

OpenText™ Fortify on Demand Plugin for IntelliJ IDEA

Software Version: 23.1

User Guide

Document Release Date: March 2023

Software Release Date: March 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2017-2023 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 November 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 IntelliJ IDEA 5
 - Installing the Fortify on Demand Plugin for IntelliJ IDEA 6
 - Configuring the Fortify on Demand Plugin for IntelliJ IDEA 6

- Uploading Code to Fortify on Demand 8

- Reviewing Analysis Results 15
 - Opening Analysis Results 15
 - Analysis Results in the Fortify on Demand Plugin for IntelliJ IDEA 17
 - Analysis Trace Icons 18
 - Reviewing Issues 19
 - Auditing Issues 20
 - Locating the Source Code Associated with Static Scan Issues 21

- Send Documentation Feedback 22

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 IntelliJ IDEA and use it to upload code for static analysis to OpenText™ Fortify on Demand and open analysis results for remediation. This plugin works with Android Studio and other JetBrains IDEs as listed in the JetBrains Marketplace. The procedures in this guide reference the IntelliJ IDEA interface and the instructions might be slightly different for the other IDEs.

This section contains the following topics:

Requirements for Using the Fortify on Demand Plugin for IntelliJ IDEA	5
Installing the Fortify on Demand Plugin for IntelliJ IDEA	6
Configuring the Fortify on Demand Plugin for IntelliJ IDEA	6

Requirements for Using the Fortify on Demand Plugin for IntelliJ IDEA

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

- Your OpenText™ Fortify on Demand login credentials or your SSO login URL if your organization has configured SSO for the tenant
- An API root URL.

For a list of data center API root URLs, see the *OpenText™ Fortify on Demand User Guide*.

- 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 IntelliJ IDEA automatically package all the necessary dependencies and source code (including files required for a Debricked open source scan), you must have a locally installed OpenText™ Fortify ScanCentral SAST client version 22.1.2 or later and Fortify on Demand Plugin for IntelliJ IDEA version 23.1 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 IntelliJ IDEA

To install the IntelliJ plugin:

1. From the IDE, open the Settings dialog box as follows:
 - On Windows or Linux, select **File > Settings**.
 - On macOS, select **<IDE_name> > Preferences**.
2. In the left pane, select **Plugins**.
3. Select the **Marketplace** tab, and then in the search box type Fortify on Demand.
4. Click **Install**.
5. Click **OK**.

