

OpenText™ Fortify on Demand Plugin for Eclipse

Software Version: 23.1

User Guide

Document Release Date: August 2023

Software Release Date: August 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2010-2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on August 15, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support/documentation>

Contents

- Preface 4
 - Contacting Fortify Customer Support 4
 - For More Information 4
 - About the Documentation Set 4
 - Fortify Product Feature Videos 4

- Getting Started 5
 - Requirements for Using the Fortify on Demand Plugin for Eclipse 5
 - Installing the Fortify on Demand Plugin for Eclipse 5
 - Setting up Automatic Updates 6
 - Configuring the Fortify on Demand Plugin for Eclipse 7

- Uploading Code to Fortify on Demand 8

- Reviewing Analysis Results 16
 - Opening Analysis Results 17
 - Analysis Results in the Fortify on Demand Plugin for Eclipse 19
 - Analysis Trace Icons 20
 - Reviewing Issues 21
 - Auditing Issues 23
 - Locating the Source Code Associated with Static Scan Issues 23
 - Closing Analysis Results 24

- Send Documentation Feedback 25

Preface

Contacting Fortify Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

<https://www.microfocus.com/support>

For More Information

For more information about Fortify software products:

<https://www.microfocus.com/cyberres/application-security>

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following OpenText Product Documentation website:

<https://www.microfocus.com/support/documentation>

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText Community:

<https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements>

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

<https://www.youtube.com/c/FortifyUnplugged>

Getting Started

This guide describes how to install the Fortify on Demand Plugin for Eclipse and use it to upload code for static analysis and open analysis results for remediation.

This section contains the following topics:

Requirements for Using the Fortify on Demand Plugin for Eclipse	5
Installing the Fortify on Demand Plugin for Eclipse	5
Setting up Automatic Updates	6
Configuring the Fortify on Demand Plugin for Eclipse	7

Requirements for Using the Fortify on Demand Plugin for Eclipse

To use the Fortify on Demand Plugin for Eclipse, you must have the following:

- An API root URL.
For a list of data center API root URLs, see the *Fortify on Demand User Guide*.
- Your Fortify on Demand login credentials or your SSO login URL if your organization has configured SSO for the tenant.
- To upload your code to Fortify on Demand:
 - Your login account must have the Start Static Scan permission.
 - To have the Fortify on Demand Plugin for Eclipse automatically package all the necessary dependencies and source code (including files required for a Debricked open source scan), you must have a locally installed Fortify ScanCentral SAST client version 22.1.2 or later.
You can download the Fortify ScanCentral SAST client from the Fortify on Demand Tools page. For installation instructions, see the README.txt file included in the downloaded ZIP.

Installing the Fortify on Demand Plugin for Eclipse

The following instructions describe how to do obtain the Fortify on Demand Plugin for Eclipse directly from Fortify on Demand. Alternatively, you can install it using the Eclipse Marketplace Client.

To install the Fortify on Demand Plugin for Eclipse:

1. From Eclipse, select **Help > Install New Software**.
The install wizard starts at the **Available Software** page.
2. Click **Add**.

3. (Optional) In the **Name** box, type a name for the update site.
4. In the **Location** box, type `https://tools.fortify.com/fodeclipseplugin`.

Note: You might need to configure a proxy in Eclipse to reach the location.

5. Click **OK**.

The **Work with** box displays your new repository.

6. Expand the **Fortify on Demand Plugins** node.
7. Select one or more of the following the check boxes for the tools you want to install:
 - **FoD Analysis Results Remediation** enables you to review analysis results for an application and release so you can audit and remediate issues in your code.
 - **FoD C++ Project Dependencies Upload (optional, requires CDT)** automatically finds all included library references and adds them to your package. You do not need this tool if you do not use a CDT environment to create C++ projects in Eclipse. You may, however, install the plugin anyway. If you leave the **Contact all update sites during install to find required software** option selected, it automatically installs necessary libraries from the official Eclipse update site.
 - **FoD Java Project Dependencies Upload (optional, requires JDT)** automatically finds JAR files from your classpath library containers that reference JAR files outside of the workspace—such as JRE or libraries referenced from a Maven or Ivy repository— and includes them in the package. Note that this is done recursively for all dependent projects. Typically, you already have JDT installed, so Fortify recommends that you install this plugin. For example, if you use RAD you already have JDT.
 - **FoD Source Code Upload (generic)** enables you to package projects from your workspace. It finds project dependencies.

8. Click **Next**.

The install wizard lists the items to be installed on the Install Details page.

