Code Insight 6.14.2 SP1 Release Notes

May 2021

Introduction

These Release Notes pertain to the 6.14.2 SP1 release of Code Insight, formerly known as Palamida Enterprise Edition (EE). For information specific to earlier versions, refer to previous Release Notes documents.

This document contains the following major topics:

Payload Summary for Code Insight 6.14.2 SP1

The following is a summary of the functionality that has been added or updated in Code Insight in version 6.14.2 SP1:

- New functionality and enhancements, as described in New Features and Enhancements.
- Resolved issues, as described in Resolved Issues.

Supported Platforms and Technology

The following sections list the platforms and technology currently supported by Code Insight systems:

Operating Systems

Code Insight is tested and validated on the following operating systems. Also see additional information in Possible Compatible Operating Systems and Additional Notes About Supported Operating Systems.

Supported	Recommended
Ubuntu 18.04	Ubuntu 18.0.4
Ubuntu 16.04	RHEL 7.2, 7.8, or 8.2 Enterprise (64-bit)
Ubuntu 14.0.4	CentOS 7 (64-bit)
RHEL 7.2, 7.8, or 8.2 Enterprise (64-bit)	Win 10 Enterprise or Professional (64-bit)
RHEL 7.0 (64-bit)	Windows Server 2016 Datacenter
RHEL 6.5 (64-bit)	
CentOS 7 (64-bit)	
CentOS 6.5 (64-bit)	
Win 10 Enterprise or Professional (64-bit)	
Win 8.1 Enterprise or Professional (64-bit)	
Win 7 Enterprise or Professional (64-bit)	
Windows Server 2016 Standard	
Windows Server 2016 Datacenter	
Windows Server 2012 Enterprise or Professional (64-bit)	

Possible Compatible Operating Systems

The following operating systems might be compatible but are not tested with each release:

- Mac OS (all versions)
- Windows Server 2008 R2 Enterprise Edition (64-bit)
- Windows XP Professional (64-bit)
- Windows 7 Ultimate (64-bit)
- CentOS 5 (64-bit)
- Others (contact technical support)

Additional Notes About Supported Operating Systems

Note the following additional information about supported operating systems:

- CentOS 6*x* versions reach EOL (End of Life) status on November 30, 2020.

- Code Insight does not support a configuration in which the Core Server runs on a Windows instance and a Scan Server runs on Linux instance. For more information, see "Single Server vs. Multiple Server Deployments" in the *Code Insight Installation and Administration Guide*.

Databases

Code Insight is tested and validated on the following databases. Also see additional information in Additional Notes About Database Support.

Supported	Recommended

• MySQL 5.6, 5.7, 8
• Oracle 11g, 12c, 18c, 19c
• MS SQL Server
  ◦ 2012 r2 Enterprise
  ◦ 2014 Enterprise
  ◦ 2016 Enterprise
	• MySQL 5.7, 8
	• Oracle 12c, 19c
	• MS SQL Server
	  ◦ 2012 r2 Enterprise
	  ◦ 2014 Enterprise
	  ◦ 2016 Enterprise

Additional Notes About Database Support

Note the following about database support:

- Oracle 11g has an end-of-life status. There is no guarantee that this Oracle version continues to work properly with Code Insight.
- MS SQL Server 2012 is not recommended for use in large-scale and high-volume scanning environments.
- The MySQL 5.0-5.5 database version has been used to run Code Insight in the past but has not been fully verified as part of the current release.

***Note** ▪ Ensure that you use appropriate supported database driver with Code Insight. Other versions are not guaranteed to be compatible. See Software for details.*

Hardware

The following describes hardware requirements for Code Insight:

- Supported Hardware Configurations
- CPU Specifications

Supported Hardware Configurations

Use the following table to determine hardware requirements for Code Insight components. (Also see Additional Notes about Hardware Requirements and CPU Specifications.)

Component	Supported	Recommended

Scan Server	• 32 GB RAM
	• At least 1.25 TB hard disk space for the following (assuming that the Scan Server and Compliance Library are hosted on the same instance):
	  ◦ Codebases (materials to be scanned)
	  ◦ Workspaces (scanned results)
	  ◦ Compliance Library (approximately 1 TB)
		• 32 GB or 64 GB RAM depending on expected load
		• 1.5 TB hard disk space for the following (assuming that the Scan Server and Compliance Library are hosted on the same instance):
		  ◦ Codebases (materials to be scanned)
		  ◦ Workspaces (scanned results)*
		  ◦ Compliance Library (approximately 1 TB)
		* Performance can benefit significantly if the workspace directory is located on a Solid State Drive (SSD) drive

Core Server	• 16 GB RAM • At least 650 MB of space for product and attachments See the **Database Server** entry below if hosting both Core Server and database on the same machine	• 32 GB RAM (required if Core Server and database reside on same machine) • 30 GB of space for product and attachments See the **Database Server** entry below if hosting both Core Server and database on the same machine
Client	• 8 GB RAM	• 16 GB RAM
Database Server	**Database Sizing:** • The recommendation is that you have a DBA configure your database as you would for any other Enterprise Web Application. • For disk space, the recommendation is to start with a base of 30 GB (for SQL Server, 50 GB) to accommodate the Code Insight Data Libraries and other data related to users, teams, projects, and such. If you install the database on the same machine as the Core Server, calculate the hard-drive requirement by adding the database base size to the recommended Core Server disk space. (Also see Additional Notes about Hardware Requirements.) • After starting with the base size, scale up by 2 MB for every 5,000 files scanned. Begin by estimating how much you will scan in the first 6 months, and add that to the 30 GB base size. • As for data volume, Code Insight does not move enormous amounts of data, nor does it have extremely high concurrent transaction rates.	

Additional Notes about Hardware Requirements

Note the following about hardware requirements:

- Ensure that you allocate sufficient buffer pool size to the database. Otherwise, the Electronic Update might not complete. For MySQL, set the innodb buffer pool size to a minimum of 1 G (`innodb_buffer_pool_size = 1G`).
- For SQL Server, it is strongly recommended that the database and the Core Server reside on the same machine (with a minimum hard-drive requirement of 50 GB for the database and 30 GB for the Core Server, for a total of 80 GB).

CPU Specifications

The following table lists CPU specifications based on the memory requirements for your Code Insight hardware configuration, as described in Supported Hardware Configurations.

For example, if you intend to use the recommended 32 GB RAM for the Core Server (as listed in Supported Hardware Configurations), the CPU specifications for the machine running the Core Server include 2-CPU, each at least 2 GHZ+, with 8+ cores (as listed below).

Memory	CPU (Cores)
64 GB	2-CPU (each at least 2 GHZ+) with 8+ cores
32 GB	2-CPU (each at least 2 GHZ+) with 8+ cores
16 GB	2-CPU (each at least 2 GHZ+) with 4+ cores

Software

Code Insight requires or supports the following software:

- Software Packages
- Supported Browsers

Also see Additional Notes about Software Requirements.

