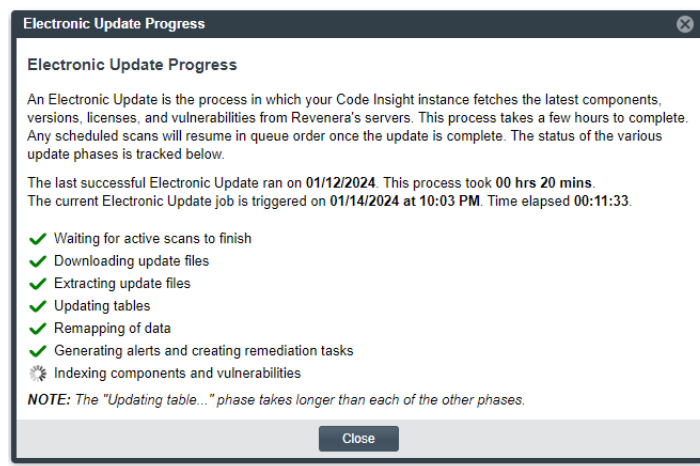
New Feature to Monitor the Progress of an Electronic Update Phase by Phase

As in previous releases, whenever an Electronic Update is running, a notification message is displayed in the header of the Code Insight user interface, indicating that an update is in progress. This notification message has now been enhanced to include a link that opens an **Electronic Update Progress** pop-up window, enabling users to track the progress of each phase of the update.



This window lists the phases of the update in sequential order, and, as each phase completes, it is marked with a green check. The window also provides the following information:

- The start date of the Electronic Update and its current elapsed time.
- The date on which the last successful Electronic Update was run and its total execution time. If no successful update has run previously, this line of information is not displayed on the window.



The window tracks phases for both server and local Electronic Updates. For complete information, refer to the following sections in the user documentation:

- “Tracking the Progress of an Electronic Update” in the *Code Insight Installation & Configuration Guide*
- “Monitoring the Progress of Electronic Update Phases” in the *Code Insight User Guide*

Jobs Queue

The following enhancements to the Code Insight **Jobs** queue are now available. (For complete information about the queue, refer to “Monitoring the Code Insight Jobs Queue” in the *Code Insight User Guide*.)

- [Job Types and Filters Added for the Applying Policy at the Project and Global Levels](#)
- [New Filter by Scan Server](#)
- [Improved Queue Management of Multiple Project Copy Jobs](#)

Job Types and Filters Added for the Applying Policy at the Project and Global Levels

Two features introduced in this release run as jobs in the **Jobs** queue.

Job Type of Feature	Feature Description
Apply Policy - Project	Applies current review policy associated with a specific project across all inventory in the project. See Forced Automatic Review by Policy Across All Published Inventory in a Project in this document.
Apply Policy - Global	Applies the selected review policy across inventory in all projects associated with the policy in the Code Insight instance. See Forced Automatic Review by Policy Across Published Inventory in All Projects in this document.

You can filter the **Jobs** queue by either of these new job types.

New Filter by Scan Server

You can now filter the **Jobs** queue to one or more of the Scan Server aliases (including disabled Scan Servers) listed in the **Scan Server** column. You cannot filter using the **N/A** (Core Server) value.

Scan Server	Triggered By	Queued On
N/A	Sort Ascending	01/19/2024 at 12:00 AM
N/A	Sort Descending	01/18/2024 at 12:00 AM
N/A	Columns	01/18/2024 at 12:00 AM
N/A	Filters	Scanner1 at 11:00 PM
N/A	admin	Scanner2 at 10:59 PM
N/A	admin	01/17/2024 at 10:59 PM
N/A	admin	01/17/2024 at 10:59 PM
N/A	admin	01/17/2024 at 10:59 PM

For complete information, refer to “Filtering the Jobs Queue by Column” in the *Code Insight User Guide*.

Improved Queue Management of Multiple Project Copy Jobs

In previous releases, when a **Project Copy** job was in progress or scheduled, a user could not trigger another **Project Copy** job for the same or another project.

Now, **Project Copy** jobs for the same and other projects can exist in the **Jobs** queue concurrently. The first copy job triggered will be the first one placed in **Active** state. The remaining copy jobs triggered continue in a **Scheduled** state and are run based on the appropriate queue order.

Installation, Upgrades, and Configuration

The following enhancements have been added to the Code Insight installation, upgrade, or configuration experience.

Support for Forcing SSO Authentication

You can now force SSO authentication when users access Code Insight through SSO. This enforcement is enabled through a new property called `force.sso.authentication` in the `PAS_GLOBAL_PROPERTIES` table in the Code Insight database.

By default, this option is disabled. However, the option should be enabled if Code Insight is configured for Microsoft Azure SSO and in situations where users receive the message “Error Validating SAML” after attempting to log in through SSO.

For complete information, refer to “Option to Force Authentication with SSO” in the *Code Insight Installation & Configuration Guide*.

Code Insight Support for Signing SAML Requests

In an SSO environment, Code Insight can now be configured (as the Service Provider) to sign all SAML requests sent to the Identity Provider. In general, this configuration is optional when setting up Code Insight for SSO. However, it might be necessary if your organization’s security policy requires such a signature.

For the steps needed to perform this configuration, refer to “(Optional) Configuring Code Insight to Sign SAML Requests” in the *Code Insight Installation & Configuration Guide*.

Tomcat Upgrade

Code Insight has updated its Tomcat version to 9.0.84 to address security vulnerabilities associated with the previous 9.0.80 version used by Code Insight.

Project Inventory

The following enhancements to the project inventory are now available.

- [Automatic Review by Policy After Editing Published Inventory](#)
- [Automatic Review by Policy When Saving New Inventory on the Project Inventory Tab](#)

- [Forced Automatic Review by Policy Across All Published Inventory in a Project](#)
- [Forced Automatic Review by Policy Across Published Inventory in All Projects](#)
- [Package URL Property Now Listed for Inventory](#)
- [Additional New Fields Added to Project Inventory Details](#)
- [Inventory Priority Now Editable Through “Update Inventory” API](#)

Automatic Review by Policy After Editing Published Inventory

An automatic policy review is now triggered for a published inventory item when you click **Save** after updating the item's component, license, or usage properties.

During the review, the review policy criteria defined for the project associated with the inventory item is applied to the item. If the inventory item meets at least one of the criteria, its current **Review Status** value is overwritten with an **Approved** or **Rejected** status. If the item meets no policy criteria, its status remains as is.

