OpenText™ Fortify Azure DevOps Extension

Software Version: 9.4

User Guide

Document Release Date: September 2024
Software Release Date: September 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

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 September 30, 2024. 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

Contacting 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 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 Fortify Community:

https://community.microfocus.com/cyberres/fortify/w/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

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.

Software Release / Document Version	Changes
9.4	Updated: • Streamlined Fortify on Demand topics and removed discontinued Fortify on Demand tasks. Added: • "Adding a DAST Automated assessment task" on page 24
8.10	Updated: • Added information about Fortify ScanCentral SAST client requirements and troubleshooting (see "Requirements for the Fortify ScanCentral SAST task" on page 35 and "Troubleshooting the Fortify ScanCentral SAST task" on page 40)
8.9	Updated: • Added information on packaging files required for Debricked open source scans (see "Adding a Static Assessment task" on page 18)
8.8	Updated: • Updated polling to poll for static and Sonatype scan statuses and results; removed support for release pipelines (see "Adding a Static Assessment task" on page 18)
8.6	Updated: • Changes made for uploading scan results to Fortify Software Security Center including the ability to trigger a build failure based on the scan results (see "Adding a Fortify Static Code Analyzer Assessment task" on page 11 and "Adding a Fortify ScanCentral SAST Assessment task" on page 36)

Fortify Azure DevOps Extension

The Fortify Azure DevOps Extension (formerly the Fortify VSTS Extension) adds static and dynamic analysis to your continuous integration (CI) and continuous delivery (CD) builds. This integration helps you identify application vulnerabilities earlier in the software development lifecycle.

This document describes how to use the Fortify Azure DevOps Extension. This document assumes that you have a working knowledge of Azure DevOps and know how to use Azure Pipelines for your CI/CD solutions. This extension includes the tasks described in the following table.

> **Note:** If you use any Fortify Azure DevOps task that requires access to an external server such as Fortify Software Security Center or Fortify ScanCentral (SAST or DAST) and the server's certificates are self-signed, then you must extend the node.js predefined root certificate authority (CA) with extra certificates. Do this by setting the NODE_EXTRA_CA_CERTS environment variable. For more information, see the node.js command-line options documentation.

Task (version)	Description	More information
Fortify Static Code Analyzer Install (7.x)	The Fortify Static Code Analyzer Installation task automatically installs and configures Fortify Static Code Analyzer.	"Getting started with Fortify Static Code Analyzer" on page 9
Fortify Static Code Analyzer Assessment (7.x)	The Fortify Static Code Analyzer Assessment task enables you to run Fortify Static Code Analyzer as a build step. After the analysis is complete, the scan results are available as a Fortify Project Results (FPR) file. You can publish the FPR as a build artifact. To review the scan results, download this artifact and open it in either Fortify Audit Workbench or Fortify Software Security Center. You can also configure the task to upload the scan results to a Fortify Software Security Center server.	"Getting started with Fortify Static Code Analyzer" on page 9
Fortify on Demand Static Assessment 9.x)	The Fortify on Demand Static Assessment task submits a static scan	"Getting started with Fortify on Demand" on page 16

Task (version)	Description	More information
	request and uploads code to Fortify on Demand as a build step. The scan results are available in Fortify on Demand.	
FoD DAST Automated (2.x)	The FoD DAST Automated task submits an automated dynamic scan request to Fortify on Demand as a build step. The scan results are available in Fortify on Demand.	"Getting started with Fortify on Demand" on page 16
Fortify ScanCentral SAST Assessment (7.x)	The Fortify ScanCentral SAST Assessment task submits a static scan request to a ScanCentral SAST Controller (using a ScanCentral SAST client) as a build step. You can also configure the task to upload the scan results to Fortify Software Security Center.	"Getting started with Fortify ScanCentral SAST" on page 34
Fortify ScanCentral DAST Assessment (7.x)	The Fortify ScanCentral DAST Assessment task submits a dynamic scan request to Fortify ScanCentral DAST as a build step. You can view the scan results in Fortify Software Security Center.	"Getting started with Fortify ScanCentral DAST" on page 41
Fortify WebInspect Dynamic Assessment (7.x)	The Fortify WebInspect Dynamic Assessment task automatically submits a dynamic scan request to Fortify WebInspect as a build step. Fortify WebInspect scans your Web application or Web services for vulnerabilities based on the settings specified in the Scan Settings file.	"Getting started with Fortify WebInspect" on page 42