Software Packages

The following software packages are supported and/or required:

Software	Description	Download URL	
Java JDK	Required on each instance where a Code Insight server—the Core Server and each remote Scan Server—is installed. Select one of these JDK types. (Use the latest Java update when possible.) • Oracle JDK 8u281 (64-bit) You must purchase a license from Oracle to ensure that you receive updates. • Zulu OpenJDK 8.52.0.23 (8u282b08) (64-bit) from Azul	**Oracle JDK 8**	http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
		Zulu Open JDK 8	https://www.azul.com/downloads/zulu/
Java JRE	Oracle JRE 8u281 (64-bit) required on client server to launch Detector. In general, use the latest Java update when possible. You must purchase a license from Oracle to ensure that you receive updates.  ***Note*** ▪ *Not required for Workflow-only installations or on client servers that already have the JDK installed.*	**Oracle JRE 8**	http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html
Database Client	Required to access the Code Insight database server and to execute database scripts (but not required if the database is to be managed directly from the database server). Any basic client application or command line client interface may be used. Several options are listed on the right.	**MySQL**	http://www.heidisql.com/download.php
		Oracle	http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html
		MS SQL Server	https://msdn.microsoft.com/en-us/library/mt238290.aspx

Software	Description	Download URL	
JDBC Database Driver	Required on each instance where a Code Insight server—the Core Server and each remote Scan Server—is installed to enable access to the database. Download the driver corresponding to your database type and do one of the following: ● If using the supplied installer (`codeinsight_6.x.jar`) to install Code Insight, copy the driver `.jar` file to the directory containing the installer. The installation process automatically copies the driver to the `tomcat\lib` location. ● If manually installing Code Insight, copy the downloaded `.jar` file to the following location: `<Code Insight_ROOT_DIR>\<version>\tomcat\lib\`	**MySQL**	**mysql-connector-java-5.1.45.jar (MySQL 8):** https://downloads.mysql.com/archives/c-j/ (select Product Version 5.1.45 and download) **mysql-connector-java-5.1.x-bin.jar (MySQL 5.6, 5.7):** http://dev.mysql.com/downloads/connector/j/5.1.html
		Oracle	**ojdbc8.jar (Oracle 18c, 19c):** https://www.oracle.com/database/technologies/appdev/jdbc-ucp-183-downloads.html **ojdbc6.jar (Oracle 11g, 12c R1) or ojdbc7.jar (Oracle 12c R2):** http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html
		MS SQL Server	Use this site to download the driver appropriate for the type of Java JDK (JDK or OpenJDK) that you are using: https://docs.microsoft.com/en-us/sql/connect/jdbc/system-requirements-for-the-jdbc-driver?view=sql-server-2017
Other	An email account is required to send email notifications from the Code Insight server.		

Additional Notes about Software Requirements

Note the following about software requirements:

- Support for Java 7 (JDK and JRE) was removed in Code Insight 6.12.0. Ensure that you use Java 8 (JDK and JRE) with a compatible update version.
- Code Insight provides support for Zulu OpenJDK 8 only. Other OpenJDK applications might work with Code Insight but are not recommended.
- Support for Java 11 is not available.
- Java software updates released after the Code Insight 6.12.3 release date are not guaranteed to be compatible. If you encounter an issue running a newer update, notify support, which will resolve these issues on a best effort basis and issue a hotfix as needed.

- For the Oracle 19c database, the recommendation is to use the ojdbc8.jar database driver (as listed in this table), not the ojdbc10.jar driver.

Supported Browsers

Code Insight supports the following browsers:

Supported	Recommended
• Firefox (latest stable version) • Google Chrome (latest stable version) • Internet Explorer 10, 11	• Firefox (latest stable version) • Google Chrome (latest stable version) • Internet Explorer 11

Ports

Code Insight typically uses the following ports:

Port	Details
1433/1521/3306	Database Server Access Port (MS SQL Server, Oracle, MySQL)
8888/443	Tomcat (http/https)
465	External SMTP (mail) Server
389	External Authentication Directory Server (Active Directory/LDAP)
8005 and 8009	Tomcat Connector and Tomcat Shutdown Ports (*local access only*)

Note the following:

- All ports used by Code Insight are configurable. If any listed port is already in use or is not supported by your company policy, configure an alternative port.
- Ensure that any port that you configure for Code Insight is allowed through your system firewall.

Supported Source Code Management Products

Code Insight supports the following the Source Code Management products in its workflow:

SCM	Sample Client Download
GIT	http://git-scm.com/downloads
Subversion (SVN)	http://tortoisesvn.tigris.org/

SCM	Sample Client Download
Team Foundation Server (TFS)	https://www.visualstudio.com/downloads/
Perforce	https://www.perforce.com/downloads
ClearCase	http://www-03.ibm.com/software/products/en/clearcase

Resolved Issues

The following issues have been addressed in this release.

Issue	Summary
SCA-29246	New scriptRunner upgrade available. See ScriptRunner Upgrade.
SCA-24838	Enhancement: Users able to add an *existing* security vulnerability to a component version through the Web UI and REST API. See Ability to Associate Existing Vulnerabilities with Component Versions.
SCA-25496	Enhancement: REST and Java public API support for "last updated" timestamp for projects. See Other Enhancements and Updates to Code Insight APIs.
SCA-26366	Enhancement: NG-bridge data updates for digest matches now available as an overlay to the data in the Compliance Library. See New NG-Bridge Digest Data to Complement Compliance Library.
SCA-26668	Component and associated security vulnerabilities now being properly identified for Jenkins PRQA Plugin 3.1.0 and Jenkins XL TestView Plugin 1.2.0 inventory.
SCA-27304	Issues with the File Name analyzer technique now being managed. (The technique can associate incorrect components with inventory.) Inventory items discovered by this technique are now assigned a maximum priority level of 4 and are no longer automatically published.
SCA-27363	The curl license now being properly reported as license evidence for the curl component.
SCA-27426	SmallRye Mutiny component no longer being associated with certain false "positive" security vulnerabilities.
SCA-27688	Python component names now extracted correctly from `setup.py`.

Issue	Summary
SCA-27703	Detection Notes now showing the correct analyzer used to find evidence.
SCA-28599	Vulnerability-association issues caused by trailing zeros in versions for components collected from the Git forge now resolved.
SCA-28611	Projects copied from another project no longer losing data when the original project is deleted.
SCA-28651	NVD JSON feed metadata updated from 1.0 to 1.1 in Code Insight.
SCA-29769	WhiteHat security issue: Insufficient TLS protection when configuring HTTPS in Code Insight now addressed with appropriate SSL protocol information in the Tomcat configuration. See Security Enhancement to SSL Configuration for HTTPS.
SCA-29786	Obsolete security vulnerabilities now no longer being reported with inventory.
SCA-29886	Security vulnerabilities associated with `Node.js` no longer being erroneously associated with the components readable-stream 3.6.0 and string_decoder 1.3.0.
SCA-29887	False “positive” security vulnerabilities no longer being associated with splunkd components.
SCA-30039	Optional dependencies now being reported for transitive dependencies in POM files.
SCA-30111	Syntactical errors within scanned Gradle files now consistently handled for all dependency levels so that no inventory is reported when syntactical errors exist.
SCA-30130	Dependencies now being reported `package.json`.
SCA-30567 **SCA-30626**	False “positive” security vulnerabilities no longer being associated with spring-cloud components.
SCA-30890	Inaccurate information in response descriptions in the REST API Swagger documentation now corrected.
SCA-31407	No longer able to add a custom security vulnerability that has the same name as another vulnerability.