Additionally, if the current **Review Status** value of the inventory item was manually set, users are given the option *not* to perform the review so that the status is not overwritten.

This feature applies to published inventory on the **Project Inventory** tab and in the **Analysis Workbench**. An overwritten status in one location is reflected in the other location.

For complete information, refer to “Editing Inventory from the Analysis Workbench” or “Editing Inventory from the Project Inventory Tab” in the *Code Insight User Guide*.



Note - An automatic review is also performed when you edit specific inventory properties (as described above) using the **Update inventory** REST API. See [Updates to Existing APIs](#).

Automatic Review by Policy When Saving New Inventory on the Project Inventory Tab

An automatic policy review is now triggered whenever you create an inventory item from the **Project Inventory** tab. (The item is automatically saved as a published item.)

During the review, the review policy criteria defined for the project associated with the inventory item is applied to the item. If the item meets at least one of the criteria, its **Review Status** value is assigned an **Approved** or **Rejected** status. If the inventory item meets no policy criteria, it is given a **Not Reviewed** status.

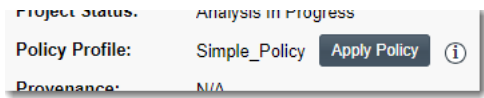
For complete information, refer to “Creating Inventory from the Project Inventory Tab” in the *Code Insight User Guide*.



Note - An automatic review is also performed when you create an inventory item using the **Create inventory** REST API. See [Updates to Existing APIs](#).

Forced Automatic Review by Policy Across All Published Inventory in a Project

A project reviewer can now force an automatic review of all published inventory in a given project based on the project's associated review policy profile. To initiate the review, the reviewer clicks the new **Apply Policy** button next to the **Policy Profile** field on a project's **Summary** page. (Clicking the **Information** icon next to the button shows the current review criteria defined for the policy profile.)



During the review, the project's review policy is applied to project inventory. If an inventory item meets at least one of the criteria, the item is assigned an **Approved** or **Rejected** status, overwriting the current status. The review status of those inventory items that meet no policy criteria remains as is. (Note that the user can configure the review *not* to overwrite any current status that was manually set for inventory.)

This feature provides a means to automatically apply changed policy criteria across inventory without having to wait for a scan or manually unpublish and re-publish inventory items individually to trigger a review.

























When triggered, the operation runs as an **Apply Policy - Project** job in the **Jobs** queue.

For complete information, refer to “Forcing an Automatic Review of All Inventory in a Project” in the *Code Insight User Guide*.

Forced Automatic Review by Policy Across Published Inventory in All Projects

A policy manager can now force an automatic review of published inventory across all projects currently associated with a given review policy profile. To initiate the review, the policy manager clicks the new **Apply Policy - Global** icon for the policy on the **Policy** page.

A screenshot of the Code Insight SCA Policy page. The page has a header with 'revenera | SCA' and a 'POLICY' tab. Below the header is a table with columns: Name, Description, Updated By, Updated On, and Actions. The table lists several policies, including 'shuttest', 'TestPolicy12', 'TestPolicy', 'Simple_Policy', and 'Default License Policy Profile'. The 'Simple_Policy' row is highlighted, and its 'Actions' column shows an 'Apply Policy' button and a 'Global' icon, which is circled in red. The 'Global' icon is a small square with a circle inside, and the 'Apply Policy' button is a small rectangle with the text 'Apply Policy'.

Name	Description	Updated By	Updated On	Actions
shuttest		shubha s	February 6, 2024 at 3:51 am	  
TestPolicy12		Trupti Sangpal	February 7, 2024 at 6:28 am	  
TestPolicy		Trupti Sangpal	February 6, 2024 at 9:09 pm	  
Simple_Policy		shubha s	January 31, 2024 at 10:05 am	  
Copy of Apply Policy - PProject-Trp		Trupti Sangpal	January 19, 2024 at 4:18 am	  
Apply Policy - PProject-Trp		Trupti Sangpal	January 18, 2024 at 8:44 am	  
Copy of Default License Policy Profile	This is a default license profile for shipped applications	Trupti Sangpal	January 18, 2024 at 5:55 am	  
Default License Policy Profile	This is a default license profile for shipped applications	shubha s	February 5, 2024 at 11:53 am	  

During the review, the **Review Status** value of those inventory items that meet at least one of the current policy criteria will be overwritten with an **Approved** or **Rejected** value, based on the criteria. The status of those inventory items that meet no policy criteria will remain as is.

This feature provides a way to automatically apply changed policy criteria across inventory without having to wait for a scan or manually unpublish and re-publish inventory items individually in order to apply the changed policy.

When triggered, the operation runs as an **Apply Policy - Global** job in the **Jobs** queue.



Important - Currently the feature is available for only Code Insight instances that use the MySQL database. Also, no option is currently available to skip overwriting any review status that was manually set for inventory.

For complete information about this feature, refer to “Forcing an Automatic Review of Inventory Across All Projects” in the *Code Insight User Guide*.

Package URL Property Now Listed for Inventory

The **purl** property has been added to inventory details on the **Project Inventory** tab and in the **Analysis Workbench** to display the package URL for the component represented by the inventory item.

This read-only value is retrieved from the Code Insight data library and is applicable to only those components associated with a non-custom version. If no package URL is available for the component in the data library or the component has a custom version, the value for this field is **N/A**.

This property is also available in certain API responses. See [Updates to Existing APIs](#).

Additional New Fields Added to Project Inventory Details

The following new properties have been added to the details for a given inventory item on the **Project Inventory** tab:

- **Created By**—Designates either **System** (for an inventory item that was automatically generated by a Code Insight scan) or, for a manually created inventory item, the first and last name of the user who created the item.
- **Created On**—The date and time that the inventory item was created.
- **Updated On**—The date and time that the inventory item was updated. If the item has not been updated since its creation, this value will be the same as the **Created On** value.

Inventory Priority Now Editable Through “Update Inventory” API

The **priority** property for an inventory item can now be updated through the **Update inventory** API. See [Updates to Existing APIs](#). Previously you could do so only through the Code Insight user interface.

Project Management

The following enhancements to Code Insight project management are now available.

Triggering of Multiple Project Copy Jobs Now Allowed

More than one **Project Copy** job can now be queued concurrently in the **Jobs** queue. For more information, see [Improved Queue Management of Multiple Project Copy Jobs](#) in this document.

Forced Automatic Review Across Inventory

A project reviewer can now force an automatic review of all published inventory in a given project based on the project’s associated review policy profile. For more information, see [Forced Automatic Review by Policy Across All Published Inventory in a Project](#) in this document.