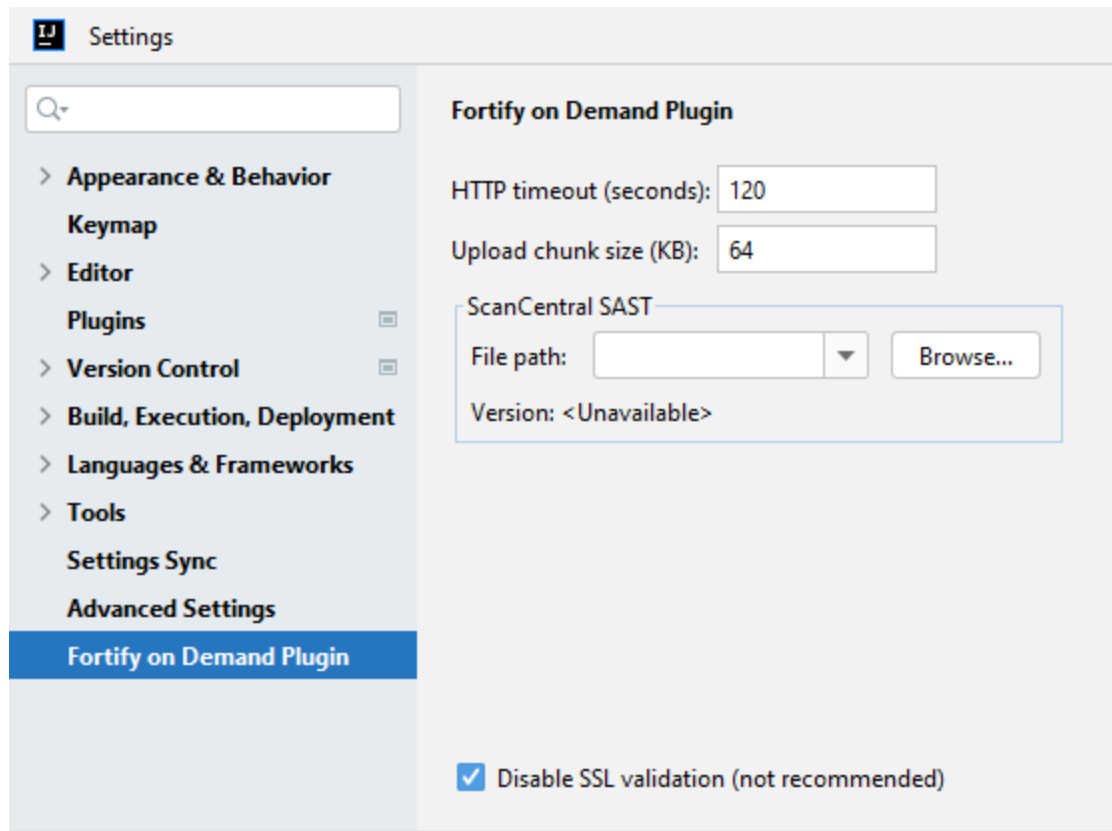
The **Tools** menu now includes the **Fortify on Demand** commands.

Configuring the Fortify on Demand Plugin for IntelliJ IDEA

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

To configure the IntelliJ plugin options:

1. From the IDE, select **Tools > Fortify on Demand > Options**.



2. To change the amount of time to wait when 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).
3. To change the size of individual pieces that are 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.
4. If you are using 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.
You can download the Fortify ScanCentral SAST client from the Tools page. For installation instructions, see the README.txt file included in the downloaded ZIP.
After you specify the path to the Fortify ScanCentral SAST client, its version is displayed.
5. To enable the plugin 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.