Getting started with Fortify Static Code Analyzer

To configure the Fortify Azure DevOps Extension to use Fortify Static Code Analyzer, you must have experience using Fortify Static Code Analyzer in a standalone environment. You can use Fortify Azure DevOps Extension with Fortify Static Code Analyzer 16.11 and later versions. For detailed information about how to use Fortify Static Code Analyzer, see *OpenText™ Fortify Static Code Analyzer User Guide* in Fortify Static Code Analyzer and Tools Documentation.

Requirements for Fortify Static Code Analyzer tasks

Make sure that you have the following information needed to configure the Fortify Static Code Analyzer installation and complete the preparation steps before you run a scan on your application:

- A Fortify license file (`fortify.license`)
- To run Fortify scans in your build definitions, you must first set up a build agent pool of agents that are configured with all the prerequisites to build the application.

  To prepare an agent for the analysis, install the required build software based on your target application's source code, and then confirm that you can successfully build your application on the agent.

  > **Note:** The Fortify Static Code Analyzer tasks are not supported on Microsoft-hosted agents. OpenText recommends a minimum of 16 GB of RAM and a quad-core processor to run Fortify Static Code Analyzer.

- To scan .NET projects, the agent must have a full installation of Visual Studio and devenv included in the path environment variable. One way to do this is to launch the Developer Command Prompt and run the agent's `configureAgent` or `runAgent` scripts to connect to Azure DevOps.
- You can perform the scan phase on the local agent or remotely using Fortify ScanCentral SAST. To run a scan with Fortify ScanCentral SAST, you must have the following:
  - A Fortify Software Security Center server that is configured to integrate with ScanCentral SAST Controller
  - A Fortify Software Security Center authentication token of type CIToken
- To trigger a build failure based on scan results produced with Fortify ScanCentral SAST, you must use Fortify ScanCentral SAST version 22.1.0 or later (see "Adding a Fortify Static Code Analyzer Assessment task" on page 11).
- To upload the scan results to Fortify Software Security Center, you must have a Fortify Software Security Center authentication token of type CIToken.
- To perform the scan using Fortify ScanCentral SAST and to upload scan results to Fortify Software Security Center, you need to set up an Azure DevOps service connection to Fortify Software Security Center.

  Create a **Generic** service connection and provide the Fortify Software Security Center server URL and the decoded value of a Fortify Software Security Center authentication token of type CIToken. Leave the **username** box empty.

Installing Fortify Static Code Analyzer

To install Fortify Static Code Analyzer, you have the following two options:

- "Using the Fortify Static Code Analyzer Install task" below

  This installs Fortify Static Code Analyzer with built-in defaults.
- Use the Fortify Static Code Analyzer installer manually on your agent machines.

  This option gives you more control over your installation. For installation instructions, see the *OpenText™ Fortify Static Code Analyzer User Guide* in Fortify Static Code Analyzer and Tools Documentation.

Using the Fortify Static Code Analyzer Install task

The **Fortify Static Code Analyzer Install** task automatically installs and configures Fortify Static Code Analyzer on the target agents.

Perform this install task one time for each agent (or when you upgrade to a new version of Fortify Static Code Analyzer). OpenText recommends that you create a build definition dedicated to setting up agents. You must target this build step to each agent you plan to enable in your build pool.

Before you use the **Fortify Static Code Analyzer Install** task:

- Make sure that you can successfully build your application on the agent where you are installing Fortify Static Code Analyzer.
- You must have both the Fortify Static Code Analyzer installer executable and the `fortify.license` file available using an addressable file path on the agent.
- Make sure that the agent's work directory is close to the root to avoid issues with the Windows maximum path length limitation (MAX_PATH).

