

OpenText™ Fortify on Demand Extension for Visual Studio

Software Version: 22.2

User Guide

Document Release Date: December 2022

Software Release Date: December 2022

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 Extension for Visual Studio 5
 - Installing the Fortify on Demand Extension for Visual Studio 6
 - Configuring the Fortify on Demand Extension for Visual Studio 6

- Uploading Code to Fortify on Demand 8

- Reviewing Analysis Results 13
 - Opening Analysis Results 13
 - Analysis Results 15
 - Analysis Trace Icons 17
 - Reviewing Issues 18
 - Auditing Issues 19
 - Locating the Source Code Associated with Static Scan Issues 20
 - Logging Out 21
 - Locating the Log Files 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 Extension for Visual Studio and use it to upload code to OpenText™ Fortify on Demand for static analysis and open analysis results for remediation.

This section contains the following topics:

Requirements for Using the Fortify on Demand Extension for Visual Studio	5
Installing the Fortify on Demand Extension for Visual Studio	6
Configuring the Fortify on Demand Extension for Visual Studio	6

Requirements for Using the Fortify on Demand Extension for Visual Studio

To use the Fortify on Demand Extension for Visual Studio, you must have the following:

- An API root URL.
For a list of data center API root URLs, see the *OpenText™ 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 Extension for Visual Studio 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 Extension for Visual Studio version 22.2 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.

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.

Installing the Fortify on Demand Extension for Visual Studio

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Fortify on Demand Extension for Visual Studio:

1. In Visual Studio, access the dialog box to manage extensions.
2. Search the Visual Studio Marketplace for Fortify on Demand.
3. Download and install the Fortify on Demand Extension for Visual Studio.

Note: To install this extension as an administrator and allow all users to use the extension, download the VSIX file from the Visual Studio Marketplace and then install it using VSIXInstaller with the `/admin` option from the Command Prompt.

Configuring the Fortify on Demand Extension for Visual Studio

You can configure how the Fortify on Demand Extension for Visual Studio connects to Fortify on Demand and specify the location of the Fortify ScanCentral client executable.

To configure the Visual Studio extension:

1. From the Visual Studio Fortify extension menu, select **Options**.

The screenshot shows the 'Fortify on Demand Options' dialog box. It features a blue title bar with the text 'Fortify on Demand Options' and a close button. The main content area is divided into several sections. At the top, there is a 'Default API Root URL' section with a text box containing 'https://api.ams.fortify.com' and a 'Clear Portal History' link. Below this are two checkboxes: 'Disable SSL Validation' and 'Use Proxy'. The 'Proxy Configuration' section includes 'Proxy URL' and 'Proxy Port' text boxes, and a 'Proxy Authentication' checkbox with 'Proxy Username' and 'Proxy Password' text boxes. The 'ScanCentral SAST' section has a 'File Path' text box with a browse button and 'Version: Unavailable' text. At the bottom are 'OK' and 'Cancel' buttons.

2. In the **Default API Root URL** box, enter the API root URL.
3. To allow the extension to accept any server certificate, select the **Disable SSL Validation** check box.

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

4. If you require a proxy server (and you have not yet configured a proxy in the Windows Internet options),
select **Use Proxy**, and then follow these steps:
 - a. In the **Proxy URL** box, type the URL for your proxy server.
 - b. In the **Proxy Port** box, type the port for the proxy server.
 - c. If you require authentication for your proxy server, select **Proxy Authentication** and provide the authentication credentials.
5. 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. 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.

Note: If you do not specify the location of the Fortify ScanCentral client in the configuration options, then the first time you upload your project to Fortify on Demand using ScanCentral packaging, you are prompted to specify the location.