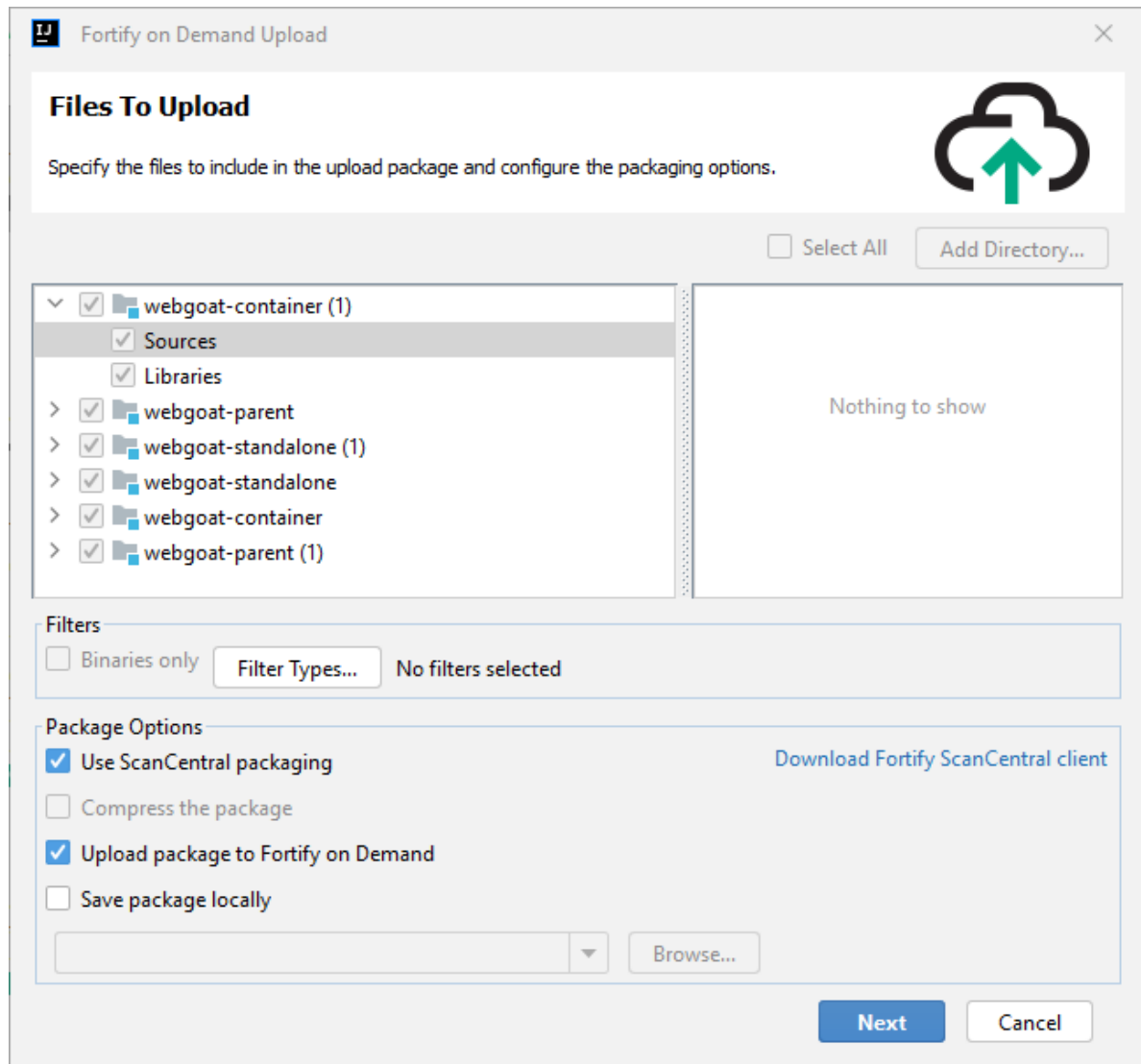
- A project open in IntelliJ IDEA or Android Studio
- To include a Debricked open source scan for this solution and automatically package the project with all the required files, verify that you have the following:
 - Fortify ScanCentral SAST client version 22.1.2 or later
 - Fortify on Demand Plugin for IntelliJ IDEA 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 *OpenText™ 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 Plugin for IntelliJ IDEA:

1. From the IDE, select **Tools > Fortify on Demand > Upload project**.
The Fortify on Demand Upload wizard opens.

Files to Upload



The left pane displays all the open modules.

2. To automatically package the project with Fortify ScanCentral SAST client, select **Use ScanCentral packaging**.

Fortify ScanCentral client can automatically package all the necessary dependencies and source code required for the scan. To use this feature, you must have a locally installed Fortify ScanCentral SAST client and specify the installation location in the plugin configuration (see "[Configuring the Fortify on Demand Plugin for IntelliJ IDEA](#)" on page 6).

To download the Fortify ScanCentral SAST client:

- a. Click **Download Fortify ScanCentral client**.
- b. Log in to Fortify on Demand and download the ScanCentral Client utility from the Tools page.

For instructions on how to install the Fortify ScanCentral SAST client, see the README.txt file included in the downloaded ZIP.

3. To manually select all the files you want to upload (without using the Fortify ScanCentral SAST client):

- a. Clear the **Use ScanCentral packaging** check box.
- b. Select the files you want to upload.