9. Click **Next**.

10. Read the **End User License Agreement**, and then select **I accept the terms of the license agreement**.

11. Click **Finish**.

12. When the installer prompts you to restart Eclipse, click **Yes**.

The Eclipse menu bar now includes the **Fortify** menu.

Setting up Automatic Updates

To set up an automatic update notification in Eclipse:

1. Open the **Eclipse Preferences** dialog.

If you need help with this, see the **Eclipse Help**.

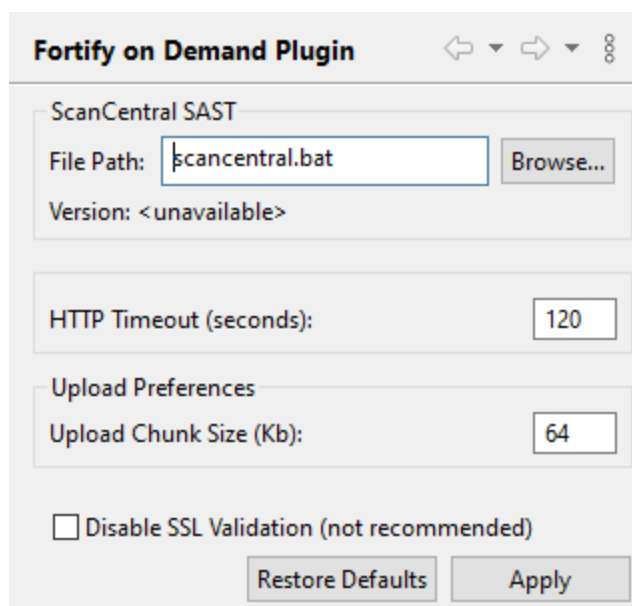
2. Select **Available Software Sites**, and make sure that the Fortify on Demand update site <https://tools.fortify.com/fodeclipseplugin> is selected.
3. Select **Automatic Updates**, and then select the **Automatically find new updates and notify me** check box.
4. Select the notification options you want.
If an update is available, you will see a notification icon in the tray at the bottom of the Eclipse window.

Configuring the Fortify on Demand Plugin for Eclipse

You can configure options for uploading source code and for communicating with Fortify on Demand at any time.

To configure Fortify on Demand Plugin for Eclipse options:

1. From the Eclipse menu bar, select **Fortify > Configure Fortify on Demand Plugin**.



2. To use the Fortify ScanCentral SAST client to package your code, under **ScanCentral SAST** click **Browse** to the right of **File Path** to specify the location of the executable.
After you specify the path to the Fortify ScanCentral SAST client, its version is displayed.
3. To change the amount of time to wait for communicating with Fortify on Demand before giving up, type the time in seconds in the **HTTP Timeout** box.
Valid values for HTTP timeout are 0 through 21600 (6 hours). A value of 0 indicates that there is no timeout. The default HTTP timeout is 120 seconds (2 minutes).
4. To change the size of the individual pieces that is uploaded to Fortify on Demand, type the size in kilobytes in the **Upload Chunk Size** box.

The packaged source code is uploaded in chunks for optimal performance and reliability. The valid chunk size values are 1 through 10000 KB. To upload a large file with a stable connection, you can specify larger chunks sizes. To upload a small file with a connection that is not as reliable (for example, a wireless connection), use the default chunk size of 64 KB or smaller.

5. To enable the Fortify on Demand Plugin for Eclipse to accept any server certificate, select the **Disable SSL Validation** check box.

Note: For security reasons, selecting this option is not recommended.

6. Click **OK**.

Uploading Code to Fortify on Demand

Before you start, make sure you have the following:

- Your Fortify on Demand login credentials

Note: To upload your code, you must have the Start Static Scan permission.

- One or more projects open in Eclipse
- To include a Debricked open source scan for the projects and automatically package the project with the file required to detect dependencies, verify that you use the following:
 - Fortify ScanCentral SAST client version 22.1.2 or later
 - Fortify on Demand Plugin for Eclipse version 23.1 or later

Note: To include a Debricked open source scan for the project without using the Fortify ScanCentral SAST client, make sure your project includes the file required to detect dependencies as described in the *Fortify on Demand User Guide* before you upload the code to Fortify on Demand. You must manually verify that all the files to package are selected including the required file prepared for open source scanning.