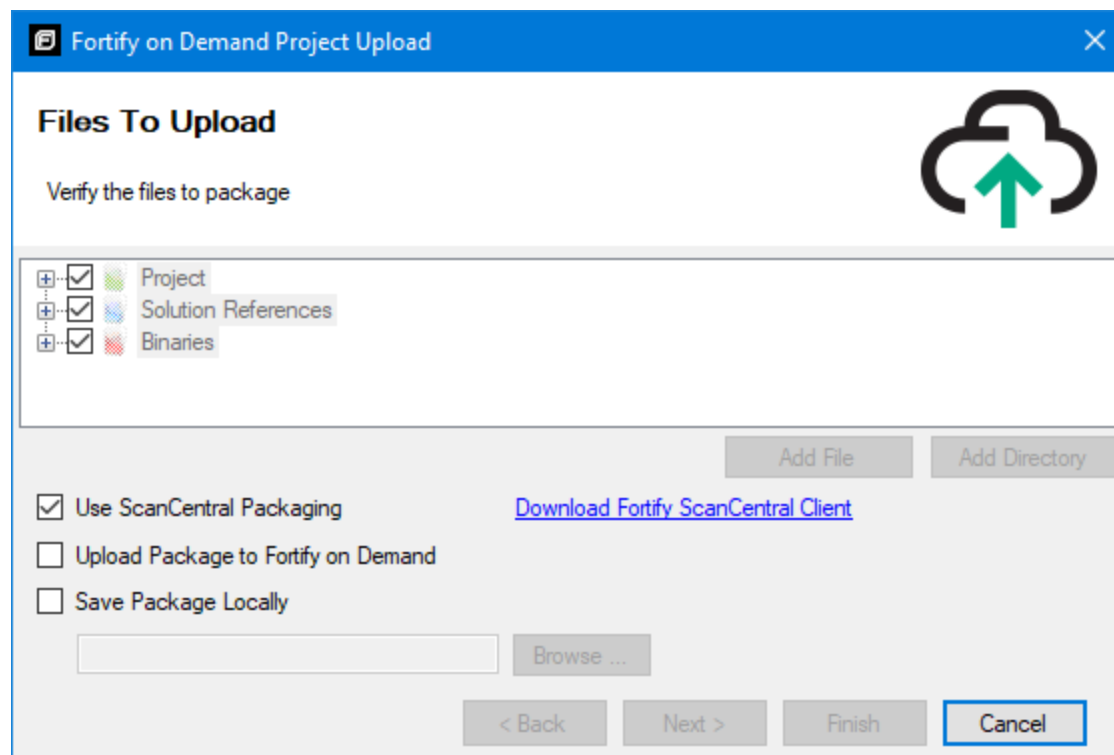
6. Click **OK**.

Uploading Code to Fortify on Demand

To upload source code to Fortify on Demand from Visual Studio:

1. From the Fortify on Demand extension menu, select **Upload Projects to Fortify on Demand**. The Fortify on Demand Project Upload wizard opens.

Files to Upload



2. Select all 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.

- a. (Optional) To include a file that is not listed, click **Add File**, and then browse to and select a file to add to your package.

The wizard now displays an **Extra Files** node and shows the full path to the file you added.

- b. (Optional) To include a directory that is not listed, click **Add Directory**, and then browse to and select the directory to add to your package.

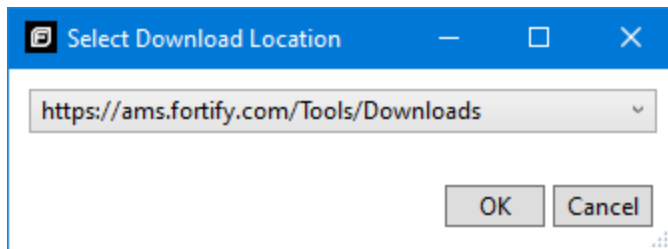
The wizard now displays an **Extra Directories** node and shows the directory you added.

3. 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.

To download the Fortify ScanCentral SAST client:

- a. Click **Download Fortify ScanCentral Client**.



- b. Select a location from which to download the Fortify ScanCentral SAST client, and then click **OK**.
 - c. 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.
4. To upload the package to Fortify on Demand, select the **Upload Package to Fortify on Demand** check box.
 5. To save the package to a local directory:
 - a. Select the **Save Package Locally** check box, click **Browse**, and then navigate to a folder where you want to save the package.
 - b. Click **Save**.
 6. Click **Next**.

If you selected **Use ScanCentral Packaging** and you have not configured the location of the Fortify ScanCentral SAST client executable, do the following:

- a. In the Select Fortify ScanCentral executable dialog, navigate to the Fortify ScanCentral client executable file.
 - b. Click **Open**.
7. If you did not select the **Upload Package Fortify on Demand** check box, the package is only saved locally. Click **Finish**.

