**HP Fortify**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl.No** | **Version** | **Author** | **Reviewer** |
| **1.** | **Initial Draft** | **Ramya A**  **(ramya.a@sap.com)** | **Hifza** |

Contents

[**Fortify 2**](#_Toc428370881)

[**Security Testing with HP Fortify 2**](#_Toc428370882)

[**HP Fortify Static Code Analyzer (SCA) 3**](#_Toc428370883)

[**HP Fortify Static Code Analyzer Features 3**](#_Toc428370884)

[**Step 1: Learn About HP Fortify Software Security Center 18**](#_Toc428370885)

[**Introduction 18**](#_Toc428370886)

[**Technology 18**](#_Toc428370887)

[**Automatic Results Prioritization 20**](#_Toc428370888) [**20**](#_Toc428370889)

[**Step 2: Learn the Security Process 22**](#_Toc428370890)

[**Overview 22**](#_Toc428370891)

[**Instructions 22**](#_Toc428370892)

[**Step 3:Plan For Secure Development 23**](#_Toc428370893)

[**Overview 23**](#_Toc428370894)

[**Instructions 23**](#_Toc428370895)

[**3. Plan to Review New Vulnerabilities 23**](#_Toc428370896)

[**4. Plan to Remediate Existing Vulnerabilities 24**](#_Toc428370897)

[**Step 4: Review Scan Results 25**](#_Toc428370898)

[**Overview 25**](#_Toc428370899)

[**Instructions 25**](#_Toc428370900)

[**Analysis - Applied By You 26**](#_Toc428370901)

[**Understanding the issue 26**](#_Toc428370902)

[**Step 5. Remediate Planned Issues 27**](#_Toc428370903)

[**Overview 27**](#_Toc428370904)

[**Instructions 27**](#_Toc428370905)

[**Details 27**](#_Toc428370906)

[**Recommendations 28**](#_Toc428370907)

# Fortify

HP Fortify Software Security Center is a suite of tightly integrated solutions for fixing and preventing security vulnerabilities in applications. It eliminates software security risk by ensuring that all business software— whether it is built for the desktop, mobile or cloud—is trustworthy and in compliance with internal and external security mandates. HP Fortify Software Security Center secures all software in the enterprise, regardless of whether it is developed in-house, procured from 3rd party vendors, or running in production.

# Security Testing with HP Fortify

Security testing with HP Fortify Software Security Center helps you quickly gain an accurate picture of risk in your applications, no matter if they’re developed in-house or by vendors. It provides you with the broadest set of security testing capabilities available, such as:

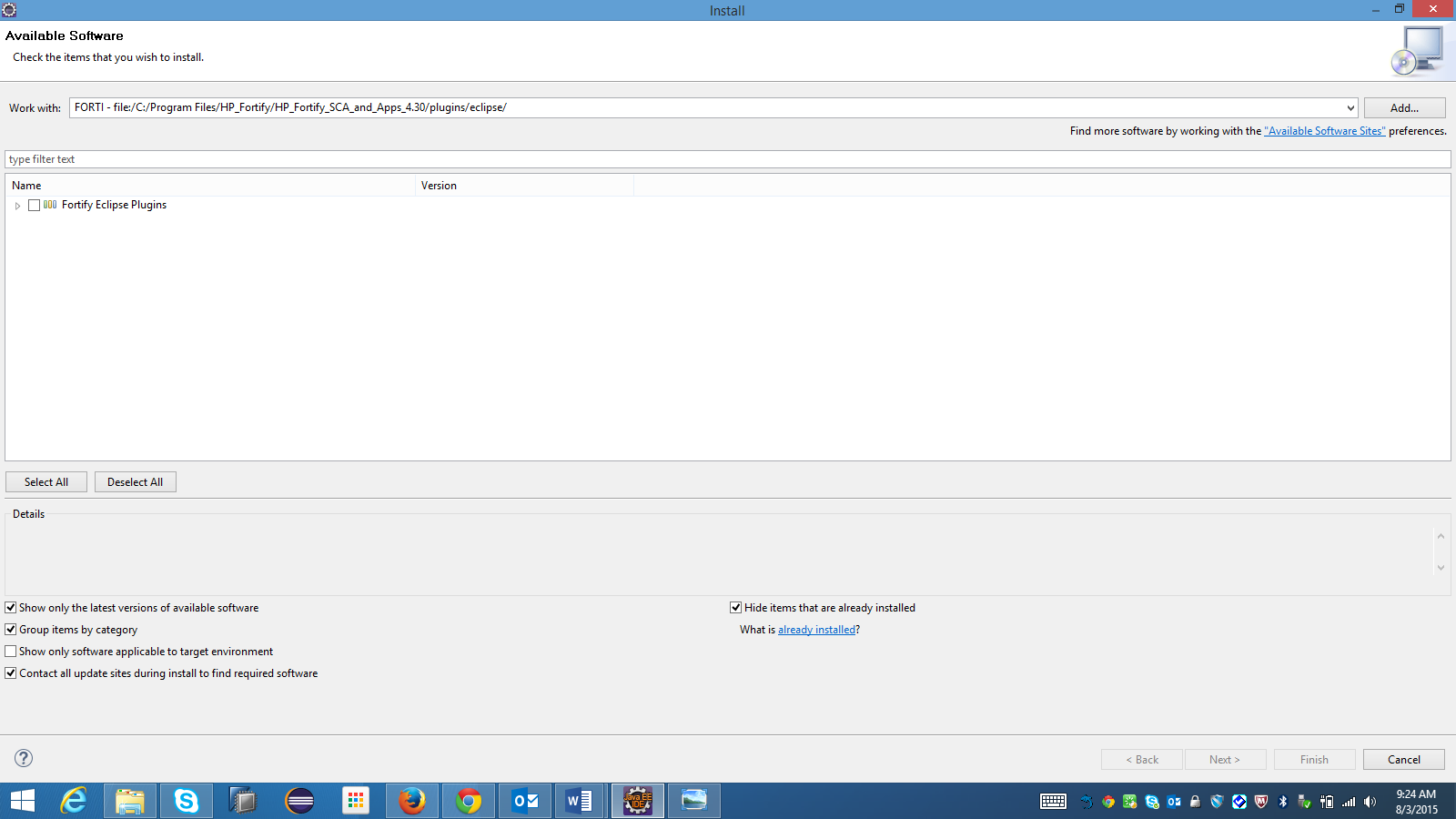
|  |  |
| --- | --- |
|  | ****HP Fortify Static Code Analyzer (SCA)**** The earlier you find security flaws during development, the less impactful they are to fix. To be effective, source code analysis must be more than thorough and accurate. It also should provide you actionable insight into the root causes of security problems, while helping prioritize which vulnerabilities to address first.  The HP Fortify Static Code Analyzer (SCA) in HP Fortify Software Security Center helps you meet all of these needs. It uses HP Fortify’s award winning static analysis to provide the most far-reaching vulnerability detection in source code available today. It delivers key functionality required for an effective Software Security Assurance (SSA) program.  With HP Fortify SCA you canpinpoint root causes of security vulnerabilities in source code, receive prioritized results sorted by severity of risk, and get guidance on how to fix vulnerabilities in line-of-code detail. As a result you can ensure your software is trustworthy, reduce the costs of finding and fixing application vulnerabilities,andestablish the foundation for secure coding best practices. **HP Fortify Static Code Analyzer Features** HP Fortify SCA provides root-cause vulnerability detection through the most comprehensive set of secure coding rules available and supports the widest array of languages, platforms, build environments (Integrated Development Environments, or IDEs) and software component APIs.   * Conduct static analysis to pinpoint root causes5 of security vulnerabilities in source code * Detect more than 480 types of software security vulnerabilities across 20 development languages—the most in the industry. * Receive prioritized results sorted by severity of risk and  guidance on how to fix vulnerabilities in line-of-code detail * Ensure compliance with application security mandates   **Requesting access to Fortify**  You can request access to Fortify via the [self-services](https://codescan-selfservice.wdf.sap.corp/fortify/)   1. To install Fortify SCA (the Source Code Analyzer), you will need a license. Please click on "request license" to get it automatically by email. Obtaining a Fortify SCA license results in no cost for you or your cost center, they are covered by our department.   cid:image001.jpg@01D0C940.A063CF50   1. To be able to log in to the Fortify server, you need to register your user to the LDAP repository. For this, please click on "request access". You should now be able to log in to the Fortify SSC (https://fortify1.wdf.sap.corp/ssc/) via SSO using your id-number and password. 2. To get access to a particular project, please click on "request access" and select the project that you would like to work on. To ease your search, you can click on the "Project Name" header to specify a filter. All users that have access to the project will be notified that you have requested access.   **Installation and Configuration Fortify SCA**   You will find the installer [here](file:///\\dwdf213.wdf.sap.corp\sec_scan\Public\Fortify\Installation) . Here is the step by step procedure how to install Fortify 4.3. SCA  **Link to download fortify**  \dwdf213.wdf.sap.corp\sec\_scan\Public\Fortify\Installation\v4.30 - recommended\HP\_Fortify\_SCA\_and\_Apps\_4.30\_Windows\_TF302-15214.zip-HP\_Fortify\_SCA\_and\_Apps\_4.30\_windows\_x64.exe   * Step 1: Start setup * Step 2: Accept the license agreement * Step 3: Choose Installation directory * Step 4: Choose the plugins that are relevant for you.     https://wiki.wdf.sap.corp/wiki/download/attachments/1613883449/comp.png?version=1&modificationDate=1405557913000&api=v2   * Step 5 : Navigate to your Fortify license * Step 6 : Set the Update server url to <https://fortify1.wdf.sap.corp/ssc/>   https://wiki.wdf.sap.corp/wiki/download/attachments/1613883449/fortify1.png?version=1&modificationDate=1405557914000&api=v2   * Step 7 : Choose "NO" when asked for migration from previous version * Step 8 : Start installation * Step 9: Finish installation without checking the checkbox for security content update:   C:\Users\C5228150\Desktop\impodocuments\thumbnail.png  **Configuring Fortify SCA**  **Command Line**  The following configuration steps will help you make sure that you can produce analysis results and commit them to the [Fortify SSC Server.](https://fortify1.wdf.sap.corp/ssc/)[open with IE]    **Importing the Root Certificate**  Since the .crop top level domain is now globally available, no CA can sign an SSL certificate for our internally-used-only [Fortify server](https://fortify1.wdf.sap.corp/ssc/) .That is why we have to use our internal SAPGlobalRootCA certificate to obtain an SSL certification and provide a secure connection to the SSC Server. SAPGlobalRootCA.cer is by default not trusted by the jre's packaged with the Fortify installation which are used by the Fortify command line tools. To import the certificate, please do the following:   1. Get the certificate from: [getCertificates](file:///\\dwdf213.wdf.sap.corp\sec_scan\Public\Fortify\Installation) [\\dwdf213\sec\_scan\Public\Fortify\Installation\ SAPGlobalRootCA.cer] 2. Open a command prompt in **admin** mode 3. Import the cert in the jre. Please adapt the location of the keytool[C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\jre\bin] in the following command if you haven't kept the default path during installation:   **C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\jre\bin>keytool -import –trustcacerts -alias rootCA -file "\\dwdf213\sec\_scan\Public\Fortify\Installation\SAPGlobalRootCA.cer" -keystore "C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\jre\lib\security\cacerts"**  **Please use default password as “changeit”**  **If the keystore already has this alias, then the command will fail. In this case the following line will help:**  **C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\jre\bin\keytool -delete -alias rootCA -keystore "C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\jre\lib\security\cacerts"**  **Configuring the Fortify SSC connection**  Run **scapostinstall.cmd** from the bin directory in your Fortify Installation.   * Select [2] Settings * Select [3] Software Security Center Settings * Select [1] Server URL * Enter: https://fortify1.wdf.sap.corp/ssc/ * Select [6] Get Updates from Software Security Center * Enter: true * Select [7] Software Security Center Username * Enter: <your SAP\_GLOBAL username> * Select [q] * Exit     **Updating the Rulepacks**  Run <Fortify install dir>\bin\fortifyupdate.cmd.  **Installing the HP Fortify Plugin for Eclipse Locally**  Start Eclipse. 🡪Select Help → Install New Software.  https://wiki.wdf.sap.corp/wiki/download/attachments/1082329454/Install%20new%20software.png?version=1&modificationDate=1326372998000&api=v2 |
|  |  |

In the install dialogue click the button "Add...". In the "Add Repository" dialogue click the button "Local..." (See screenshot below). Navigate to the folder plugins\eclipse within you Fortify SCA installation e.g.

