



**SecureAssist Eclipse Plugin**

**User Guide**

August 2016

Copyright © 2016 by Codiscope, LLC. All rights reserved. No part or parts of this documentation may be reproduced, translated, stored in any electronic retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the copyright owner. Codiscope retains the exclusive title to all intellectual property rights relating to this documentation.

The information in this documentation is subject to change without notice and should not be construed as a commitment by Codiscope. Codiscope makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data, or claims for or on behalf of user's customers) that may be suffered by the user.

Codiscope and the Codiscope logo are trademarks of Codiscope, LLC. Other brands and products are trademarks of their respective owner(s).

Codiscope, LLC  
20 Park Plaza, Suite 1400  
Boston, MA 02116  
Phone: + 1 (617) 804-5428  
[info@codiscope.com](mailto:info@codiscope.com)

[codiscope.com](http://codiscope.com)

# Table of Contents

<b>1</b>	<b>SecureAssist Setup</b> .....	<b>1</b>
	What is SecureAssist?.....	1
	Install the SecureAssist Plug-in .....	1
	Activate a License.....	3
	Updating SecureAssist.....	4
	Set Up SecureAssist Views .....	5
<b>2</b>	<b>Scanning</b> .....	<b>6</b>
	Scanning Individual Files .....	6
	<i>Automatic Scans</i> .....	6
	<i>Manual Scans</i> .....	6
	Scanning an Entire Project .....	6
<b>3</b>	<b>Reviewing Issues</b> .....	<b>8</b>
	Individual Files .....	8
	<i>Viewing Findings</i> .....	8
	<i>Grouping Results</i> .....	9
	Reviewing an Entire Project .....	10
	<i>Viewing</i> .....	10
	<i>Grouping and Sorting</i> .....	10
	<i>Filtering</i> .....	11
	<i>Exporting</i> .....	12
	Suppressing Issues.....	12
	Deactivating a Rule for a File or Session .....	13
	Tracing Untrusted Sources with the Call Chain .....	14
<b>4</b>	<b>Fixing Issues</b> .....	<b>16</b>
	View Guidance for an Issue.....	16
	Rescanning Corrected Code .....	16
<b>5</b>	<b>Project Metadata</b> .....	<b>17</b>
<b>6</b>	<b>Preferences</b> .....	<b>19</b>
	License Details .....	19
	Review Settings.....	19
	Deactivating a Rule Permanently .....	19
<b>7</b>	<b>More Support</b> .....	<b>21</b>

# 1 SecureAssist Setup

## What is SecureAssist?

Codiscope SecureAssist™ is an IDE plug-in for Eclipse that helps you eliminate critical problems earlier in the SDLC by pointing out vulnerabilities while you are writing code and teaching you how to fix them yourself. When you open or save a file, SecureAssist quickly scans the code in the background and identifies security issues. At any time, you can review the issues, identify possible problems, and then learn how to fix any vulnerabilities—long before your code goes into production.

## Install the SecureAssist Plug-in

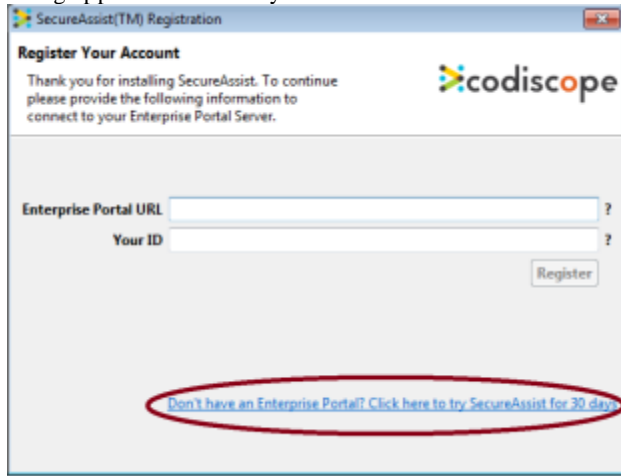
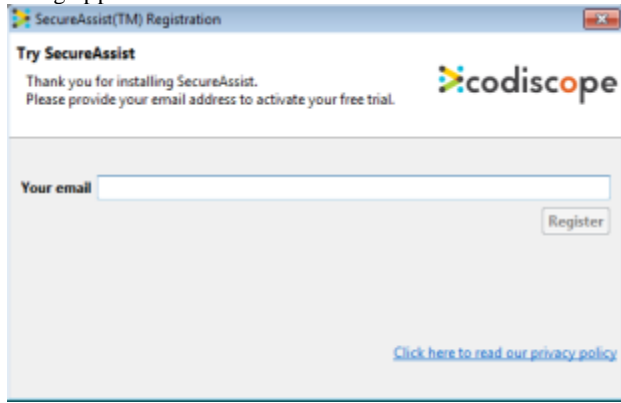
SecureAssist installation instructions for the various versions of Eclipse follow. To ensure your Eclipse environment meets the minimum system requirements, go to our [IDE compatibility page](#).