To upload source code to Fortify on Demand from Eclipse:

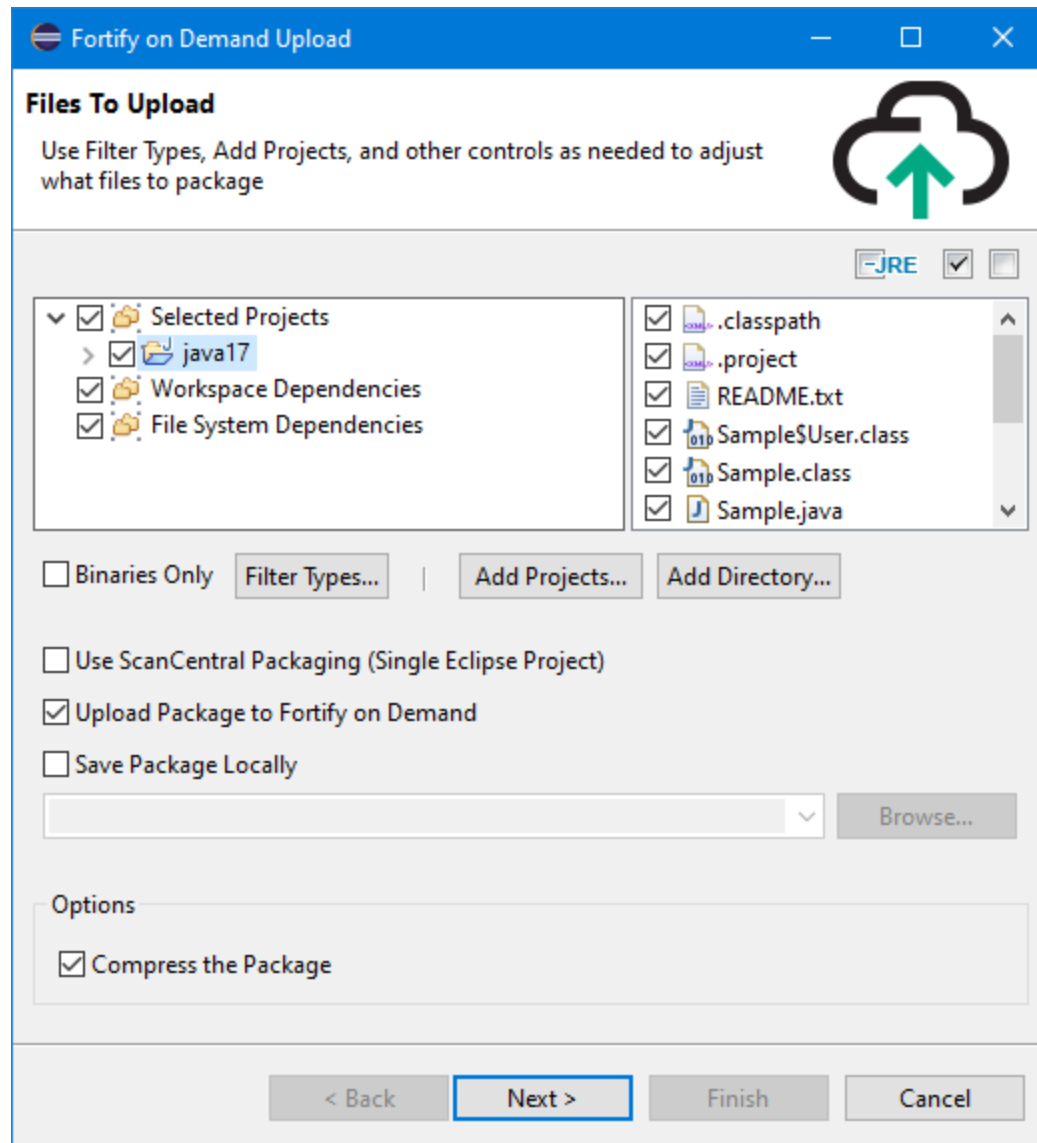
1. Select one or more projects in Eclipse.

Note: To use the Fortify ScanCentral SAST client to package the code for upload, you must select only one project.

2. Select **Fortify > Upload Projects to Fortify on Demand**.

The Fortify on Demand Upload wizard opens.

Files to Upload (page 1 of 3)



Note: By default, if you have only one project selected, then the left panel displays only **Resources collected by ScanCentral**. To upload your project without using Fortify ScanCentral SAST, clear the **Use ScanCentral Packaging** check box.

In the left panel, the tree view lists the following items:

- **Selected Projects**—Projects and folders you selected for upload
- **Workspace Dependencies**—Dependent projects that were detected and added automatically
- **File System Dependencies**—Dependent Java and C++ libraries that are not in the workspace
These libraries are typically needed to scan your code correctly. We recommend that you include them in your package.

The right panel displays the files contained in the folder selected in the left panel.

- To automatically package the project with the Fortify ScanCentral SAST client, select **Use ScanCentral Packaging**.