This task can:

- Install Fortify Static Code Analyzer unless it is already installed.
- Configure the installation with a user-provided `fortify.license` file.
- Install the latest Fortify Security Content allowed by the Fortify license.

To configure the Fortify Static Code Analyzer install task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.

3. Find and add the **Fortify Static Code Analyzer Install** task.
4. Provide the information described in the following table.

Field	Description
Display name	Type a name for the task.
Fortify SCA installer path	Type the full path to the Fortify Static Code Analyzer installer on the agent. For example, `C:\<location_on_agent>\Fortify_SCA_and_Apps_<version>_windows_x64.exe`.
Fortify SCA license file	Type the full path to the `fortify.license` file on the agent. For example, `C:\<location_on_agent>\fortify.license`.
Update Fortify Security Content	(Optional) Select whether to update the Fortify Security Content.
Proxy host	(Optional) Specifies a proxy host required for connection to the Fortify Rulepack update server.
Proxy port	(Optional) Specifies a proxy port required for connection to the Fortify Rulepack update server.
Targeted Visual Studio environment	Select the Visual Studio environment for your application.

Adding a Fortify Static Code Analyzer Assessment task

Use the **Fortify Static Code Analyzer Assessment** task to run Fortify Static Code Analyzer as a build step. After you run the build and the scan is complete, the scan results are available as a Fortify Project Results (FPR) file. You can publish the FPR and Fortify Static Code Analyzer log files as build artifacts. To review the scan results, download the FPR artifact and open it in either Fortify Audit Workbench or Fortify Software Security Center. You can also configure the task to upload the FPR to an existing Fortify Software Security Center server for enterprise vulnerability management.

To configure a Fortify Static Code Analyzer Assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Add the **Fortify Static Code Analyzer Assessment** task.

4. Provide the general information described in the following table.

Field	Description
Display name	Type a name for the task.
Fortify SCA license file	(Optional) Provide the path to a Fortify license file. If specified, it overwrites the `fortify.license` file on the build agent where Fortify Static Code Analyzer is currently installed. This path must be the location of a Fortify license file that is different than where Fortify Static Code Analyzer is already installed. **Note:** The user running the agent should have the proper permission to write to the Fortify Static Code Analyzer installation directory.
Build ID for Fortify SCA	Type a unique identifier for the scan.
Update Fortify Security Content	(Optional) Select whether to update your installed Fortify Security Content by downloading the latest Fortify Secure Coding Rulepacks and metadata from the Fortify Rulepack update server.
Run SCA clean	(Optional) Select whether to remove any temporary files from a previous scan for the specified build ID.
Enable verbose logging	(Optional) Select whether to send verbose status messages to the console and to the log file.
Enable debug logging	(Optional) Select whether to include debug information in the log file, which is useful for Customer Support to help troubleshoot issues.

5. To run translation, configure the following settings under **Translation Options**:
   a. Select the **Run Fortify SCA translation** check box.
   b. From the **Application type** list, select the type of project you want to analyze.

      The configuration settings dynamically change based on your selection.
   c. Specify the information required to translate the application.

Application Type	Description
.NET	In the **Projects for Fortify SCA analysis** box, type the relative path to the solution or project file name.

Application Type	Description
Java	Specify the classpath, source version, sourcepath, source files, build tool options, source files (this can be a build file), and any other additional files to include in the scan.
Other	Specify any build tool options, source files, and any other additional files to include in the scan.

d. (Optional) In the **Additional Fortify SCA translation options** box, specify any additional Fortify Static Code Analyzer translation options. For example, the following option excludes test files from the translation:

```
-exclude **tests/**
```

See *OpenText™ Fortify Static Code Analyzer User Guide* in Fortify Static Code Analyzer and Tools Documentation for more information about translation options.

6. To run a scan, configure the following settings under **Scan Options**:

   a. Select the **Run Fortify SCA scan** check box.

   b. From the **Scan type** list, select whether you want to perform a local scan or a remote scan using Fortify ScanCentral SAST.

   c. (Optional) In the **Additional Fortify SCA scan options** box, specify any additional scan options.

   d. (Optional) In the **Custom Rulepacks** box, specify custom rules.