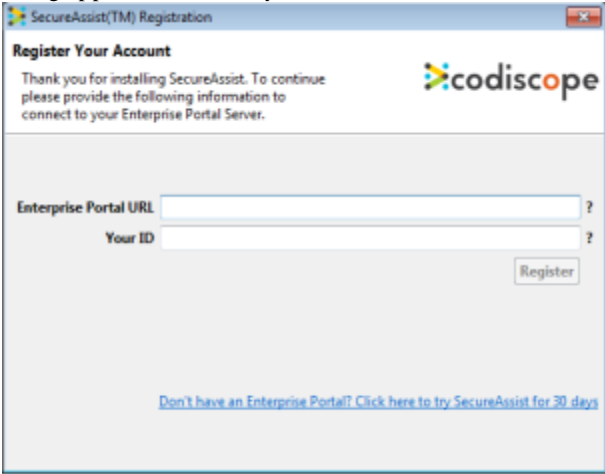
IDE Version	Install Instruction
Eclipse 4.3-4.5	<ol style="list-style-type: none"> <li>1. In Eclipse, select <b>Help &gt; Install New Software</b>. The Install dialog appears.</li> <li>2. Click <b>Add</b>. The Add Repository dialog appears.</li> <li>3. Enter the location of the SecureAssist update folder: <ul style="list-style-type: none"> <li>▪ Local installation: If you have a local copy of SecureAssist (e.g., you downloaded a trial version), click <b>Local</b>, browse to the SecureAssist update folder, then click <b>OK</b>.</li> <li>▪ Remote installation: If your company installed SecureAssist on an internal server, enter a name and the URL to your company's update site, then click <b>OK</b>.</li> </ul> </li> <li>4. On the Install dialog for Available Software, select <b>SecureAssist Features</b>. If you have the PHP supported library and PHP Development Tools (PDT) installed, also select <b>SecureAssist PHP Support</b>. If you do not have the appropriate PHP libraries, do not select this option as it may trigger errors when you use Eclipse.</li> <li>5. Click <b>Next</b>.</li> <li>6. Review and accept the license agreement, then restart Eclipse to complete the installation.</li> <li>7. For CentOS and Red Hat Linux operating systems, additional libraries need to be installed for SecureAssist windows to display correctly. <ol style="list-style-type: none"> <li>a. From the Linux command line, execute <code>yum install webkitgtk</code> and <code>yum install epel-release</code>.</li> <li>b. From the CentOS 7.2 or RHEL 7.2 command line, execute <code>yum install webkitgtk.x86_64</code>.</li> <li>c. Modify <code>/etc/profile</code> by adding the following to the bottom: <code>"export SWT_GTK3=0"</code></li> <li>d. If intending to access Eclipse via VNC, run Eclipse with <code>'export DBUS_SESSION_BUS_ADDRESS=""'</code>.</li> </ol> </li> </ol>



## Activate a License

After you install SecureAssist, you need to activate its license. The following table describes the activation steps for trial and enterprise licenses.

License Type	Activation Instructions
<i>Trial</i>	<p>Once the license expires after 30 days, you must upgrade to continue using SecureAssist.</p> <ol style="list-style-type: none"> <li>After installing SecureAssist, restart Eclipse. The Registration dialog appears automatically.           <div data-bbox="613 611 1230 1083" data-label="Image">  </div> </li> <li>Click the URL at the bottom of the dialog. The Trial Registration dialog appears.           <div data-bbox="613 1146 1230 1545" data-label="Image">  </div> </li> <li>Enter your email in the text box, then click Register. A popup will confirm your trial registration.</li> </ol>

License Type	Activation Instructions
<i>Enterprise</i>	<ol style="list-style-type: none"> <li data-bbox="558 302 1242 365">1. After installing SecureAssist, restart Eclipse. The Registration dialog appears automatically.</li> </ol>  <ol style="list-style-type: none"> <li data-bbox="558 844 1242 898">2. If it is not already prepopulated, enter your <b>Enterprise Portal URL</b>. If you don't know the URL, contact your IT administrator.</li> <li data-bbox="558 907 1242 961">3. In <b>Your ID</b>, enter your email address or network ID. If you're unsure what to enter, contact your IT administrator.</li> <li data-bbox="558 970 1242 1003">4. Click <b>Register</b>. A popup will confirm your registration.</li> </ol>

## Updating SecureAssist

When SecureAssist issues a new version or upgrade, use the Eclipse Update Manager to update your copy.

1. In Eclipse, go to the **Help** menu and select the update or configuration option. Your selection depends on which Eclipse version you are using.