Enter FoD Login Credentials

If you selected to upload the package, the **Enter FoD Login Credentials** page is displayed. 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 the next page).

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.

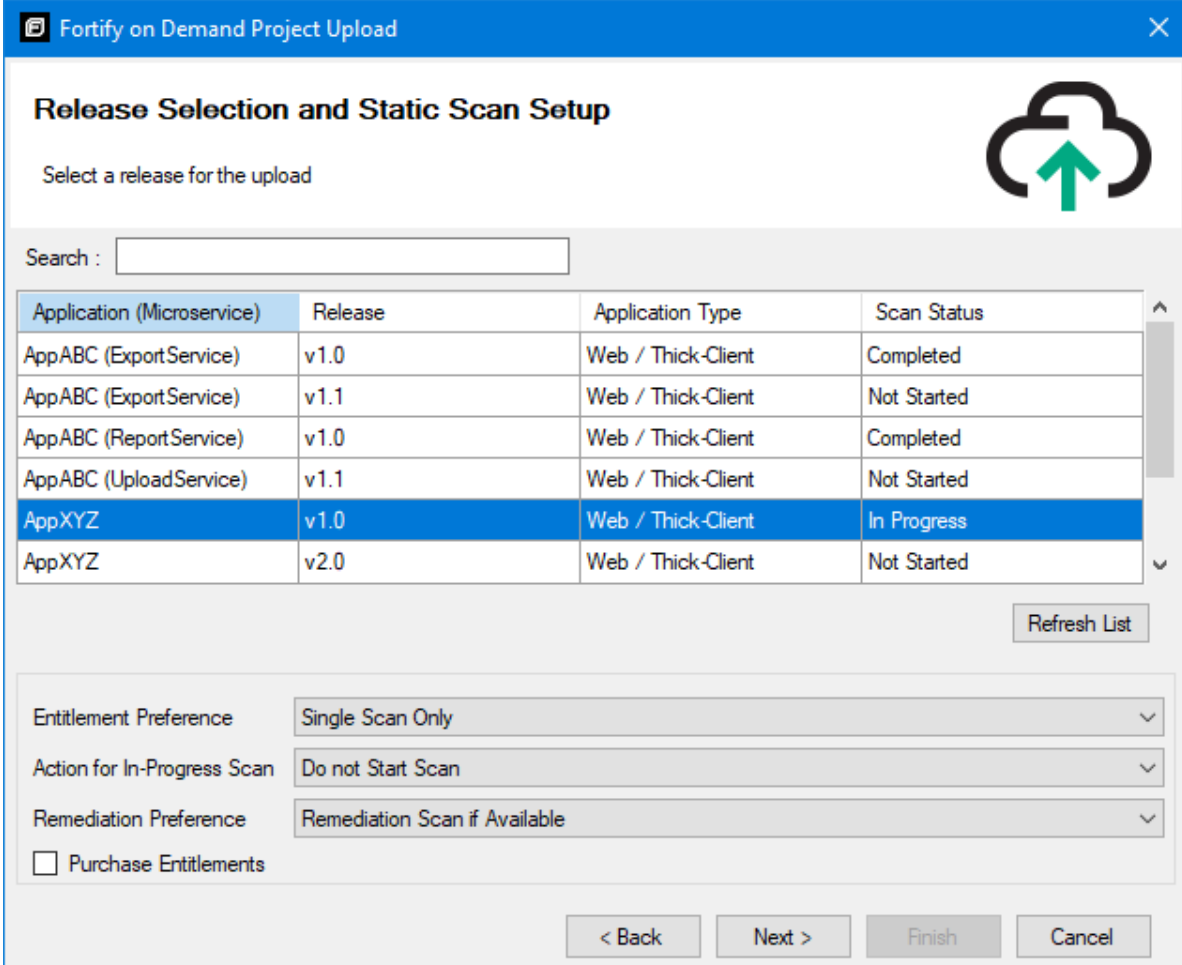
Login Method	Procedure
Provide your Fortify on Demand credentials.	<ol style="list-style-type: none">a. Provide your Username, Password, and Tenant ID.b. To save your credentials, select the Remember Login Credentials check box. <div data-bbox="886 695 1401 837" style="background-color: #f0f0f0; padding: 5px;">Note: For security reasons, the Fortify on Demand Extension for Visual Studio does not save your password.</div>c. To configure your network preferences, click Connection Settings.
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.c. To configure your network preferences, click Connection Settings.