   Specify custom rules files (*.xml or *.bin) separated by spaces or specify a directory that contains custom rules.

   e. If you selected a scan type of **ScanCentral** in step b, then in the **Fortify SSC service connection** box, specify an Azure DevOps service connection to Fortify Software Security Center. For more information, see "Requirements for Fortify Static Code Analyzer tasks" on page 9.

   f. To upload the scan results to Fortify Software Security Center, do the following:

      i. Select the **Upload results to SSC** check box.

      ii. If you have not already done so, in the **Fortify SSC service connection** box, specify an Azure DevOps service connection to Fortify Software Security Center. For more information, see "Requirements for Fortify Static Code Analyzer tasks" on page 9.

      iii. Specify an application version that exists in Fortify Software Security Center by providing one of the following:

      - An application name and an application version name.
      - A Fortify Software Security Center application version ID.

Note: If you provide both application name and version and an application ID, the extension uses the application ID for the upload regardless of the selected application version type.

iv. (Optional) To connect to Fortify Software Security Center with a proxy server, specify the proxy information.

Note: Use the following syntax for the **Proxy URL**:

```
<protocol>://<address>:<port>
```

v. (Optional) To trigger a build failure based on the scan results, type a search query in the **Build failure criteria** box.

For example, the following search query causes the build to fail if any critical issues exist in the scan results:

```
[fortify priority order]:critical
```

See *OpenText™ Fortify Software Security Center User Guide* in Fortify Software Security Center Documentation for a description of the search query syntax.

By default, the task returns a warning when the build failure criteria is met. To fail the build instead, select **FAIL** from the **Task results when build failure criteria is met** list.

vi. (Optional) To specify how long to poll Fortify Software Security Center to determine if FPR processing is finished, type the time in minutes in the **Polling timeout** box.

If no value or a value of 0 is specified, polling continues until FPR processing finishes or stops due to errors. The valid values are 0–10080.

vii. (Optional) To specify how frequently to poll Fortify Software Security Center to determine if the FPR processing is finished, in the **Polling interval** box, specify an interval (in minutes).

The valid values are 1–60 and the default value is 1 minute.

Important! If the FPR processing requires approval, then this step will not complete until approval is granted through Fortify Software Security Center.

As an alternative to uploading scan results to Fortify Software Security Center, you can add a standard Azure DevOps **Publish Pipeline Artifact** build step to collect the scan results and log files.

Note: To ensure that you obtain scan log files when you publish artifacts, make sure that you select the **Continue on error** check box in the task configuration. Otherwise, if the assessment fails, the artifact collection task does not start.

Troubleshooting the Fortify Static Code Analyzer Assessment task

Unable to Find sourceanalyzer

The agent running the scan must have the location of Fortify Static Code Analyzer included in the execution path. By default, the Fortify Static Code Analyzer installer adds itself to the path.

If you see this error, make sure that the Fortify Static Code Analyzer installation location is part of the OS execution path. You might need to restart your agent to pick up changes made to the OS path.

Unable to Connect to Fortify Software Security Center for Upload

- Make sure that your application name, version name, and service connection are correctly configured.
- If your Fortify Software Security Center is configured to use HTTPS, make sure that the JDK keystore in the Fortify Static Code Analyzer installation is configured to accept the Fortify Software Security Center server certificate.

Getting started with Fortify on Demand

A Fortify on Demand account is required to use the Fortify Azure DevOps Extension with Fortify on Demand.

Adding Fortify on Demand credentials in Azure DevOps

Before adding a Fortify on Demand task to your pipeline, you need to obtain appropriate Fortify on Demand credentials and add them in Azure DevOps. Service connections are used to manage Fortify on Demand credentials in Azure DevOps. You can create a Fortify service connection to store Fortify on Demand credentials.

