codiscope

SecureAssist Visual Studio Package User Guide

April 2017

Synopsys, Inc.
690 E. Middlefield Road
Mountain View, CA 94043
Phone: +1 (650) 584-5000
www.synopsys.com

Table of Contents

1 SecureAssist Setup

What is SecureAssist?

SecureAssist™ is an IDE package for Visual Studio 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 Package

SecureAssist installation for Visual Studio is straightforward. It allows users to install SecureAssist either per user or per machine (requires administrator rights).

To ensure your Visual Studio environment meets the minimum system requirements, go to our IDE compatibility page.

Setup installation logs (named log.txt) will be created at the same location as setup.exe.

Please make sure to close running instances of the Visual Studio IDE before starting installation of SecureAssist Package.

Installation in the UI

1. Close all instances of Visual Studio.
2. Copy Setup.exe to a location where you have read/write access (typically on your local drive).
3. Run the Setup.exe installation by double-clicking the file. The SecureAssist Setup Wizard opens.
   Note: Setup will identify available IDEs and extensions to see whether any version of SecureAssist is previously installed. All options and buttons will be disabled until this background task is completed.
4. Select whether to install for current user or for all users of the machine. (Installation for all users requires administrative rights.)
5. Click **Install**. The License Agreement is displayed.
6. Choose the IDEs for which SecureAssist package needs to be installed.
7. Click **Install.** The installation begins.

In case of enterprise installation, an ActivationConfig.xml file is also located along with Setup.exe. This can be configured to add predefined

values to the server URL and to disable the certificate dialog during enterprise license activation.

Installation Using the Command Line

SecureAssist can be installed from the command line as well. It accepts following parameters:

- ***q***—Quiet Mode. Determines whether installation will show any UI or not. Accepts values *true or false.*
- ***l***—Log file path. Path to installation logs. Accepts value as a path to the log file. Setup logs (named ExecLogs.txt) will be saved in the same directory as VSIX logs.
- ***allUsers***—Determines whether installation is done for current user or for all users. Accepts values *true or false.*
- ***type***—Determines installation type. Accepts value *enterprise.*
- ***url***—Enterprise portal URL to activate license from. If provided, comes pre-loaded on activation screen.
- ***acceptCertificateDialogDisabled***—Determines whether SSL certificate dialog is displayed while activating.

Note: In case Setup is run silently and the VS IDE is opened while running setup.exe, installation will stop and the corresponding warning message will be saved in ExecLogs.txt.
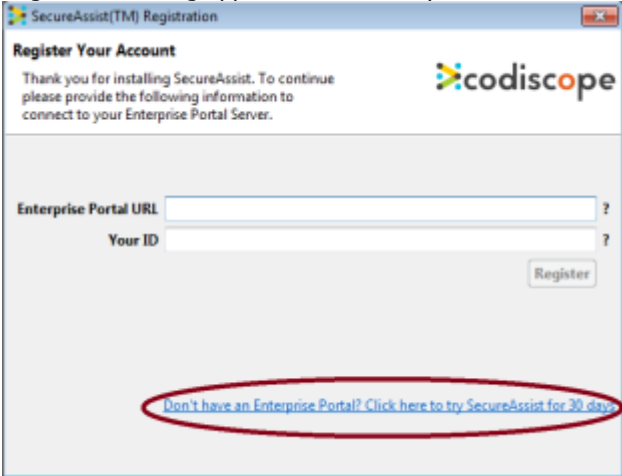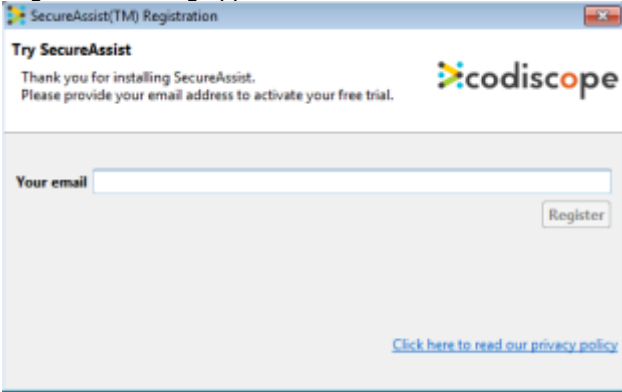
Note: Command line parameters are case-insensitive.
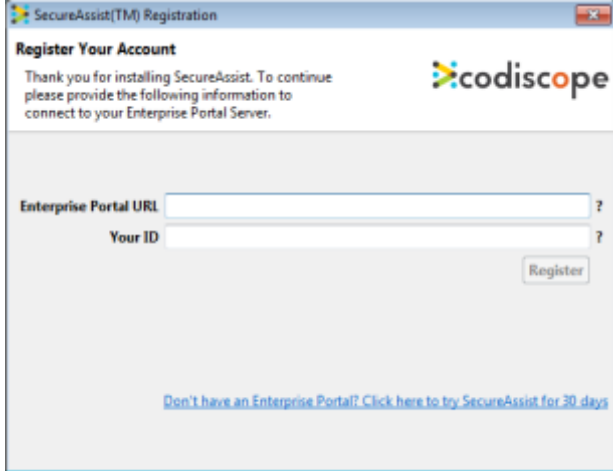
Here is an example of installing SecureAssist Package from Command line with all parameters.

