

---

# **Micro Focus Fortify Extension for Visual Studio Code**

Software Version: 20.1.0

## **User Guide**

Document Release Date: Revision 1: January 2021

Software Release Date: December 2020



## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## Warranty

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

## Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

© Copyright 2020-2021 Micro Focus or one of its affiliates

## Trademark Notices

All trademarks, service marks, product names, and logos included in this document 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 January 25, 2021. 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 Micro Focus Fortify Customer Support .....	4
For More Information .....	4
About the Documentation Set .....	4
Change Log .....	5
Chapter 1: Introduction .....	6
Software Requirements .....	6
Installing the Fortify Extension for Visual Studio Code .....	7
Related Documents .....	8
Micro Focus Fortify ScanCentral SAST .....	8
Micro Focus Fortify Software Security Center .....	9
Micro Focus Fortify Static Code Analyzer .....	9
Chapter 2: Using Fortify Extension for Visual Studio Code .....	11
Uploading Code to Fortify on Demand for Assessment .....	11
Performing a Local Analysis with Fortify Static Code Analyzer .....	12
Performing an Analysis Remotely with Fortify ScanCentral SAST .....	14
Send Documentation Feedback .....	16

# Preface

## Contacting Micro Focus 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/solutions/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 Micro Focus Product Documentation website:

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

# Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

<b>Software Release / Document Version</b>	<b>Changes</b>
20.1.0 / Revision 1: January 2021	Updated: <ul style="list-style-type: none"><li>• <a href="#">"Uploading Code to Fortify on Demand for Assessment" on page 11</a> - Added note about language support.</li></ul>
20.1.0	Initial release

# Chapter 1: Introduction

The Fortify Extension for Visual Studio Code uses Micro Focus Fortify Static Code Analyzer and Fortify security content to uncover security vulnerabilities (issues) in your project.

The Fortify Extension for Visual Studio Code provides three ways to analyze your source code for security vulnerabilities. The following sections describe any prerequisites for each analysis method and the instructions for how to use it.

Analysis Method	Procedure
Upload your currently opened project to Fortify on Demand for static assessment.	<a href="#">"Uploading Code to Fortify on Demand for Assessment" on page 11</a>
Run a locally installed version of Fortify Static Code Analyzer on the currently opened project. To view the results, open the Fortify Project Results (FPR) file in Micro Focus Fortify Audit Workbench.	<a href="#">"Performing a Local Analysis with Fortify Static Code Analyzer" on page 12</a>
Run a remote analysis using Micro Focus Fortify ScanCentral SAST.  You can upload the analysis results in Micro Focus Fortify Software Security Center.	<a href="#">"Performing an Analysis Remotely with Fortify ScanCentral SAST" on page 14</a>

## Software Requirements

The Fortify Extension for Visual Studio Code works with the Fortify software listed in the following table.

Software	Version	Notes
Micro Focus Fortify Static Code Analyzer	20.2.0 or later	To scan your project locally with Fortify Static Code Analyzer, you must either: <ul style="list-style-type: none"> <li>• Make sure that the PATH environment variable includes the sourceanalyzer executable</li> <li>• Have the full path to the Fortify Static Code Analyzer installation directory</li> </ul>

Software	Version	Notes
Micro Focus Fortify Software Security Center	20.2.0 or later	To upload scan results to Fortify Software Security Center, make sure that you have one of the following types of Fortify Software Security Center authentication tokens: <ul style="list-style-type: none"><li>• ScanCentralCtrlToken - ScanCentral Controller token</li><li>• CIToken - Continuous integration token</li></ul>
Micro Focus Fortify ScanCentral SAST	20.2.0 or later	To perform a Fortify Static Code Analyzer analysis on a remote system using Fortify ScanCentral SAST, make sure that you have either: <ul style="list-style-type: none"><li>• A ScanCentral Controller URL</li><li>• A Fortify Software Security Center URL and an authentication token of type ScanCentralCtrlToken</li></ul> Fortify ScanCentral SAST supports analysis for .NET applications in C# and VB.NET (.NET Core, .NET Standard, and ASP.NET), ABAP, Apex, Classic ASP, ColdFusion, Java, JavaScript, PHP, PL/SQL, Python, Ruby, T-SQL, TypeScript, and Visual Basic 6.0.  <b>Note:</b> Analysis of .NET projects requires .NET Framework version 4.7.2 or later.
Fortify on Demand	N/A	To upload your project to Fortify on Demand for assessment, make sure that you have: <ul style="list-style-type: none"><li>• Fortify ScanCentral SAST standalone client installed and included in the PATH environment variable</li><li>• Fortify on Demand credentials</li></ul>