To add your Fortify on Demand credentials in Azure DevOps:

1. In an Azure DevOps project, navigate to the project settings .
2. Under **Pipelines**, select **Service connections**.
3. Click **New service connection**.
4. Select **Fortify** from the list and click **Next**.

   The Add Fortify service connection window appears.
5. Select the method of authentication:
   - **Basic Authentication**: requires personal access token with the `api-tenant` scope
   - **Token Based Authentication**: requires API key with the `api-tenant` scope

   See the Fortify on Demand documentation for instructions on creating a personal access token and API key.
6. Complete the following fields:

Field	Description
Connection name	Specify a name for your service connection.
API URL	Specify your data center's API root URL: • US: https://api.ams.fortify.com • EMEA: https://api.emea.fortify.com • APAC: https://api.apac.fortify.com • SGP: https://api.sgp.fortify.com • FedRAMP: https://api.fed.fortify.com • Trial: https://api.trial.fortify.com

Portal URL	Specify your data center's domain URL.
Proxy Host (optional)	Specify the URL of the proxy server.
Proxy Port (optional)	Specify the port of the proxy server.
Username, Personal Access Token, Tenant ID API Key, API Secret	• If you selected **Basic Authentication**, specify the account username, personal access token, and tenant code. • If you selected **Token Based Authentication**, specify the API key and secret.

7. Click **OK**.

   Your new service connection is saved.

Setting up a Fortify on Demand Static Assessment

Perform the following tasks to set up a Fortify on Demand Static Assessment:

- Download and install the Fortify ScanCentral SAST client on the agent. See "Downloading and installing the Fortify ScanCentral SAST client" below. This part is optional if you are using a Microsoft-hosted agent.
- Configure static scan settings. You can configure scan settings from the Fortify on Demand portal before submitting the assessment or from Azure DevOps as part of the task settings.
- Add the Fortify on Demand Static Assessment task to a pipeline in an Azure DevOps project. See "Adding a Static Assessment task" on the next page.

Downloading and installing the Fortify ScanCentral SAST client

A stand-alone Fortify ScanCentral SAST client is offered for automatically packaging all necessary dependencies and source code required for static scanning and the files required for Debricked open source scanning. The following languages are supported: .NET and .NET Core (MSBuild projects), Apex, Classic ASP, ColdFusion, Dockerfiles, Go, Java (Gradle and Maven projects), Javascript/Typescript, PHP, Python, and Ruby.

The latest version of the Fortify ScanCentral SAST client is available from the Tools page in the portal. Installation instructions are available in the README.txt file stored in the zip file.

Important! The stand-alone Fortify ScanCentral SAST client is a component of the on-premises Fortify ScanCentral SAST software and is used to package code to send to a Controller for scanning. Fortify Azure DevOps Extension uses only the packaging feature of the Fortify ScanCentral SAST client. Details that are relevant to packaging your source code has been provided.

For more information about using the Fortify ScanCentral SAST client, see the Fortify Software Security Center Documentation. Select the documentation version that corresponds to your installed version.

- Software requirements: "Fortify ScanCentral SAST Client Software Requirements" in *Fortify Software System Requirements*
- Supported build tools: "Fortify ScanCentral SAST Sensor Languages and Build Tools" in *Fortify Software System Requirements*
- Command-line options: "Package Command" in *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*

Adding a Static Assessment task

You can add the **Fortify on Demand Static Assessment** task to your build pipeline using the classic editor or the YAML editor in Azure DevOps. The following instructions describe how to add a static assessment task to a build pipeline using the YAML editor.

> **Note:** The **Fortify on Demand Static Assessment** task does not support release pipelines.

To add a static assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Find and select **Fortify on Demand Static Assessment** from the task list.