Setup.exe q="true" l="c:\secureAssist\log.txt" allUsers="true" type="enterprise" url="csa-portal url" acceptCertificateDialogDisabled="true"

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
Trial	Once the license expires after 30 days, you must upgrade to continue using SecureAssist. 1. After installing SecureAssist, restart Visual Studio. The Registration dialog appears automatically. 2. Click the URL at the bottom of the dialog. The Trial Registration dialog appears. 3. Enter your email in the text box, then click **Register**. A popup will confirm your trial registration.

License Type	Activation Instructions
Enterprise	1. After installing SecureAssist, restart Visual Studio. The Registration dialog appears automatically. 2. If it is not already prepopulated, enter your **Enterprise Portal URL**. If you don't know the URL, contact your IT administrator. 3. In **Your ID**, enter your email address or network ID. If you're unsure what to enter, contact your IT administrator. 4. Click **Register**. A popup will confirm your registration.

Update SecureAssist

When SecureAssist issues a new version or upgrade, simply click on the new setup.exe to upgrade your current version of SecureAssist. Setup.exe detects all available versions, and allow users to either uninstall previous versions or upgrade to the latest version.

EXCEPTION! If you currently have version 2.4.1 or below, first you must uninstall your current installation (using normal uninstall procedures OR by double-clicking setup.exe and choosing to uninstall SecureAssist) before upgrading to the newest version.

Uninstall SecureAssist

There are several methods for uninstalling SecureAssist.

- **UI**. Setup.exe, when run, searches for installed versions of SecureAssist and, if found, enables an Uninstall option, along with an informational message listing all IDEs on which SecureAssist is previously installed.
  Note: This option is available from 3.0.2 onwards and will remove SecureAssist from all versions of Visual Studio on which SecureAssist was previously installed. In case installation was done for all users (with an administrative account), uninstall will also require administrative privileges.
- **Command Line**. You can run Setup.exe from the command line and pass the argument uninstall="true". You can also pass other parameters that Setup.exe accepts (q/ l – for Quiet mode / log file path) along with this parameter.
- **Extension Manager**. You can navigate to Extension Manager under Tools in the Visual Studio IDE to disable/uninstall SecureAssist for a particular version of IDE.

Set Up SecureAssist Views

SecureAssist has several views in Visual Studio 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 Visual Studio sessions until you manually close it. The following table describes the views.

Pane	Description
Issue List	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.
Project Review	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.
Call Chain	Lists the files and lines of code an untrusted source passes through to create a given potential vulnerability.
Guidance	Displays secure coding guidance on an issue selected in the Issue List or Project Review.
Guidance Search	Allows a text search of SecureAssist guidance.