Scanning and Automated Discovery

This release includes the following enhancements to Code Insight scans and the Automated Analysis techniques used to discover and report inventory during scans.

Support for Reporting Inventory Found in RPM Spec Files

Code Insight scans now reports top-level inventory found in RPM .spec files. For complete information, refer to “Automated Analysis” in the *Code Insight User Guide*.

REST API Enhancements

This release includes the following changes to the Code Insight REST interface.

- [New APIs](#)
- [Updates to Existing APIs](#)

New APIs

No new APIs have been added in this release.

Updates to Existing APIs

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

Table 1 ▪ Updates to Existing APIs

Resource	API Name/Endpoint	Method	Function Change Description
Component	Component search /components/search	GET	The new purl property, showing the package URL, is now listed for each inventory item in the response. If no package URL is available for the inventory item, the value is N/A . See Package URL Property Now Listed for Inventory .
	Get component version details /components/versions/{id}		
	Get component /components/{componentId}		

Table 1 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
Inventory	Get the inventories of file/folder Ids /inventories/search	GET	The new purl property, showing the package URL, is now listed for each inventory item in the response. If no package URL is available for the inventory item, the value is N/A . See Package URL Property Now Listed for Inventory .
	Get details of an inventory /inventories/{inventoryId}		
	Create Inventory	POST	An automatic review by policy is triggered on the item once the item is created. See Automatic Review by Policy When Saving New Inventory on the Project Inventory Tab .
	Update inventory	PUT	<p>This API has been enhanced as follows:</p> <ul style="list-style-type: none"> • If inventory item's component, license, or any usage properties were edited, an automatic review by policy is triggered on the item once the update is complete. See Automatic Review by Policy After Editing Published Inventory. • Users are now able to update the priority property for a given inventory item. Possible values are P1 (highest), P2, P3, or P4 (lowest). <p>If the priority value is not updated, existing logic for automatically setting the priority is used. For example, a Work in Progress inventory item is, by default, set to P3. If the inventory item is updated to a component with critical or high confidenceLevel, the priority of the inventory item is automatically set to P1 in the user interface.</p>

Table 1 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
Jobs	Get jobs details based on filters /jobs	GET	Two new job types— Apply Policy - Project and Apply Policy - Global —have been added as available filters for setting up the request. The response includes either Apply Policy - Project or Apply Policy - Global for the jobType property if response was filtered on this value. For details, see Forced Automatic Review by Policy Across All Published Inventory in a Project and Forced Automatic Review by Policy Across Published Inventory in All Projects .
	Get job details based on the jobId provided /jobs/{jobId}		The response can now include one of the new job types— Apply Policy - Project or Apply Policy - Global —for the jobType property when applicable.
License	License lookup /licenses/lookup	GET	Responses now include a new custom property indicating whether the license was manually created (true) or not (false).
	License lookup based on short name /licenses/{shortName}		
Project API	Get Project Inventory /project/inventory/{projectID}	GET	The new purl property, showing the package URL, is now listed for each inventory item in the response. If no package URL is available for the inventory item, the value is N/A . See Package URL Property Now Listed for Inventory .
	Get Inventory Summary of the project /projects/{projectID}/inventorySummary		

Resolved Issues

The following issues were resolved in the Code Insight 2024 R1 release.

Issue	Description
SCA-11520	Review policies were not being applied as expected during rescans and other events. This has been resolved with the following new features that automatically apply policy: <ul style="list-style-type: none">• Forced Automatic Review by Policy Across All Published Inventory in a Project• Forced Automatic Review by Policy Across Published Inventory in All Projects
SCA-37347	Certain users (including Microsoft Azure SSO users) were receiving the message “Error Validating SAML” whenever they attempted to log in through SSO. This issue has been resolved with an enhancement that forces SSO authentication during login. See Support for Forcing SSO Authentication .
SCA-45800	A Copy Project operation that used (as its source) a codebase synchronized to Code Insight through a Subversion instance was creating two sets of codebase files on the target project. This issue has been resolved.
SCA-43625	Server shutdowns occurred when simultaneous custom-component indexing and searching were taking place. This issued has been fixed as part of the SCA-50663 resolution (shown later in this list).
SCA-49410	The README for the Audit Migration tool has been corrected to reflect the appropriate instructions for the latest version of the Migration tool.
SCA-50663	Performing multiple Edit or Add operations on custom components could cause the Code Insight Core Server to fail with a Java Runtime Environment error. This issue has been resolved.
SCA-50872	Previously, when a transitive scan was run on a codebase, dependency inventory for one or more specific packages in the codebase were not always not listed in scan results. (However, when a scan was run on an individual package, the dependencies were listed.) This issue has been resolved.
SCA-50947	When a user removed a dependency from a manifest file (or removed the file itself) in a codebase that had been scanned by a remote agent plugin, the results of a rescan could still show the inventory item and its associated file. This issue has been resolved.
SCA-51135	Previously, after a new ALM instance was saved on the ALM tab on the Administration page and the page then refreshed, the instance might no longer be visible on the tab nor be available for selection on the ALM Settings tab in projects. This issue has been resolved.
SCA-51393	The issue with a rescan not detecting inventory in a newly added manifest file has been resolved.
SCA-51424	Tomcat has been upgraded to version 9.0.84 to address security vulnerabilities associated with the previous version used by Code Insight. See also Tomcat Upgrade .

Issue	Description
SCA-51504	Rescanning two identical files in the same codebase could create duplicate inventory. This issue has been resolved by ensuring that a full rescan yields the same results a first-time scan. (However, an incremental rescan on identical files can still result in duplicate inventory.)
SCA-51609	Previously, the fact that Code Insight (as a Service Provider) did not sign SAML requests conflicted with the security policy of some customer organizations. Code Insight now supports the optional configuration to sign SAML requests sent to the Identity Provider. See Code Insight Support for Signing SAML Requests .
SCA-51631	Dependencies were not being reported from all manifest files during a scan on codebase synchronized to the Scan Server through a Git instance. This issue has been resolved.
SCA-51656	Scans did not complete due to an exception that occurred during the resolution of dependencies in the automated analysis. This issue has been resolved.
SCA-51659	Instructions for configuring Code Insight as a Windows service have been corrected in the “Running Code Insight as a Service” section of the <i>Code Insight Installation & Configuration Guide</i> .
SCA-51664	The Get project inventory and Get details of an inventory REST API no longer fail when inventory is associated with alerts that have no mapping to vulnerabilities.
SCA-51670	No error message was being produced when REST API failed due to the problem described in SCA-51664 (see the previous issue listed). The resolution of SCA-51664 fixed this issue as well.
SCA-51821	The Get Inventory Summary of the Project API has been enhanced to fetch the SPDX ID or short name for licenses.
SCA-51829	The TLS-version error that occurred when Code Insight attempted to send email notifications has been resolved.
SCA-52135	Instructions in the “Enabling an HTTPS Connection” section of the <i>Code Insight Installation & Configuration Guide</i> have been updated to reflect the correct Connector protocol information for the SSL certificate, as listed in the <code>server.xml</code> file.