IDE Version	Install Instruction
Eclipse 4.3-4.5	<ol style="list-style-type: none"> <li data-bbox="690 1409 1242 1518">1. Select <b>Help -&gt; Check for Updates</b>. The system scans for updates and shows any found on the Available Updates dialog.</li> <li data-bbox="690 1518 1242 1564">2. Select <b>SecureAssist</b>, then click <b>Next</b>.</li> </ol>

2. If shown the licenses or updates, review and accept them.
3. Restart Eclipse to complete the installation.

## Set Up SecureAssist Views

SecureAssist has several views in Eclipse to work with. Issue List is the primary view and **MUST** be displayed for SecureAssist to operate. Once a view is opened, it remains displayed in future Eclipse sessions until you manually close it. The following table describes the views.

Pane	Description
<i>Issue List</i>	The main view. You must have the Issue List open for SecureAssist to function. It displays potential security vulnerabilities in the active file, and updates automatically each time an individual file is opened or saved.
<i>Project Review</i>	Allows SecureAssist to review an entire project rather than a project file. Reviewing a project takes longer than reviewing a single file and requires more memory.
<i>Call Chain</i>	Lists the files and lines of code an untrusted source passes through to create a given potential vulnerability.
<i>Guidance</i>	Displays secure coding guidance on an issue selected in the Issue List or Project Review.
<i>Guidance Search</i>	Allows a text search of SecureAssist guidance.

### ● Display a View

Remember that the first time you restart Eclipse after installing SecureAssist, you must manually select at least the Issue List for SecureAssist to function.

1. Open a file in Eclipse.
2. Select **Window -> Show View -> Other** to open the Show View dialogue, then expand the SecureAssist folder to display the SecureAssist views.
3. Select Issue List and any other desired views, then click **OK**. The views you selected will now appear in the Eclipse Workbench.



## 2 Scanning

### Scanning Individual Files

#### Automatic Scans

SecureAssist runs in the background without disrupting your work. Once the Issue List is open and you open a file, SecureAssist automatically reviews it for potential security issues, and the Issue List immediately populates with a list of all issues found in the scan.

#### Manual Scans

SecureAssist scans files in the background when you open them. Once you change a file, you can initiate a scan manually on demand.

##### ● Manually Initiate a Scan on a Single File

1. Once you've finished your changes, save your file in Eclipse.  
**OR**  
Click the **Review file** icon in the Issues List view.



The Issue List immediately populates with a list of all issues found in the scan.

### Scanning an Entire Project

SecureAssist is designed to detect issues as you write them, in a single file. However, you can also use it to review an entire project or resource. A resource can be a package or folder within a project.

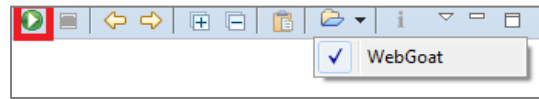
**Warning!** Project reviews use more memory than a single file review. Ensure your Eclipse environment meets the system requirements listed on our [IDE compatibility page](#).

##### ● Scan a Project

You can scan a resource from the Project Review view or the context menu of Package Explorer navigator in Eclipse.

1. In Eclipse, ensure that the SecureAssist Issue List and Project Review views are open.
2. Initiate a project scan by **EITHER**:

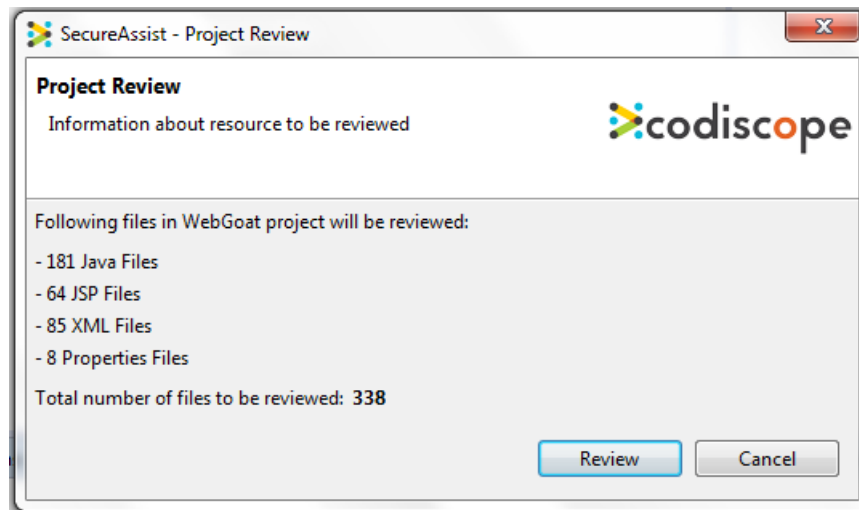
In Project Review, click the **Select Project** icon to display a list of all open projects in the workspace, select the desired project, then click the green arrow.



**OR**

In the Package Explorer, right-click the resource you want to review, then select **SecureAssist -> Review**.