3. Click **Next.**
4. If your tenant requires two-factor authentication, then do the following:
 - a. 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 Extension for Visual Studio 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 to which you want to upload.



The screenshot shows a dialog box titled "Fortify on Demand Project Upload" with a close button (X) in the top right corner. The main heading is "Release Selection and Static Scan Setup". Below the heading is the instruction "Select a release for the upload" and a cloud icon with a green arrow pointing up. A search box is labeled "Search :". Below the search box is a table with the following data:

Application (Microservice)	Release	Application Type	Scan Status
AppABC (ExportService)	v1.0	Web / Thick-Client	Completed
AppABC (ExportService)	v1.1	Web / Thick-Client	Not Started
AppABC (ReportService)	v1.0	Web / Thick-Client	Completed
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

Below the table is a "Refresh List" button. Underneath are three dropdown menus: "Entitlement Preference" (set to "Single Scan Only"), "Action for In-Progress Scan" (set to "Do not Start Scan"), and "Remediation Preference" (set to "Remediation Scan if Available"). There is also a checkbox for "Purchase Entitlements" which is currently unchecked. At the bottom are four buttons: "< Back", "Next >", "Finish", and "Cancel".

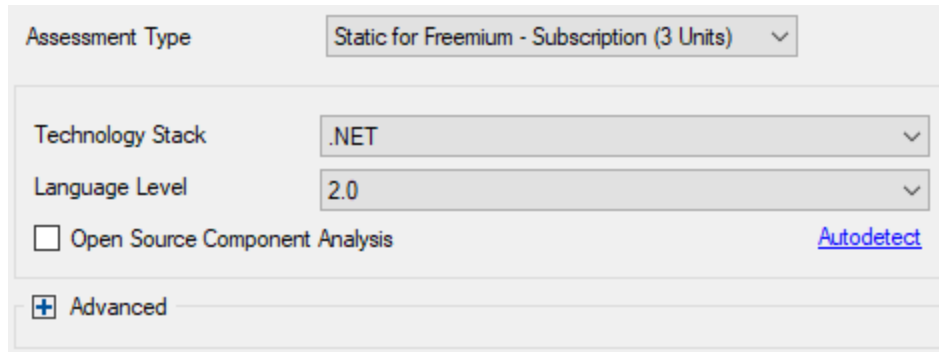
To quickly find an application and release, type the name or partial name of an application or release in the **Search** box. The search is case-sensitive. To clear the search results, clear the **Search** box.

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

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 the appropriate assessment type from the **Assessment Type** list.

Note: Steps 6 through 9 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.



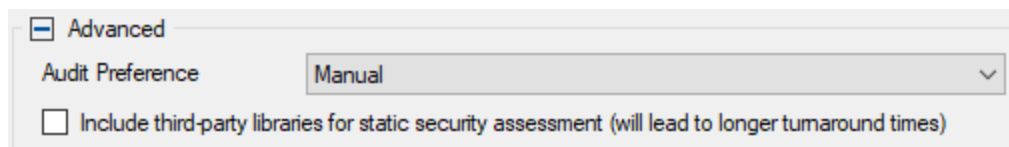
7. Specify the **Technology Stack** and the **Language Level**.

Alternatively, you can click **Autodetect** and the technology stack and language level fields are automatically populated.

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, click **Advanced**.



Make selections for the options described in the following table.

Option	Description
Audit Preference	<p>This option is only available if enabled for your tenant.</p> <p>The audit preference settings are:</p> <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.

Option	Description
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.

10. Click **Next**.
A status bar shows your upload progress.
11. After the upload is complete, click **Finish**.
Information about the IDE (name and version) used for this upload is saved and shown in the scan summary.