For a single Eclipse project, the Fortify ScanCentral SAST client can automatically package all the necessary dependencies and source code that is required for the scan. To use this feature, you must have a locally installed Fortify ScanCentral SAST client.

Note: This option is not available if you have more than one project selected.

- Select the files you want to upload.

Note: These options are not available if you are using the Fortify ScanCentral SAST client to automatically package the code.

To refine the items to upload, perform one or more of the procedures described in the following table.

Item Upload Refinement	Procedure
Remove JRE files from the upload package.	<ul style="list-style-type: none"> • Click -JRE.
Omit specific files located in an item listed in the tree view.	<ol style="list-style-type: none"> a. Select an item in the tree view. b. Clear the check boxes for the files you want exclude from your upload package.
Upload only binary files (EAR, EXE, CLASS, DLL, JAR, and WAR files).	<ul style="list-style-type: none"> • Select the Binaries Only check box.
Upload only specific file types.	<ol style="list-style-type: none"> a. Click Filter Types. b. In the Select Types dialog box, select the check boxes for the file types that you want to upload. c. To include file types not listed, in the Other extensions box, type the extensions for any additional file types to upload. If you want to list more than one extension, separate them with commas. d. Click OK. <p>The extensions you select are displayed under the Filter Types button.</p>
Upload one or more	<ol style="list-style-type: none"> a. Click Add Projects.

Item Upload Refinement	Procedure
additional projects.	b. In the Folder Selection dialog box, navigate to and select the additional project to upload and click OK .
Upload additional external resources.	a. Click Add Directory . b. In the Browse for Folder dialog box, navigate to and select the resources to upload, and then click OK . After you add a folder, you can select specific files within it. <div data-bbox="630 659 1401 877" style="background-color: #f0f0f0; padding: 5px;">Notes:<ul style="list-style-type: none">○ Subfolders are included.○ Folders with native Unicode symbols in them are not supported.</div>

5. To upload the package to Fortify on Demand, leave the **Upload Package to Fortify on Demand** check box selected.
6. To save the package to a local directory:
 - a. Select the **Save package locally** check box.
 - b. Click **Browse** and then navigate to and select a local folder.
 - c. Type a name for the package, and then click **Save**.
7. To reduce the size of the package, select the **Compress the Package** check box.

This option is not available if you are using the Fortify ScanCentral SAST client to package the project for upload. Although this reduces the size of the package to be uploaded, the packaging process takes longer.
8. Do one of the following:
 - If you are saving the package locally without uploading it to Fortify on Demand, click **Finish**.
 - To upload the package to Fortify on Demand, click **Next** to proceed to the **Fortify on Demand Login Credentials** page.

Fortify on Demand Login Credentials (page 2 of 3)

Fortify on Demand Upload

Fortify on Demand Login Credentials

✘ No username specified
No tenant specified

API Root URL:

[Clear Portal History](#)

Fortify on Demand Credentials

Username:

Password:

Tenant ID:

Use Identity Provider

SSO Login URL:

Remember Login Credentials

[Configure Network Connection](#)

1. In the **API Root URL** box, type an API root URL.
For a list of data center API root URLs, see the *Fortify on Demand User Guide*.
2. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none">a. Provide your Username, Password, and Tenant ID.b. To save your credentials, select the Remember Login Credentials check box. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">Note: For security reasons, the Fortify on Demand Plugin for Eclipse does not save your password.</div>c. To configure your network preferences, click Configure Network Connection, and then follow the instructions provided by Eclipse help.

Login Method	Procedure
	<p>Note: If your organization uses the NTLM proxy, specify a domain\user name instead of only a user name for authentication. Instead of using the Native provider option in Eclipse, Fortify suggests that you use the Manual option and specify your data manually.</p>
<p>Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.</p>	<ol style="list-style-type: none"> a. Select Use Identity Provider. b. In the SSO Login URL box, type the URL provided by your Security Lead. c. To configure your network preferences, click Configure Network Connection, and then follow the instructions provided by Eclipse help. d. Provide your proxy information. <p>Note: For Linux platforms, you might need to provide your proxy information in the <code>eclipse.ini</code> file.</p> <ol style="list-style-type: none"> i. Add the following two lines at the end of the file: <ul style="list-style-type: none"> -Dnetwork.proxy_host=<proxyhost> -Dnetwork.proxy_port=<port> ii. Restart Eclipse. <p>For more information, see http://www.eclipse.org/swt/faq.php#browserproxy.</p>

3. Click **Next**.
4. If your tenant requires two-factor authentication, then do the following:
 - a. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**) and click **OK**.
 - b. After you obtain the security code delivered using the method you selected, type the code in the **Security Code** box and click **OK**.