Issue	Summary
SCA-31536	The `changeWorkspaceSettings.groovy` script now executing successfully. (The "java.io.NotSerializableException" error no longer occurs.)

New Features and Enhancements

The following features and enhancements were introduced in this release:

- New NG-Bridge Digest Data to Complement Compliance Library
- Ability to Associate Existing Vulnerabilities with Component Versions
- ScriptRunner Upgrade
- Security Enhancement to SSL Configuration for HTTPS
- "Last Updated" Timestamp on Projects Now Available Through API
- Other Enhancements and Updates to Code Insight APIs

New NG-Bridge Digest Data to Complement Compliance Library

Starting with the 6.14.2 SP1 release, Code Insight will support a secondary data source, NG-bridge, for digest matches as an overlay to the data in the Compliance Library. NG-bridge is Code Insight's next generation bridge solution that complements the Compliance Library (CL) with digest-match data beyond that provided in CL 2.43. The NG-bridge component is included with Code Insight and is a separate module that runs along-side the product to support exact-matching functionality.

Updates to the NG-bridge data source are planned on a regular basis and will keep the MD5 data for exact-file matching up to date. Each NG-bridge data update release is incremental, providing only changes since the last update release.

For more information about the NG-bridge data updates, how to configure the updates, and how the NG-bridge data is processed during scans, see "Managing NG-Bridge Updates for Code Insight" in the *Code Insight Installation & Administration Guide.*

Ability to Associate Existing Vulnerabilities with Component Versions

Previously, the Code Insight Web UI allowed users to create a security vulnerability that had not yet been identified in the Code Insight data library and associate it with a component version. In this release, users can now associate an *existing* security vulnerability with the component version—that is, a vulnerability already identified in the Code Insight data library but currently not associated with the component version.

The user can also disassociate such a vulnerability from the component version, just as they were able to do previously for any new vulnerabilities they created and added to the version.

Additionally, new REST APIs are available to associate an existing security vulnerability to an existing component version and to disassociate a custom vulnerability from a component version. (See New REST APIs.)

Note that only users with permission to write to components can manually add new or existing security vulnerabilities to a component version and disassociate any of these vulnerabilities from the version (as controlled by the `component.write.access.user.list` property in `<codeInsightInstallPath>\config\core\core.properties`).

ScriptRunner Upgrade

A new version of the Code Insight scriptRunner module is now available. In this latest version, the Groovy shell used by the scriptRunner has been upgraded from 1.5.4 to 3.0.6. Users who want to use the new scriptRunner must download the module from the Flexera Product and License Center (accessible from the **Other Resources** menu in the Revenera Customer Community), and replace the existing scriptRunner folder with the new one. (This new version is not installed with Code Insight 6.14.2 SP1. Only the previous scriptRunner is shipped with this release.)

Users who have installed the new scriptRunner must review and possibly modify any previously created custom scripts that they intend to execute with this scriptRunner version to ensure that the scripts run properly.

Security Enhancement to SSL Configuration for HTTPS

When configuring HTTPS for Code Insight, you must update the `tomcat\https\server.xml` file in your Code Insight installation directory with site-specific information (see “Enabling HTTPS for a Code Insight Server” in the *Code Insight Installation & Administration Guide*). For security purposes starting in this release, the default value for the `sslEnabledProtocols` parameter in SSL section of this file has been changed from `"TLSv1.2,TLSv1.1,TLSv1"` to `"TLSv1.2"`:

```
...
keystorePass="palamida"
clientAuth="false"
sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"
keystorePass="palamida"
...
```

Whenever you manually configure this file for HTTPS configuration, ensure that you do not change the default `"TLSv1.2"` to another value.

This new default is included in the `server.xml` file when you install (or upgrade to) Code Insight 6.14.2 SP1 and future versions.

“Last Updated” Timestamp on Projects Now Available Through API

Starting in this release, the Code Insight data library (PDL) now stores the timestamp for the last time a project was updated. (The information is stored in `Last_Updated_Date` column for the project in the `pas_project` database table.) This timestamp is updated each time a project is created, updated, copied, or deleted and each time a workspace is created or deleted. See the following topics:

- REST APIs Updated to Return “Last Updated” Timestamp for Projects
- Java Methods Updated to Return “Last Updated” Timestamp for Projects

REST APIs Updated to Return “Last Updated” Timestamp for Projects

The following Code Insight public REST APIs have been updated to return the **lastUpdatedDate** attribute for a given project in their responses:

- **/project/getProjectByID**
- **/project/getProjectByWSUUID**
- **/project/projectId**

Java Methods Updated to Return “Last Updated” Timestamp for Projects

The following Code Insight public Java methods belonging to the **ProjectDataCover** class have been updated to return the **lastUpdatedDate** attribute for a given project in their responses:

- **getProject**
- **getProjectsForCatalogItemsByItemName**

Other Enhancements and Updates to Code Insight APIs

In addition to the enhancement described in “Last Updated” Timestamp on Projects Now Available Through API, these new APIs and API updates are also available in this release:

- New REST APIs
- Updates to Existing Java API

For complete information about the Code Insight public REST interface and Java methods, select **Help** in the upper right corner of the Code Insight Web UI and then, from the **Documentation** tab, select the appropriate link:

- For Code Insight REST documentation, select **Public REST API Swagger Doc**.
- For the Code Insight Java method documentation, select **Public API Javadoc**.

You can also find this documentation in the `/docs` directory of your Code Insight installation.

New REST APIs

The following new REST APIs are now available.

Resource	API Name	Method	Description
Component	`associateVulnerability ToComponentVersion/ {versionId}/ {vulnerabilityId}`	POST	Manually adds a security vulnerability currently existing in the Code Insight data library to a component version.
	`disassociate Vulnerabilityfrom ComponentVersion/ {versionId}/ {vulnerabilityId}`	POST	Removes a custom security vulnerability from a component version. (The custom vulnerability is not removed from the Code Insight data library.) A custom vulnerability is either a user-created or an existing vulnerability that was manually added to a component version through the Code Insight Web UI or a public API.

Updates to Existing Java API

The following Code Insight public Java API has been updated:

Resource	API Name	Change
Reference Data ServiceCover	`deleteVulnerability(long, long)`	Now checks the following before removing the custom security vulnerability from the component version: ● The vulnerability passed is valid. ● The vulnerability and component version passed are associated.

Deprecations and Notifications

This sections lists Code Insight deprecations and other important notifications about Code Insight functionality:

- Analyzer Available Only by Manual Enablement
- End of Support for Java 7
- Point Detector Functionality No Longer Supported
- End of Support for Secunia Community Site

Analyzer Available Only by Manual Enablement

The Analyzer is available for workspace scans and reporting only if it is manually enabled in your Code Insight installation. By default, it is no longer displayed as an option on the **Automated Analysis** tab nor are its associated reports available for generation from the **Schedule Scan/Report** dialog.