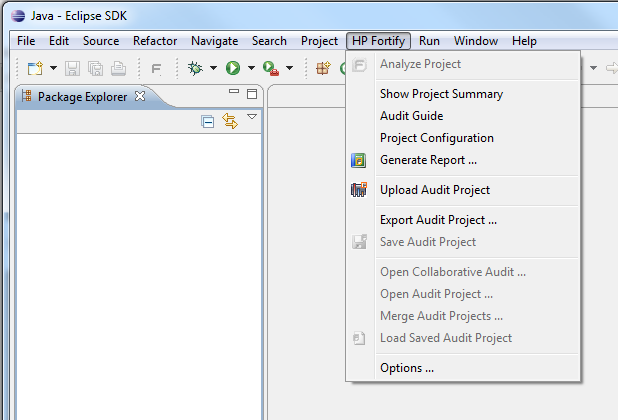
C:\Program Files\HP\_Fortify\HP\_Fortify\_SCA\_and\_Apps\_4.30\plugins\eclipse. Click OK. Click OK again to close the "Add Repository" dialogue.

Check all available Fortify Eclipse plugins (as shown in screen image below) and click "Next".

Update site: file://C:/Program%20Files/HP\_Fortify/HP\_Fortify\_SCA\_and\_Apps\_4.30/plugins/eclipse/ - file:/C:/Program Files/HP\_Fortify/HP\_Fortify\_SCA\_and\_Apps\_4.30/plugins/eclipse/



Proceed with installation wizard by accepting the license agreement and restarting Eclipse when prompted. After restarting a menu item "HP Fortify" should be available in Eclipse:



**Configuring the Fortify SSC Connection**

When you enter the Options dialogue for the first time you will be prompted to navigate to your license file. Please navigate to the folder where your license is located. A copy of the license will be in the Fortify installation directory. Also, the Eclipse plugin will prompt you locate the SCA executable. Please select *sourceanalyzer.exe* in the *bin* folder of your Fortify SCA installation directory. Go to HP Fortify --> Options --> Server Configuration 1. Check the "Update Security Content from Software Security Center" option 2. Enter <https://fortify1.wdf.sap.corp/ssc/> in the input field "Server URL:" in the are Software Security Center Configuration area

**Certificate Import**

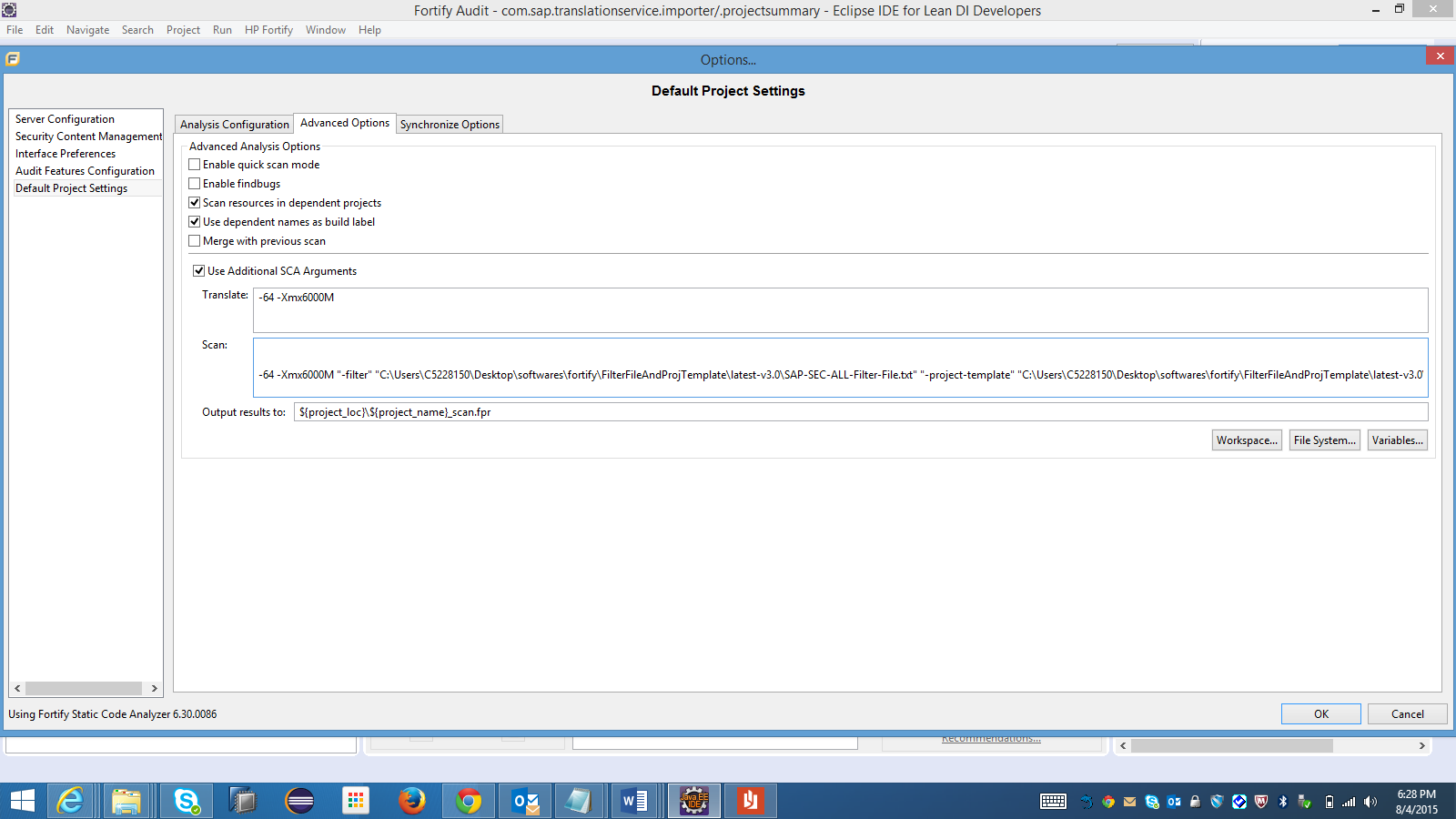
C:\Program Files\Java\jre7\bin>keytool.exe -import -trustcacerts -file C:\Users\C5228150\Desktop\softwares\fortify\SAPGlobalRootCA.cer -alias apphost2 –keystore "C:\Program Files\Java\jre7\lib\security\cacerts”

**Updating Rulepacks**

HP Fortify --> Options --> Security Content Management and click on "Update Security Content" If you have imported the SAPNetCA root certificate into your system jre as described above, you should be able to establish a connection to the Fortify server. If you encounter an error message mentioning "defaulttemplate.xml" which blocks the update, please go to <Fortify install dir>\core\config\rules and remove defaulttemplate.xml.

**Additional Advanced Analysis Options**

Go to  HP Fortify --> Options --> Default Project Settings --> Advanced Options Here you have the option configure additional arguments which will be taken into account for analysis you do from Eclipse Check the checkbox "Use Additional SCA Arguments" and copy the following into the Scan box: -64 -Xmx6000M "-filter" "\\\dwdf213\sec\_scan\Public\Fortify\FilterFileAndProjTemplate\latest-v3.0\SAP-SEC-ALL-Filter-File.txt""-project-template"\\\dwdf213\sec\_scan\Public\Fortify\FilterFileAndProjTemplate\latest-v3.0\SAP-SEC-Project-Template.xml [[getTemplateFiles](file:///\\dwdf213.wdf.sap.corp\sec_scan\Public\Fortify)]



|  |
| --- |
| **Updating Rulepacks** |

HP Fortify --> Options --> Security Content Management and click on "Update Security Content" If you have imported the SAPNetCA root certificate into your system jre as described above, you should be able to establish a connection to the Fortify server. If you encounter an error message mentioning "defaulttemplate.xml" which blocks the update, please go to <Fortify install dir>\core\config\rules and remove defaulttemplate.xml.

**Scanning Projects**

The Eclipse Plugin automatically includes all source files from dependent projects in scans. Although you can scan individual packages and files (see Scanning Individual Files and Packages), SCA scan results are more accurate if you scan an entire project at once

. Note: The Eclipse plugin does not support scanning multiple projects at the same time. To scan a project:

1. Open the project in the Java perspective in Eclipse.

2. In the Package Explorer view, select the project.

3. Do one of the following:

•On the toolbar, click the **HP Fortify icon**.

•Select **HP Fortify → Analyze Project**.

After the scan begins, a progress bar in the Scanning window enables you to follow the process. After the scan finishes, the results are loaded into and displayed in the Fortify Audit perspective in Eclipse.

**Scanning Individual Files and Packages**

You can also scan individual files and packages.

Note: HP Fortify does not recommend this method, because analysis results are more accurate when an entire project is scanned at once.

To scan individual files or packages:

1. From Eclipse, open the project in the Java perspective.

2. In the Package Explorer view, right-click the file or package to scan, and then select **Advanced** **scan** Project Component from the shortcut menu.

**About the Scan Results File Name and Directory**

By default, after you scan a project, the Eclipse plugin assigns the results file (FPR file) a name in the format <Project Name>Scan.fpr and places it in a new project folder in your Eclipse working directory. You can, if you prefer, store your project scan results file under a different name and directory.

To change the default directory and FPR file name for all projects, use the HP Fortify Options dialog box. To change the default directory and FPR file name for a specific project, use the Eclipse Properties window.

**Changing the Default Location and FPR File Name for all Projects**

To specify a default FPR file name and directory for all projects:

1. Select HP Fortify → Options.

2. In the left panel of the Options dialog box, select Default Project Settings.

3. In the right panel, select the Advanced Options tab.

4. Select the Use Additional SCA Arguments check box.

5. Do one of the following:

•In the Output results to box, type the absolute path for FPR files.

•To specify a name and a static workspace folder for FPR files, click Workspace, and then, in the Folder Selection window, navigate to and select a workspace relative directory.

•To specify a name and a static folder that is not part of your workspace, click File System, and then select a directory for FPR files.

•To specify a name and a dynamic path that changes based on the project you are analyzing, click Variables, and then, in the Select Variable window, select core Eclipse variables to specify the relative path for FPR files.

**About HP Fortify Reports**

The Eclipse Plugin provides a flexible reporting infrastructure based on user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. The following sections provide information about the default reports and report templates, instructions on how to modify existing reports, and how to create your own reports.

Opening HP Fortify Report Templates to open a report template:

1. Select HP Fortify → Generate Report.

The Generate Reports dialog box opens.