Migration and Installation Notes

The following sections described special notes about the migration to (or installation of) Code Insight 2024 R1. This information is currently not in the 2024 R1 user documentation.

Enabling the Library Refresh

When the Library Refresh was introduced in Code Insight 2023 R3 SP1, it was enabled by default. In the 2023 R4 and later releases, the Library Refresh has been disabled by default. If you want to enable it after you have migrated to or installed the current release, use the following procedure. Once enabled, the Library Refresh runs daily at the time you configure during its enablement.



Task

To enable the Library Refresh, do the following:

1. Migrate to (or install) Code Insight 2024 R1.
2. Start the Tomcat server.



Note - This step is required. That is, you must successfully start Tomcat at least once at some point before you perform the configuration described in the Step 4. If you attempt to perform Step 4 before initially starting Tomcat, your configuration is overridden the first time Tomcat is started, resulting in the Library Refresh remaining in a disabled state.

3. Run the following query to verify that the Library Refresh is definitely disabled:

```
select * from PAS_GLOBAL_PROPERTIES where KEY_='library.refresh.cronspect';
```

The returned value should be **na**, indicating that the Library Refresh is disabled. Go on to Step 4 to proceed with enabling the Refresh.

If a cron value is returned instead of **na**, the Library Refresh has already been enabled, and no further configuration is needed. However, if you want to reset the Refresh schedule to a different time, perform the next step.

4. Run the following query that enables the Library Refresh through the configuration of the clock time for its daily run. The following query sets the cron expression as '**0 0 0 * * ?**', which, in turn, configures the Refresh to run daily at 12 am.

```
UPDATE PAS_GLOBAL_PROPERTIES SET VALUE_= '0 0 0 * * ?' WHERE KEY_ =  
'library.refresh.cronspect';
```

To specify different clock time for the daily Refresh, set the values in the cron expression accordingly using this format:

'<seconds> <minutes> <hours (in 24-hour format)> * * ?'

For example, the cron value '**0 41 14 ? * ***' represents the following:

- 0 seconds
- 41 minutes
- 14 hours

In this example, the Library Refresh is configured to run daily at 2:41 pm.

5. Restart Tomcat.

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 Publication and Review](#)

- [Custom Detection Rules](#)
- [Data Library, Library Refreshes, and Electronic Updates](#)
- [Export and Import](#)
- [Installation, Upgrades, and Configuration](#)
- [Inventory History](#)
- [Manual Codebase Analysis](#)
- [Performance](#)
- [Project Inventory](#)
- [Project Management](#)
- [Project Reporting](#)
- [REST APIs](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Code Management \(SCM\) Support](#)
- [Vulnerability Suppression/Unsuppression](#)
- [Web UI](#)
- [Code Insight Security Issues](#)

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 Publication and Review

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

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.

Custom Detection Rules

The following are known issues when managing custom detection rules.

SCA-48572: No error message indicating “Inventory Name” value in rule exceeds limit

When you attempt to save a custom detection rule with an **Inventory Name** value that exceeds its 255-character limit, the rule is not saved, and no error message is displayed to describe the problem.

Workaround: If you enter a value for **Inventory Name**, ensure that has no more than 255 characters.

SCA-48564: Changes to “Inventory Name” in custom detection rules not applied to inventory during rescans

When you update an existing value in the **Inventory Name** field for a custom detection rule, a rescan or forced full rescan does not apply the change to the inventory name.

Workaround: Create a new project and perform a fresh scan so that the name change is correctly applied to the inventory item.

Data Library, Library Refreshes, and Electronic Updates

The following are known issues related to the Code Insight data library, the daily Library Refresh, which reports new vulnerabilities associated with inventory, or the Electronic Update, which keeps Code Insight systems up to date with the latest data-library information.

SCA-51662: Electronic Update banner and job showing status as active when job is actually waiting for scans to complete

The Electronic Update banner and the **PDL Update** job for an Electronic Update is showing that the job is active when it is actually waiting for scans to complete, as recorded correctly in the log.

Workaround: None exists.

SCA-51313: Electronic Update banner displaying even though the Update is not executing

The Electronic Update banner, indicating that an update is currently running, is being displayed even though the Update is not running. This error occurs under these circumstances:

- An Electronic Update that is added to the **Jobs** queue during a currently running scan or rescan is flagged as **Active** in the queue even though its state should be **Scheduled**. (However, the Update is actually waiting for the scan or rescan to finish.) See [SCA-51296: Electronic Update or License Refresh showing “Active” when added to Jobs queue during an “Active” scan or rescan](#).
- An Electronic Update is added to the **Jobs** queue while a License Refresh is currently running. (The Electronic Update is properly placed in a **Scheduled** state and is waiting for the Refresh to finish.)

Workaround: None exists.

SCA-51296: Electronic Update or License Refresh showing “Active” when added to Jobs queue during an “Active” scan or rescan

An Electronic Update or Library Refresh that is added to the **Jobs** queue during a currently running scan or rescan is flagged as **Active** in the queue even though its state should be **Scheduled**. Note, however, that the Update or Refresh is actually waiting for the scan or rescan to finish, as correctly recorded in the log file.

Workaround: None exists.

SCA-51293: Electronic Update or License Refresh failing with “Cannot delete or update a parent row: a foreign key constraint fails”

An Electronic Update or License Refresh can fail when orphan custom components (that is, custom component versions not linked to any inventory items) have licenses mapped to them.

Workaround: Run a SQL query to clean the component version and their licenses. Contact Revenera Support for details.

SCA-43568: Sequential creation of multiple custom components with similar names resulting in incorrect component search counts and pagination

As of 2022 R4, Code Insight starts the background process of indexing a custom component in the Code Insight data library as soon as the component is created or updated. If multiple custom components with similar names are sequentially created/updated and indexed in the background, the search results for these components might show incorrect search counts and pagination.

Workaround: After the custom-component updates are indexed, run an Electronic Update to fix the indexes.