● Display a View

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

1. Open a file in Visual Studio.

2. Select **Tools** -> **SecureAssist Views**.

3. Select Issue List and any other desired views, then click **OK**. The views you selected will now appear in the Visual Studio window. You may drag and drop these views to display them as you choose.

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 Visual Studio.
   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 a Project, Folder, or Solution

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, folder, or solution.

Warning! Project reviews use more memory than a single file review. Ensure your Visual Studio environment meets the system requirements listed at our IDE compatibility page.

● Scan a Project

You can scan a resource from the Project Review view OR the context menu of Solution Explorer in Visual Studio.

1. In Visual Studio, ensure that the SecureAssist Issue List and Project Review views are open.

    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.
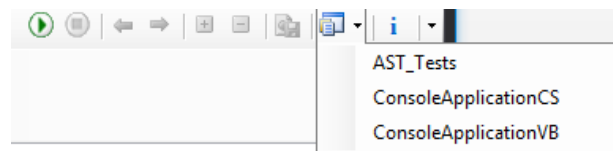
    OR

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

    The Review dialog opens, displaying any compilation errors existing in files selected for review (making the scan findings for these files inaccurate), total number of files to review, and the maximum time specified for review of a single file, and the estimated maximum amount of time the project review could take (actual time will likely be much shorter).
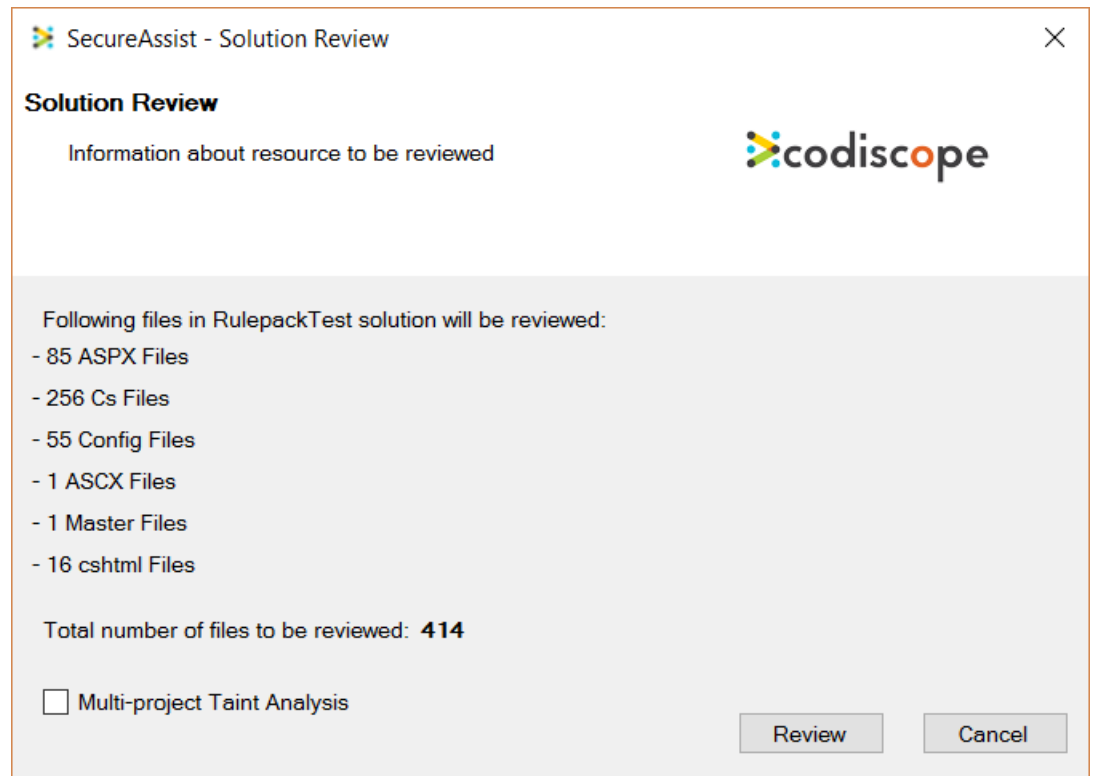
2. If desired, edit the maximum time to be spent in single file review (between 20 and 300 seconds). If files are not scanned completely within the time selected, an error will be reported in the Review Summary dialog once the scan is complete.