The Fortify on Demand Plugin for Eclipse allows you three attempts to provide the security code. If necessary, click **Resend Code** to have a new security code sent to you.

Release Selection and Static Scan Setup (page 3 of 3)


1. Select the application and release for your upload package.

The screenshot shows the 'Release Selection and Static Scan Setup' dialog box. The title bar reads 'Fortify on Demand Upload'. The main heading is 'Release Selection and Static Scan Setup' with a sub-heading: 'Specify Entitlement Preference, Action for In-Progress Scan, Remediation Preference, and the Entitlement Purchase selection for this package'. A search box is present with the label 'Search:'. Below it is a table with columns: Application (Microservice), Release, Application Type, and Scan Status. The table contains three rows of data. Below the table are three dropdown menus for 'Entitlement Preference' (Single Scan Only), 'Action For In-Progress Scan' (Do not Start Scan), and 'Remediation Preference' (Remediation Scan if Available). There is a checkbox for 'Purchase Entitlements' and a checked checkbox for 'Upload in background'. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.


Application (Microservice)	Release	Application Type	Scan Status
abcProject	1.0	Web / Thick-Client	Not Started
abcProject	2.0	Web / Thick-Client	Completed
abcProjectXYZ	0.9	Web / Thick-Client	Not Started

If you have permission, you can create a new release for an existing application.

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box and press **Enter**. To clear the search results, clear the **Search** box, and then press **Enter**.

Note: To refresh the list of applications, click **Refresh** .

To create a new release for an existing application:

- a. Click **Create New Release** .
- The Create a Release dialog box opens.
- b. Select an application from the **Application** list.
- c. In the **Release Name** box, type a unique name for the release.
Valid characters include letters, digits, underscores, and spaces.
- d. (Optional) Type a description for the new release.
- e. From the **SDLC Status** list, select a Software Development Life Cycle stage.

- f. (Optional) From the **Microservice** list, select a microservice.
 - g. (Optional) Select **Copy State from Existing Release** to copy vulnerabilities and other details from a previous release to the new one, and then select the release that you want to copy from the list.
 - h. Click **OK**.
2. Select an **Entitlement Preference** from the list.
If multiple entitlements are available, the scan will use the oldest entitlement. If the release has an active subscription, the scan will use the active subscription.
 3. From the **Action for In-Progress Scan** list, select what should happen if the selected release scan status is **In Progress**.
You can choose to not start the scan, cancel the in-progress scan and start the new scan, or queue the new scan.
 4. From the **Remediation Preference** list, select whether to run a remediation scan.
 5. To purchase entitlements for this scan (if available), select the **Purchase Entitlements** check box.
 6. Select an assessment type from the **Assessment Type** list.

Note: Steps 6 through 9 (shown under **Static Scan Details**) are only applicable if the selected release does not have scan settings configured yet. The fields described in these steps are hidden if the scan settings are already configured.

Static Scan Details

999865 Unit(s) Available

Assessment Type: Static Assessment - Subscription (4 Units)

Technology Stack: JAVA/J2EE

Language Level: 11

Open Source Component Analysis

Autodetect

Advanced

To upload your project, you must select an assessment type that is less than or equal to the entitlements that you have available.

7. Specify the **Technology Stack** and the **Language Level**.
These fields display the values automatically detected for the selected Eclipse project. The **Autodetect** command can identify Java, C/C++, PYTHON, Ruby, and CFML projects. If you have previously used the Fortify on Demand Plugin for Eclipse, the technology stack and language level that you used previously are restored.

- If you want open source libraries identified in the analysis (and you have entitlements for this feature), select the **Open Source Component Analysis** check box.
The open source scan results include identified open source components and associated security issues.
- To specify additional advanced scanning and auditing preferences, click **Advanced**, and then make selections for the options described in the following table.

Option	Description
Audit Preference	This option is only available if enabled for your tenant. The audit preference settings are: <ul style="list-style-type: none">Manual—A security expert manually reviews the scan results and removes false positivesAutomated—False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review. This can reduce the turnaround time.
Include third-party libraries for static security assessment	Authorizes Fortify on Demand to assess the code for vulnerabilities to include in reports, vulnerability count, and risk rating. Selecting this option indicates that your organization has received consent from all third-party vendors to scan their libraries.

- To upload your package in the background, leave the **Upload in background** check box selected.

Note: Packaging the contents occurs in the foreground, but the upload is performed in the background.