SCA-40194: Duplicate inventory issues for MIT-related components

The Code Insight MIT data-library update does not fix inventory items with names that include multiple licenses separated by commas (instead of ORs), as shown in this example:

```
jquery (MIT, MIT License)
```

On a rescan, duplicates might be created for such inventory items:

jquery (MIT, MIT License)

jquery (MIT)

Two possible workarounds are available.

Workaround 1: Before starting the rescan, select the option **On data import or rescan, delete inventory with no associated files** on the **Manage Project > Edit Project > General** tab accessed from the project's **Summary** tab. This option deletes the original inventory item as long as it is system-generated.

Workaround 2: Manually delete the original inventory item in the **Analysis Workbench** by right clicking the item and selecting **Delete inventory**. You must repeat this step for each such inventory item.

SCA-31562: Component license remapping issues from MIT-Style to MIT for inventories

Remapping Issues have occurred once the latest Electronic Update (available from Code Insight 2021 R4 and later) has been run. These issues involve the remapping of licenses from MIT-Style to MIT for inventories. The next two sections combined illustrate a typical remapping issue.

Before running the Electronic Update available at the release of Code Insight 2021 R4 and later:

The following inventory mapping existed in inventory:

concurrent-ruby 1.1.9 (MIT License)

This component was mapped with License id 744.

After running the Electronic Update available at the release of Code Insight 2021 R4 and later:

The inventory item was remapped as follows:

concurrent-ruby 1.1.9 (MIT-Style)

The license short name had been changed (in this example, from MIT License to MIT-Style). However, the mapped license ID remained 744. Ideally this component should be remapped to MIT, which is License id 7.

Workaround: Follow these steps:

1. Click **Inventory** on the main Code Insight window to open the **Inventory** view, showing inventory across projects.
2. Switch from **My Projects** to **All Projects**.
3. Search for the inventories containing the string *(MIT-Style)*.
4. Locate the **Possible Licenses** value for a given inventory. If this value is **MIT** (Id 7) *and* the term *MIT-Style* is in the inventory name or is the value of **Selected License**, then an incorrect license remapping has been performed for this specific inventory item. One incorrect license remapping is a possible indicator of other incorrect remappings.
5. Run the Code Insight cleanup SQL script to correct the license mappings for the inventory in your Code Insight system. (To obtain this script, download the codeinsight-MITCleanupPackage archive from the Product and Licensing Center, and extract the script and its instructions.)

Export and Import

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

SCA-52508: Customers not able to open certain manually created inventory items that have been imported

When project data is exported, the data includes whether the inventory item was created by the system or manually by a user. When the exported data is then imported *and* it contains inventory that was flagged as manually created, consider the following import scenarios:

- **Scenario 1**—The data is imported to the same machine from which it was exported, but a given user who created one or more inventory items in the data has since been deleted from the Code Insight database.
- **Scenario 2**—The data is imported to a different machine, and the given user who created one or more inventory items does not exist on this machine.

In either scenario, the import process successfully completes, but customers are not able to open the inventory items created by the deleted or non-existing user.

Recommendation for Scenario 1: Do not delete the user (who created the inventory item) from database. Instead, disable the inactive user.

Workaround: Contact Technical Support for assistance.

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, Upgrades, and Configuration

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

SCA-48759: Longer Tomcat startup during migration to 2023 R3 or later due to new column creation

A new column was added to the `pse_inventory_groups` table in Code Insight 2023 R3 to support the reporting of dependency scope. During a migration to Code Insight 2023 R3 or later, the creation of this column (performed through Liquibase) can slow down the initial Tomcat startup if the number of inventory items is large. (For example, if the inventory count is 15,000, the initial Tomcat startup can take 30 minutes to complete.)

Workaround: None exists.

SCA-35918: Upgrades to Code Insight possibly more time-consuming than previous upgrades

Upgrading to Code Insight might take longer than previous upgrades, especially if the number of inventory items in your Code Insight system has increased since the last upgrade. For example, an upgrade for a system with about 1 million inventory items can now take around 15-20 minutes, which might be longer than your previous upgrades. The extra time needed for the upgrade is due the **Inventory History** feature (introduced in 2021 R3), which requires that the inventory items for all projects be processed for inclusion in the history.

Note, however, that once an inventory item is included in the history, it does not need to go through this initialization process in subsequent upgrades.

Workaround: None exists. If you have any concerns about the time taken for this process, contact Revenera Support for assistance.

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. 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 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 results in an error.

If this blocking 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>.)

Inventory History

The following are known issues with the Inventory History feature.

SCA-52088: Inventory history incorrectly recording an “Associated Files” update after manual creation of an inventory item

When an inventory item is manually created or updated through the Code Insight user interface or the REST API, the **View History** window is registering an **Associated Files** update that never occurred. The PSE_INVENTORY_GROUPS_AUD table in the Code Insight database is also recording this update.

Workaround: None exists.

SCA-51192: “Associated Files” record not displayed when other modified fields have been saved along with it

A separate **Associated Files** record is not displayed in the **Inventory History** window if other fields such as **Encryption**, **URL**, and more have been updated and saved along with it.

Workaround: None exists.

SCA-36420: Inventory URL and Description attributes shown as updates in Inventory History without their being modified

After an initial transaction is performed against an inventory item (such as editing or viewing the item), entries for the **URL** and **Description** properties are displaying in the **Inventory History** window even though these properties were never modified as part of the transaction. These two initial entries will remain in the history. However, any future transactions against the inventory item will not create an update entry for the **URL** or **Description** property unless the value for either property has actually changed.

Workaround: None exists.

Manual Codebase Analysis

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

SCA-46104: Not able to retrieve Advanced File Search results when using same criteria but with distinct values and AND logic

The Advanced File Search feature does not retrieve the expected results when you define a filter using multiple criteria that are the same (but with a distinct value for each criterion) and apply AND logic to the criteria. Files known to meet all the specified criteria are not listed in the **File Search Results** pane.

SCA-44366: Error thrown when navigating file search results

When you use the **Enter search string...** field at the top of the **Codebase Files** pane to search for files by name, you can use the Next or Previous button adjacent to the field to navigate to the search results highlighted in the codebase tree. However, if you click these buttons a rapid pace, you can generate an error (although the UI does not hang).

Workaround: Click the buttons at a slower pace.

SCA-41440: “Show File Evidence” right-click option on “File Search Results” pane not working at node, folder, and sub-folder levels

When you right-click an alias node, codebase node, folder, or sub-folder in the **File Search Results** pane in the **Analysis Workbench**, and then select **Show File Evidence**, the **Evidence Details** tab on the right displays the message “No Evidences found”.