2. Select a report template from the Report list.

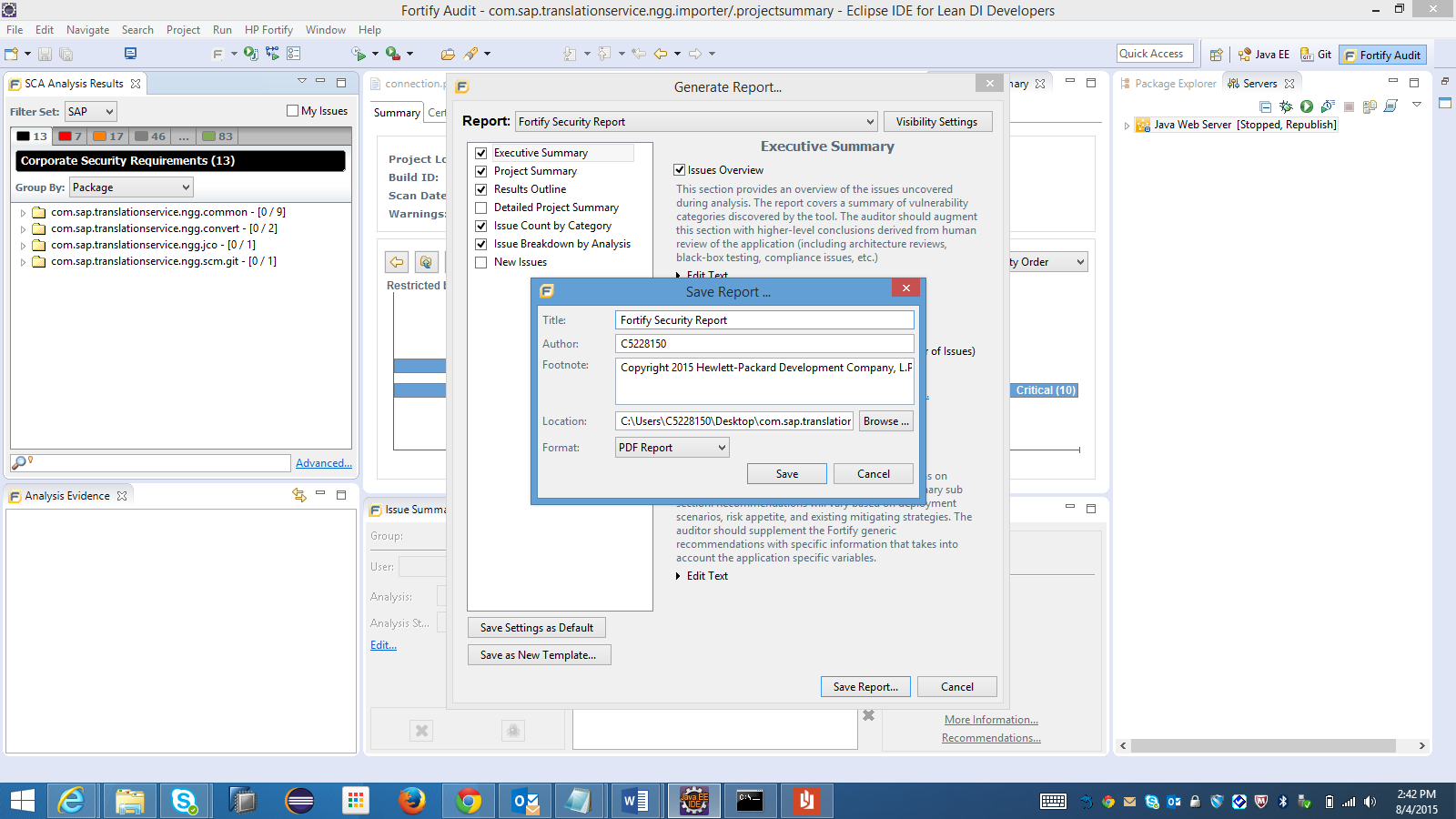
The Generate Report dialog box displays the report template settings. Generating Reports After you select a report template and specify report settings, you generate the report to view the results. You can save report results as PDF, RTF, and XML files. To run a report:

1. Select HP Fortify → Generate Report. The Generate Reports dialog box opens.

2. Select a report template from the Report list.

3. (Optional) Make changes to the report section settings.

4. Click Save Report. The Save Report dialog box opens.



5. Make any necessary changes to the report details, including its location and format. Note: If you save the file in rich text format (RTF), the report can be opened only in Microsoft Word or WordPad.

6. Click Save. The report is generated and saved as a file in the format you selected.

**About Specifying Resources to Scan**

The Eclipse Plugin automatically includes all source files from dependent projects in scans of selected projects. For JAR files included in the project you select to scan, if the source exists in the workspace for a given JAR, the Eclipse Plugin includes the source in the scan.

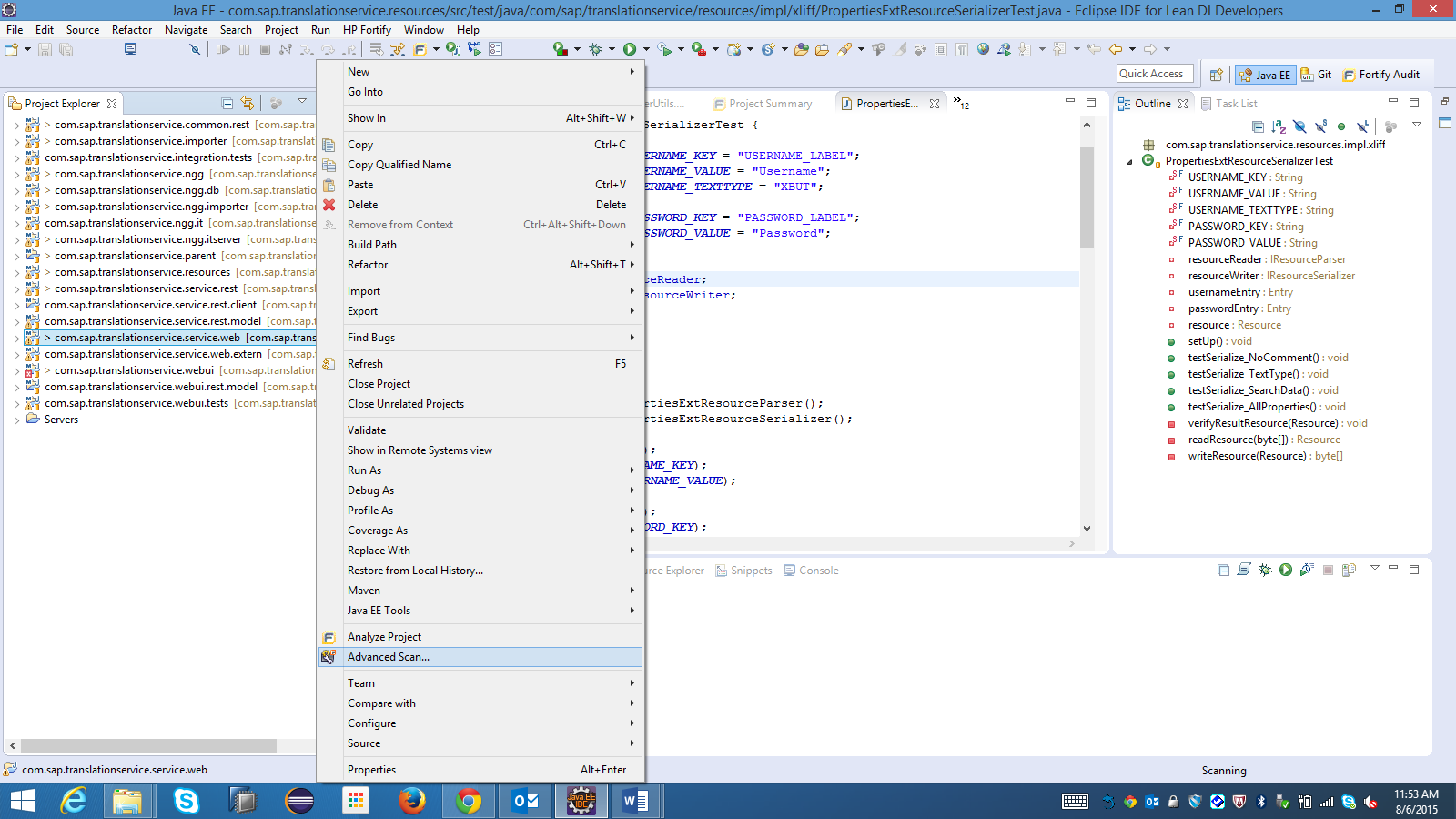
**Viewing the Resources and Classpath to be scanned**

To see the project resources and classpath to be scanned if you select a project, and then select **HP Fortify → Analyze Project**:

1. From the Java view in Eclipse, do one of the following:

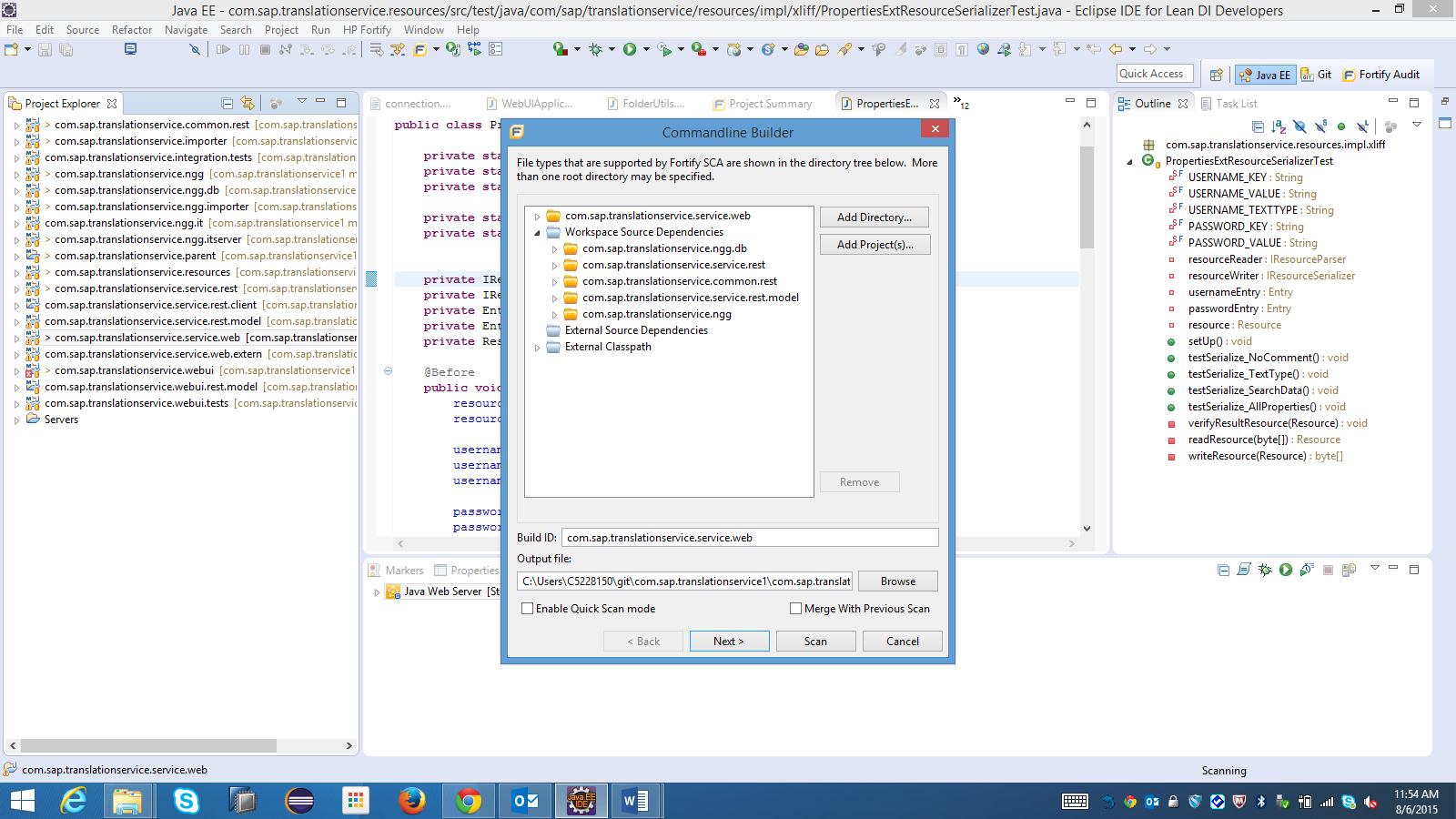
•Right-click a project name, and then select Advanced Scan from the shortcut menu.