To re-enable the Analyzer in your Code Insight installation, update the `disableAnalyzer` property, located in the `scanEngine.properties` file, to `false`. For details, see the online help or the *Code Insight Installation and System Administration Guide*.

End of Support for Java 7

Support for Java 7 (JDK 7 and JRE 7) is no longer available as of Code Insight 6.12.0. If you are currently using Code Insight with Java 7, upgrade to Java 8 to ensure that your application runs in a secure environment.

Point Detector Functionality No Longer Supported

As of the 6.12.3 release, Point Detector functionality is no longer supported.

End of Support for Secunia Community Site

The Secunia Community site will become inaccessible at the end of February. As of the 6.13.1 release, links to Secunia Advisories on the **Vulnerabilities** dialog and on reports are disabled. Note, however, that a future release of Code Insight will incorporate the following changes to once again provide access to Secunia data:

- Deliver additional Secunia Advisory properties (currently visible on the Secunia Community site) to Code Insight through the Electronic Update service.
- Provide a new Get Vulnerability Details REST API to obtain the additional Secunia Advisory data.
- Develop a new “vulnerability details” interface to display additional Secunia Advisory data.

Known Issues

The following sections provide information you need to be aware of when using the various functional areas of Code Insight:

- Project Copy
- Reporting
- Scanning and Analysis
- ScriptRunner and Scripting
- SPDX Generator Report
- Web UI
- Workflow

APIs

The following are known issues related to the Code Insight public REST and Java APIs.

REST API Component Search hangs in non-summary mode (SCA-330/PAS-11184)

The REST API for component search hangs when searching for components that have a large amount of associated data. For example, searching for Apache Tomcat (ID 33045) with **summaryOnly** view disabled results in an error.

Workaround: Search with the summary mode turned on, as in the example:

```
http://localhost:8888/palamida/api/component/componentData?componentIds=33045&summaryOnly=on
```

Limitation for REST API to update requests

The REST API to update a request may be used to update any request attribute in the request except for the selected component. To update the requested component, use the new `updateRequestedComponent` API included in this release. You may also use `updateRequestedVersion` and `updateRequestedLicense` to update the version and license without affecting other data.

Codebase Search

The following are known issues related to codebase searches in Code Insight.

Issues with Code Search highlights in UTF-8 files (PAS-10849)

UTF-8 files do not display correctly in Detector, and highlighting is either unavailable or shifted by one or more characters. Detector supports only encodings for which each character is a single byte, such as US-ASCII and ISO-8859.

Workaround: Switch the file type from “Auto” to “Binary”, and use “CTRL-F” to locate the search result within the file.

Code Search hanging during index process

Some customer scans have hung during indexing while in Tika processing. To avoid this problem, set `indexTikaParseLen = 0` in `scan.properties`.

Component Research

The following are known issues related to the lookup process for and management of third-party and OSS components.

Longer lookup load time for components with large number of versions and security vulnerabilities (SCA-28857)

If a component is associated with a large number of versions and security vulnerabilities (such as the linux-kernel component is), the load time for the component lookup can increase significantly.

Issues with the deletion of multiple CPE names for a component (SCA-28509)

When you attempt to delete multiple CPE names for a given component, the following issues can occur:

- Only the first name is deleted.
- Deleted names are not being added to the PSE_DELETED_ENTITIES table (used to keep track of the deleted items so that they are not restored during an Electronic Update).

Electronic Updates

The following are known issues related to the Code Insight Electronic Update process.

Unicode data on SQL Server (PAS-11158)

Some PDL columns in the Code Insight database schema do not currently support UTF-16 characters. As a result, users may see duplicate key errors in core.update.log when running Electronic Update on SQL server. This issue has been partially addressed in the current release of Code Insight, available as part of migration and will be fully resolved in the next release. SQL server users are advised to ignore duplicate key errors when running an electronic update.

Electronic Update buffer pool size

If you experience a failure when running Electronic Update on a MySQL or SQL Server database, ensure that the Buffer Pool Size systems is set to a minimum of 1 GB. Look for an out-of-memory error in the logs. See the Knowledge Base or contact support if you need further instructions.

Installation and Configuration

The following are known issues related to the Code Insight installation and configuration.

Multiple-Server Configuration Limitation (SCA-26837)

Code Insight does not support a configuration in which the Core Server runs on a Windows instance and a Scan Server runs on Linux instance.

Enabling the AJP connector in the Tomcat installation

The Apache Tomcat version installed with Code Insight 6.14.2 (and later) provides the Apache JServ Protocol (AJP) connector, which is disabled by default at installation. Although Code Insight does not require this connector, you might need it to support a Tomcat load-balancing scenario for your Code Insight environment. For instructions on how to manually enable and disable this connector, refer to the following KB article:

https://community.flexera.com/t5/FlexNet-Code-Insight-Customer/Enabling-the-Apache-JServ-Protocol-Connector-in-Tomcat/ta-p/146179/jump-to/first-unread-message

Migration and Backup

The following are known issues related to upgrading Code Insight.

Backward compatibility of Export/Import scripts

In Code Insight 6.11.2, changes were introduced to the Export/Import scripts to allow export and import of inventory questions/answers, comments and inventory status. Note that this functionality requires the updated scripts *and* product APIs that are only available in Code Insight 6.11.2 and later. The scripts will not export these entities on earlier versions of the product.

To export data from an older version of Code Insight and import it into Code Insight 6.14.2 SP1, do one of the following:

- Update your Code Insight instance to Code Insight 6.14.2 SP1 by following standard migration procedures. Use the export script shipped with Code Insight 6.14.2 SP1 to export the data and the import script (also shipped with Code Insight 6.14.2 SP1) to import the data.
- Use the export script designed to work with your version of Code Insight to export the data. Use the import script shipped with Code Insight 6.14.2 SP1 to import the data.

***Note** ▪ Neither of these procedures processes inventory questions/answers, comments, or inventory status.*

Project Copy

The following are known issues related to the project copy feature.

Project Copy error after switching request forms (SCA-313/PAS-11127)

Project Copy is not supported for projects that contain requests that reference more than one request form. No workaround is available.

Reporting

The following are known issues related to the Code Insight reporting.

Workspace Evidence Report – detected license does not match Auto-WriteUp (PAS-11071/SCA-285)

Workspace Evidence Report shows no “Detected License” value even though Auto-WriteUp has detected groups with licenses.

Scanning and Analysis

The following are known issues related to the Code Insight scanning and analysis process.

Inventory automatically published during previous scan now unpublished after rescan

Starting in 6.14.2 SP1, Code Insight scans no longer publish those inventory items that are identified by the File Name analyzer technique alone. Additionally, this inventory is now assigned a maximum priority of **Low**. These changes were implemented to address previous issues incurred by this technique. However, with the introduction of these changes, inventory previously detected and published by this technique only might now become unpublished *upon a rescan*. (Keep in mind that the changes are applicable to only new scans and rescans run from 6.14.2 SP1 forward.)