The Resource Review dialog opens, displaying the total number of files to review by file type.



3. Click **Review** to begin the project scan. The Project Review populates with a list of all issues found in the scan.

## 3 Reviewing Issues

### Individual Files

#### Viewing Findings

Once SecureAssist finishes scanning, results are displayed in the Issue List for you to review. Individual issues are also indicated in the code view by a Rule Importance/Severity icon in the left margin.

#### ● View the Findings for an Individual File

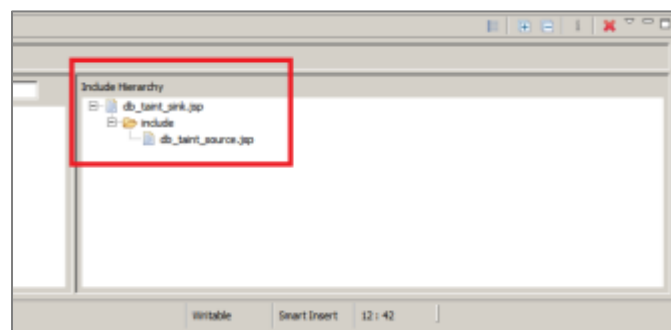
View the findings in the Issue List. From there, you can go quickly to the specific line of code where that vulnerability exists.

1. Navigate to the Issue List.

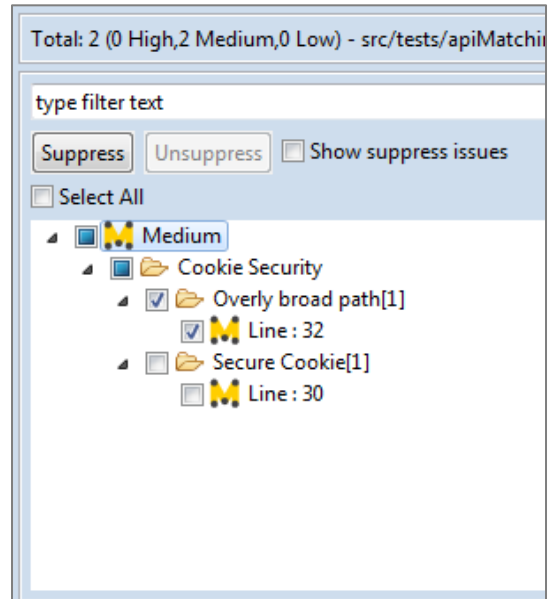
By default, results in the Issue List are grouped by Rule Importance (potential severity), Rule Category, and finally Rule Title, with individual issues listed in line order under Rule Title. The three levels of Rule Importance are:

- **H High.** Critical issues identified using taint analysis, including injection attacks and weak cryptography.
- **M Medium.** Moderate issues identified without taint analysis (e.g., via a smart search for APIs that are known to be insecure).
- **L Low.** Troubling issues found using regular expression rules, typically informational findings.

**Note:** When you review JSP files, a hierarchy pane appears within the Issue List, displaying the hierarchy of JSP files.



- Expand the folders until you see the line numbers of the issues.



- Click the line number of the issue you want to review. The line of code where the issue occurs is highlighted in the code editing window.
- To view a brief description of the issue, hover your cursor over the highlighted code (or the icon in the left margin).

## Grouping Results

By default, the results are grouped by rule importance first, but you can change the primary grouping to rule category, rule importance, rule title, or line number.

### ● Group the Results of an Individual Scan

- In the Issue List, click the **Group By** icon to display the grouping options.

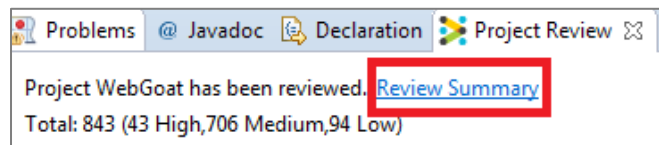


- Select the group you want to use as the primary grouping.

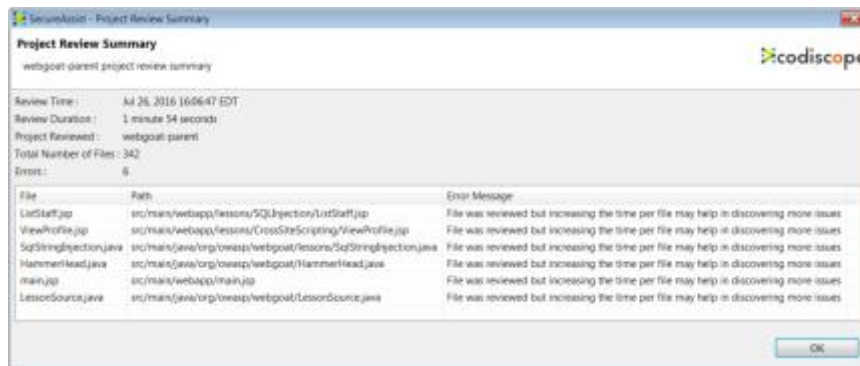
# Reviewing an Entire Project

## Viewing

Once the review is complete, issues are displayed in the Project Review view grouped by rule importance (severity).