However, when you select **Show File Evidence** at the file level in the **File Search Results** pane, the evidences properly are listed on the **Evidence Details** tab as expected.

This behavior occurs whether the files were scanned by a Scan Server or a scan-agent plugin.

Workaround: None exists.

SCA-41964: Empty results when Advanced Search with “File Path” criterion attempts to fetch 2000 or more results

An **Advanced Search** using the **File Path** criterion can produce empty results in the **Analysis Workbench** if the search attempts to retrieve 2000 or more results. This issue can occur whether searching a file system scanned by a remote scan agent or a codebase scanned by a Scan Server.

This issue does not occur when the search fetches less than 2000 results.

Workaround: None exists.

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 Inventory

The following are known issues with the review process for Code Insight project inventory.

SCA-44107: Unable to delete an inventory item with a large number of associated files

Attempts to delete an inventory item associated with a large number files (50KB or more) can fail.

Workaround: None exists.

SCA-44077: Deletion of a top-level inventory item causing deletion of dependency inventory

When a user deletes a top-level inventory item, all of its dependent inventory items are also deleted.

Workaround: None exists.

SCA-41263: License text shown twice in As-Found License Text field in Analysis Workbench

In the **Analysis Workbench**, the text for a license can be repeated twice for some components (such as the component glob) when the license file contains more than one license.

Workaround: None exists.

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

Project Management

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

SCA-52395: Missing details in logs for policy application at the project level compared to policy application at the global level

The log information for an **Apply Policy - Project** job has fewer details than the log for an **Apply Policy - Global** job. The **Apply Policy - Project** job includes general information—the project name, the name of the project's policy profile, the project's total number of inventory items, the time taken to complete the policy review, and the timestamp of completion. However, the time taken to apply the different types of criteria (component, license, and vulnerability) and total number inventory items impacted by each criteria type is not logged for the **Apply Policy - Project** job as it is for the **Apply Policy - Global** job.

Workaround: None exists.

SCA-41957: Project Copy performance slower when the Code Insight database resides on a separate machine

Processing time for Project Copy increases when the Code Insight database resides on a machine different from the machine where the Core Server resides. Project Copy processing is most efficient when the Core Server, Scan Server, and database reside on the same machine.

Workaround: None exists.

SCA-41862: Increased time for Project Copy and other operations when Project Copy runs in parallel

If a Project Copy is triggered when any other operation—such as an import, export, scan, or report generation—is also running in your Code Insight system, the processing time for the Project Copy as well as for the other operation (especially an import, export, or scan) will be relatively greater than if these operations were run at separate times.

Workaround: In general, perform the listed operations at separate times for better performance. Ensure that Project Copy does not run in parallel with any of these operations.

SCA-41682: Project dashboard of copied project shows both Scanner and Remote Scans sections even though source project was only remotely scanned

The project dashboard of the copied project shows both Scanner and Remote Scans sections info even though the source project was scanned by a scan agent only. Only the Remote Scan section should be displayed.

Workaround: None exists.

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.

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-52409: Execution of the same configured “Update inventory” REST API triggering automatic review

When you call the **Update inventory** REST API to update a specific inventory item, an automatic review (by policy) is automatically triggered on the item once the update is complete. (The review is triggered only if the inventory’s component, license, or usage properties were edited.) However, if you call this API again on the inventory item even though no attributes of the item have changed since the previous update, the review is erroneously triggered again. The policy should not be triggered again since no new edits have occurred.

Workaround: None exists

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.

Scan Agent Plugins

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

SCA-51042: Generic plugin “transitive” scan with non-runtime-dependency reporting disabled still reporting such dependencies in Gradle codebase

A generic plugin scan whose profile is configured with **All Transitive Dependencies** and has **Report Non-Runtime Dependencies** disabled is still reporting non-runtime dependencies in a Gradle codebase.

Workaround: None exists.

SCA-50830: Scans on Linux instances not reporting transitive dependencies for the netty-handler dependency added to build.gradle

A scan fails to report the transitive dependencies of the netty-handler component because one the dependencies is operating-system dependent.

Workaround: None exists.

SCA-50489: Generic plugin scan on Gradle codebase reporting duplicate inventory and file associations

A Gradle-codebase scan performed by the generic plugin using an **Only First Level Dependencies** or **All Transitive Dependencies** scan profile with **Report Non-Runtime Dependencies** enabled or disabled can incorrectly report the following from the build.gradle and libs.versions.toml files.

- Duplicate top-level inventory
- Duplicate dependency inventory
- Duplicate associated files

Workaround: None exists.

SCA-48543: Unable to install Jenkins scan-agent plugin on Jenkins Server

The Code Insight Jenkins scan-agent plugin requires certain Jenkins dependency plugins that Jenkins automatically installs before the scan agent is installed. Jenkins will download only those dependency plugin versions that are compatible with the baseline-support version of the Jenkins Server (currently, 2.332.1). For example, Jenkins will download the **Pipeline: Groovy** dependency version that has been updated to support Jenkins Server 2.332.1 or later.

Consequently, if you are running a pre-2.332.1 Jenkins Server, some of the downloaded dependencies might be incompatible your server version, causing the Jenkins scan-agent plugin installation to fail. In this situation, consider migrating the server to version 2.332.1 or later. If migration is not feasible, you must manually install an older version of the dependency plugins that is compatible with your server version. For the list of required dependency plugins for the Jenkins Server, refer to the [Plugins Index](#) on the Jenkins site.

SCA-46097: Docker Images name with “/” causing scan to fail

A Docker Images plugin scan on a Docker image fails if the image name contains a forward slash (/), but the command that runs the scan does not include a valid tag for the name.

Workaround: If the Docker image name contains a forward slash, be sure that the command that runs the scan includes a valid tag for the image name. The following example command illustrates the correct <name>:<tag> format required in the command:

```
./code-insight-docker-plugin.sh -image alpinelinux/darkhttpd:latest
```

In the example, **alpinelinux/darkhttpd** is the image name containing a forward slash, and **latest** is the added tag (preceded by a colon).

SCA-44239: Delta file calculation during rescan not synchronized with scan

The Docker Images plugin can sometimes acknowledge files that have not changed since the previous scan as changed in the rescan. This error can impact scan time.

Workaround: None exists.