   The static assessment task settings appear.
4. Complete the following fields:

Field	**Description**
Source code location	Specify the path on the agent where the source code files are located. You can use predefined variables for the source code directory, such as `$(Build.SourcesDirectory)`. Do not use `$(Build.ArtifactStagingDirectory)` or `$(Build.ArtifactDirectory)`, as these locations can cause errors when compressing the source code prior to transmission.
ScanCentral file location	Specify the path on the agent where the Fortify ScanCentral SAST client executable is located. For example, `C:\Program Files\Fortify_ScanCentral_Client_21.1.0_x64\bin`. If the field is left empty, the latest version of the Fortify ScanCentral SAST client will automatically be downloaded on the agent. **Note:** The Fortify ScanCentral SAST version and the installed Java version must be compatible. If the Java version is incompatible, the task

Field	Description
	will fail.
Fortify Connection	Select an existing service connection or click **+New** to add a new service connection. For more information, see "Adding Fortify on Demand credentials in Azure DevOps" on page 16.

5. In the **Application/Release Options** section, select the method of identifying the release from the **Pick a Release** list:

   - **Release ID**
   - **BSI Token**
   - **New Application and Release**

6. Follow the procedure for the selected method:

Method	Procedure
Release Id	In the **Release ID** field, specify the 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.
BSI token	In the **Build Server Integration Token** field, specify the BSI token.
New Application and Release	Complete the following fields to create an application and/or release: • **Application Name**: specify the application name. If a unique value is provided, an application will be created. **Note:** If you are working with an existing application, updates to application settings will be applied where applicable. • **Business Criticality**: select the business criticality. • **Application Attributes**: specify required and optional application attributes as `<attributeName1>: <attributeValue1>; <attributeName2>: <attributeValue2>; ...` • **Application Type** (not applicable to existing applications): select the application type. • **Microservice Application** (not applicable to existing applications): select the check box to scan the application as a microservice application. The

Method	Procedure
	microservice feature must be enabled for the tenant. • **Microservice Name**: If the application consists of microservices, specify the microservice name. If a unique value is provided, a microservice will be created. **Note:** An application can have a maximum of 10 microservices. • **Release Name**: specify the release name. A unique value must be provided. • **SDLC Status**: select the SDLC status. • **Owner ID**: specify the owner ID.

7. In the **Entitlement Options** section, complete the following fields:

Field	Description
Entitlement Options	Select the method of determining the entitlement to use: • **User-selected entitlement**: the user specifies the entitlement. Provide the entitlement ID in the **Entitlement ID** field. • **Auto-selected entitlement**: Fortify on Demand determines the entitlement. 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.
Entitlement Preference	Select the entitlement preference.
Purchase Entitlements	(Optional, available for **Auto-selected entitlement**) Select the check box to purchase an entitlement if none is available for the specified entitlement preference. The purchase entitlements feature must be enabled for the tenant.

8. In the **Scan Options** section, complete the following fields:

> **Note:** Updates to scan settings are retained for subsequent scans.

Field	Description
Choose Scan Settings Source	Select the method of specifying the scan settings: - **Create/Override Existing Scan Settings if any** (required if you are creating a release) Complete the following fields: ○ **Assessment Type Id**: specify the assessment type ID ○ **Audit Preference**: select the audit preference - **Use Existing Saved Scan Settings**
Action if Scan In Progress	If the release has an in progress scan, select the action to take: - **Do Not Start Scan**: do not start a new scan and fail the task - **Cancel Scan In Progress**: cancel the scan in progress and start a new scan (if the scan in progress scan can be automatically canceled) - **Queue**: queue the scan (if the scan queue limit has been reached, the scan will be canceled)
Remediation Preference Type	Select whether to run a remediation scan.
Build Type	Select the method of packaging the application files. All selections except for **None** invoke the Fortify ScanCentral SAST client to package the application files.

9. Follow the procedure for the selected build type:

Field	Procedure
Go (ScanCentral)	**Open Source Component Analysis**: select the check box to include open source component analysis.[1]
Maven, Gradle	Complete the following fields: - **Technology Stack**: select the technology stack.[2] - **Language Level**: select the language level.[2] - **Open Source Component Analysis**: select the check box to include open source component analysis.[1,2]