On the Project Review, click the **Review Summary** hyperlink to display the total number of files, the duration of the scan, and the list of files with errors.

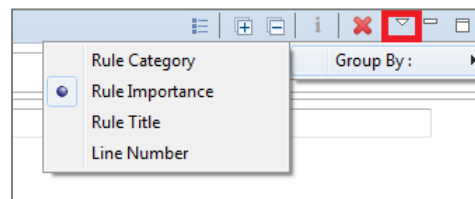


## Grouping and Sorting

By default, the results are grouped by rule importance first in descending order, but you can change the primary grouping to rule category, rule importance, rule title, or line number, in ascending or descending order.

### ● Group the Results of a Project Review

1. In the Project Review, click the **Order** icon to display the drop-down menu, then select **Group By**.



2. Select the group you want to use as the primary grouping.

### ● Order Results of a Project Review

1. With the Project Review view open, click the **Order** icon to display the drop-down menu, then select **Order**.

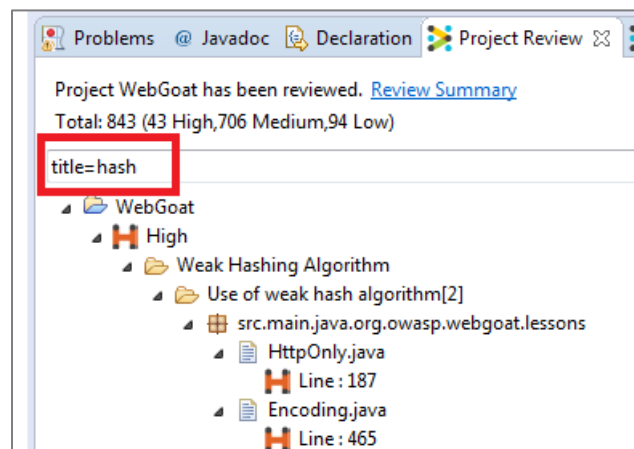
2. Select **Ascending** or **Descending**.

## Filtering

You can filter the results of a project review to display issues with matching package, rule category, rule title, filename, and description.

### ● Filter Results of a Project Review

1. In Project Review in the search box, type one of the following fields you wish to search, followed by an equal sign:
  - **package=** Searches for text only in package names
  - **category=** Searches for text only in rule category
  - **title=** Searches for text only in rule title
  - **filename=** Searches for text in file names
2. After the equal sign, type the text you wish to search for.



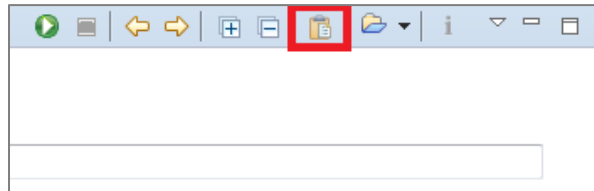
The results appear as you enter the text, sorted in descending order.

## Exporting

You can export findings from the Project Review to an XML file.

### ● Export Project Review Results

1. In the Project Review view, click the **Export Results** icon.



2. Select a location to save the exported results. The folder called “CSA-  
<Project-Name>” containing the results is saved in the selected location.

## Suppressing Issues

Sometimes you may not wish to view certain issues when reviewing results in SecureAssist. The **Suppress Issue** feature allows you to do this for both individual files and entire projects.

When you suppress an issue, SecureAssist either hides the issue completely or displays it in the Issue List grayed out so you can easily identify it as suppressed. **Show Suppressed Issues** is a toggle that turns display of suppressed items on and off. When suppressed items are displayed, you can still get guidance by double-clicking the issue in the Issue List or Project Review. However, there will be no sign of the issue in the Editing view.

A suppressed issue *will remain suppressed for the remainder of the current Eclipse session.*

### ● Show/Hide Suppressed Issues

1. Select the **Show Suppressed Issues** checkbox.  
**OR**  
Right-click anywhere in the Issue List or Project Review, and select **Show Suppressed Issues**.

Any issues that have been previously suppressed should appear with their icons grayed out.

2. Deselect the **Show Suppressed Issues** checkbox.  
**OR**  
Right-click anywhere in the Issue List or Project Review and deselect **Show Suppressed Issues**.

All suppressed issues will now be hidden.

## ● Suppress an Issue

There are two ways to suppress an issue.

### Suppress One or More Issues

1. Select one or more issues using the checkboxes.
2. Click the **Suppress** button. Depending on whether **Show Suppressed Issues** is selected, the selected issues are either hidden from view OR their icons appear grayed out to indicate they are suppressed.

