

How to merge scan files



This page has been made public for vendors
Question

My analysis is lost when I re-scan my code with Fortify, how do I carry analysis forward for new scans?

Answer

Fortify provides tools to merge the audit comments from an audited FPR scan file into a new scan. This will carry forward audit data and mark issues that are no longer in the scan as "removed." There are several ways to merge Fortify audit data . Each option will be discussed below.

Option 1: Audit Workbench GUI

You can merge audit data into your project from another file. Audit data consist of the custom tag values and comments added to issues from Audit Workbench. Audit Workbench merges comments in a chronological list as it updates custom tag values. If the custom tag values conflict (the same tag is set to different values) Audit Workbench prompts you to resolve the conflict.

Note : Keep in mind that Audit Workbench:

- Does not merge issues
- Shows only the most recent scan
- Shows only the issues from the most recent scan

Ensure that the projects you merge contain the same analysis information, that is the scan was on the same source code project (no missing libraries or files), the SCA settings were the same, and the scan was performed using the same security content.

To merge projects:

1. Open a project in Audit Workbench.
2. Click **Tools > Merge Audit Projects** .

The Select an FPR File dialog box opens.

3. Select an FPR file, and then click **Open** .

The Merge dialog box opens.

Note : After you select an FPR, Audit Workbench might prompt you to choose between the project template in the current FPR and the project template in the FPR you are merging in.

4. To confirm the number of issues added or removed from the file, click **OK** .

Note: If the scan is identical, Audit Workbench does not add or remove issues.

If you scanned your code from within Audit Workbench and then perform a rescan of the code from Audit Workbench, Audit Workbench merges the analysis results with those from the previous scan to determine which issues are new, which have been removed, and which were uncovered in both scans.

For more information, see the HPE Fortify Audit Workbench User Guide section, "About Working with Audit Data."

Option 2: Using the HPE Fortify Audit Project Command-line Utility

You can also use the HPE Fortify Audit Project command-line utility (`bin\FPRutility.bat` for Windows) to merge audit data. This utility enables you to merge an audited project, verify the signature of the FPR, or migrate earlier HPE Fortify Audit Projects to the current format.

The `FPRutility -merge` option combines the analysis information from two FPR files into

HPE Fortify Version	4.42 and later
Programming Language	<input checked="" type="checkbox"/> C/C++ <input checked="" type="checkbox"/> .NET <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Objective-C <input checked="" type="checkbox"/> Other
Fortify Audit Workbench	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Fortify IDE Plugin	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Other Fortify Component	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Request code review tools, validations, and support [HERE](#).

a single FPR file using the values of the primary project to resolve conflicts.

To merge FPR files:

```
FPRUtility -merge -project <primary.fpr> -source  
<secondary.fpr> -f <output.fpr>
```

To merge FPR files and set instance ID migrator options:

```
FPRUtility -merge -project <primary.fpr> -source  
<secondary.fpr> -f <output.fpr>  
-iidmigratorOptions "<iidmigrator_options>"
```

For more information, including command-line options, see the HPE Fortify Static Code Analyzer User Guide, section "Merging FPR Files".

Option 3: Using the HPE Fortify Eclipse Plugin

If you use the HPE Fortify Eclipse Plugin to scan your code and audit the results, you can also use the Eclipse plugin to merge audit projects.

To merge projects:

1. Open a project in Eclipse Plugin.
The Audit window opens.
2. Select **HPE Fortify > Merge Audit Projects** .
3. Select an FPR file, and then click **Open** .
The Progress Information dialog box opens. When complete, the Merge dialog box opens.
4. Click **OK** to confirm the number of issues added or removed from the file.
Note: If the scan is identical, no issues are added or removed.

The project now contains all audit data from both result files.

When you re-scan a project from Eclipse, the plugin does not automatically merge the results from the previous scan with the results from the new scan. However, if you want to see specifically what issues have been fixed and which issues were introduced since the earlier scan, you can configure the plugin to merge scan results.

To enable the Eclipse Plugin to merge the results of the next scan you run with results from the previous scan:

1. Select **HPE Fortify > Options** .
2. In the left panel of the Options dialog box, select **Default Project Settings** .
3. In the right panel, click the **Advanced Options** tab.
4. In the **Advanced Analysis Options** section, select the **Merge with previous scan** check box.
5. Click **OK** .

Note: You can override this merging option for a given project by configuring project properties.

For more information, see the HPE Fortify Plugin for Eclipse Installation and Usage Guide section, "Merging Audit Data."

Option 4: Using the HPE Fortify Visual Studio Plugin

If you use the HPE Fortify Visual Studio Plugin to scan your code and audit the results, you can also use the Visual Studio plugin to merge audit projects.

To merge projects:

1. Open a project in Visual Studio Fortify Plugin.
The Audit window opens.
2. Select **HPE Fortify > Merge Audit Projects** .

3. Select an FPR file, and then click **Open** .
The Progress Information dialog box opens. When complete, the Merge dialog box opens.
4. Click **OK** to confirm the number of issues added or removed from the file.
Note: If the scan is identical, no issues are added or removed.

The project now contains all audit data from both result files.

For more information, see the HPE Fortify Package for Microsoft Visual Studio Installation and Usage Guide section, "Merging Audit Data."

References

- HPE Fortify Static Code Analyzer User Guide, "Merging FPR Files"
- HPE Fortify Audit Workbench User Guide, "About Working with Audit Data"
- HPE Fortify Plugin for Eclipse Installation and Usage Guide section "Merging Audit Data"
- HPE Fortify Package for Microsoft Visual Studio Installation and Usage Guide section "Merging Audit Data"