Workaround: The previously published inventory items are still available. Access the **Detector**, locate those inventory items that were previously published, and republish the inventory as needed.

Code Insight not applying default port in startup URL (SCA-23973)

If the URL that starts up the Code Insight Core Server and each Scan Server does not include a port, Code Insight does not automatically apply a default port, causing the startup to fail.

Workaround: Before starting a Code Insight server, ensure that the URL used to start up the server explicitly identifies the port (`80` for HTTP, `443` for HTTPS).

Group Builder reports not shown if Scan Servers have different “disableAnalyzer” values (SCA-21054)

Group Builder reports are not generated if multiple Scan Servers are configured with different values for the `disableAnalyzer` property in their `scanEngine.properties` file.

Workaround: If possible, configure all Scan Servers with the same value (`true` or `false`) for the `disableAnalyzer` property.

Multi-archived files not being associated with inventory (SCA-18782)

CodeAware uses a third-party utility provided by Apache to untar files. This utility does not recognize gz archives as valid and thus is unable to extract their contents for association with inventory during a scan.

CodeAware groups without associated component/version not being published (SCA-17301)

CodeAware groups without a selected component/version are not published to inventory. The Analyst should review the groups and associated findings for completeness and accuracy, and manually publish them to inventory based on their assessments.

Deleted groups reappearing on rescans (SCA-16931)

System-generated groups that were deleted during the auditing process are reappearing on a rescan.

Core Server not recognizing other Scan Servers when one becomes unresponsive (SCA-16549)

The Core Server fails to recognize other Scan Servers (in a multiple scan-server configuration) when one of the servers becomes unresponsive. You can check the Code Insight logs to determine which server is unresponsive so that you take appropriate action such as force-restarting the server.

Added product catalog entries not showing up in the request form until submitted (SCA-4490)

When some product catalog items are added while creating a request, the items do not show up on the creation page. However, when the request is submitted, the entries are shown.

Inventory not showing license text on Inventory Page for Cocoapod packages (SCA-4451)

When a Cocoapod package is scanned, the workspace inventory page does not show the license text when you click **View As-Found License Text**.

License matches in CSS files match entire file content (SCA-289/PAS-11021)

When a CSS file has license text included, scan results match the whole file to a license. No workaround is available. However, this issue will be addressed in the next generation of the product.

Exception during commit on Oracle: ORA-01400: cannot insert NULL into PALAMIDA.PSE_SCANNED_ITEMS.NAME (SCA-278/PAS-10636)

This error occurs when scanning files inside archives that do not have a proper name.

Workaround: Rename the files or scan with archives “off”.

Scan hangs with for file paths containing special characters (PAS-11096)

The issue occurs due to non-UTF8 encoding. We are investigating a fix for the next release.

Analyzer: P1-P3 legends are not showing colors in (PAS-11074)

Priority colors are not showing correctly in the Bill of Materials in IE, Firefox and Edge.

Workaround: Use Chrome.

Group and tag counts for files inside archives (PAS-10134)

When files inside archives are added to/removed from groups, are tagged/untagged, or are marked as reviewed/unreviewed, group and tag file counts are not affected—that is, they do not increase or decrease. This behavior applies to all scan settings including the "scan files inside archives=on" setting.

For example, if a workspace contains 20 files total, one of which is an archive `foo.zip` with 1000 inner files, marking 1000 inner files as reviewed will *not* increase the "Reviewed" tag count.

This behavior is in place after considering extensive feedback from customers who reported that including archive files in the count skews the perception of the amount of total work done. Per the example, seeing the number of files reviewed jump to over 1000 would confuse most auditors. For this reason, Code Insight does not include inner files of archives in the file counts. Best practice is to always mark the outer archive as reviewed when dealing with archives.

Tag Archive for Scanning group/tag counts (PAS-10110)

Code Insight offers the option to tag a specific archive for scanning so that files inside archives are processed for indicators in future scans. Note that group and tag file counts will not be updated to include files inside the archives when this tag is turned on. We will continue to work on this feature pending customer feedback about how to process file counts for archives. See the Group and tag counts for files inside archives (PAS-10134) issue for additional information.

Detector file tree count is inconsistent with group/tag counts (PAS-9917)

It is not uncommon to see a Detector file tree count differ from the group/tag counts. The count in the lower left-hand corner of Detector represents the total number of *nodes* currently available in the Detector file tree. In the presence of inner files of archives (which are not included in group/tag file counts, this number is typically larger than the group/tag count. For additional information regarding this count, see the "Archive File Counts/Nested Archives" section of the *Code Insight User Guide*.

Incremental scan affects file counts (PAS-2829)

The workspace file counts incorporate files that have been deleted prior to last scan if incremental scan is disabled. Files that have been deleted prior to the last scan may still be counted toward the total file with and without indicators value.

Workaround: Enable incremental scanning.

Copyrights with multi-byte characters may not be detected by the scanner (PAS-2774)

If a copyright statement contains multi-byte characters, the copyright will be classified as -unparseable- rather than as a valid copyright with a valid copyright holder. No workaround is available.

Ignore workspace matches is not reliable (PAS-2405)

The Ignore Workspace Matches option for components in Detector (whether done one at a time or in bulk) does not always suppress all matches to this component.

Workaround: Mark any groups created for the component you wish to ignore as "Ignored".

Limitations for custom inventory statuses

Currently custom inventory items are not available for inventory searches and are not supported in the Detector and in APIs.

Procedure to disable the display of RubySec security advisories

For various reasons, when analyzing and reviewing project inventory, a customer might not want to view vulnerabilities available from *all* security data sources supported by Code Insight. The following property has been added to the `core.properties` file to disable (or enable) the display of security vulnerability information gathered from RubySec advisory sites. By default, the property is set to `false`. By setting it to `true`, vulnerability data from RubySec advisories is *not* displayed.

```
disable.rubysec=true
```

Additionally, if you make a change to this property, Code Insight must be restarted and an Electronic Update performed to put the change into effect.

The following property has also been added to enable (or disable) the ability to force an Electronic Update. By default, the property is set to `false`. By setting it to `true`, the user can manually trigger an Electronic Update as needed (using the Manual Update facility accessed through **Administration | Updates**):

```
enable.forceupdate=true
```

Analyzer configuration to parse transitive dependencies in POM files

As of 6.12.1, the Analyzer executes as an autorun script that no longer needs to process the `analyzer.properties` file for configuration purposes. In general, the Analyzer parses transitive dependencies of jar files in a `pom.xml` file, but the autorun script is limited to parsing only those files found within the scan root folder of the workspace. A setting in the formerly used `analyzer.properties` file, however, parses transitive dependencies in POM files whether those dependencies are within or outside of the scan root folder of the workspace.