- Click **Finish** to upload your code to Fortify on Demand.
Information about the IDE (name and version) used for this upload is saved and shown in the scan summary.

Reviewing Analysis Results

From the Eclipse IDE, you can open the Fortify on Demand analysis results for an application and release to remediate and audit.

This section contains the following topics:

Opening Analysis Results	17
Analysis Results in the Fortify on Demand Plugin for Eclipse	19

Reviewing Issues	21
Auditing Issues	23
Locating the Source Code Associated with Static Scan Issues	23
Closing Analysis Results	24

Opening Analysis Results

If you already have analysis results open, you can use this procedure to close the current analysis results and open the analysis results for a different application and release.

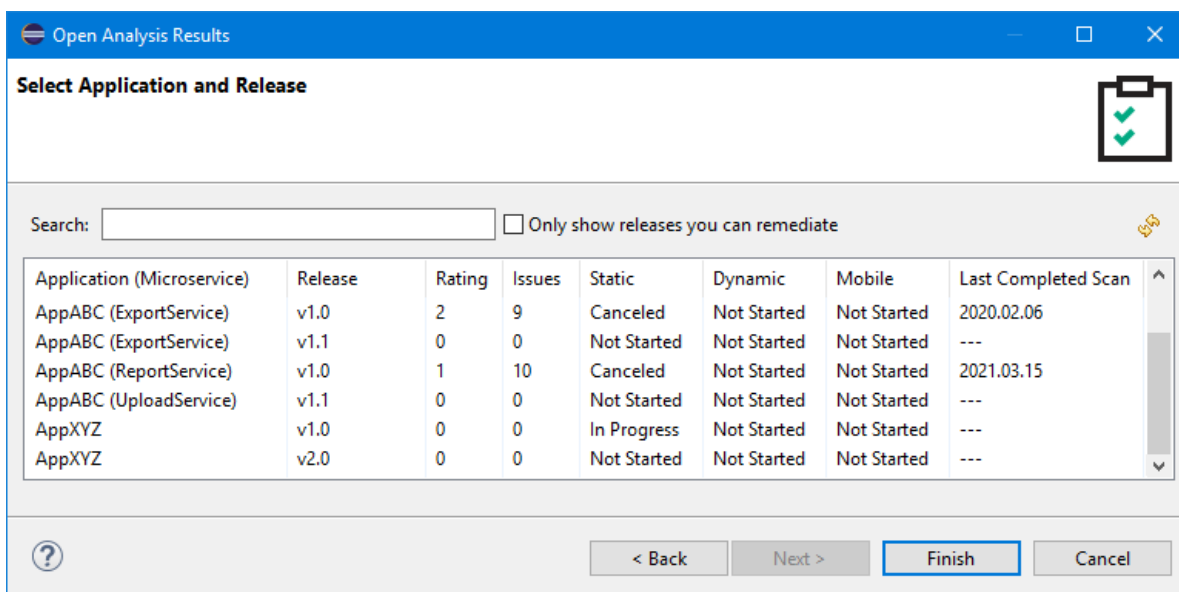
To open the analysis results:

1. In Eclipse, select **Fortify > Open Analysis Results**.
The Fortify on Demand Open Analysis Results wizard opens.
2. In the **API Root URL** box, type an API root URL.
For a list of data center API root URLs, see the *Fortify on Demand User Guide*.
3. Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none">a. Provide your Username, Password, and Tenant ID.b. To save your credentials, select the Remember Login Credentials check box. Note: For security reasons, the Fortify on Demand Plugin for Eclipse does not save your password.c. To configure your network preferences, click Configure Network Connection, and then follow the instructions provided by Eclipse help. Note: If your organization uses the NTLM proxy, specify a domain\user name instead of only a user name for authentication. Instead of using the Native provider option in Eclipse, Fortify suggests that you use the Manual option and specify your data manually.
Use Single Sign-On (SSO) for Fortify on Demand if your organization has	<ol style="list-style-type: none">a. Select Use Identity Provider.b. In the SSO Login URL box, type the URL provided by your Security Lead.c. To configure your network preferences, click Configure


Login Method	Procedure
configured SSO for its tenant.	<p>Network Connection, and then follow the instructions provided by Eclipse help.</p> <p>d. Provide your proxy information.</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p>Note: For Linux platforms, you might need to provide your proxy information in the <code>eclipse.ini</code> file.</p> <ul style="list-style-type: none"> i. Add the following two lines at the end of the file: <ul style="list-style-type: none"> -Dnetwork.proxy_host=<proxyhost> -Dnetwork.proxy_port=<port> ii. Restart Eclipse. <p>For more information, see http://www.eclipse.org/swt/faq.php#browserproxy.</p> </div>

4. Click **Next**.
5. If your tenant requires two-factor authentication, then do the following:
 - a. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**) and click **OK**.
 - b. After you obtain the security code delivered using the method you selected, type the code in the **Security Code** box and click **OK**.
 The Fortify on Demand Plugin for Eclipse allows you three attempts to provide the security code. If necessary, click **Resend Code** to have a new security code sent to you.
6. Select an application and release for the analysis results you want to open.