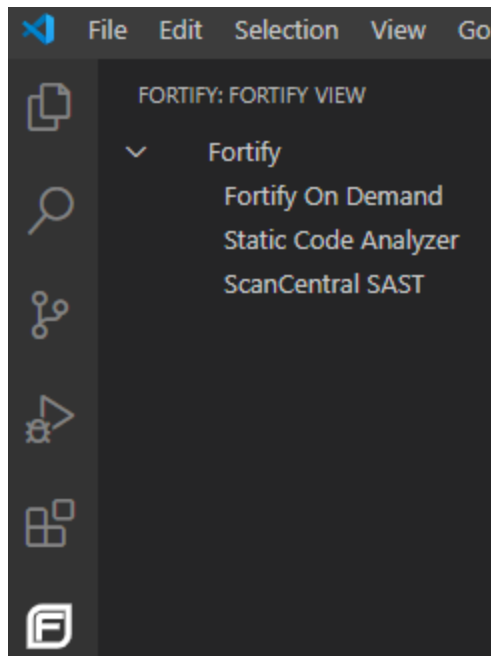
## Installing the Fortify Extension for Visual Studio Code

You can install this extension on a computer running Windows, Linux, or macOS.

To install the Fortify Extension for Visual Studio Code:

- Install the Fortify Extension for Visual Studio Code from the Visual Studio Marketplace.  
See the Visual Studio Code documentation for instructions about how to install an extension.

After the extension is successfully installed, the Fortify icon (📄) is included in the VS Code activity bar. Click this icon to see the Fortify commands in the VS Code side bar.



## Related Documents

This topic describes documents that provide information about Micro Focus Fortify software products.

**Note:** You can find the Micro Focus Fortify Product Documentation at <https://www.microfocus.com/support/documentation>.

## Micro Focus Fortify ScanCentral SAST

The following document provides information about Fortify ScanCentral SAST. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-software-security-center>.

Document / File Name	Description
<i>Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide</i> SC_SAST_Guide_<version>.pdf	This document provides information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their Fortify Static Code Analyzer



Document / File Name	Description
	process.

## Micro Focus Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-software-security-center>.

Document / File Name	Description
<i>Micro Focus Fortify Software Security Center User Guide</i> SSC_Guide_<version>.pdf	<p>This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use Software Security Center.</p> <p>It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project.</p>

## Micro Focus Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-static-code>.

Document / File Name	Description
<i>Micro Focus Fortify Static Code Analyzer User Guide</i> SCA_Guide_<version>.pdf	<p>This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.</p>

Document / File Name	Description
<i>Micro Focus Fortify Static Code Analyzer Custom Rules Guide</i> SCA_Cust_Rules_Guide_<version>.zip	<p>This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues.</p> <p><b>Note:</b> This document is included only with the product download.</p>

# Chapter 2: Using Fortify Extension for Visual Studio Code

This section contains the following topics:


- Uploading Code to Fortify on Demand for Assessment .....11
- Performing a Local Analysis with Fortify Static Code Analyzer ..... 12
- Performing an Analysis Remotely with Fortify ScanCentral SAST .....14

## Uploading Code to Fortify on Demand for Assessment

**Note:** The Fortify on Demand task supports packaging of JavaScript and TypeScript projects for scanning.

You need to have the standalone Fortify ScanCentral SAST client on the system where Fortify Extension for Visual Studio Code is installed to upload code to Fortify on Demand. You can obtain the Fortify ScanCentral SAST client from the Fortify on Demand Tools page. For instructions on using the Fortify ScanCentral SAST client, see the README file is stored inside the zip file.

To upload the opened project to Fortify on Demand for assessment:

1. If the extension is not open, click **Fortify**  in the activity bar.
2. Click **Fortify on Demand** in the VS Code side bar.
3. From the **API root URL** list, type your data center's API root URL.
4. (Optional) Select the **Use proxy** check box to connect through a proxy and provide the settings described in the following table.

Field	Description
<b>Proxy host</b>	Type the URL of the proxy server.
<b>Proxy port</b>	Type the port of the proxy server.
<b>Use HTTPS</b>	Select the check box to connect using HTTPS.
<b>Use proxy credentials</b>	Select the check box if the proxy server requires authentication. Type the account credentials on the proxy server.

5. Select an authentication method and provide the relevant credentials described in the following

table.

Authentication Method	Procedure
API credentials	<ol style="list-style-type: none"><li>In the <b>Key</b> box, type the API key.</li><li>In the <b>Secret</b> box, type the API secret.</li></ol>
User credentials	<ol style="list-style-type: none"><li>In the <b>Username</b> box, type the account username.</li><li>In the <b>Password</b> box, type the account password.</li><li>In the <b>Tenant ID</b> box, type the tenant ID.</li></ol>
Personal access token	<ol style="list-style-type: none"><li>In the <b>Username</b> box, type the account username.</li><li>In the <b>Secret</b> box, type the personal access token.</li><li>In the <b>Tenant ID</b> box, type the tenant ID.</li></ol>

- In the **Release ID** box, type the Fortify on Demand release ID.