Reviewing Analysis Results

From Visual Studio, 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	13
Analysis Results	15
Reviewing Issues	18
Auditing Issues	19
Locating the Source Code Associated with Static Scan Issues	20
Logging Out	21
Locating the Log Files	21

Opening Analysis Results

From Visual Studio, you can open Fortify on Demand analysis results for an application and release to remediate and audit. 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 the Fortify on Demand extension menu, select **Open Analysis Results**.
The Fortify on Demand Open Analysis Results wizard opens.

Enter FoD Login Credentials

Note: If you have already logged in to Fortify on Demand, then the next step is to select an application and release (see "[Select a Release](#)" on the next page).

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="886 737 1401 879" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">Note: For security reasons, the Fortify on Demand Extension for Visual Studio does not save your password.</div>c. To configure your network preferences, click Connection Settings.
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.c. To configure your network preferences, click Connection Settings.

3. Click **Next.**
4. If your tenant requires two-factor authentication, then do the following:
 - a. 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 Extension for Visual Studio allows you three attempts to enter the security code. If necessary, click **Resend Code** to have a new security code sent to you.

Select a Release

1. Select an application and release for the analysis results you want to open.

Application (Microservice)	Release	Rating	Issues	Static	Dynamic	Mobile	Last Completed Scan
AppABC (ExportService)	v1.0	2	9	Completed	Not Started	Not Started	2020.02.06
AppABC (ReportService)	v1.0	1	11	Completed	Not Started	Not Started	2021.03.15

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. The search is case-sensitive. To clear the search results, clear the **Search** box.

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

2. Click **Finish**.

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

Analysis Results

After the analysis results are opened, the Fortify on Demand Extension for Visual Studio displays four audit-focused windows. The **Analysis Results** window displays the results. The **Analysis Trace, Issue Summary**, and **Audit Summary** windows are open, 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 **Show Windows** from the Fortify extension menu and select the window you want to open.

The following table describes the Fortify windows.

Window	Description
Analysis Results	<p>The Analysis Results window provides a way to group and select the issues to audit.</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> <p>Note: If you close this window, the analysis results are closed. To re-open analysis results, select Open Analysis Results from the Fortify extension menu.</p>
Analysis Trace	<p>The content of this window depends on the scan type:</p> <ul style="list-style-type: none">• 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.• Dynamic Analysis Results—After you select an issue in the Analysis Results view, the Analysis Trace view displays details about the request parameters. <p>This window also provides an abstract that briefly describes the issue.</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. The Recommendations tab displays recommendations to remediate the issue, along with tips and references for further research.</p>

Window	Description
Audit Summary	<p>After you select an issue in the Analysis Results window, the Audit Summary window displays audit information for the selected issue and you can edit the issue, add comments, and review the audit history. For more information, see "Auditing Issues" on page 19.</p>

The text editor window is where the Visual Studio extension 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** 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

Icon	Description	Icon	Description
	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;"> <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

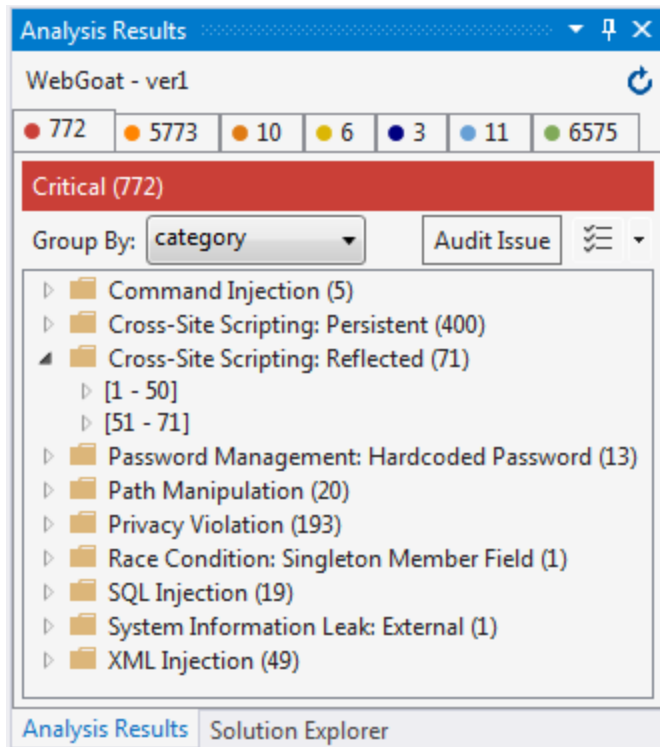
Reviewing Issues

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 the icon.