SCA-44209: Associated files not available in Syft findings for Docker Images plugin scans on Centos

File associations are not available for inventories reported by Syft during a Docker Images plugin scan on a Centos agent machine. This issue does not occur for scans performed by the same plugin on RedHat Enterprise Linux and Ubuntu machines.

Workaround: None exists.

SCA-44073: Invalid file association for transitive dependencies generated from go.sum

During a transitive scan, inventory generated from the go.sum file can have an invalid association to go.mod.

Workaround: None exists.

SCA-43034: No valid error message for scan failure when using current plugin with older Code Insight release

A current scan-agent plugin is not compatible with an earlier Code Insight release. Therefore, any attempt to run a scan-agent plugin with a Code Insight release previous to the plugin release results in failure. However, no appropriate message for this type of failure is provided.

Workaround: None exists.

SCA-42606: Seemingly “Successful” completion of Docker plugin scan despite errors

A Docker plugin scan can fail on a codebase/artifact system containing large archive files but a small /tmp partition. However, the scan status can still show “SUCCESS” (although the agent log might record the error that caused the failure).

Workaround: None exists.

SCA-41197: SHA-1 calculated for only files scanned during agent rescans subsequent to re-enablement of SHA-1

When SHA-1 is disabled and then re-enabled, any subsequent rescan by a scan agent calculates a SHA-1 value for only those files that are scanned (that is, updated or new files). SHA-1 is not calculated for those files that are skipped by the scan because they remained unchanged since previous scan.

Workaround: None exists.

SCA-41154: No scan agent support for full rescans

Prior to Code Insight 2022 R2, scan agents plugins performed only full scans. Starting 2022 R2, scan agents now support *only* incremental rescans. After the scan agent's initial full scan of a file system, any subsequent rescans are incremental only; no forced full rescans are supported. However, a full rescan should automatically occur whenever Automated Analysis rules change, a new Code Insight version introduces new rules or data library changes, or the scan-profile settings change. Currently, no logic exists to support such an automatic full rescan when these conditions exist.

Workaround: None exists.

SCA-40626: I/O exception during Jenkins plugin scan after deletion of “.codeinsight” folder from Jenkins agent

Users can delete the .codeinsight folder from the Jenkins agent if needed. However, once the folder is deleted, scans scheduled for the Jenkins plugin might fail with an I/O exception.

For your reference, this folder is identified as \$user_dir.codeinsight, where \$user_dir is as follows:

- /home/<user>/ on Linux
- C:/Users/<user>/ on Windows

Workaround: Restart the Jenkins server.

SCA-38346: NVD calls are not going through proxy for plugin scans

When a proxy is enabled for the generic scan-agent plugin or the Jenkins plugin, NVD calls bypass the proxy during scans.

Workaround: None exists.

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-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 an upgrade to a Jenkins scan-agent plugin, a downgrade button option is available in the Web UI. Clicking on the option results in a 404 error.

Workaround: None exists.

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

For scan agent plugins not updated from 1.x (supports only legacy inventory-only projects) to 2.x, the scan results might show published inventory items that have no associated licenses. This occurs when the scan agent finds no license evidence in the codebase files or when Code Insight is able to map to the component, but multiple licenses are associated with it. In this case, the inventory item is created using Compliance Library data. It might show one or more *possible* licenses but most likely no selected license. Since the **Analysis Workbench** is not available for the legacy “inventory only” plugins, the user cannot not resolve the license issue.

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

Scanning and Automated Discovery

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

SCA-52370: Duplicate inventories generated when PKG-INFO and setup.py files exist in the same module but setup.py is missing information

When PKG-INFO and setup.py exist in the same module in the codebase but setup.py is missing package details such as name or version (or the package has different root folder name), duplicate inventory is being generated. In general, the inventory item found in PKG-INFO is listed with the correct name and version; the item found in setup.py is listed with the inventory name but no version.

Workaround: None exists.

SCA-51080: Scans not reporting dependencies in NPM codebase containing package-lock file

Dependency inventory is not being reported during scans on NPM codebases containing a package-lock.json created with a recent version of the NPM node js tool.

However, note that, if the scan is unable to read a package-lock.json file, it resolves the versions and locates transitive dependencies from the NPM registry. As a result, there actually is no loss of inventory.

Workaround: Not required since the scan still has a means to locate dependencies and resolve versions found in package-lock.json.

SCA-50977: Non-runtime dependencies marked as runtime during “transitive” scans on Gradle codebases

Non-runtime dependencies are being reported as runtime dependencies during scans (configured with **All Transitive Dependencies** in their profiles) on Gradle codebases. However, the total number of inventories is still correct. The issue might be the result of the use of an external API to collect transitive dependencies.

Workaround: None exists.

SCA-50958: “build.gradle” files incorrectly associated with top-level inventory reported from libs.version.toml during “transitive” scans

Transitive scans on Gradle codebases might incorrectly associate the `build.gradle` and `build.gradle.kts` files with top-level inventory reported from the `libs.versions.toml` file. This issue occurs when a `libs.versions` reference is available in the `build.gradle` file.

Workaround: None exists.

SCA-50448: Invalid duplicate transitive dependencies reported for Gradle codebases

A Gradle-codebase scan using an **Only First Level Dependencies** or **All Transitive Dependencies** scan profile with **Report Non-Runtime Dependencies** enabled or disabled can sometimes report invalid duplicate transitive dependencies for a given dependency.

Workaround: None exists.

SCA-49499: Scan not identifying correct podspec file in inventory name when multiple podspec files exist

When multiple podspec files exist in the root directory of a cocoapod project, the scan can fail to identify the correct file for “project_name” in the “[Dependency of project_name]” suffix used in those inventory names that identify dependencies. (Scan results are random as to when the correct or incorrect file is identified.)

Workaround: None exists.

SCA-49181: Migrated project scan showing incorrect detection notes for inventory though mapping to Debian forge and URL is successful

After a scan on a migrated project, an inventory item whose component is found in the Debian forge is showing incorrect detection notes even though the component is successfully mapping to the Debian forge and URL. As a result, the inventory is not getting published.

Workaround: Create a new project and do a fresh scan of the codebase.

SCA-48341: Scans on Windows Server platform hang when codebase contains linux.tar files

When a Scan Server that runs on a Windows Server platform scans a codebase containing `linux.tar` files, the scan can hang indefinitely unless you stop and restart Tomcat.