To ensure that transient dependencies external to the scan root folder are parsed, enable the "transitive dependencies" functionality available in `analyzer.properties`:

1. Navigate to **Administration | Metadata**.
2. Select the **Project** tab.
3. Click the **Add Project Metadata Field**, and follow these steps to create a metatdata field:
   a. In the **Name** and **Display Name** fields, enter **`Analyzer Resolve Transitive Dependencies`**.
   b. Select **Yes/No** for **Input Type**.
   c. Click **Save**.
4. Click **My Projects**, and open a project.
5. Click the **View Project Metadata** button on the **Summary** tab.
6. Click **Edit**, and select **Yes** for **Analyzer Resolve Transitive Dependencies**.
7. Click **Save**.

For each project workspace scanned with the Analyzer enabled, transitive dependencies are parsed, even those external to the scan root folder.

ScriptRunner and Scripting

The following are known issues related to the scriptRunner and scripting.

Warnings generated for scripts executed by upgraded scriptRunner (SCA-33640, SCA-22643)

When a script is executed using the upgraded scriptRunner (see ScriptRunner Upgrade), a “loader constraint violation” warning might be erroneously issued. Users can ignore this message since script execution is not impacted. This issue will be a addressed in a future release.

Unable to run configurePalamidaAnalyzer.groovy script (SCA-33436)

Currently, users are unable to use the scriptRunner to execute the `configurePalamidaAnalyzer.groovy` script.

NoSuchMethodError on some scripts/reports (PAS-10740)

This issue occurs due to a potential mismatch in the ant and ant-launcher jars. If you encounter a “NoSuchMethodError” when attempting to run a script or report, replace the ant-launcher jar file in the webapps directory with `ant-launcher-1.8.3.jar`.

Space in command-line argument to scriptRunner Scripts

Some users are reporting issues in running scriptRunner scripts if the command line argument to the script contains a space. This issue can be addressed by surrounding the line argument with single or double quotes.

For example, to pass the project name “My Project” to the `exportWorkspaceData.groovy` script, use the following commands:

Linux

```
./scriptRunner.sh -u myUser -c http://localhost:8888/palamida/ ../scripts/
    exportWorkspaceData.groovy -project 'My Project'
```

Windows

```
./scriptRunner.bat -u myUser -c http://localhost:8888/palamida/ ../scripts/
    exportWorkspaceData.groovy -project "My Project"
```

Changes to scriptRunner library jars causing issues for older scripts

Scripts that rely on older POI libraries may not work in this version of the product.

Workaround: Manually add the libraries to the /scriptRunner/lib directory, and modify scriptRunner.conf file to include the jars. As an alternative, modify the script for compatibility with POI 11.

SPDX Generator Report

The following are known issues related to the SPDX Generator Report.

License matches include more text than just license (SCA-2327)

The SPDX Generator Report shows too much license text in some cases. This is due to license detection limitations in Code Insight. We hope to resolve this issue in the near future with a new regex implementation for license matching.

Workaround: Ensure that you perform a review of all group license data, and make modifications to the "As-Found License Text" group field value to override any automated extracted licenses processed by the report.

Copyright detection captures non-copyright strings

The SPDX Generator Report displays non-copyright strings in some cases. This is due to a limitation to automated copyright detection in Code Insight.

Workaround: Ensure that you perform a review of all group copyright data, and make modifications to the "Copyright Text" group field value to override any extracted copyrights processed by the report.

Custom associations of components not being copied during Project Copy

Custom associations of components to namespaces are not copied over during a project copy.

Workaround: Re-apply the custom association for each target workspace once the project copy completes.

Web UI

The following are known issues related to the Code Insight Web UI.

Research page not sorting properly with "Important Only" Turned Off (SCA-20764)

When you unselect **Important Only** on the **Research** page for components, the results are sorted by page, not by the total number of records.

Review Status column sorting with "Show All" unchecked (PAS-11129)

Users may see review status out of order when sorting on a subset of available items.

Workaround: Use "Show All" when sorting.

Web session timeout taking user to Login.htm instead of SSO login (PAS-10238)

This issue applies only to SSO environments. In the case that the user is taken to the Login.htm page instead of back to the last accessed page, users should use the browser's "back" button to return to the page. As an alternative, the Login.htm page may be modified to instruct the user to start a new session. For example, "Sorry, your session has expired—please close and relaunch your browser to start a new session".

Workflow

The following are known issues related to the Code Insight workflow.

Dynamic constraint definition with non-visible values (PAS-10794)

Dynamic default values and rules support the dynamic change of the values in a dropdown list based on the value entered in another field. However, this only works if the dropdown list form field is currently visible/editable in the current state. No workaround is available.

Technical Notes

The following sections provide technical information not included in the current user documentation.

- Configuring Dynamic Selection of a Request Reviewer

Configuring Dynamic Selection of a Request Reviewer

This Code Insight feature (also called the People Picker) allows a user to select an individual (such as a manager) as the designated assignee for a component request at a particular review level. For example, your company's business logic might dictate that the first review on a request for an OSS component be performed by the requester's direct manager. Code Insight supports this scenario by allowing the workflow project owner to designate a form field that enables the selection of an appropriate reviewer for a particular review level. At runtime, the requester can then use this field to search a pool of managers in order to choose one assignee to continue the review process.

The following procedure provides an example of how to update the short request form (`request_form_short.sql`) and long request form (`request_form_long.sql`) for your database to add a reviewer selection field. Both scripts are located for your database type in the `dbScripts` directory of your Code Insight installation directory.

Task ***To configure a new field for the dynamic selection of a reviewer:***

1. Execute the following appropriate update scripts in your database to display a reviewer selection field for a specific review level on the short or long request form. Note the following about the scripts:

   - The attribute name in the example is `PeoplePickerList`; the displayed field name is **People Picker List**. However, you can provide your own names for the attribute and field.
   - The attribute must have an `INPUT_TYPE` and `TYPE` value of `P`.

   Short Form Scripts

   Run both scripts to update the short request form with a viewer selection field:

   ```
   INSERT INTO PAS_REQ_DEF_ATTR
   (ID_,REQUEST_DEFINITION_ID_,STAGE_ID_,SEQUENCE_,NAME_,DISPLAY_TEXT_,INPUT_TYPE_,TYPE_,HEL
   P_TEXT_) VALUES (1111,1,1100,13,'PeoplePickerList','People Picker List','P','P',NULL);

   INSERT INTO PAS_REQ_DEF_ATTR_ACCESS_RULE (ID_, REQ_DEF_ATTR_ID_, ACCESS_TYPE_,
   WORKFLOW_ROLE_ID_, REVIEW_LEVEL_, REVIEW_LEVEL_STATE_) VALUES (111101,1111,'E',1,0,'E');
   ```

   Long Form Scripts

   Run both scripts to update the long request form with a viewer selection field:

   ```
   INSERT INTO 6110db.PAS_REQ_DEF_ATTR
   (ID_,REQUEST_DEFINITION_ID_,STAGE_ID_,SEQUENCE_,NAME_,DISPLAY_TEXT_,INPUT_TYPE_,TYPE_,HEL
   P_TEXT_) VALUES (2112,1,2100,12,'PeoplePickerList','People Picker List','P','P',NULL);

   INSERT INTO 6110db.PAS_REQ_DEF_ATTR_ACCESS_RULE (ID_, REQ_DEF_ATTR_ID_, ACCESS_TYPE_,
   WORKFLOW_ROLE_ID_, REVIEW_LEVEL_, REVIEW_LEVEL_STATE_) VALUES (211201,2112,'E',1,0,'E');
   ```

2. As an administrator, create a user list to which to point the new attribute. For instructions on creating a user list, refer to the "Administration Menu: Users Option" topic in the online help or in the *Code Insight User Guide*. This list must contain the specific users (for example, managers) from which you want the person creating the request to select a reviewer. Be sure that the **User List Type** is set to **Reviewer**.