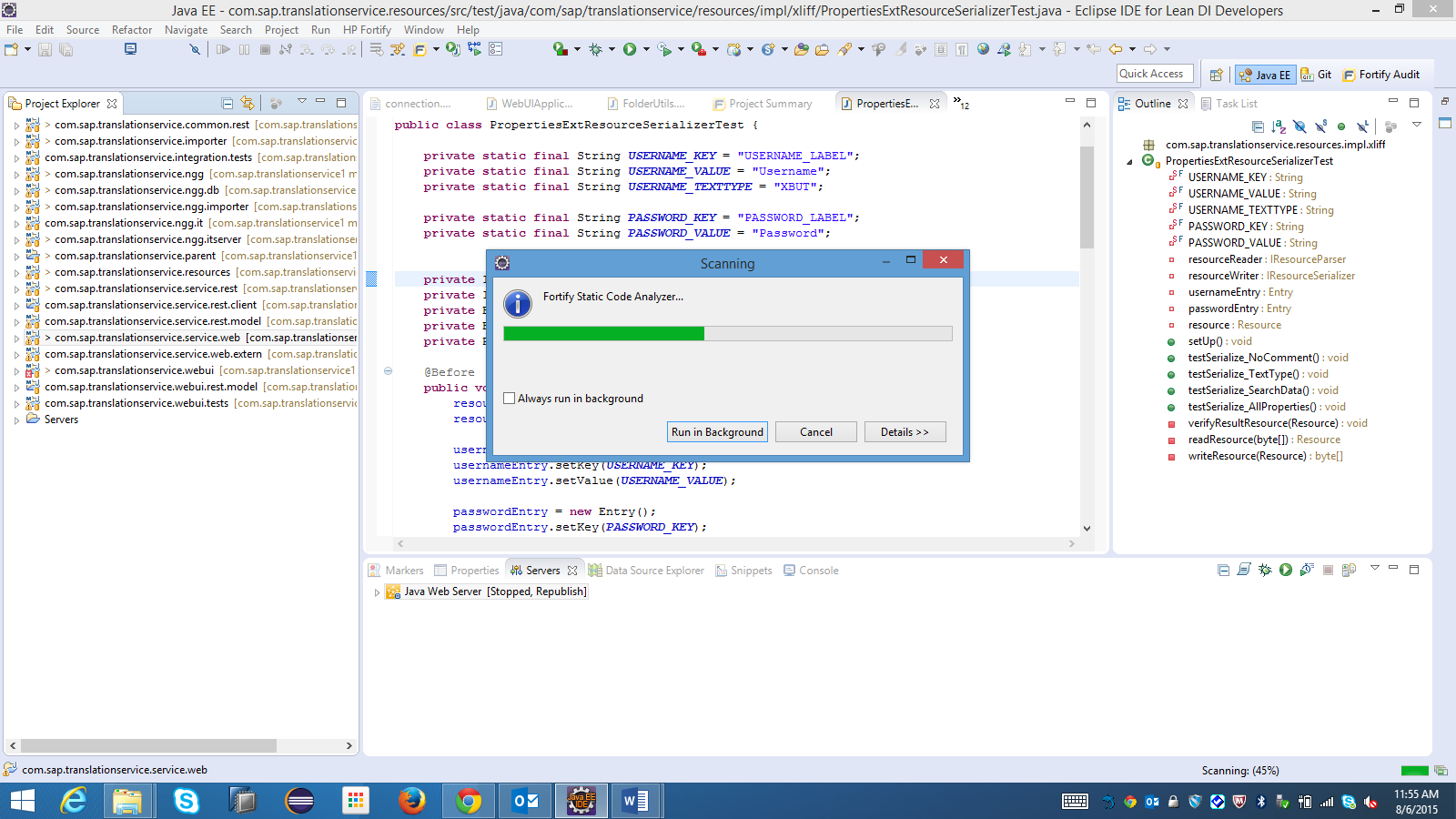
•Select a project name, and then select **HP Fortify → Advanced Scan.**



The Command Builder opens.

2. Expand the directory tree





The Command Builder displays the project resources and classpath to be scanned. If you have “Scan resources in dependent projects” enabled, you can see any dependent projects under the **Workspace Dependencies root**.

**About Viewing Scan Results**

After a scan is completed (or, after you open an existing audit project), summary results are displayed in the SCA Analysis Results section (top left) and in the Project Summary section (top center) of the Fortify Audit view.

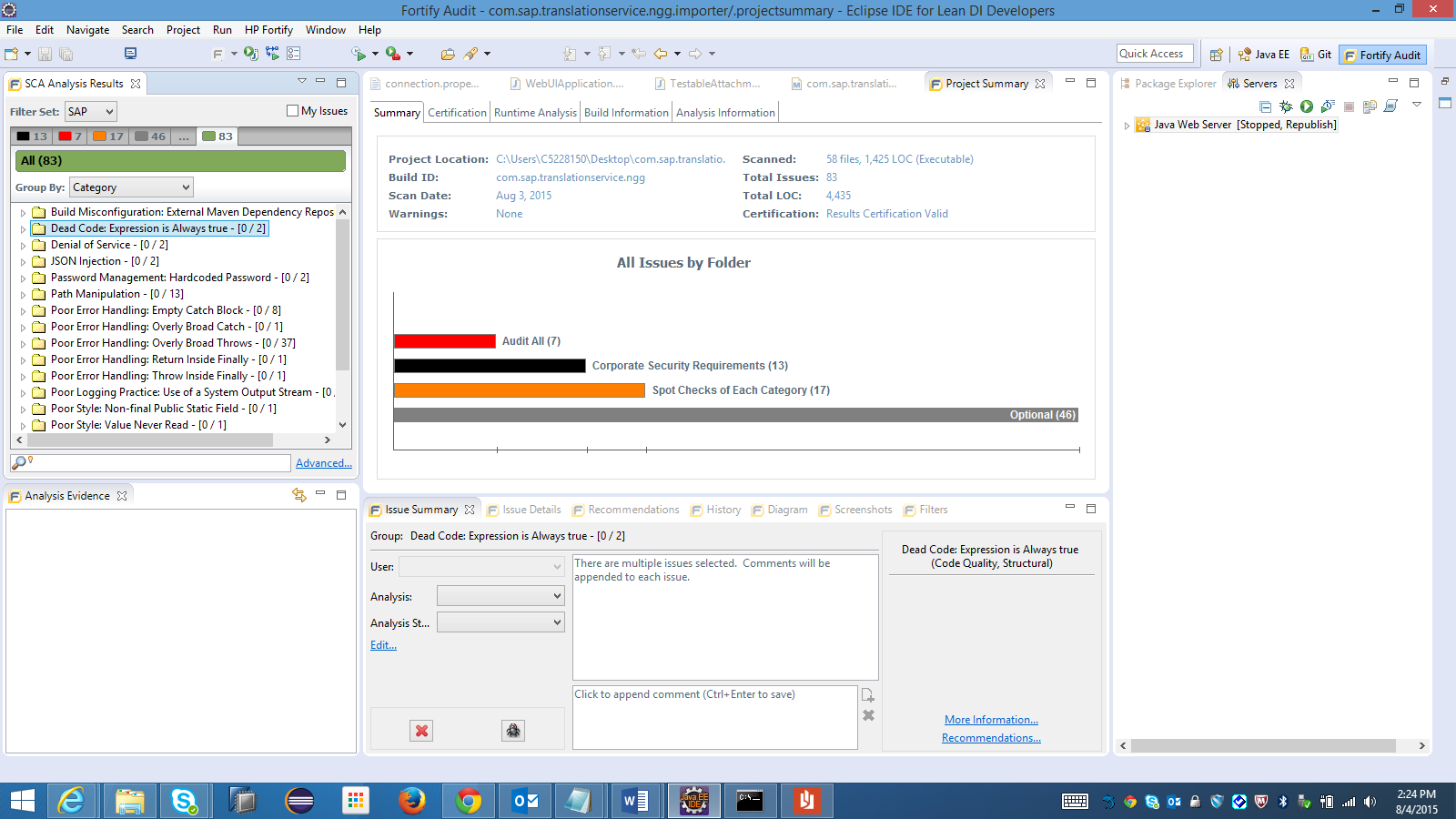
**Viewing Summary Graph Information**

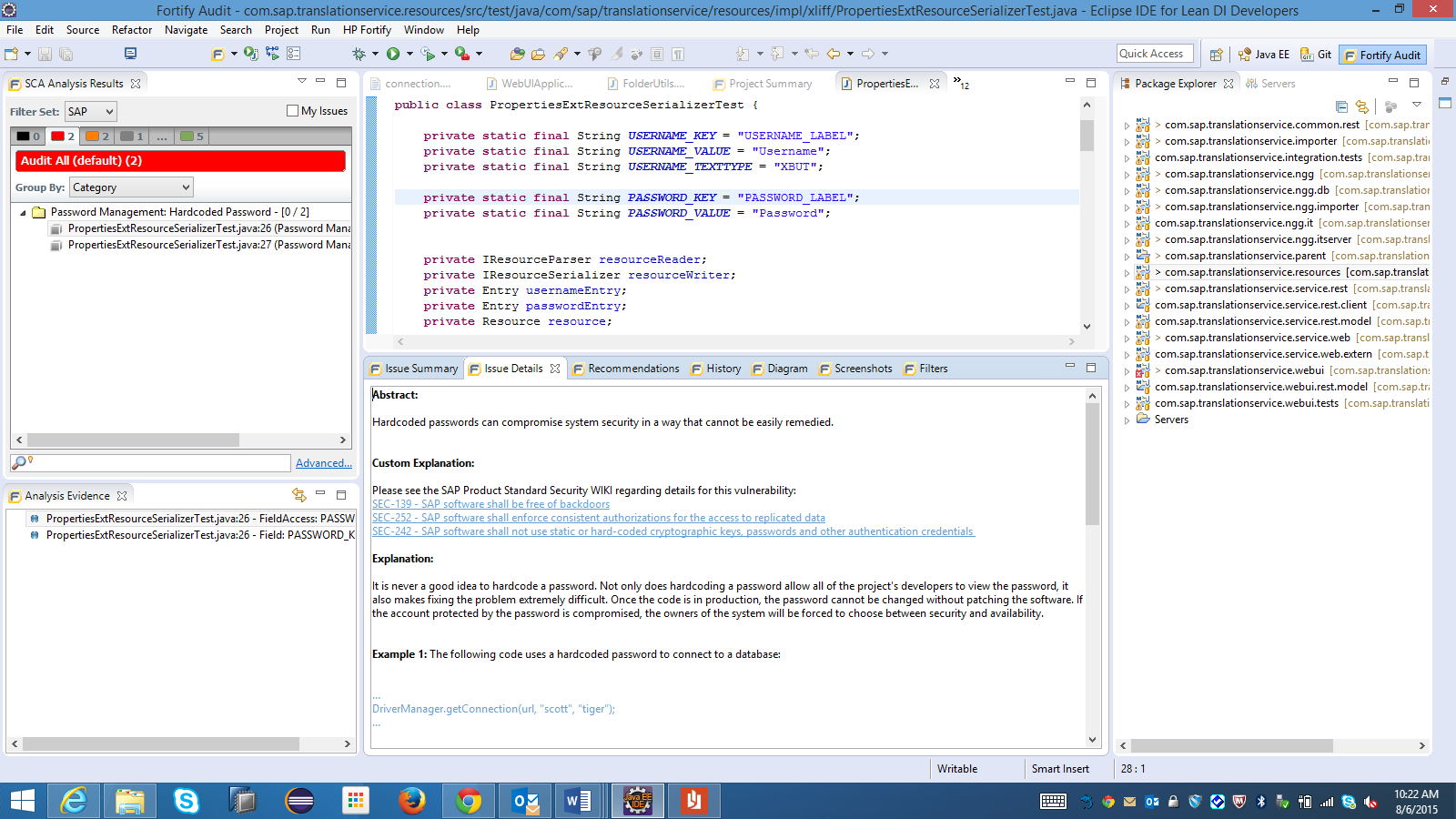
The summary graph displayed in the **Project Summary** section provides multiple perspectives on the sets of issues, grouped by priority (Critical, High, Medium, and Low) uncovered during a scan. You can drill down in the graph to see detailed information about each issue set, and create various bar charts for issues based on a selected issue attribute.

To access details about issue sets in an audit project:

1. Scan your project source code or open an existing audit project in Eclipse.

After the results are loaded, the Project Summary view at the top center of the workspace displays the Summary tab, which includes the summary graph. The summary graph initially displays issues sorted into the Critical, High, Medium, and Low folders. Note: If you change the selection in the Filter Set list (issues panel), the summary graph changes accordingly.





**Opening the Project Summary View**

The Project Summary view displays detailed scan information on the tabs described in this section To open the Project Summary view:

1. Open an FPR file.

2. Select HP Fortify → Show Project Summary.

**About the Summary Tab**

The Summary tab shows high-level information about the project.

**About the Certification**

The Certification tab displays the result certification status. Results certification is a check that the analysis has not been altered since it was produced by HP Fortify Static Code Analyzer or HP Fortify Runtime Application Protection.

**About the Runtime Analysis Tab**

If Runtime analysis data are available, the Runtime Analysis tab displays the following run information:

•Number of issues found by HP Fortify Runtime Application Protection

•Build ID

•Engine version

•Dates and times the run started and ended

•Machine on which the scan was run About the Build Information Tab The Build Information tab displays the following information:

•Build details such as the build ID, number of files scanned, source last modified date, and the date of the scan, which may be different than the date the files were translated

•List of files scanned, with file sizes and timestamps .