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

File Upload Refinement	Procedure
Omit specific modules.	<ul style="list-style-type: none"> • In the left pane, clear the check box for the module you want to exclude from your upload package.
Omit specific files located in a module listed in the left pane.	<ol style="list-style-type: none"> a. Select a folder in the left pane. b. In the right pane, 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. Click OK.
Upload additional external resources.	<ol style="list-style-type: none"> a. Click Add Directory. b. In the Browse for Folder dialog box, navigate to and select the resources to upload, and then click Open. After you add a folder, you can select specific files within it. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Notes:</p> <ul style="list-style-type: none"> ◦ Subfolders are included. ◦ Folders with native Unicode symbols in the name are not supported. </div>

4. To upload the package to Fortify on Demand, leave the **Upload package to Fortify on Demand** check box selected.

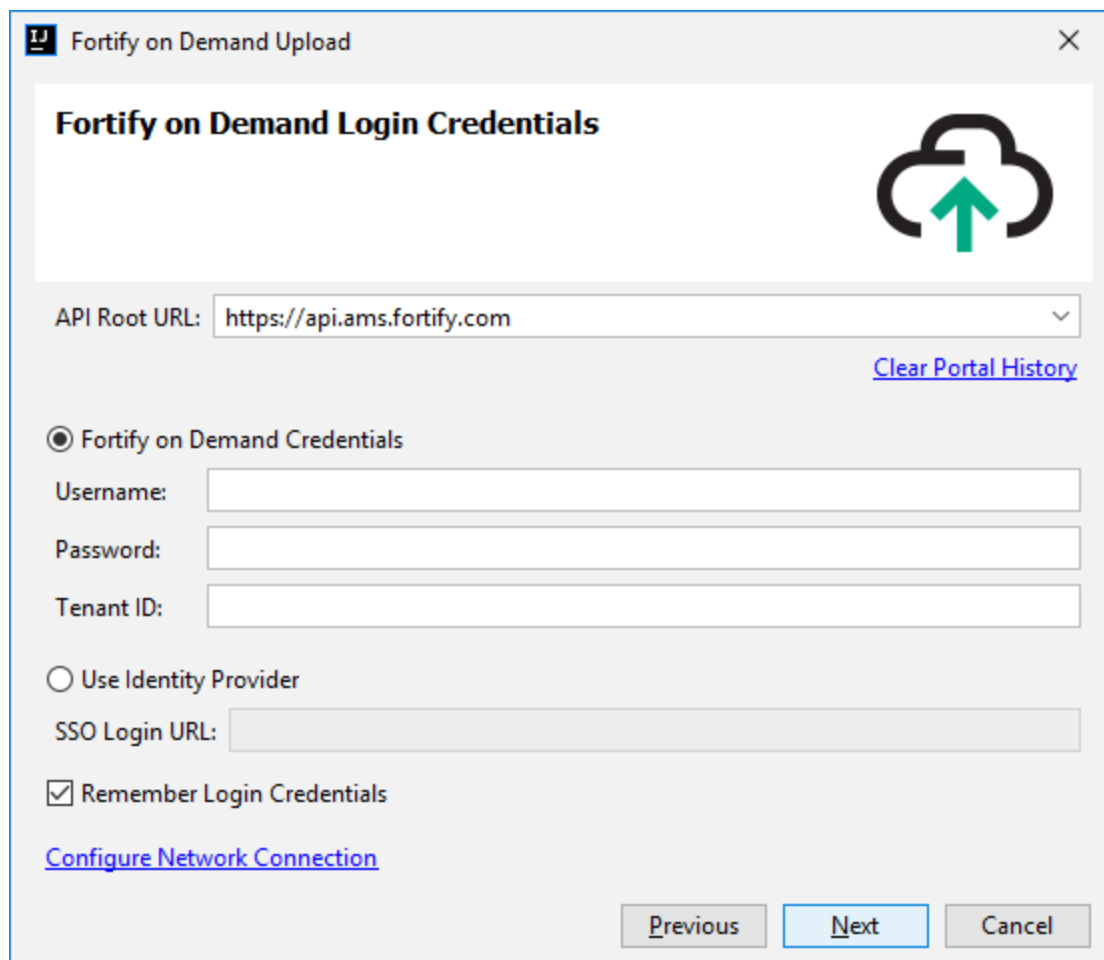
5. To save the package to a local directory:

- a. Select the **Save package locally** check box.
- b. Click **Browse**, and then navigate to a folder where you want to save the package.
- c. Type a name for the package, and then click **Save**.