### Suppress One Issue

1. Right-click on the line number in the Issue List or Project Review view.
2. Select **Suppress Issue** from the popup menu. Depending on whether **Show Suppressed Issues** is selected, the issue is either hidden from view OR its icon appears grayed out to indicate it is suppressed.

## ● Unsuppress an Issue

You can unsuppress an issue after it has been suppressed. To do so, **Show Suppressed Issues** must be selected. There are two ways to unsuppress an issue.

### Unsuppress One or More Issues

1. In the Issue List or Project Review, ensure that **Show Suppressed Issues** is selected.
2. Select one or more suppressed issues using the checkboxes.
3. Click the **Unsuppress** button. The issues are un-suppressed, their icons are displayed in color, and the issues are now highlighted in the Editing view and indicated by icons in the left margin.

### Unsuppress One Issue

1. In the Issue List or Project Review, ensure that **Show Suppressed Issues** is selected.
2. Right-click the desired suppressed issue and select **Unsuppress Issue** from the popup menu. The issue is un-suppressed, its icon is displayed in color, and the issue is now highlighted in the Editing view and indicated by an icon in the left margin.

## Deactivating a Rule for a File or Session

To stop viewing results for a given vulnerability altogether, you can deactivate the rule that creates those issues in SecureAssist. Unlike suppressed issues,

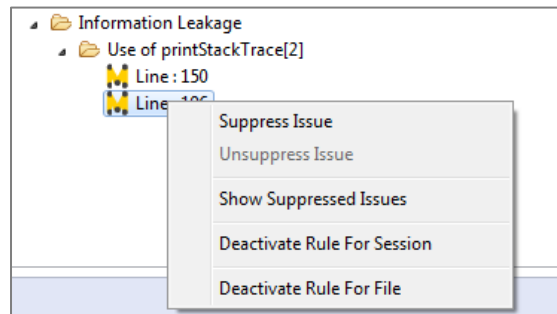


issues resulting from deactivated rules are always hidden until you reactivate the rule. You can deactivate a rule for an active file or all files for the remainder of the Eclipse session. *When Eclipse closes or restarts, the rule is reactivated.*

**Important!** This feature is available only when you are scanning an individual file.

### ● Deactivate a Rule

1. In the Issue List view, right-click an issue in the target rule folder to display the pop-up menu.



2. Select:  
**Deactivate Rule for Session.**  
**OR**  
**Deactivate Rule for File.**

All issues related to the target rule will be hidden for the remainder of the Eclipse session.

### ● Reactivate a Rule

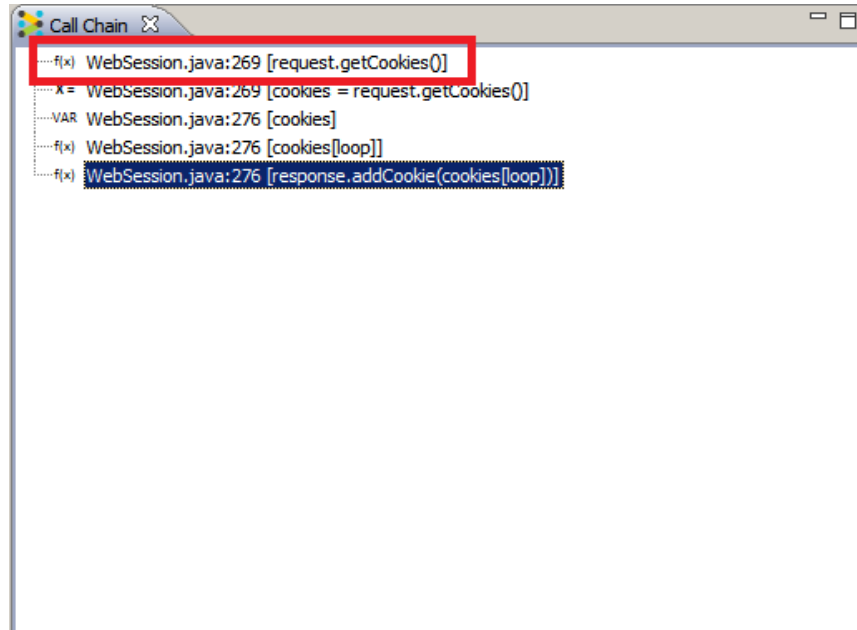
1. Right-click anywhere in the Issue List view, then select **Activate Rules for Session** OR **Activate Rules for File** from the popup menu. A flyout menu will display a list of all the rules that have currently been deactivated.
2. Select the specific rule you wish to reactivate. All issues identified by that rule will now appear in the Issue List.

## Tracing Untrusted Sources with the Call Chain

The Call Chain view traces how data from an untrusted source enters and passes through an application to create the specific issue selected in the Issue List or Project Review. It does this by displaying the files and specific code lines through which the data traveled. This information can greatly help you in diagnosing and remediating the issue.