•Libraries referenced for the scan About the Analysis Information Tab The Analysis Information tab shows the SCA version that performed the scan, details about the computer on which the scan was run, the user who started the scan, platform, scan date, machine name, and the time required to scan the code.

The **Analysis Information tab** includes the following subtabs:

• **Security Content:** Lists information about the Rulepacks used to scan the source code.

• **Properties**: Displays the SCA properties files settings

• **Command line Arguments**: Displays the command-line options used to analyze the project

• **Warnings**: Lists any and all errors and warnings that occurred during the analysis. To view details about a listed warning, click the warning.2.To see a different view of the high priority issues, click the High bar.

By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values). Note: The example here shows information for scan results that have been partially audited. If these results were from a fresh, unaudited scan, no analysis information would be available. The graph would just display a single bar representing all (unaudited) high priority issues.

**Synchronizing with Software Security Center**

**Step 1: Learn About HP Fortify Software Security Center**

**Introduction**

HP Fortify Software Security Center provides a set of capabilities across the SDLC to automate detection of security vulnerabilities within internal applications. The goals of the Fortify Project are to:

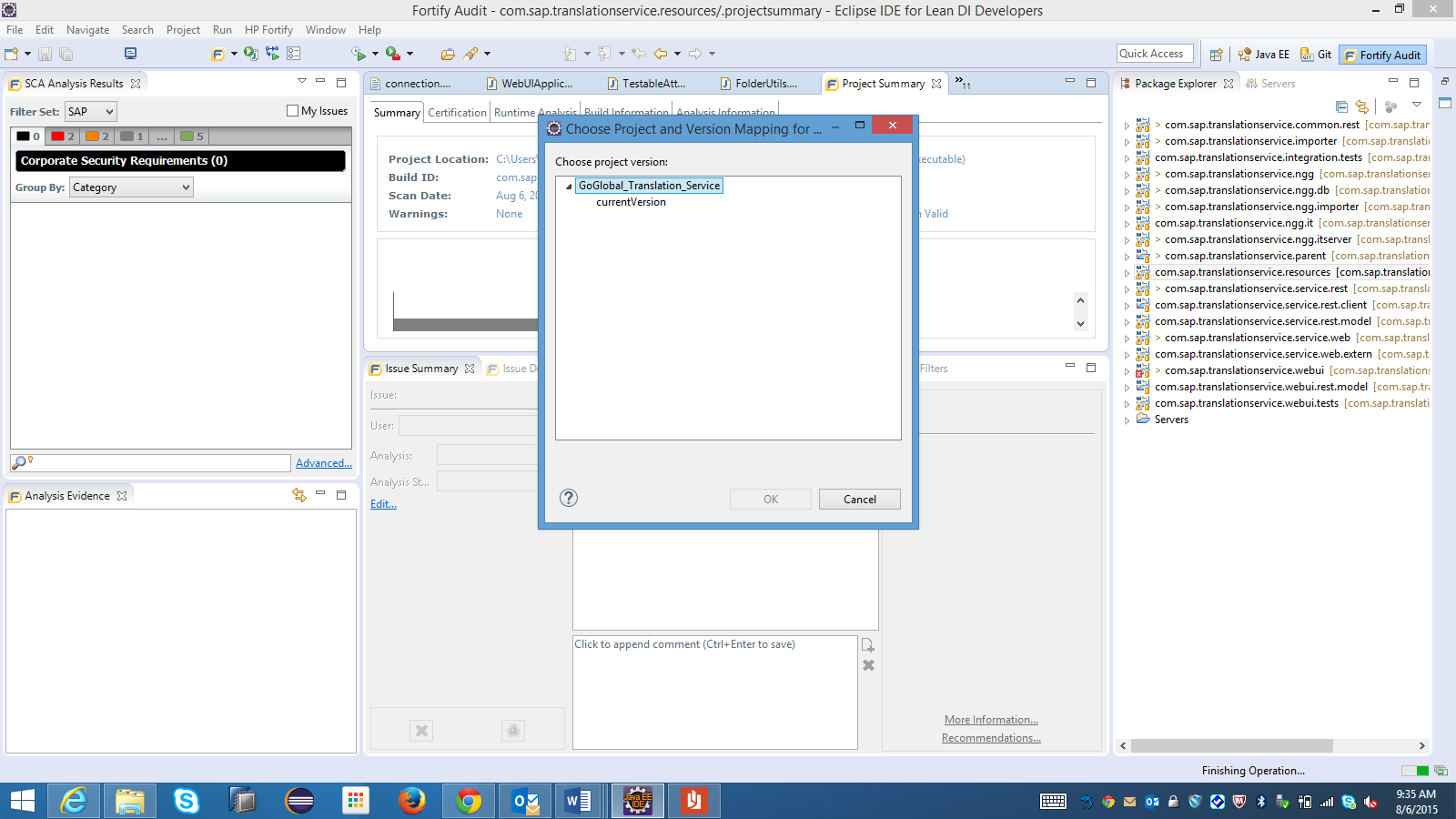
1. Identify and prioritize a baseline of existing vulnerabilities.
2. Prevent new vulnerabilities from being introduced.
3. Remediate existing vulnerabilities and lower the baseline.

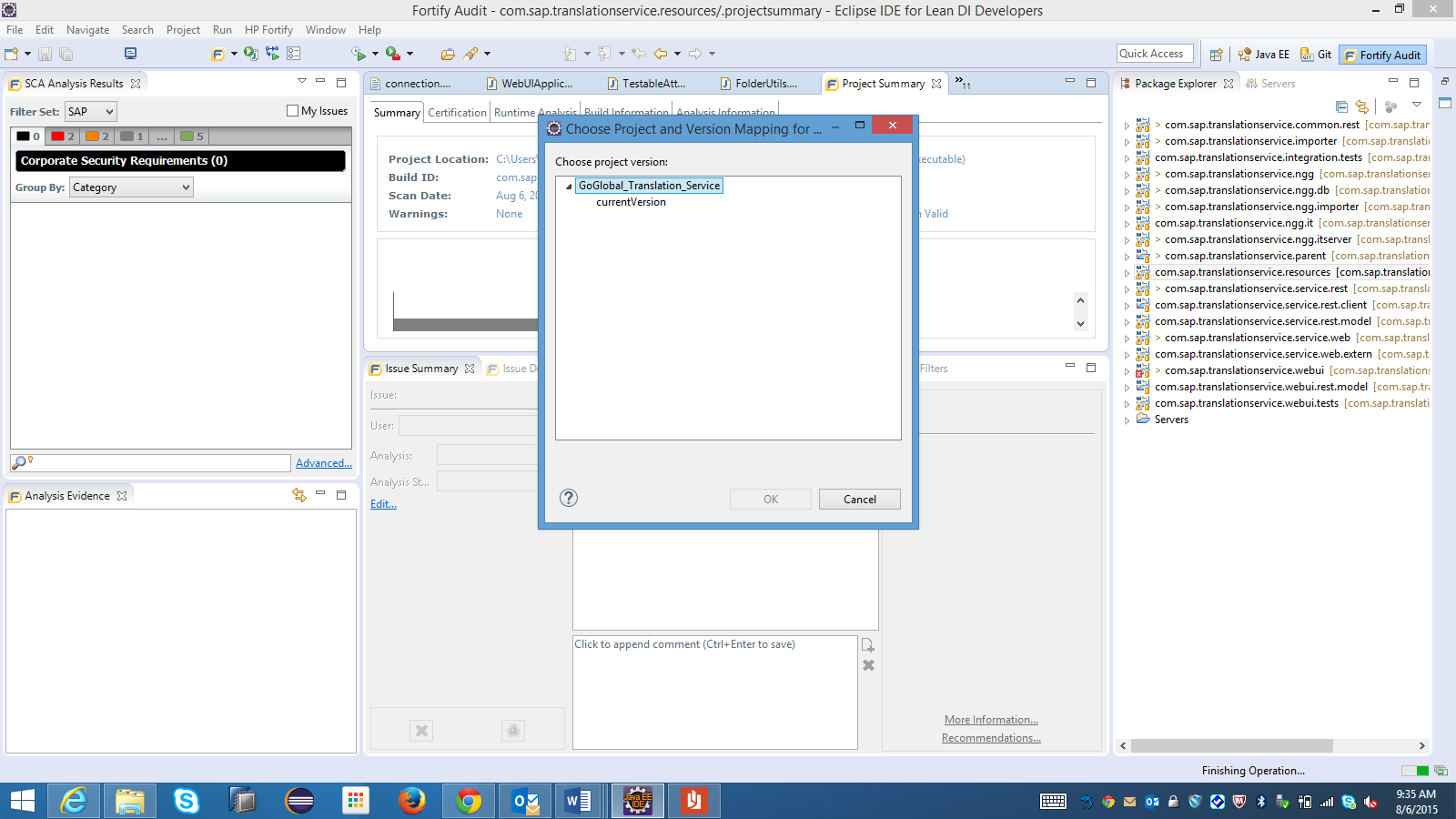
**Technology**

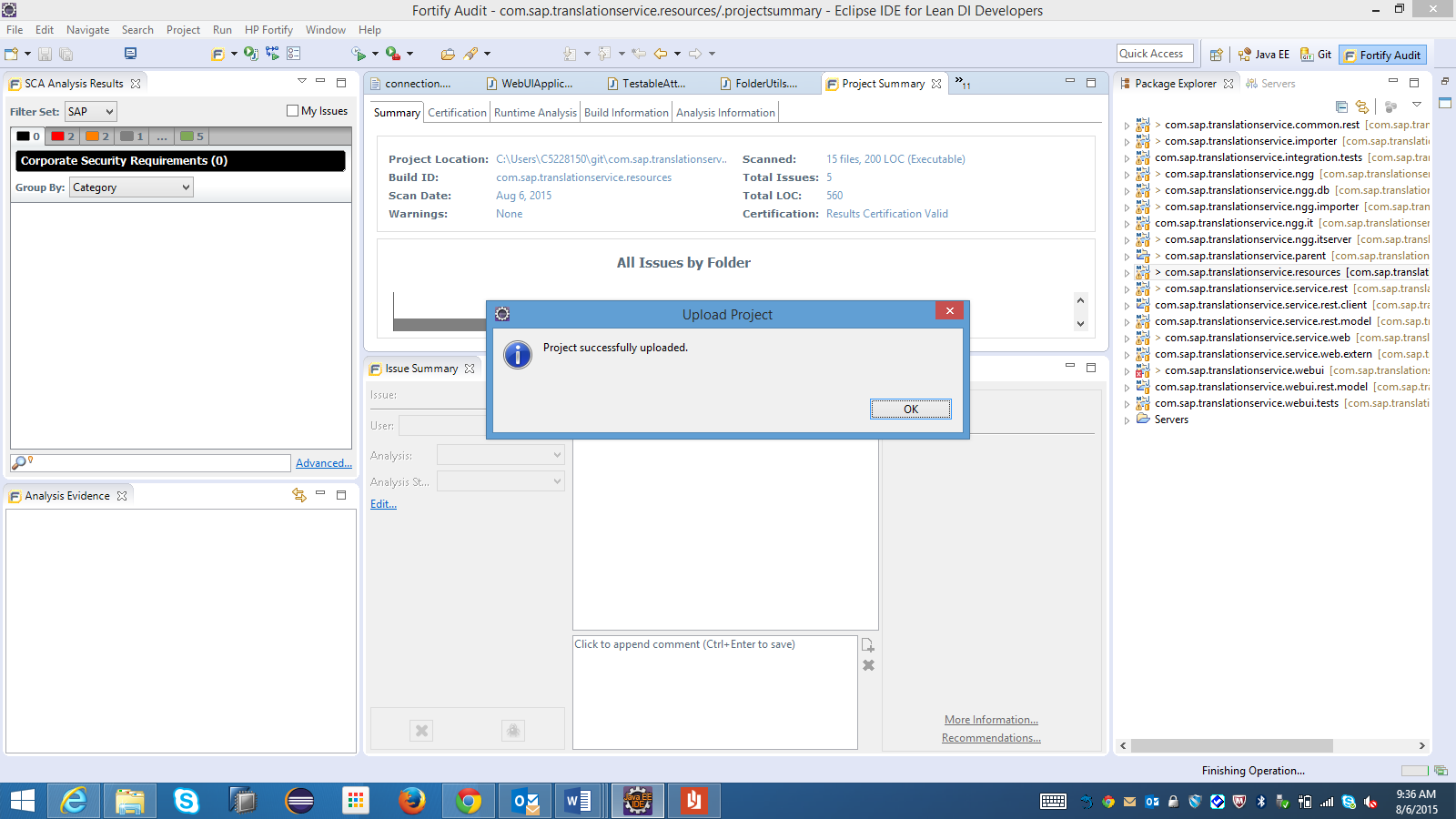
HP Fortify provides two distinct products for generating and viewing security results:

|  |  |  |
| --- | --- | --- |
|  | **⇐ Synchronizes To ⇒** |  |
| **Audit Workbench & IDE Plugins Installed on your desktop and/or build server** |  | **Software Security Center Centralized server** |
| * Provides scanning capabilities to find vulnerabilities in code * Provides visibility into individual Software Security Center projects * Provides complete scan diagnostics |  | * Browser-based repository of static, dynamic, and real-time security results * Aggregates and correlates results from HP Fortify SCA, HP WebInspect, HP Fortify RTA, and various 3rd party utilities * Provides alerts and notifications * Provides trending and metrics over time against individual projects or a full portfolio |

The Eclipse Plugin enables you to automatically upload your changes to a project version on Software Security Center each time you load, merge, save and/or scan your local project. This automatic synchronization helps facilitate collaborative auditing, and enables you to synchronize any offline changes each time you connect to the server.