   For purposes of this example, the user list created is called `ReviewList`.

3. In your Code Insight installation directory, open the `config/core/core.properties` file in a text editor, and add the following line to identify the new property:

   ```
   <REQUEST_ATTRIBUTE_NAME>.filtered.userlist = <USER_LIST_NAME>
   ```

   where:

   - `<REQUEST_ATTRIBUTE_NAME>` is the name of the attribute (the `<NAME>` value used in the script in step 1).
   - `<USER_LIST_NAME>` is the name of the user list created in step 2.

   For this example, you would enter the following:

   ```
   PeoplePickerList.filtered.userlist = ReviewList
   ```

4. (Optional) Note that, by default, requesters can select their own name from this list of potential reviewers when it is opened in the Code Insight user interface. If you want to disable the ability of requesters to select themselves as reviewers (for security reasons, for example), set the following property to `true` in `core.properties`:

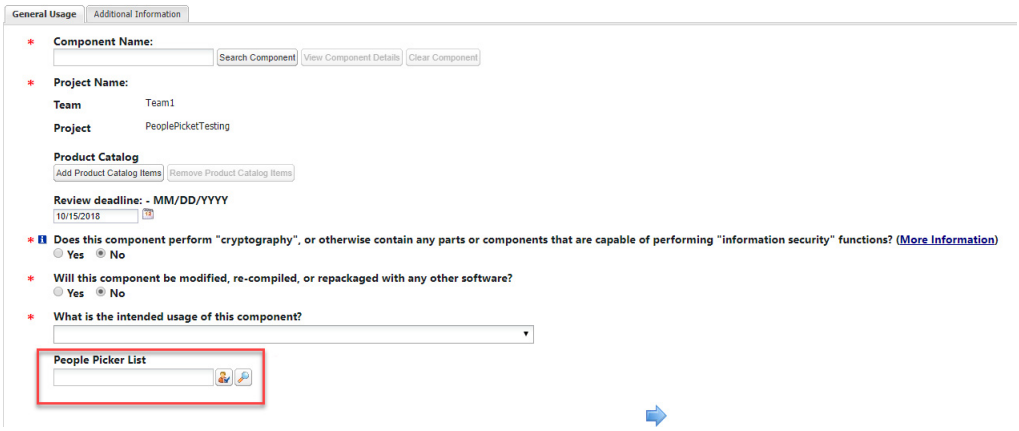
   ```
   people.picker.disable.self.approve=true
   ```

   With this configuration, when requesters attempt to select their own name, they receive a message stating their inability to do so and forcing them to make another selection.

5. Restart the Code Insight Core Server.

6. In Code Insight user interface, open a project, navigate to the appropriate "review level" tab on the **Project Details** page, and select the newly created field from the **Select request form field containing reviewers for this review level drop-down list**. In this example, you would select **People Picker List**.

7. Log in to Code Insight as a requester, navigate to the **Requests** dashboard, and select **Add New Request**. to add a new request for the project. On the **Usage** tab of the page, you will see the new field containing the user list.



Migrating Your Current Code Insight Version to 6.14.2 SP1

The following describes the process for migrating your current version of Code Insight to the latest version:

- Requirements
- Preparing the Environment
- Upgrading Code Insight
- Verifying the Upgrade
- Note about SSL Configuration for HTTPS
- Reverting to a Previous Version

Requirements

The following sections describe the requirements for migrating to Code Insight 6.14.2 SP1:

- Supported Code Insight Versions for Migration to 6.14.2 SP1
- Additional Requirements

Supported Code Insight Versions for Migration to 6.14.2 SP1

You can migrate any of the following Code Insight versions to the 6.14.2 SP1 version: 6.14.2, 6.14.1, 6.14.0, 6.13.*x*, 6.12.*x*, 6.11.*x*, 6.10.3, and 6.10.0. To migrate from Code Insight versions older than 6.10, contact Revenera Support. (Support contact information is available from the **Get Support** menu on the Revenera Community site https://community.revenera.com.)

Additional Requirements

You will need the following to perform the upgrade:

- The plain text database password for the user and database defined in `core.db.properties`.
- Enough free disk space to perform backups. Check the size of your workspaces directory, which may be large.
- The Code Insight 6.14.2 SP1 distribution zip file. Contact your Flexera representative if you do not have a copy.
- The appropriate JDBC driver for OpenJDK 8 (downloaded to the `tomcat\lib` directory) if you are switching from Oracle JDK to Zulu OpenJDK for your SQL Server database. You can locate and download the driver from this site:

  https://docs.microsoft.com/en-us/sql/connect/jdbc/system-requirements-for-the-jdbc-driver?view=sql-server-2017
- The `migrationImport.groovy` script, located in the `scriptRunner\scripts` directory of your 6.14.2 SP1 application directory. This script copies the properties and configurations from your existing application directory (`OLD_DIR`) to the new application directory (`NEW_DIR`) and notifies you of any additional steps needed.
- The `migrate.sh`/`migrate.bat` script, located in the `scriptRunner\bin` of your 6.14.2 SP1 application directory. This script migrates your existing database schema from the existing version of Code Insight to the new version.
- Outgoing Internet access on port 22 for the Core Server to have the Electronic Update run automatically at its scheduled time once the upgrade is complete. Otherwise, you must run the Electronic Update manually.
- (If you have custom core reports) The initial custom SQL scripts used to install your custom core reports.

- (Optional) The `migrateFromAnalyzerToCodeAware.groovy` script located in of your 6.14.2 SP1 application directory. This script updates workspaces that were previously configured for the Analyzer to now use CodeAware. If you do not run this script, CodeAware is *not* automatically selected on the **Automated Analysis** tab for existing workspaces. You will need to manually select it for each workspace you intend to rescan using CodeAware.

Preparing the Environment

These instructions refer to the following variables. You can create a temporary file with this information to use as a reference throughout the migration.

Note ▪ *The following are examples for a Linux/MySQL installation. Be sure to replace the sample values below with those of your installation.*

```
# Current installed version.
OLD_VER="6.13.3"
# Current app directory.
OLD_DIR="/opt/CodeInsight/6.13.3"
# New app directory, which will be created.
NEW_DIR="/opt/CodeInsight/6.14.2 SP1"
# Base directory for backups (a 6.14.2 SP1 subdirectory will be created).
BACK_DIR="/opt/CodeInsight/backup"
# Core server only - MySQL Database info.
DB_HOST="localhost”
DB_NAME="CodeInsight"
DB_USER="myUser"
DB_PASS="myDbPassword"
# Scan servers only - Workspaces directory.
WS_DIR="/opt/CodeInsight/workspaces"
```

You can paste the above into a file on the server (for example `/tmp/code_insight_env`) and edit the values. Then you can run `source /tmp/ code_insight _env` to set the variables used in this guide. After the upgrade is complete, be sure to run `rm /tmp/code_insight_env` if the file contains the database password.