6. To reduce the package size, select the **Compress the package** check box.
Although this reduces the size of the package to be uploaded, the packaging process takes longer.
7. Do one of the following:
 - If are saving the package locally without uploading it to Fortify on Demand, click **Finish**.
A package (ZIP) is created in the location you specified.
 - 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

If you have already logged in to Fortify on Demand, then the next step is to select an application and release (see "[Release Selection and Static Scan Setup](#)" on page 13).



The screenshot shows a dialog box titled "Fortify on Demand Upload" with a close button (X) in the top right corner. The main heading is "Fortify on Demand Login Credentials" next to a logo consisting of a black cloud with a green arrow pointing upwards. Below the heading is a text field for "API Root URL" containing "https://api.ams.fortify.com" and a dropdown arrow. To the right of this field is a blue link "Clear Portal History". There are two radio button options: "Fortify on Demand Credentials" (which is selected) and "Use Identity Provider". Under "Fortify on Demand Credentials" are three text input fields for "Username:", "Password:", and "Tenant ID:". Under "Use Identity Provider" is a text input field for "SSO Login URL:". There is a checked checkbox for "Remember Login Credentials". At the bottom left is a blue link "Configure Network Connection". At the bottom right are three buttons: "Previous", "Next" (highlighted in light blue), and "Cancel".

1. In the **API Root URL** box, type the API root URL.
2. Provide your login credentials. Use one of the two methods described in the following table.

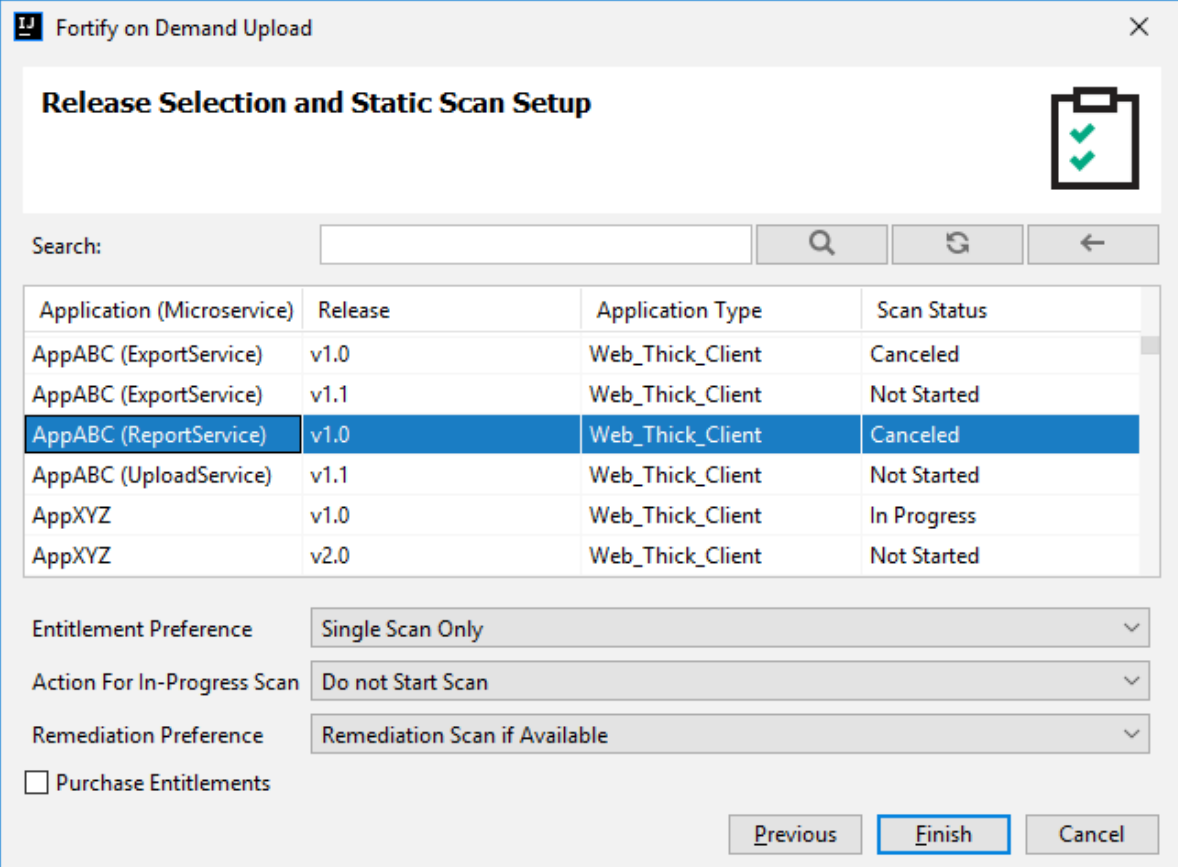
Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none">a. Provide your Username, Password, and Tenant ID.b. To save your credentials, select the Remember Login Credentials check box. <div data-bbox="808 590 1401 690" style="background-color: #f0f0f0; padding: 5px;">Note: For security reasons, the plugin does not save your password.</div>c. To configure your proxy network preferences, click Configure Network Connection, and then follow the instructions provided by the IDE help.
Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.	<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.