3. If desired, select **Multi-Project Taint Analysis**. (Multi-project taint analysis potential issues are identified when source and sink are in different projects in same solution.)

4. Click **Review** to begin the project scan. The 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.

2. Expand the folders until you see the issue line numbers.

3. 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.

4. To view a tooltip with 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

1. In the Issue List, click the **Group By** icon to display the grouping options.
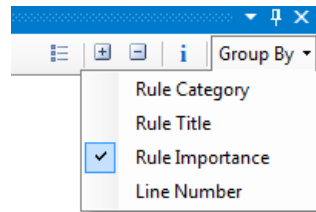
2. Select the group you want to use as the primary grouping.

Reviewing a Project, Folder, or Solution
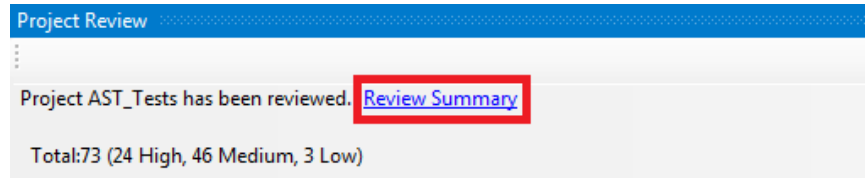
Viewing

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.
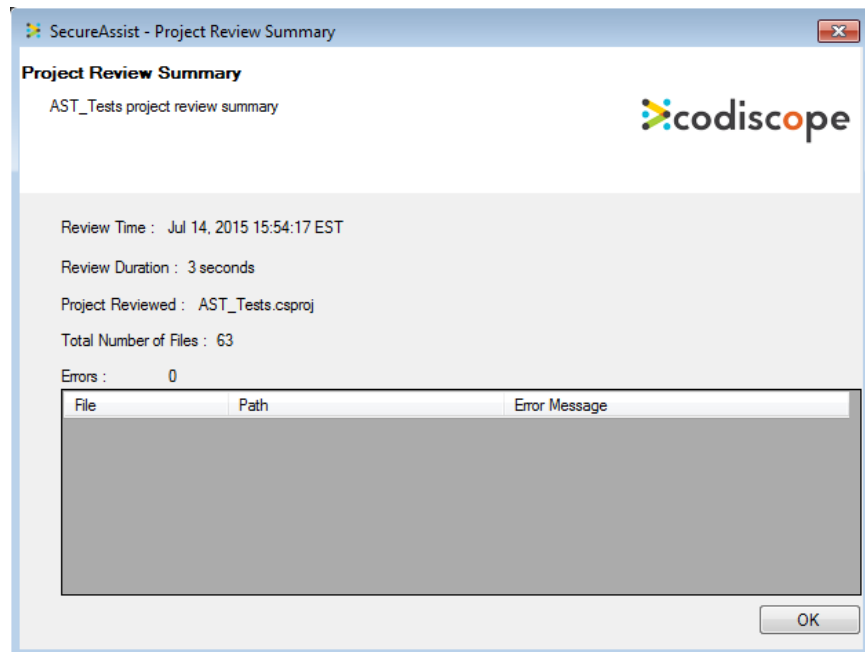
Grouping and Sorting

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 **Group By** icon to display the drop-down menu, then select the primary grouping.

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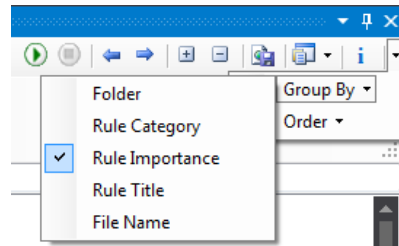
1. With the Project Review view open, click the **Order** icon to display the drop-down menu, then select **Order**.