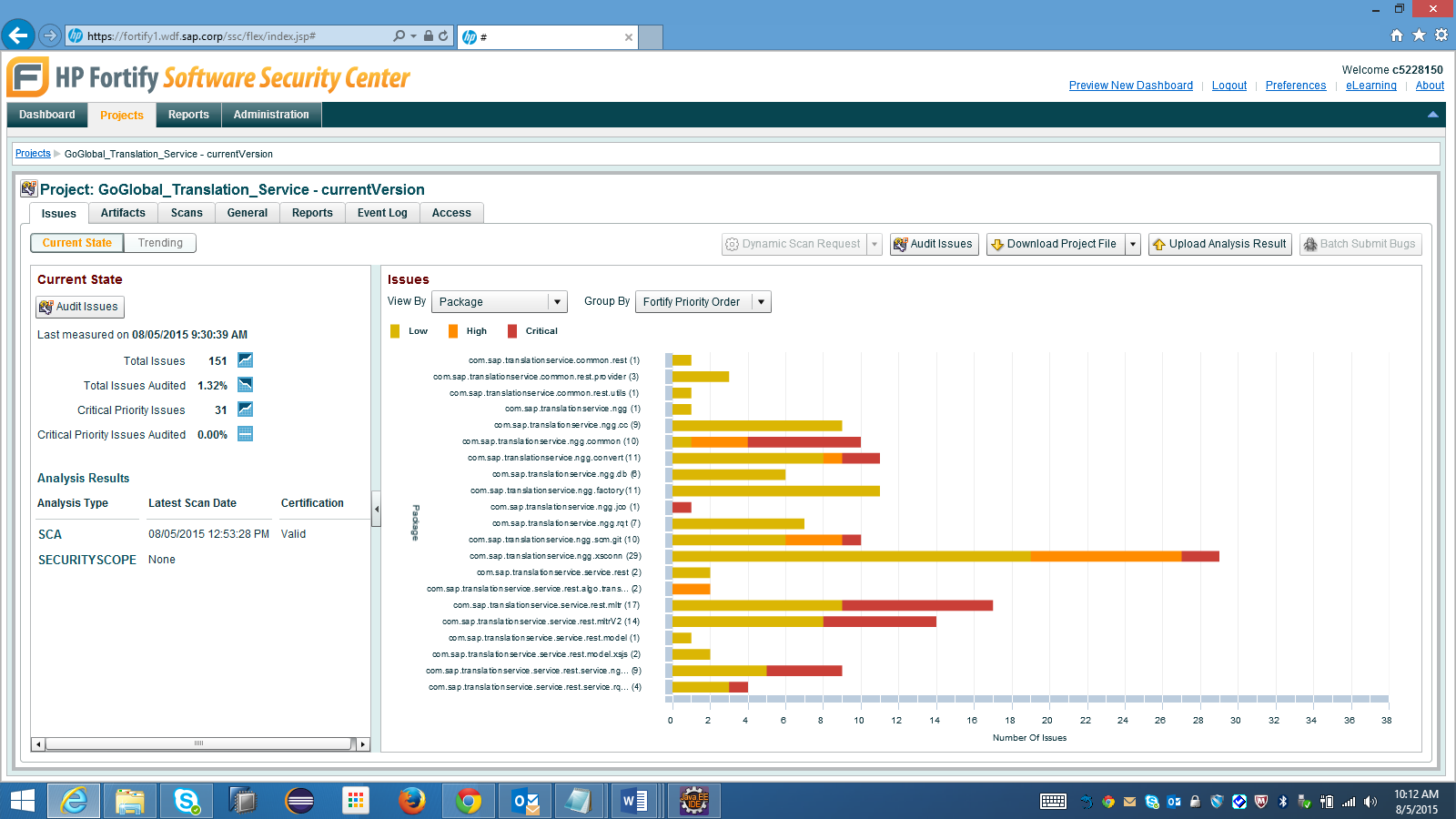




**Note:** Automatic synchronization requires that you specify a project version that already exists in Software Security Center.

If the project version does not exist in Software Security Center, you must first create it. For instructions follow this link[**Creating the project**](https://jam4.sapjam.com/wiki/show/GCvUDZu3HoA6zcpAW9MH65)

**Automatic Results Prioritization**

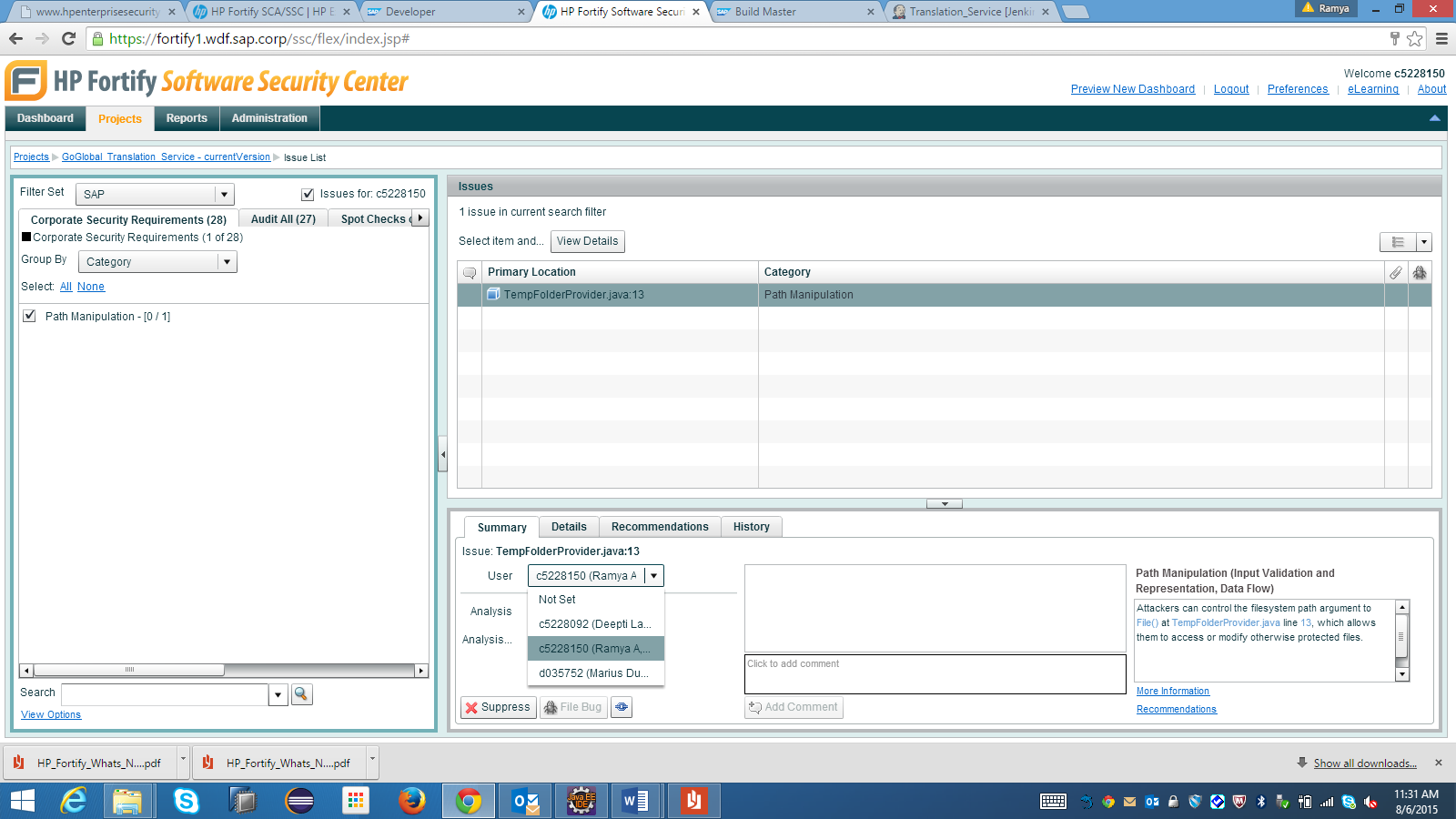


HP Fortify Static Code Analyzer prioritizes and filters issues into folders based on a customizable risk ranking.

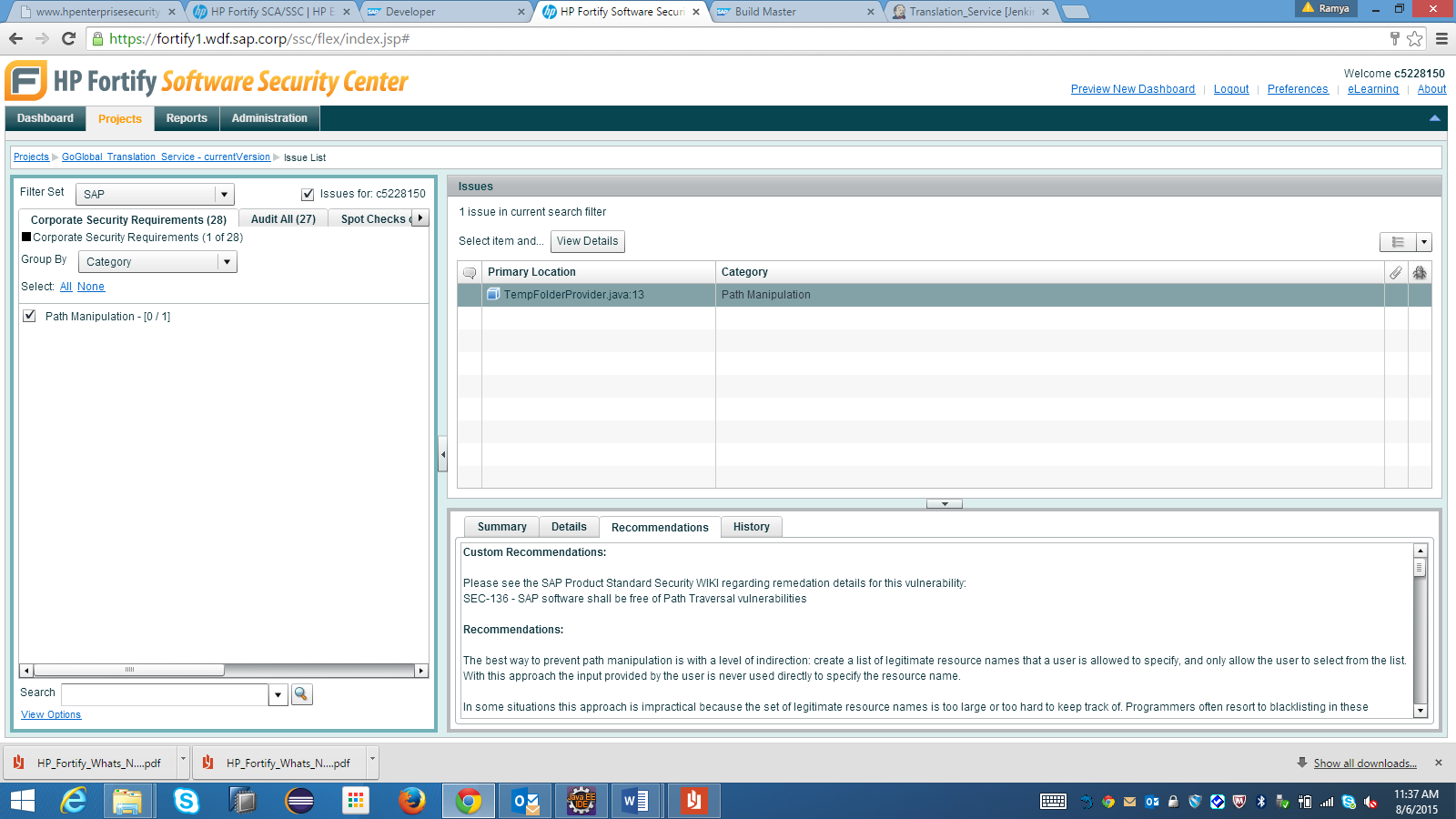
* **Critical -** Critical issues have high impact and high likelihood. Critical issues are easy to discover and exploit and result in large asset damage. These issues represent the highest security risk to the program. As such, they should generally be remediated immediately.
* **High -** High priority issues have high impact and low likelihood. High priority issues are often difficult to discover and exploit, but can result in large asset damage. These issues represent a significant security risk to the program. High priority issues should generally be remediated in the next scheduled patch release.
* **Medium -** Medium priority issues have low impact and high likelihood. Medium priority issues are easy to discover or exploit, but often result in small asset damage. These issues represent a moderate security risk to the program. Medium priority issues should be remediated in the next scheduled product update.
* **Low -** Low priority issues have low impact and low likelihood. Low priority issues can be difficult to discover and exploit and typically result in small asset damage. These issues represent a minor security risk to the program. Low priority issues should be remediated as time allows.