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. Obtain the security code delivered using the method you selected.
 - c. Enter the code in the **Security Code** box, and then click **OK**.

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

Release Selection and Static Scan Setup

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



The screenshot shows the 'Fortify on Demand Upload' dialog box with the 'Release Selection and Static Scan Setup' tab selected. The dialog features a search box, a table of applications and releases, and configuration options for entitlements, scan actions, and remediation. The table below is a representation of the data shown in the screenshot.


Application (Microservice)	Release	Application Type	Scan Status
AppABC (ExportService)	v1.0	Web_Thick_Client	Canceled
AppABC (ExportService)	v1.1	Web_Thick_Client	Not Started
AppABC (ReportService)	v1.0	Web_Thick_Client	Canceled
AppABC (UploadService)	v1.1	Web_Thick_Client	Not Started
AppXYZ	v1.0	Web_Thick_Client	In Progress
AppXYZ	v2.0	Web_Thick_Client	Not Started

Configuration options shown in the dialog:

- Entitlement Preference: Single Scan Only
- Action For In-Progress Scan: Do not Start Scan
- Remediation Preference: Remediation Scan if Available
- Purchase Entitlements

Buttons at the bottom: Previous, Finish, Cancel.

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

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

66 Unit(s) Available

Assessment Type: Static Assessment - Subscription (4 Units)

Technology Stack: JAVA/J2EE

Language Level: 17

Open Source Component Analysis

Audit Preference: Manual

Include third-party libraries for static security assessment (will lead to longer turnaround times)

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**.
8. 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.

9. To specify additional advanced scanning and auditing preferences, 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 positives.• Automated—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	Authorizes Fortify on Demand to assess the code for vulnerabilities to

Option	Description
libraries for static security assessment	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.

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

This section contains the following topics:

Opening Analysis Results	15
Analysis Results in the Fortify on Demand Plugin for IntelliJ IDEA	17
Reviewing Issues	19
Auditing Issues	20
Locating the Source Code Associated with Static Scan Issues	21

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 from Fortify on Demand:

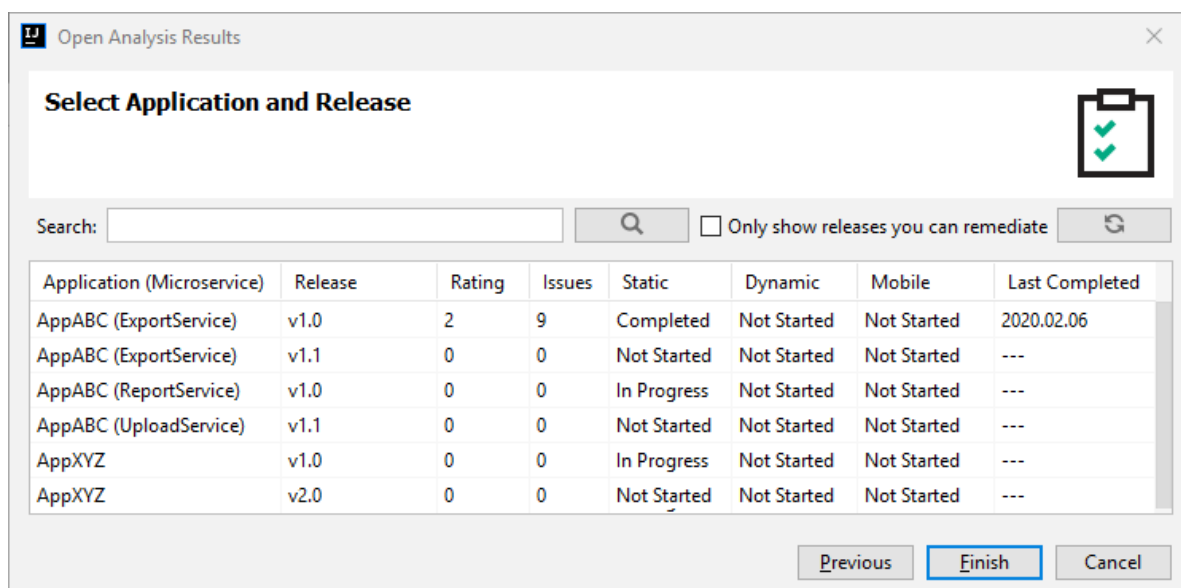
- From the IDE, select **Tools > Fortify on Demand > Open Analysis Results**.
The Fortify on Demand Open Analysis Results wizard opens.
 - In the **API Root URL** box, type the API root URL.
 - Provide your login credentials. Use one of the two methods described in the following table.

Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none">Provide your Username, Password, and Tenant ID.

Login Method	Procedure
	ii. To save your credentials, select the Remember Login Credentials check box. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> Note: For security reasons, the plugin does not save your password. </div> iii. To configure your proxy network preferences, click Configure Network Connection , and then follow the instructions provided by the IDE help.
Use Single Sign-On (SSO) for Fortify on Demand if your organization has configured SSO for its tenant.	i. Select Use Identity Provider . ii. In the SSO Login URL box, type the URL provided by your Security Lead.


- c. Click **Next**.
- d. If your tenant requires two-factor authentication, then do the following:
 - i. In the Two-Step Verification dialog box, select a delivery method for the security code (**SMS** or **Email**), and click **OK**.
 - ii. Obtain the security code delivered using the method you selected.
 - iii. Enter the code in the **Security Code** box, and then click **OK**.

The Fortify on Demand Plugin for IntelliJ IDEA allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.
- 2. Select an application and release for the analysis results you want to open.



You can only open results for an application and 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 then 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** .

3. Click **Finish**.

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

Analysis Results in the Fortify on Demand Plugin for IntelliJ IDEA

After the analysis results are opened, the Fortify on Demand Plugin for IntelliJ IDEA displays four audit-focused windows. The **Analysis Results** window displays the results. The **Analysis Trace**, **Audit Summary**, and **Issue Summary** windows are visible, but do not contain any information until you select an issue from the **Analysis Results** window.

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

The following table describes the Fortify windows.