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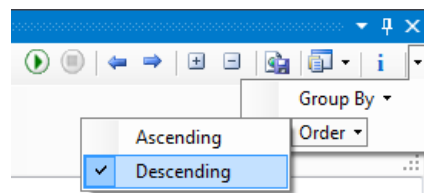
Filtering

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:

   ▪ *folder=* 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.
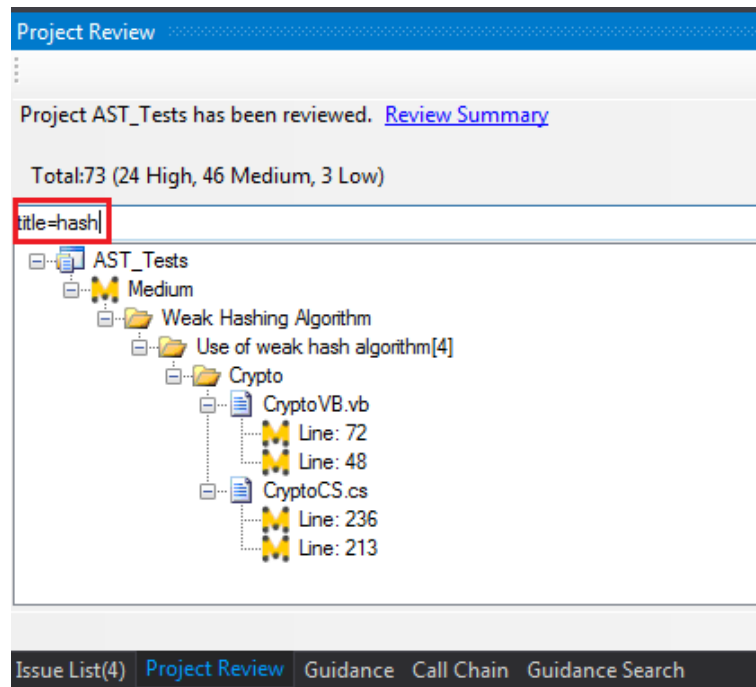
The results appear as you enter the text, sorted in descending order.

Exporting

You can export the 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 in the Issue List grayed out so that 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 indication of the issue in the Editing view.

A suppressed issue **will remain suppressed for all Visual Studio sessions of the project until you unsuppress it**.

● 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 unsuppressed, 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 unsuppressed, 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 Visual Studio session. **When Visual Studio 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 Visual Studio 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.
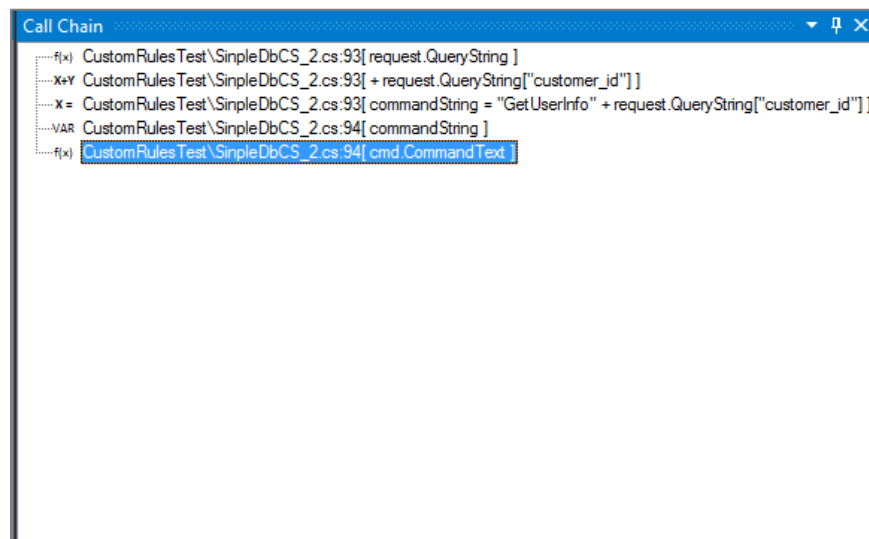
3. Click each line in the call chain to go to the line of code in the Editing view.