## ● Trace an Untrusted Source Using Call Chain

1. Ensure the Call Chain view is displayed.
2. Select the line number of an issue in the Issue List or Project Review, then click the Call Chain tab. The Call Chain view displays each line that the untrusted source passed through to create the vulnerability, from its first appearance to its last. The first line of code shows where the untrusted source was introduced.



3. Click each line in the call chain to go to the line of code in the Editing view.

## 4 Fixing Issues

SecureAssist is not only a diagnostic tool, but it also helps you determine how to fix any issues flagged from your scan. The Guidance view provides concise, contextual information to help you correct an issue. The view includes:

- Brief and extended descriptions of the vulnerability.
- Examples of the code that causes it.
- Preferred code examples showing how to correct the issue.
- Best practice recommendations to avoid the issue in the future.
- Links to outside resources including OWASP and other third-party organizations.

Depending on your preference, you can choose to display the [Guidance view at all times](#), or you can display it only when you specifically choose to for an issue.

### View Guidance for an Issue

There are several ways to view guidance for an issue, depending upon whether you previously chose to [display the Guidance view](#).

#### ● View Guidance with Guidance View Displayed

1. Click an issue in the Issue List or Project Review.  
**OR**  
 Click the icon in the Editing view next to the desired issue.

Guidance for the issue is displayed in the Guidance view.

#### ● View Guidance with Guidance View Not Displayed

You can still view guidance information for an issue without having previously chosen to display the Guidance view.

1. Double-click an issue in the Issue List or Project Review.  
**OR**  
 Right-click the icon **H** in the left margin of the Editing view, then select **Show Guidance** from the popup menu. Guidance for the issue is displayed in a pop-up version of the Guidance view.

### Rescanning Corrected Code

After fixing issues based on SecureAssist guidance, you should re-scan the code in SecureAssist to ensure issues are remediated. If the problems have been remediated, they should no longer appear in the Issue List or Project Review.

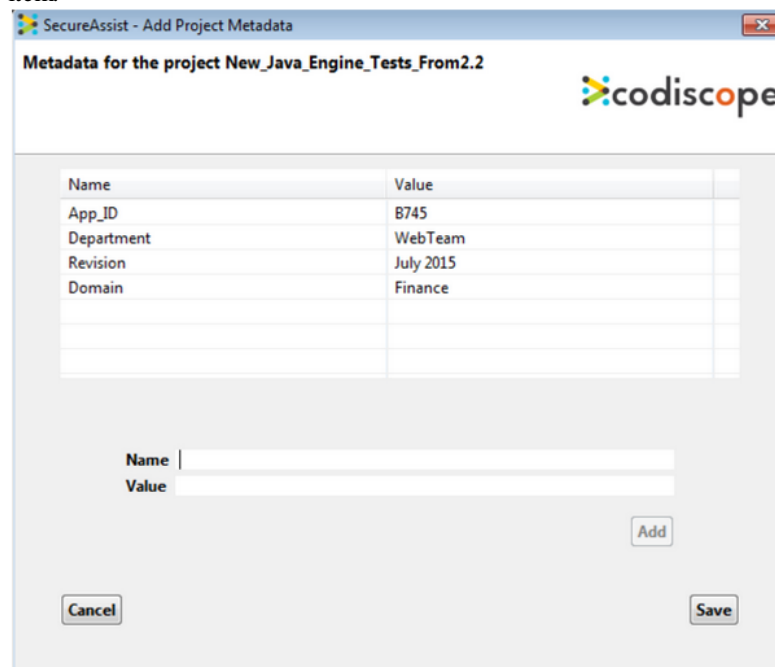
## 5 Project Metadata

Project metadata is a feature that allows you to tag your projects with additional information that is meaningful for your organization. For instance, you may have application ID schemes for a centralized application database. You can create metadata to tag that information in your projects. That metadata can then be used by the Portal for reporting.

Project metadata is specific to the project—that is, metadata in one project is reflected in that project only.

### ● Add Project Metadata

1. In the Package Explorer, right-click the desired project, then select **SecureAssist -> Add Metadata** from the menu. The **Project Metadata** dialog opens.
2. Enter a field name in **Name**, and a value for the field in **Value**. **Note:** The combination of name and value must be unique for each item.



Name	Value
App_ID	B745
Department	WebTeam
Revision	July 2015
Domain	Finance

Name |

Value |

3. Click **Add**. The new metadata item is added to the table, and the **Name** and **Value** fields are cleared.

### ● Edit Project Metadata

1. In the Package Explorer, right-click the desired project, then select **SecureAssist -> Add Metadata** from the menu. The **Project Metadata** dialog opens.