View	Description
Analysis Results	<p>The Analysis Results window 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 window).</p> <p>The color-coded tabs in the Analysis Results group the issues by severity level. The last tab contains all issues. The Group By list options sort the issues into subfolders. The option you select is applied to all visible folders.</p>
Analysis Trace	<p>For Static Analysis Results—After you select an issue in the Analysis Results window, the Analysis Trace window displays the relevant trace output. This is a set of 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>











View	Description
	<p>For Dynamic Analysis Results—After you select an issue in the Analysis Results window, the Analysis Trace window displays details about the request parameters.</p> <p>This window 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 20.</p>
Issue Summary	<p>After you select an issue in the Analysis Results window, the Issue Summary window 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).</p> <p>The Recommendations tab displays recommendations to remediate the issue, along with tips and references for additional research.</p>

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

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
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps

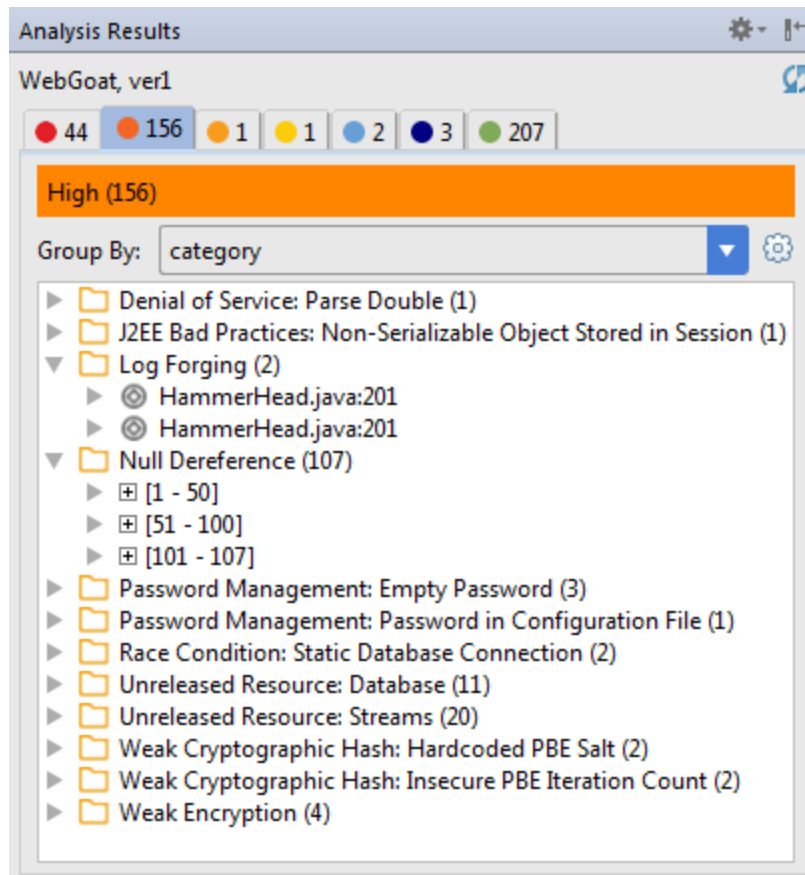
Icon	Description	Icon	Description
	The function call returns tainted data		A branch is taken in the code execution
	Passthrough, tainted data passes from one place to another Note: This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y. The x and y values are one of the following: <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 		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 are based on the selected **Group By** value.
3. To show suppressed or fixed issues, click **Set visibility options** .
4. To view the list of issues in a subfolder, expand the subfolder.

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



Note: 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]**.

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** windows 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 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 IntelliJ IDEA 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 IntelliJ IDEA to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the plugin:

- Select an issue in the **Analysis Results** window or select a line in the **Analysis Trace** window.

If the issue is located in source code available in the current project, Fortify on Demand Plugin for IntelliJ IDEA opens the relevant file in the Editor. Otherwise, the plugin attempts to download the source code from Fortify on Demand and if the relevant file is available, it is opened in the Editor.

Note: If the file was downloaded, the file name is prepended with `Remote<yyyy-mm-dd>-` where the `<yyyy-mm-dd>` is the date the file was last scanned.

The Fortify on Demand Plugin for IntelliJ IDEA highlights the line of code associated with the issue.

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 IntelliJ IDEA 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@opentext.com.

We appreciate your feedback!