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. 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. 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.
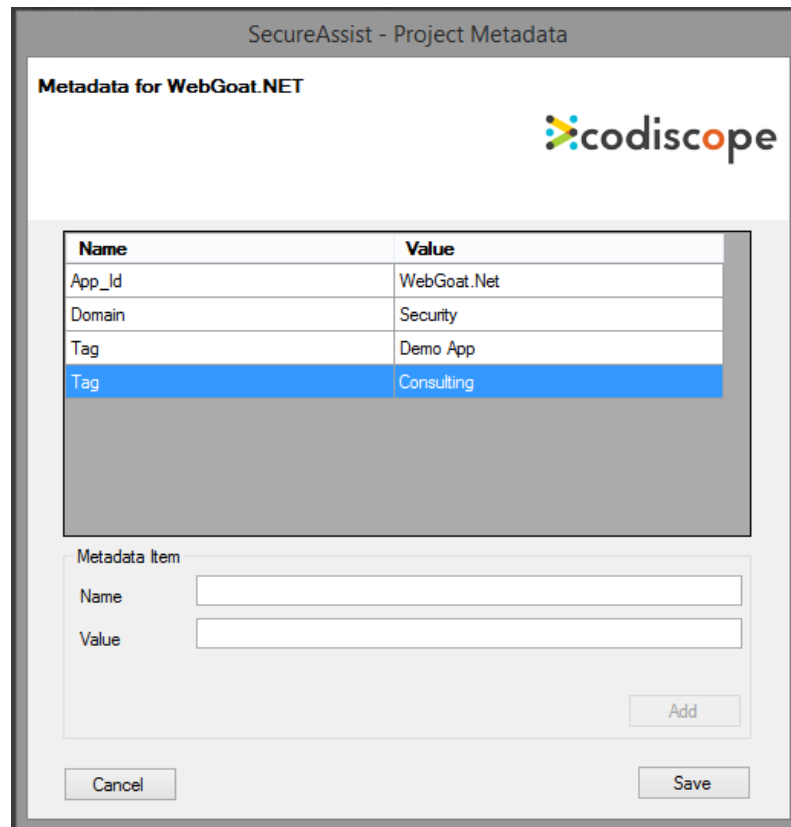
5   Project Metadata

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 Solution 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.

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 Solution 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 Solution 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 Visual Studio by selecting **Tools** -> **Options** -> **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 **Tools** -> **Options** -> **SecureAssist** -> **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 **Tools** -> **Options** -> **SecureAssist** -> **General Settings**.

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.