**Note:** The release must have saved scan settings in the portal in order for the release ID to be used as a token.


- From the **Entitlement preference** box, select the entitlement preference. 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.
- Select **Purchase entitlement** to purchase an entitlement if none is available for the specified entitlement preference. If the purchase entitlements feature is not enabled for the tenant, the Fortify Extension for Visual Studio Code log will display an error message.
- From the **Remediation preference** list, select whether to run the scan as a remediation scan.
- From the **Action for In-Progress scan** list, select the action to take if the release has an in-progress scan:
  - **DoNotStartScan**—Do not start a new scan and fail the task
  - **CancelInProgressScan**—Cancel the scan in progress and start a new scan (if the scan in progress can be automatically canceled)
  - **Queue**—Queue the scan (if the scan queue limit has been reached, the scan will be canceled)
- Click **Upload**.

If the project is successfully uploaded, the Fortify Extension for Visual Studio Code log displays a 200 OK status code and the scan ID. The Fortify on Demand Scans pages display a new scan for the release.

## Performing a Local Analysis with Fortify Static Code Analyzer

You must have Fortify Static Code Analyzer locally installed.

To scan the opened project with Fortify Static Code Analyzer:

1. If the extension is not open, click **Fortify** () in the activity bar.
2. Click **Static Code Analyzer** in the VS Code side bar.
3. In the **Static Code Analyzer executable path** box, type the path to the Fortify Static Code Analyzer executable or click **Browse** to find the file on your system.

Type sourceanalyzer to use the executable that is in the PATH environment variable. This is the default.

4. In the **Build ID** box, type a unique identifier for the analysis.
5. (Optional) In the **Scan results location (FPR)** box, type a name for the Fortify results file (for example, MyProjectA.fpr).

If you do not provide a results file name, then Fortify Extension for Visual Studio Code uses the name of the current project folder for the FPR file and saves the FPR in the current project folder.

**Note:** If you do not specify a path for the FPR, then the FPR is saved in the  
C:\Users\*<username>*\AppData\Local\Programs\Microsoft VS Code directory.

6. (Optional) To specify a custom location for the Fortify Static Code Analyzer log file, type a file name (or a full path) in the **Log location** box.

By default, the Fortify Extension for Visual Studio Code saves the log file in the following location:

- Windows: C:\Users\*<user>*\AppData\Local\Fortify\sca*<version>*\log
- Non-Windows: \$HOME/.fortify/sca*<version>*/log

where *<version>* is the version of Fortify Static Code Analyzer that you are using.

7. (Optional) To add additional Fortify Static Code Analyzer translation options:
  - a. Select the **Add SCA translation options** check box.
  - b. Type Fortify Static Code Analyzer translation options.

See the *Micro Focus Fortify Static Code Analyzer User Guide* in [Fortify Static Code Analyzer and Tools Software Documentation](#) for detailed information about the available translation options.

8. (Optional) To add additional Fortify Static Code Analyzer scan options:
  - a. Select the **Add SCA scan options** check box.
  - b. Type Fortify Static Code Analyzer scan options.

See the *Micro Focus Fortify Static Code Analyzer User Guide* in [Fortify Static Code Analyzer and Tools Software Documentation](#) for detailed information about the available scan options.

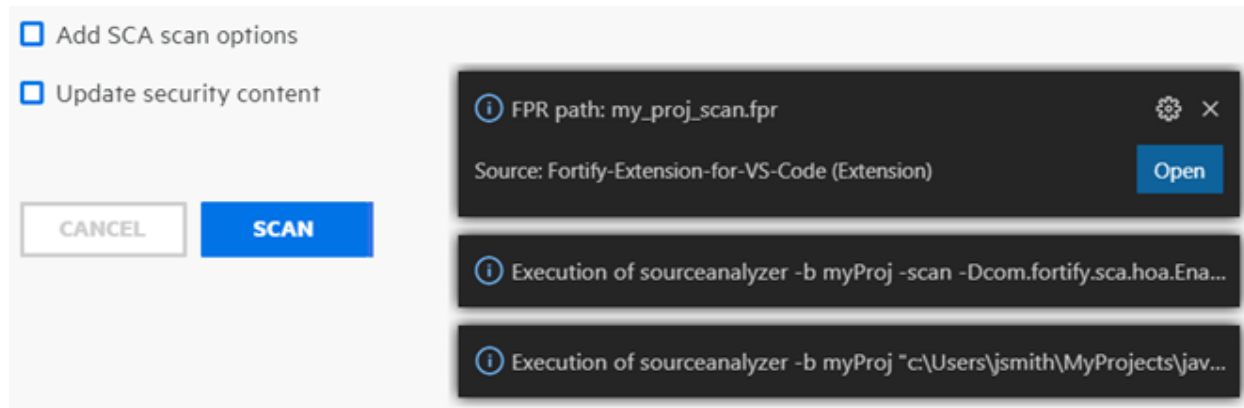
9. To download Fortify security content before the scan, select the **Update security content** check box.