Workaround: Perform *one* of these options before scanning the codebase:

- Untar the `linux.tar` file and archive the resulting folder in a zip file. Then replace the `linux.tar` file with the zip file in the codebase and upload the codebase to the Scan Server.
- In the scan profile, use a pattern to exclude the impacted files, `aux.c` and `aux.h`, from the scan, as shown in this example:

```
**/i2c/aux.c  
**/i2c/aux.h
```

Refer to “Creating Exclusion Patterns for Scan Profiles” in the *Code Insight Installation & Configuration Guide* for complete information about setting up file exclusions.

SCA-44154: Transitive dependencies not reported for golang.org/x/tools module

During a transitive scan of the tools module `golang.org/x/tools`, the Go Analyzer reports no inventory.

Workaround: The next Electronic Update will resolve this issue.

SCA-43792: Issue with Go module inventory names when associated component URL has a version suffix

When a discovered component in a Go module has a `/v<digit>` suffix in its URL, the inventory name is displayed as simply **v<digit>** in the Code Insight UI and API responses. For example, if the URL for the `blackfriday` component is `github.com/russruss/blackfriday/v2`, its inventory name is displayed as **v2**, instead of **blackfriday**.

Workaround: None exists.

SCA-43659: Security vulnerabilities not reported for Go components

Scans on Go packages are not reporting security vulnerabilities for Go components.

Workaround: None exists.

SCA-43103: Files with path change but same MD5 still being rescanned

Files whose path has changed but whose MD5 remains the same are still being rescanned even those the project’s scan profile is configured *not* to rescan unchanged files.

Workaround: None exists.

SCA-34070: 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.

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.

Source Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

SCA-52522: Credentials entered in Git URL *not* a best practice

GIT allows users to pass credentials within the repository URL if an HTTP (or HTTPS) URL is used. Consequently, when setting up SCM synchronization between Code Insight and Git (*and* Git SSH is not used), users can include credentials in the **Git Repository URL(s)** value. Note, however, that these credentials are displayed in the URL value when it is shown in other parts of the Code Insight.

Code Insight also provides the **Git Username** and **Git Password** fields in which to enter the credentials during synchronization setup. Credentials passed in these fields are *not* displayed in the URL value when it is shown in other locations in the product. Therefore, when Git SSH is not used, the best practice is to always use the **Git Username** and **Git Password** fields, not the **Git Repository URL** field, to pass the credentials.

Workaround: Use Git SSH *or* pass the user credentials through the user interface fields if an HTTP or HTTPS URL is used.

SCA-48045: scmInstances GET API not returning all URL details when any Git URL has multiple delimiters

Currently, if the scope for the **scmInstance** GET API includes at least one Git SCM instance with a repository URL that is defined with more than one delimiter (branch, tag, or commit ID), an error message similar to the following is returned. The message (with the status code 400) lists those Git URLs defined with multiple delimiters in the instance.

```
{
  "errors": [
    {
      "param": "[scmType: GIT; instanceId: 0; URL: https://github.com/sbni/
TestPublicRepo.git~master>>commit123, scmType: GIT; instanceId: 0; URL: https://
github.com/test/newtest^^tag123~branchname]",
      "message": "Branch, Tag, Commit ID are mutually exclusive."
    }
  ]
}
```

When this message is returned, details are not returned for repositories of the other URLs in the same Git SCM instance, nor are they returned for the repositories identified in the other SCM instances of any type in the project.

The missing details for the other URLs in the Git SCM instance as well as for the other SCM instances makes it difficult to obtain the information needed to update a given instance. (The request body for the PUT method requires the complete updated definition of the SCM instance.)

Workaround: When creating or updating a Git SCM instance, provide only one delimiter per URL in a Git SCM instance. Additionally, use the Code Insight UI to update SCM instance and retrieve their details.

SCA-47353: Unhelpful message when testing or synchronizing with invalid or missing credentials

When you attempt to test the connections for a specific SCM instance (or run a synchronization across all SCM instances in a project) *and* the connection credentials are invalid or missing for any instance, a message with an unhelpful error description is displayed.

Workaround: Refer to the core or catalina logs for an accurate description of the error.

SCA-46441: TFS repository failing to synchronize

The synchronization between a TFS codebase repository and a Code Insight project can fail even though the TFS instance connection is configured correctly (with a valid URL, user name, password, and other properties) in the project.

Workaround: On the **Version Control Settings** tab for the project, provide a personal access token (PAT) in the **Password** field instead of a password to enable successful synchronizations.

SCA-40067: SCM instance numbering systems used in REST API output and Web UI not in sync

The instance Ids shown in the **GET SCM Instance** API response are not in sync with SCM instance numbers generated in the Web UI.

Workaround: None exists

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.

Vulnerability Suppression/Unsuppression

The following are known issues with the Vulnerability Suppression/Unsuppression functionality.

SCA-37089: Unable to suppress/unsuppress a vulnerability for more than 2097 versions of a component all at once (in a SQL Server environment)

When a user attempts to suppress or unsuppress a security vulnerability for more than 2097 versions of a component all at once (using the **All Current Versions** scope or the **Specified Versions** scope with more than 2097 entries), the operation fails with an appropriate error message. This same problem occurs when running the **Suppress vulnerability** or **Unsuppress vulnerability** REST APIs.

This issue occurs only when the Code Insight database is SQL Server.

Workaround: Suppress or unsuppress the vulnerability using the **Specified Versions** scope with fewer entries. Repeat this operation until the vulnerability has been suppressed or unsuppressed for all desired versions.

SCA-36973: Open alert counts not automatically refreshed after vulnerability suppression

After a security vulnerability is suppressed for a component version with open an open alert associated with the vulnerability, the open alert count is not automatically refreshed to show the reduced count in the Code Insight Web UI.

Workaround: Manually refresh the browser screen.

SCA-36768: “Vulnerabilities” bar graph not automatically refreshed after vulnerability suppression

After a security vulnerability is suppressed for a component version, the count in the appropriate “severity” segment of the **Vulnerabilities** bar graph for the component version is not automatically reduced.



Note - The issue has been fixed for the bar graph on the **Inventory** view and **Project Inventory** tab. However, the issue has not been fixed for the bar graph displayed in other locations.

Workaround: Manually refresh the browser screen.

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-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.

Code Insight Security Issues

The following are current security issues involving Code Insight.

SCA-52416: New White Hat vulnerability finding—“Insufficient Transport Layer Protection”

According to a new White Hat vulnerability finding (**50934239**) in Code Insight, the SSL/TLS endpoint used by Code Insight is configured with weak SSL/TLS cipher suites. This issue will be resolved in the near future.

Legal Information

Copyright Notice

Copyright © 2024 Flexera Software

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

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

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.reverera.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.