You can only open results for a release that has had at least one successfully completed scan. Clear the **Only show releases you can remediate** check box to see all applications and releases.

To quickly find an application and release, type the name or partial name of an application or release in the **Search** box and press **Enter**. The search is case-insensitive. To clear the search results, clear the **Search** box, and then press **Enter**.

Note: To refresh the list of applications, click **Refresh** .

7. Click **Finish**.

The analysis results are displayed in the Fortify perspective. See "[Analysis Results in the Fortify on Demand Plugin for Eclipse](#)" below for a description of this perspective.

Analysis Results in the Fortify on Demand Plugin for Eclipse

After the analysis results are opened, the Fortify perspective displays four audit-focused views. The **Analysis Results** view displays the results. The **Analysis Trace**, **Audit Summary**, and **Issue Summary** views are open, but do not contain any information until you select an issue from the **Analysis Results** view. You can also open audit-related views in other perspectives, such as the Java perspective or the C/C++ perspective, and rearrange the views. You might decide to use the audit views only, and stay within a customized development perspective.

Note: To open a Fortify view that is not currently visible, select **Fortify > Show View** and select the view you want to open.

The following table describes the Fortify perspective views.







View	Description
Analysis Results	<p>The Analysis Results view provides a way to group and select the issues to audit. This view also displays the relevant trace output for issues (see the following description of the Analysis Trace view).</p> <p>The color-coded tabs in the Analysis Results group the issues by severity level. The last tab contains all the issues. The Group By list options sort the issues into subfolders. The option you select is applied to all visible folders.</p> <p>Note: If you close this view, the analysis results are closed. To re-open analysis results, select Fortify > Open Analysis Results.</p>
Analysis Trace	<p>For Static Analysis Results—After you select an issue in the Analysis Results view, the Analysis Trace view displays the relevant trace output. This is a set of</p>















View	Description
	<p>program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this evidence is the path that the tainted data follows from the source function to the sink function. See the following descriptions of the analysis trace icons.</p> <p>For Dynamic Analysis Results—After you select an issue in the Analysis Results view, the Analysis Trace view displays details about the request parameters.</p> <p>This view also provides an abstract that briefly describes the issue.</p>
Audit Summary	<p>After you select an issue in the Analysis Results view, the Audit Summary view displays audit information for the selected issue. You can edit issue information, add comments, and review the audit history. For more information, see "Auditing Issues" on page 23.</p>
Issue Summary	<p>After you select an issue in the Analysis Results view, the Issue Summary view provides detailed information about the issue. The Details tab provides an abstract of the issue, a detailed explanation, and might also include examples with descriptive text and code samples, and the scan type (static, dynamic, or mobile). The Recommendations tab displays recommendations to remediate the issue, along with tips and references for additional research.</p>

The Eclipse text editor view is where the Eclipse plugin displays the source code (if available) for static scans or the request and response details for dynamic scans. The text editor opens after you select an issue in the **Analysis Results** view.

Analysis Trace Icons

The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced


Icon	Description	Icon	Description
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution
	Passthrough, tainted data passes from one place to another <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y. The x and y values are one of the following:</p> <ul style="list-style-type: none"> • An argument index • <code>return</code>—The return value of a function • <code>this</code>—The instance of the current object • A specific object field or key </div>		A branch is not taken in the code execution
	An alias is created for a memory location		Generic
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