2. In the table, click the row of the item you wish to edit. Its values are displayed in the Metadata Item section.
3. Edit **Name** and **Value** as desired, then click **Update**. The item is updated in the table, and the **Name** and **Value** fields are cleared.

#### ● Delete Project Metadata

1. In the Package Explorer, right-click the desired project, then select **SecureAssist -> Add Metadata** from the menu. The **Project Metadata** dialog opens.
2. In the table, click the row of the item you wish to delete. Its values are displayed in the Metadata Item section.
3. Click **Delete**. The item is removed from the table, and the **Name** and **Value** fields are cleared.

## 6 Preferences

SecureAssist Preferences can be accessed in Eclipse by selecting **Windows -> Preferences -> SecureAssist**. This section describes some of the preferences you are most likely to visit.

### License Details

You can view the details of the license file on the SecureAssist Preferences page.

1. Select **Windows -> Preferences -> SecureAssist**.
2. Click Licensing to view the license details.

### Review Settings

By default, your files are scanned every time you open or save them, but you may wish to change that.

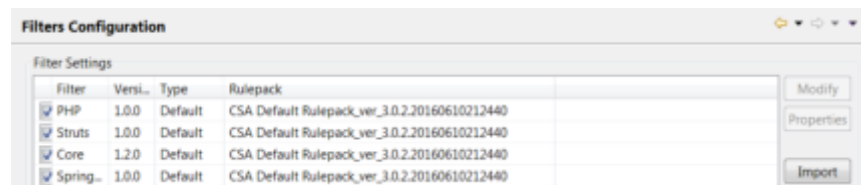
1. Select **Windows -> Preferences -> SecureAssist**.
2. Under Review Settings, deselect the option(s) you no longer want to use:
  - Review on File Save
  - Review on File Open

Note: If both options are deselected, you will need to manually initiate a file review in the Issue List.

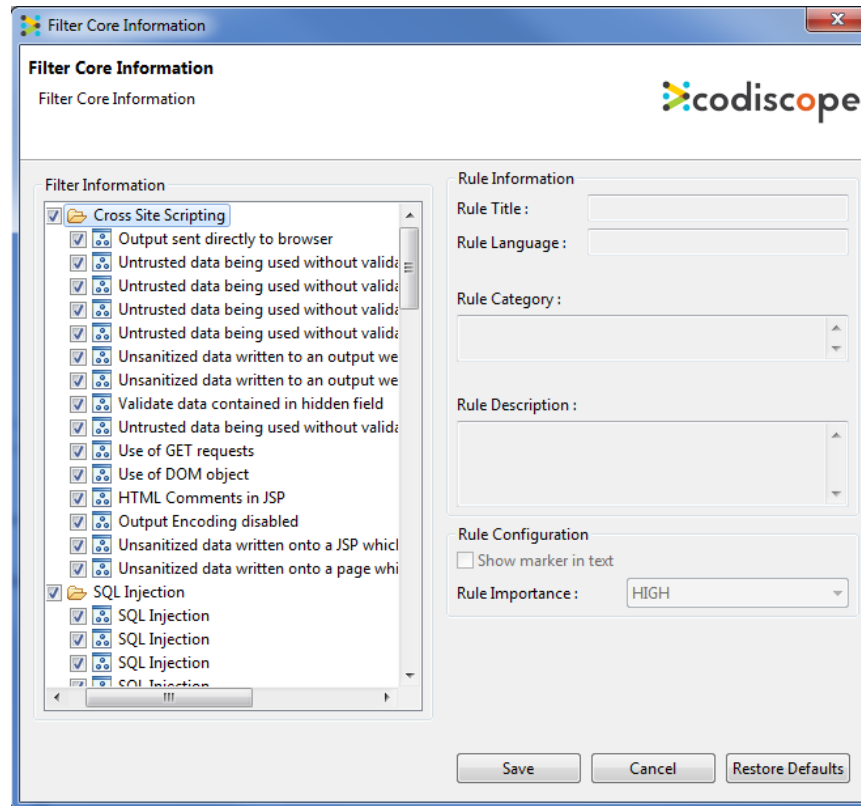
### Deactivating a Rule Permanently

There may be times you wish to deactivate a rule permanently, not just for the current Eclipse session.

1. Select **Windows -> Preferences -> SecureAssist -> Filters Configuration**.
2. Select the filter (set of rules) you want to modify.



3. Click **Modify**, then **OK**. The Filter Information dialog appears.



4. Click to deselect the checkbox next to the rule's name and click **Save**.

## 7 More Support

We hope this document has helped you get started with SecureAssist. You can submit a support request at [support.codiscope.com](http://support.codiscope.com). You will also find other manuals, release notes, system requirements, and more.

Thanks for using Codiscope SecureAssist!



[codiscope.com](http://codiscope.com)  
186 South Street  
Boston, MA 02111  
(617) 804-5428  
[info@codiscope.com](mailto:info@codiscope.com)