Investigating and Verifying Issues:

The developer tasks in the Fortify setup is to work with the analysis provided by the Security Expert according to the distribution by the Scrum Master. To look at the issues which are assigned to you, you need to go into your Project --> Audit issues --> "All" tab and select the checkbox on top saying "Issues for: <your username>":



You have to go through each of the findings that were assigned to you and try to understand why the issue was given its certain Analysis state and, based on the comment provided by the security expert, what and how you need to fix. To help you in understanding the problem, it is highly recommended to also check the details of the finding and the recommendation how to fix it (Explanation and fix recommendation exist for each single finding):



Verifying Fixes

When you have applied fixes to your code, you should inform your team's build master to trigger a new scan and upload it to the project, so that the fix can be verified.  
Due to the merging capabilities of the [Fortify server](https://fortify1.wdf.sap.corp/ssc/), if an issue has indeed been fixed, then its dataflow will not be detected in the new scan, so it will be marked as "Removed" (and not visible by default. By using this method, you should be able to reach a point where you have all issues in your project either marked as "Removed" or "Not an issue", thus making your product qualified for Q-gate.

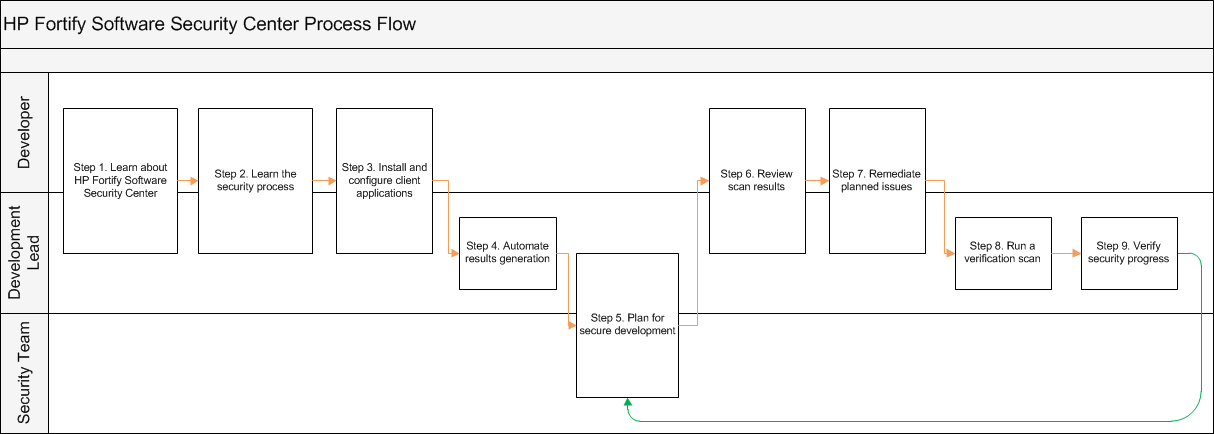
# Step 2: Learn the Security Process

## Overview

Understand the appropriate points of interaction necessary to find and fix vulnerabilities in code.

## Instructions

Development teams should coordinate with central security teams to understand internal checkpoints. Scheduling periodic automated security analysis helps development teams better understand and respond to security issues during agile sprints. The following diagram describes a common set of shared responsibilities:



# Step 3:Plan For Secure Development

## Overview

Using recent security results, development teams can plan remediation activities into their schedule and security teams can understand the timeframe. Focusing on files with the largest number of high risk vulnerabilities will provide the fastest security progress and isolate changes for quality testing.

## Instructions

There are two phases to plan for each development cycle: reviewing new vulnerabilities, and remediating existing vulnerabilities.

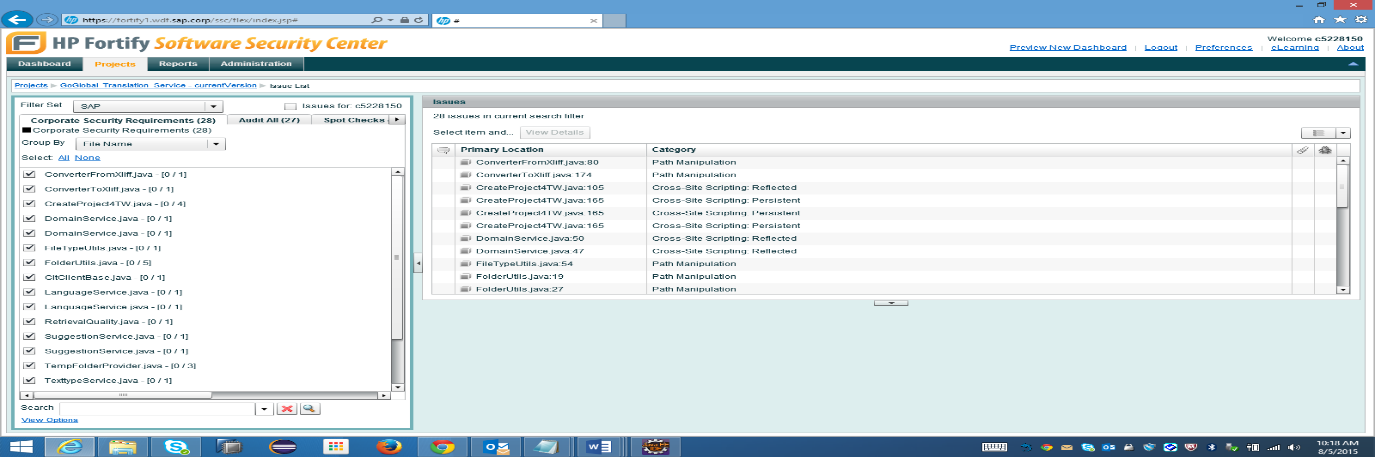
1. Open [Software Security Center.](https://fortify1.wdf.sap.corp/ssc/)
2. Use the Projects tab, select your project and click the **Audit Issues** link.
3. **Plan to Review New Vulnerabilities**

Review new vulnerabilities and prioritize what to fix during the next development cycle, or identify critical vulnerabilities to address now.

Look at the unaudited issues. Schedule an appropriate amount of time for application developers or security teams to handle.

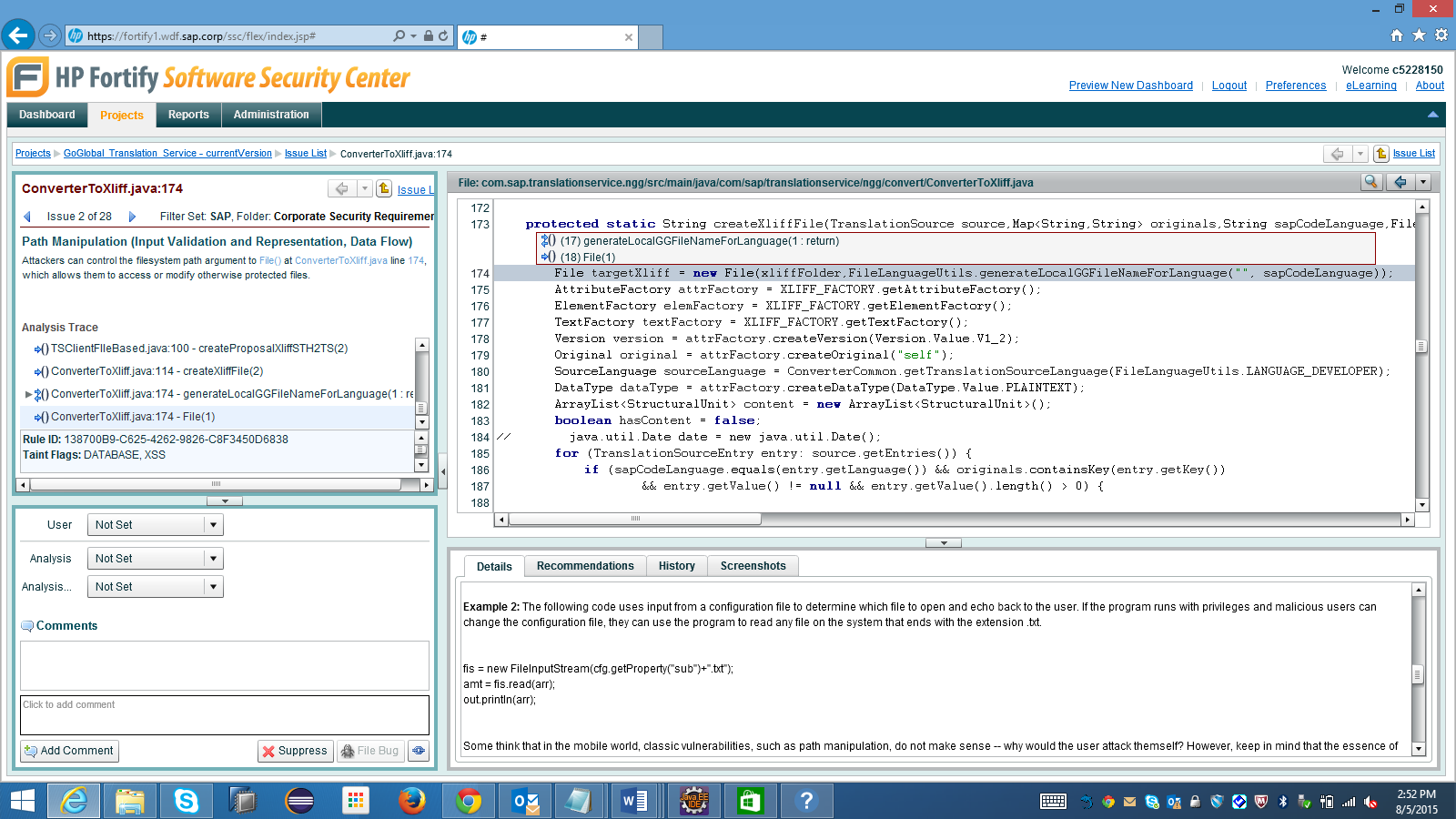
1. **Plan to Remediate Existing Vulnerabilities**

Planning to remediate vulnerabilities by category and file provides a convenient scope for developers and quality testers. Remediating high risk vulnerabilities during the development cycle will ensure that your secured code is thoroughly tested.

* 1. Group 

**Group By File Name**

* Select Item in primary location and click on view details



* 1. Look through the list to identify files with the highest number. Start reviewing at this file.