   You can also change the time / memory allotted per review for a project / solution / resource review as well as file review. Memory limits helps to avoid Out Of Memory Exceptions while reviews are in progress. You are advised to set the memory limit as per the size of your project / solution
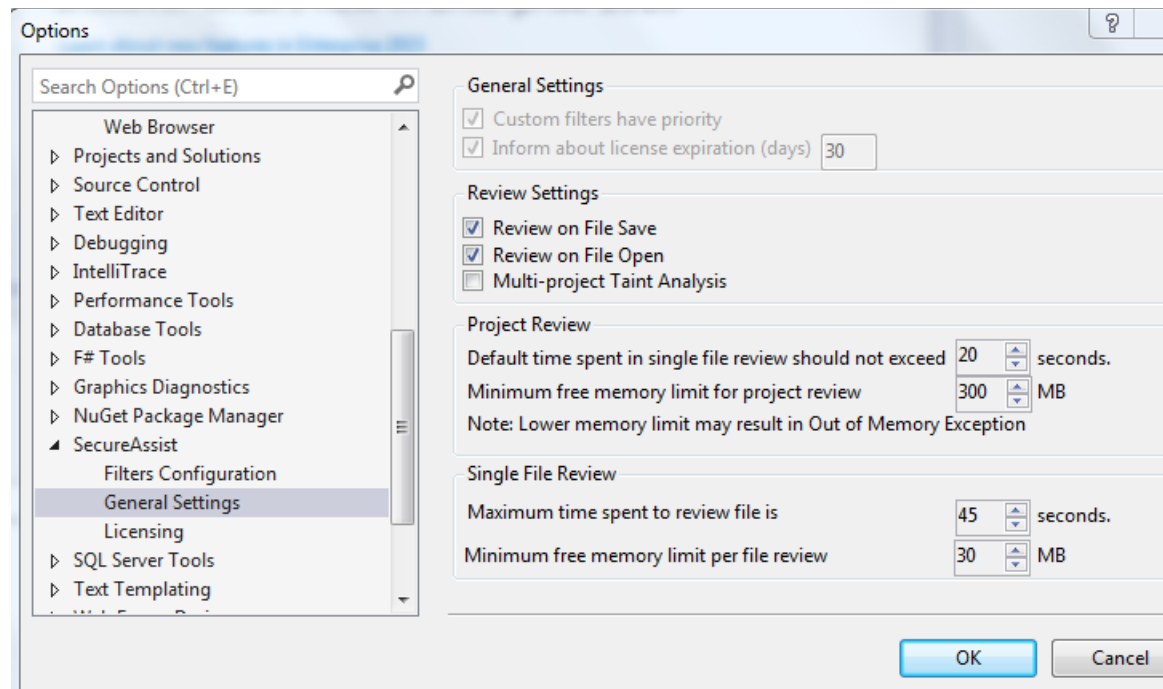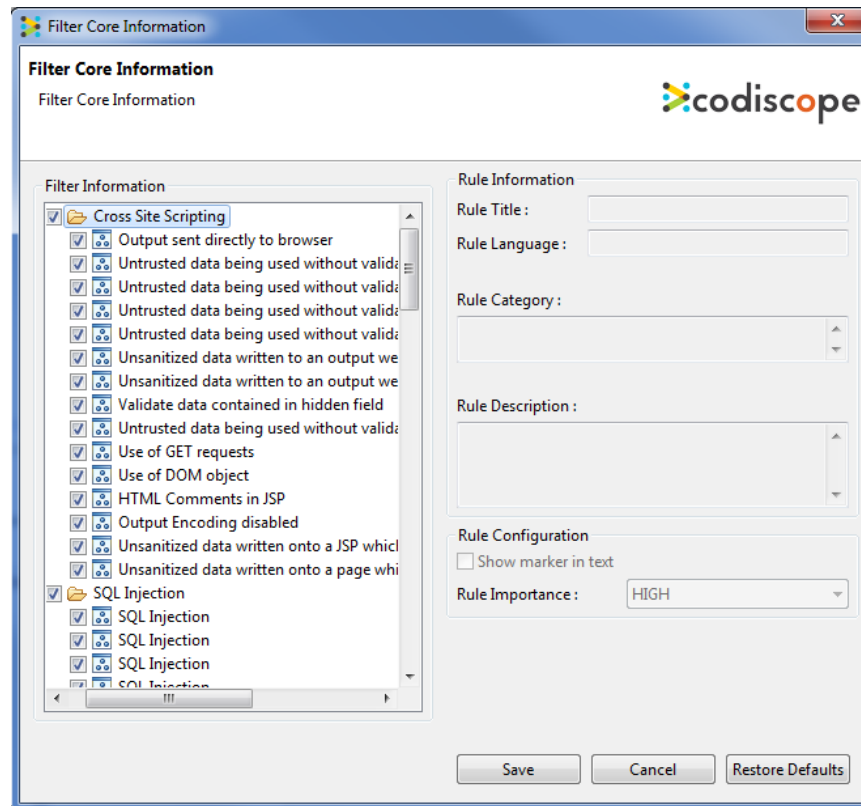
Deactivating a Rule Permanently

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

1. Select **Tools** -> **Options** -> **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. You will also find other manuals, release notes, system requirements, and more.

Thanks for using Codiscope SecureAssist!

Synopsys, Inc.
690 E. Middlefield Road
Mountain View, CA 94043
Phone: +1 (650) 584-5000
www.synopsys.com