Reviewing Issues

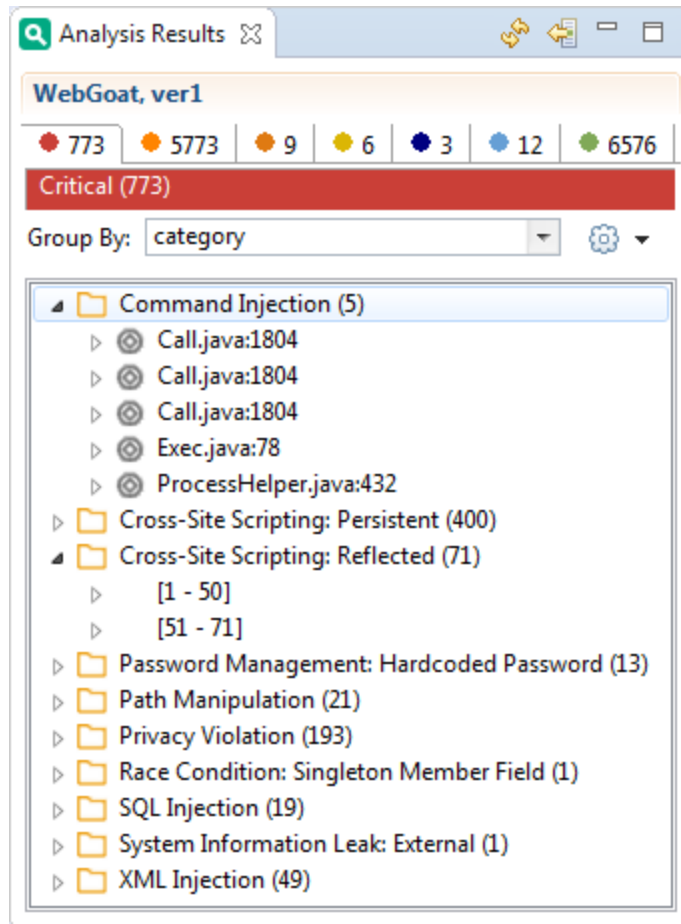
To view and select issues:

1. From the **Group By** list, select a value to use to sort issues in all visible folders into groups. The default grouping is **category**.
2. Click a colored tab to view the associated issues.

The issue type subfolders listed on each folder (tab) are based on the selected **Group By** value.


3. To show suppressed or fixed issues, click **Filter** .
4. To view the list of issues in a subfolder, expand the subfolder.

The Fortify on Demand Plugin for Eclipse retrieves the corresponding issues from Fortify on Demand.



Notes:

- If a folder contains more than 50 issues, the issues are grouped into subfolders in blocks of 50 with folder names that indicate which issues are included. For example, if a folder contains 71 issues, the first 50 issues are in a subfolder labeled **[1-50]** and the next set of issues are in a subfolder labeled **[51-71]**.
- Multiple trace paths for a single issue are shown in separate **Trace <num>** subfolders.

5. To see any updates to the analysis results made on Fortify on Demand, click **Refresh** .
6. Select an issue.

The **Analysis Trace**, **Audit Summary**, and **Issue Summary** views display information about the selected issue.

Auditing Issues

If you have the Edit Issues permission, you can assign a user, set the developer status, and add comments for issues in the **Audit Summary** view. If you have the Audit Issues permission, you can also edit the issue's auditor status and severity.

To audit an issue:

1. Make sure that the **Audit Summary** view is open.
2. From the issues list in the **Analysis Results**, select an issue.
You can select multiple issues in the **Analysis Results** view to make the same edits to multiple issues.
3. In the **Audit Summary** view, select the user to assign to the issue from **User** list.
4. To change the issue's development status, select the status from the **DeveloperStatus** list
5. To change the auditor status, select the status from the **AuditorStatus** list.
6. To change the issue severity, select an issue severity from the **Severity** list.
7. To add a comment for the issue, type your comment in the box at the bottom of the **Comments** area, and then click **Add Comment**.

Your comment is displayed in the **Comments** section.

The Fortify on Demand Plugin for Eclipse saves your changes for the Fortify on Demand application and release.

Locating the Source Code Associated with Static Scan Issues

You can use the Fortify on Demand Plugin for Eclipse to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the Fortify on Demand Plugin for Eclipse:

1. Select an issue in the **Analysis Results** view or select a line in the **Analysis Trace** view.
2. If the source code is not available in the analysis results opened from Fortify on Demand, do the following:



- a. In the Text Editor, click **Set Source Path**.
- b. In the Set Source Path dialog box, click **Browse**.

- c. Select the location of the folder that contains the source code, and then click **OK**.
- d. Click **OK** to close the Set Source Path dialog box.

Eclipse highlights the line of code associated with the issue.

Note: If the source code shown is a downloaded copy from Fortify on Demand, the file name is prepended with `Remote<yyyy-mm-dd>` - where the `<yyyy-mm-dd>` is the date the file was last scanned. The downloaded copy is not writable.

Closing Analysis Results

To close the analysis results for an application and release:

- In the **Analysis Results** view, click **Logout** .

The analysis results are closed and you are logged out of Fortify on Demand.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at <https://www.microfocus.com/support> so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify on Demand Plugin for Eclipse 23.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@microfocus.com.

We appreciate your feedback!