Upgrading Code Insight

The following commands are for Linux. Windows users may choose to perform the steps with a mouse.

1. Shut down Code Insight. For multi-server installs, shut down all servers.

   ```
   cd $OLD_DIR/tomcat/bin
   ./shutdown.sh
   ```

2. Back up the database. This step applies to the Core Server only.

   The following commands are for MySQL. If you are using Oracle or SQL Server, obtain a fresh backup from your DBA before proceeding. Make sure your DBA is available to restore the backup promptly in case it is needed.

   ```
   mkdir -p $BACK_DIR/$OLD_VER
   cd $BACK_DIR/6.14.2 SP1
   ```

```
mysqldump -h $DB_HOST -u $DB_USER --password=$DB_PASS -r migration_db.sql $DB_NAME
```

3. Backup the workspaces directory. This step applies to all Scan Servers.

```
cd $WS_DIR
tar cf $BACK_DIR/$OLD_VER/migration_ws.tar .
```

***Note** ▪ This backup can take a long time depending on the size of your workspaces directory.*

4. Backup the application directory.

```
cd $OLD_DIR
# clear the tomcat temp files
rm -r tomcat/temp/*
tar czf $BACK_DIR/$OLD_VER/migration_app.tgz .
```

5. Extract the 6.14.2 SP1 distribution zip file (`CodeInsight-6.14.2 SP1.zip`) and move it to the new directory.

```
unzip -q CodeInsight-6.14.2 SP1.zip -d /tmp
mv /tmp/CodeInsight_6.14.2 SP1 $NEW_DIR
```

6. Run the `migrationImport.groovy` script.

```
cd $NEW_DIR/scriptRunner/bin
./scriptRunner.sh -n ../scripts/migrationImport.groovy $OLD_DIR
```

7. Check the TODO log for any additional steps needed. Complete any necessary steps before continuing.

```
cat $NEW_DIR/scriptRunner/log/migration.TODO.log
```

8. Run the database schema migration. This step applies to the Core Server only.

```
cd $NEW_DIR/scriptRunner/bin
./migrate.sh $OLD_VER
```

If database errors are encountered, rerun the database schema migration after resolving the error.

9. Run the new `reports.sql` to install new reports. Use the appropriate file according to your database vendor (MySQL in this example). This step applies to the Core Server only.

***Note** ▪ The reports.sql file will overwrite any modifications to the report tables in the database. If you have custom reports, you will need to re-run the custom SQL to install them after you have run the new reports.sql file. Make sure you have your custom SQL scripts before you run this.*

```
mysql -h $DB_HOST -u "$DB_USER" --password="$DB_PASS" -D $DB_NAME \
-e "source $NEW_DIR/dbScripts/mysql/reports.sql"
```

***Note** ▪ Code Insight 6.14.2 SP1 has features that require a Data Services Enabled key. You can continue to use the application with your existing key, but there will be errors seen with the features that require this key.*

10. Start the new Code Insight application. For multi-server installs, do this after you have completed the previous steps on all servers.

    ```
    cd $NEW_DIR/tomcat/bin
    ./startup.sh && tail -f ../logs/catalina.out
    ```

11. Check the log for any errors, and resolve them before continuing.

12. (Optional) Run the `migrateFromAnalyzerToCodeAware.groovy` script to update workspaces that were previously configured for the Analyzer to now use CodeAware. (The script automatically selects CodeAware on the **Automated Analysis** tab for each of these workspaces; it ignores workspaces already configured for CodeAware.) The script will prompt you for the scope on which it should run—on all projects, on a specific project, or on a specific workspace.

    Note the following:

    - Before running the script, ensure that the property `disableAnalyzer`, located in the `scanEngine.properties` file, is set to `true`.
    - The script is needed for only those project workspaces that you intend to rescan, so select a scope that makes the most sense.
    - If you do not run this script, CodeAware is *not* automatically selected on the **Automated Analysis** tab for workspaces previously configured to use the Analyzer. For each workspace that you intend to rescan using CodeAware, you will need to manually select the CodeAware option.

13. (Optional) Rerun your initial custom SQL scripts used to install your custom core reports.

14. Log into the Web UI and run the Electronic Update. This step applies to the Core Server only.

    ***Note** ▪ Do not skip this step.*

    In most cases, the Electronic Update will be scheduled automatically. Check the **Scheduler** tab in the Web UI. If the update is not running, trigger it through **Administration > Updates**, and click **Check for Electronic Update**.

    If your application does not have outgoing Internet access on port 22, you will need to run the update manually.

    ***Note** ▪ If you run into any issues with detection of Cocoapod packages, re-run the Electronic Update.*

Verifying the Upgrade

User this procedure to verify that the upgrade is successful.

1. Log into Code Insight and go to **Help > About** to verify the version.
2. Create a test project and workspace.
3. Ensure that the Detector client launches for the workspace.

4. Close Detector and schedule a scan.

Note ▪ *If you face certificate errors on startup of the Scan Server or if you are unable to see your Scan Server from the application UI, you must import the certificate being served by Tomcat on the Scan Server into the JDK of the Core Server.*

Note about SSL Configuration for HTTPS

When configuring HTTPS for Code Insight, you must update the `tomcat\https\server.xml` file in your Code Insight installation directory with site-specific information (see "Enabling HTTPS for a Code Insight Server" in the *Code Insight Installation & Administration Guide*). For security purposes, when you migrate to 6.14.2 SP1 and later, the default value for the `sslEnabledProtocols` parameter in SSL section of this file will be `"TLSv1.2"`:

```
...
keystorePass="palamida"
clientAuth="false"
sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"
keystorePass="palamida"
...
```

Whenever you manually configure this file for HTTPS configuration, ensure that you do not change the default `"TLSv1.2"` to another value.

Reverting to a Previous Version

1. Ensure the Code Insight server is stopped. For multi-server installs, ensure all servers are stopped.
2. Restore the database. This step is performed on the Core Server only.

   The following commands restore the MySQL database. If you are using Oracle, have your DBA restore the backup.

   ```
   cd $BACK_DIR/6.14.2 SP1
   mysql -h "$DB_HOST" -u "$DB_USER" --password="$DB_PASS" -D "$DB_NAME" < db_migration.sql
   ```

3. Restore the workspaces backup. This step is performed on each Scan Server.

   Note ▪ *If you did not open, create, or scan any workspaces while the new version was running, you can skip this step.*

   ```
   cd $WS_DIR
   tar xf $BACK_DIR/6.13.3/ws_migration.tar
   ```

4. Start the previous application. For multi-server installs, do this after you have completed the previous steps.

   ```
   cd $OLD_DIR/tomcat/bin
   ./startup.sh && tail -f ../logs/catalina.out
   ```

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

Restricted Rights Legend