4. To view the list of issues in a subfolder, expand the subfolder.

The Fortify on Demand Extension for Visual Studio 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**, **Issue Summary**, and **Audit Summary** windows display information about the selected issue.

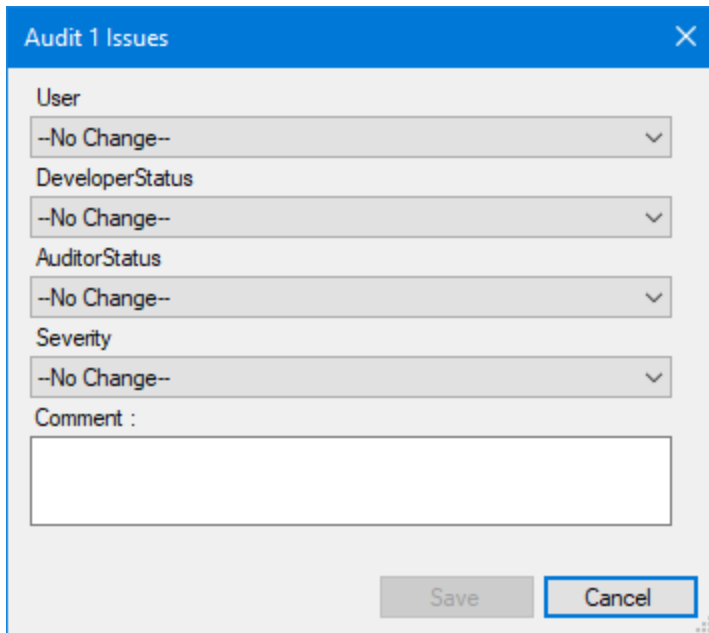
Auditing Issues

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** window. If you have the Audit Issues permission, you can also edit an issue's auditor status and severity.

Note: You can edit one or more issues from the **Analysis Results** window or you can edit one selected issue in the **Audit Summary** window.

To audit an issue:

1. From the issues list in the **Analysis Results**, select the check box to the left of the issue.
To make the same edit to multiple issues, select the check box to the left of each issue you want to audit.
2. Click **Audit Issue**.



3. From the **User** list, select the user to assign to the issue.
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 **Comment** box.
8. Click **Save**.

The extension saves your changes for the application and release on the Fortify on Demand server.

Locating the Source Code Associated with Static Scan Issues

You can use the Fortify on Demand Extension for Visual Studio 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 Extension for Visual Studio:

1. Select an issue in the **Analysis Results** window or select a line in the **Analysis Trace** window.
2. If the source code is not available in the analysis results opened from Fortify on Demand, do the following:
 - a. In the Set Source Path dialog box, click **Browse**.
 - b. Select the location of the folder that contains the source code, and then click **OK**.
 - c. Click **OK** to close the Set Source Path dialog box.

The Visual Studio extension jumps to the line of code associated with the issue in a downloaded copy of the source code.

Note: If the source code is a downloaded copy from Fortify on Demand, the file name is `<original_filename> - Downloaded.<extension>`.

Logging Out

To log out of Fortify on Demand

- From the Fortify on Demand Extension for Visual Studio menu, select **Log Out of Fortify on Demand**.

The analysis results are closed, and you are logged out from the Fortify on Demand server.

Locating the Log Files

To get help with diagnosing an issue in the Fortify on Demand Extension for Visual Studio, send the log files to support. On Windows systems, the log files are in the following directories:

- C:\Users*<username>*\AppData\Local\FortifyOnDemand
The log file is FoDVSExtension.log.
- C:\Users*<username>*\AppData\Local\Fortify\scancentral-*<version>*\log
The log files in this directory only exist if you use Fortify ScanCentral SAST client to package project for upload to 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 Extension for Visual Studio 22.2)

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!