If you are using a different Fortify Rulepack update server other than <https://update.fortify.com> or if you require proxy information for the connection, you must use the Fortify Static Code Analyzer post-install tool (scapostinstall) to configure this information before you can update Fortify security content. See the *Micro Focus Fortify Static Code Analyzer User Guide* in [Fortify Static Code Analyzer and Tools Software Documentation](#) for

more information.

10. Click **Scan**.

When the scan is complete, Fortify Extension for Visual Studio Code displays the **FPR path** in an information message .



You can:

- View the scan results in Fortify Audit Workbench by clicking **OPEN** to the right of **Scan results location (FPR)**.
- Open the log file by clicking **OPEN** to the right of **Log location**.

## Performing an Analysis Remotely with Fortify ScanCentral SAST

You must have a properly configured Fortify ScanCentral SAST installation. For more information, see the *Micro Focus Fortify ScanCentral Installation, Configuration, and Usage Guide* in [Fortify Software Security Software Documentation](#). If you are using a standalone ScanCentral client, make sure the JAVA\_HOME environment variable is set to root directory of your JRE/JDK installation. For example: JAVA\_HOME=C:\openjdk\zu1u-jdk8.0.202.

To upload the opened project for analysis by Fortify ScanCentral SAST:

1. If the extension is not open, click **Fortify** (📄) in the activity bar.
2. Click **ScanCentral SAST** in the VS Code side bar.
3. In the **ScanCentral executable location** box, type the path to the Fortify ScanCentral SAST executable or click **Browse** to find the file on your system.

The standalone Fortify ScanCentral SAST client can be installed anywhere on your system. By default, Fortify Extension for Visual Studio Code looks for the Fortify ScanCentral SAST executable in the Fortify Static Code Analyzer installation in `<sca_install_dir>/bin` directory.

4. Under **Controller connection**, select how you want to connect to Fortify ScanCentral SAST. Do one of the following:

- Select the **Controller URL** check box and then in the **Controller URL** box, type the ScanCentral Controller URL.  
  
The format for the ScanCentral Controller URL is: `<protocol>://<controller_host>:<port>/scancentral-ctrl` (for example:  
`https://myControllerHost.com:8443/scancentral-ctrl`).
- Select the **SSC URL** check box, and then provide the following:
  - i. In the **Software Security Center URL** box, type the server URL.  
  
The format for the Fortify Software Security Center URL is:  
`<protocol>://<ssc_host>:<port>/ssc` (for example:  
`http://my.domain.com:8080/ssc`).
  - ii. In the **Use Controller token** box, paste the decoded value for a Fortify Software Security Center authentication token of type ScanCentralCtrlToken.
- 5. (Optional) In the **Notification email** box, type an email address to which the ScanCentral Controller will send job status notifications.
- 6. (Optional) To upload the scan results to Fortify Software Security Center:
  - a. Select the **Upload scan results to Software Security Center** check box.
  - b. Specify an existing application name and application version.
  - c. Do one of the following:
    - If you are using the Fortify Software Security Center URL for the controller connection, select the **Use Controller token** check box.
    - In the **Continuous integration token** box, paste the decoded value for a Fortify Software Security Center authentication token of type CIToken.
- 7. (Optional) To specify additional Fortify Static Code Analyzer translation or scan options. select the **Additional options** check box and type any translation and scan options you want to include.  
  
See the *Micro Focus Fortify Static Code Analyzer User Guide* in [Fortify Static Code Analyzer and Tools Software Documentation](#) for detailed information about the available translation and scan options.
- 8. (Optional) To specify a custom location for the Fortify Static Code Analyzer log file, type a file name (or a full path) in the **Log location** box.  
  
By default, the Fortify Extension for Visual Studio Code saves the log file in the following location:
  - Windows: `C:\Users\<user>\AppData\Local\Fortify\scancentral\log`
  - Non-Windows: `$HOME/.fortify/scancentral/log`where `<version>` is the version of Fortify Static Code Analyzer that you are using.
- 9. Click **Scan**.

When the scan request to Fortify ScanCentral SAST is complete, Fortify Extension for Visual Studio Code displays the status in an information message.

You can:

- View the scan results on Fortify Software Security Center if you uploaded them to the server.
- Open the log file by clicking **OPEN** to the right of **Log location**.

# 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 Micro Focus Fortify 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 Extension for Visual Studio Code 20.1.0)**

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](mailto:FortifyDocTeam@microfocus.com).

We appreciate your feedback!