**Identify Files with highest Number**

**Step 4: Review Scan Results**

**Overview**

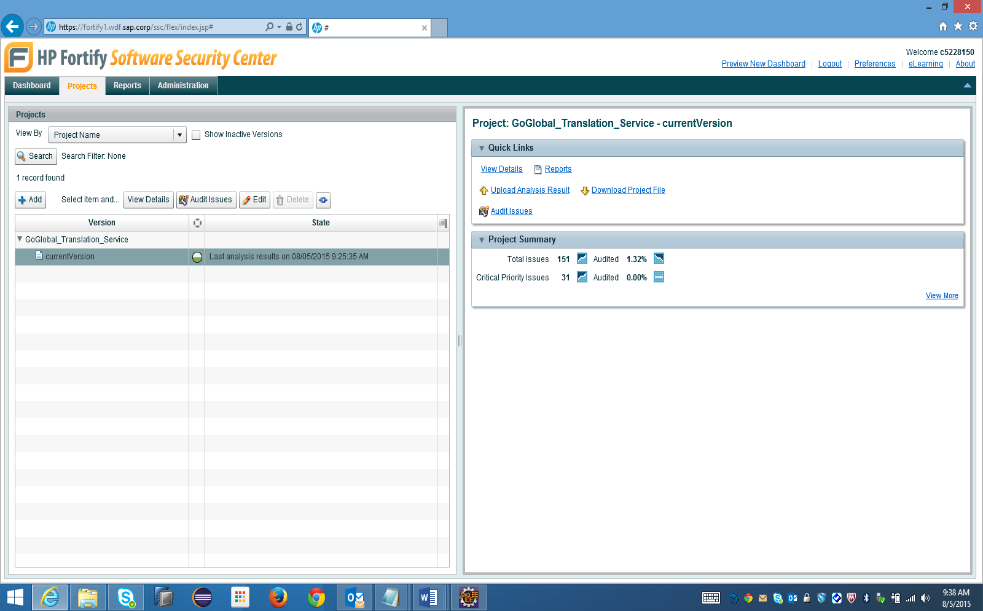
By providing a manual analysis to scan results, development teams will be able to more easily plan their remediation report. Review the output from a recent security scan to understand current known issues/vulnerabilities and plan future work items.

**Instructions**

Open the collaborative audit using your preferred application:

Audit Workbench & IDE Plugins

1. Open [Software Security Center.](https://fortify1.wdf.sap.corp/ssc/)
2. Use the Projects tab, select your project and click the **Audit issue** button.



Audit Issue

1. Provide your manual analysis to issues found during the scan. HP Fortify performs an initial prioritization by grouping its findings into folders. Start by reviewing the Critical folder, then move on to High, Medium, and Low.

**Analysis - Applied By You**

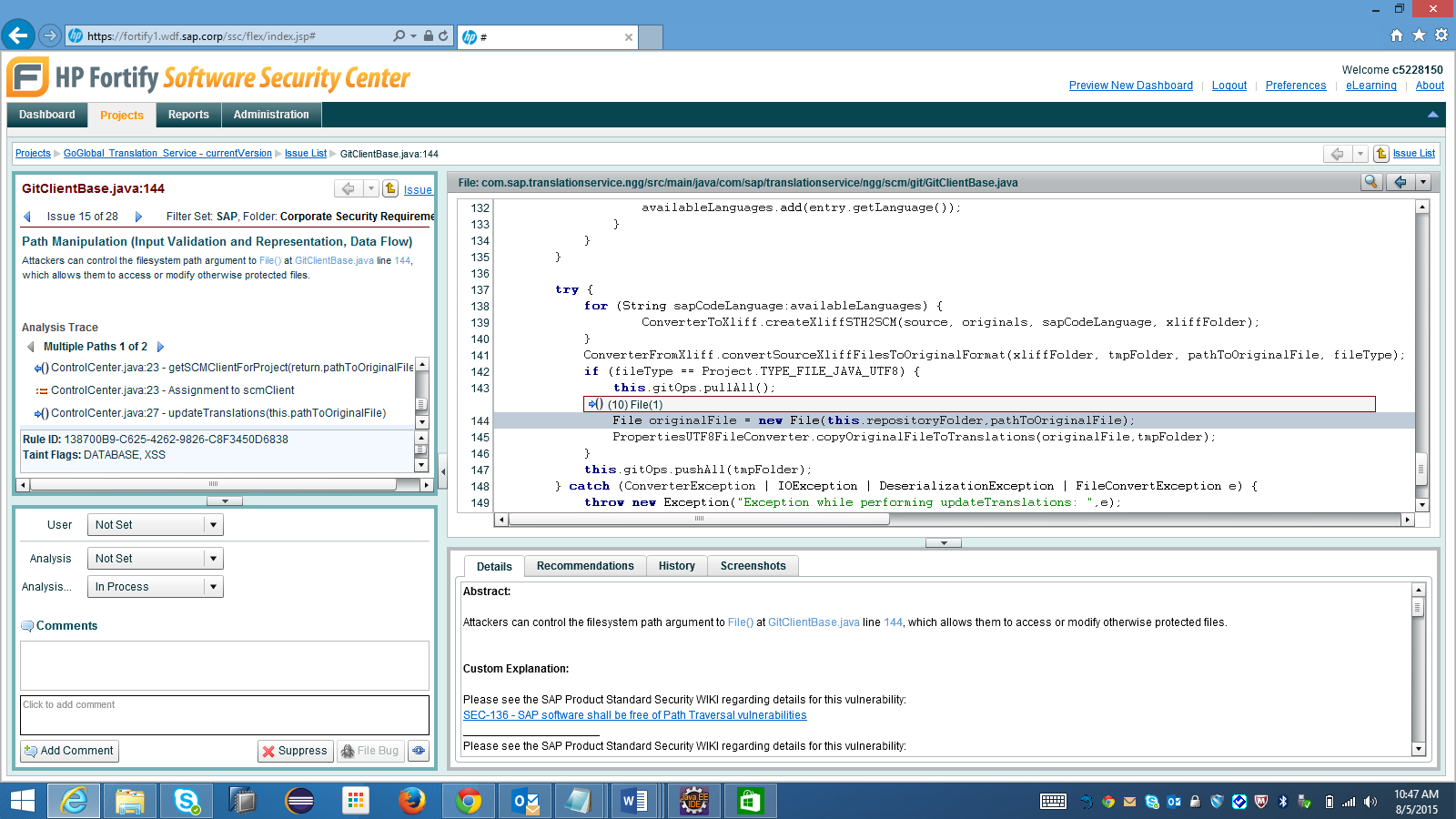
Look over the reported issues and vulnerabilities. Use the Details tab at the bottom of your window to understand a particular issue. Trace the reported issue through your code by navigating through the Analysis Evidence in the bottom-left of your window.

After understanding a issue, tag it with one of the following tags and enter any additional comments:

* + **Exploitable -** This issue represents a serious vulnerability and should be addressed with urgency.
  + **Suspicious -** The reported vulnerability looks important and should be fixed or reviewed with other developers.
  + **Bad Practice -** The reported issue is not severe but also not ideal.
  + **Reliability Issue -** A finding which may, in select situations, hamper the availability/reliability of the application.
  + **Not an Issue -** The reported issue is clearly not vulnerable in any situation and we can safely ignore it .It is important to note that an application area with limited access (such as "logged in users") may still be vulnerable as attack methods improve.

**Understanding the issue**

For each issue, Software Security Center provides details to help development and security teams better understand what is being reported. The Analysis Evidence section will allows developers to walk through each line of related code.



**Details**

**Step 5. Remediate Planned Issues**

**Overview**

Software Security Center provides in-context Details and Recommendations to help development teams understand vulnerability impact and receive remediation guidance.

**Instructions**

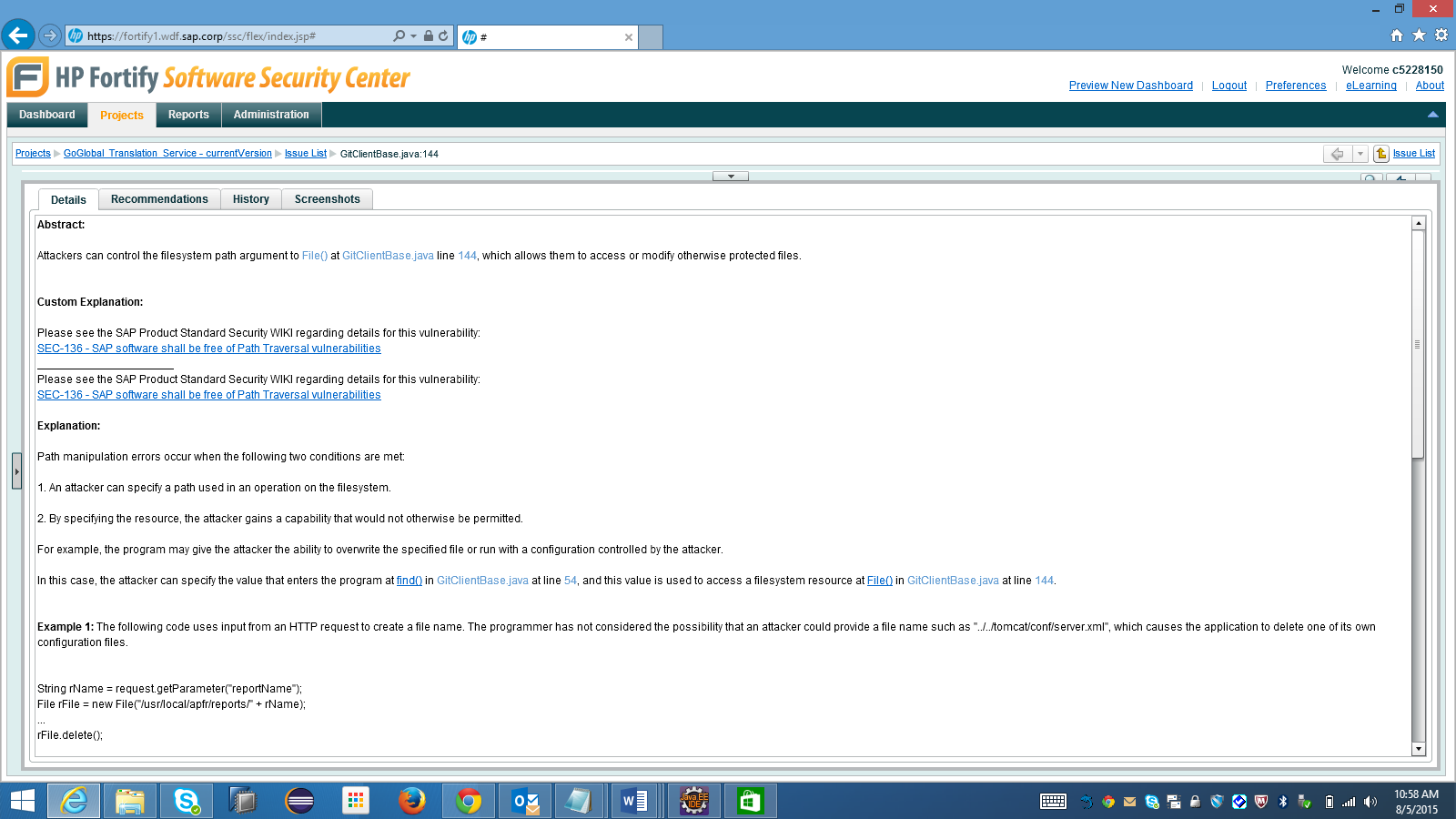
Open the collaborative audit using your preferred application:

Audit Workbench & IDE Plugins

1. Open [Software Security Center.](https://fortify1.wdf.sap.corp/ssc/)
2. Use the Projects tab, select your project and click the **Audit Issue**button.
3. Click on the particular issue you would like to work on from the Issue List.
4. Use the Details and Recommendations tabs at the bottom to identify a way to fix the issue.  
   After successful remediation, HP Fortify Static Code Analyzer will identify the patch and remove the issue from your next scan.

**Details**

Development teams can read the Details to better understand the risk posed by a particular issue.



**Recommendations**

After understanding relevant Details, developers should consult the Recommendations to receive remediation guidance. Guidance is given in the appropriate language and/or framework that was scanned. Security teams may customize Software Security Center's recommendations to account for any internal standards guidance by following the Custom Rules guide.  
Developers should look through the Analysis Evidence to identify the appropriate line of code to start remediation.