Field	Procedure
	- **Build Command**: (Optional) specify custom build parameters for preparing and building a project. For example, to invoke a Gradle build before packaging: `-Prelease=true clean customTask build` - **Build File**: (Optional) specify the path on the agent where the build file is if you are not using a default name such as `build.gradle` or `pom.xml`. For example, `myCustomBuild.gradle` - **Include Tests**: (Optional) select the check box to include the test source set (Gradle) or a test scope (Maven) with the scan. - **Skip Build**: (Optional) select the check box to disable the project preparation build step before packaging.
DotNet, MSBuild	**Important!** Packaging using MSBuild is only available on Windows agents. The MSBuild executable must be added to the PATH environment variable. You can set the environment variable by running the Batch Script task before the Static Assessment task. Set `filename` to the path of `VsDevCmd.bat` and `modifyEnvironment` to `true`. For detailed instructions on configuring the Batch Script task, see https://docs.microsoft.com/en-us/azure/devops/pipelines/tasks/utility/batch-script?view=azure-devops. If you are using a Microsoft-hosted agent, see https://docs.microsoft.com/en-us/azure/devops/pipelines/agents/hosted?view=azure-devops&tabs=yaml to determine the path of `VsDevCmd.bat`. For example, for the Windows Server 2019 with Visual Studio 2019 agent, the path is `C:\Program Files (x86)\Microsoft Visual Studio\2019\Enterprise\Common7\Tools\VsDevCmd.bat`. Complete the following fields: - **Technology Stack**: select the technology stack.[2] - **Language Level**: select the language level.[2] - **Open Source Component Analysis**: select the check box to include open source component analysis.[1,2] - **Build Command**: (Optional) specify custom build parameters for

Field	Procedure
	preparing and building a project. - **Build File**: specify the path on the agent where the build file is located. For example, `mySolution.sln`. - **Skip Build**: (Optional, MSBuild only) select the check box to disable the project preparation build step before packaging. **Note: Skip Build** is not supported in Fortify ScanCentral SAST versions 21.1.2 and later.
PHP (ScanCentral)	**Open Source Component Analysis**: select the check box to include open source component analysis.[1]
Python	Complete the following fields: - **Python Version**: select the language level.[2] - **Open Source Component Analysis**: select the check box to include open source component analysis.[1,2] - **Python Virtual Environment**: Specify the Python virtual environment location. - **Python Requirements File**: specify the Python project requirements file to install and collect dependencies.
None	Complete the following fields: - **Technology Stack**: select the technology stack.[2] - **Language Level**: if applicable, select the language level.[2] - **Open Source Component Analysis**: select the check box to include open source component analysis.[1,2]

[1] If your tenant has Debricked entitlements, OpenText recommends using version 22.1.2 or later of the Fortify ScanCentral SAST client, which packages the files required for a Debricked open source scan. Otherwise, manually generate the files and include them in the payload. For instructions on generating these files, see the Fortify on Demand documentation.

[2] Available if you are configuring scan settings.

10. In the **Poll Options** section, complete the following fields:

Field	Description
Polling Interval	Specify the length of time in minutes between polling for static and open source scan statuses and results. The default value is 1. A value of 0 disables polling. **Note:** Polling stops once either the static or open source scan is canceled, paused, or completed.
Action if Failing Policy	Select whether to complete the task and throw a warning or fail the task based on the application security policy set by your organization.

11. Click **Add**.

    The YAML code for the task is added to your pipeline. The YAML code by default specifies the latest version of the extension.

12. Save the settings.

If a scan is successfully submitted during the pipeline run, the task will be marked as succeeded. If the scan is rejected, the build logs will display the appropriate error message.

Setting up a DAST Automated assessment

Perform the following tasks to set up a DAST Automated assessment:

- Prepare your web application. See "Preparing a web application for DAST Automated assessment" below.
- Configure dynamic scan settings. You can configure scan settings from the Fortify on Demand portal before submitting the assessment or from Azure DevOps as part of the task settings.
- Add the **FoD DAST Automated** task to a pipeline in an Azure DevOps project. See "Adding a DAST Automated assessment task" below.

Preparing a web application for DAST Automated assessment

The first step in a DAST Automated assessment is to prepare your web application. For instructions on preparing the web application, see the Fortify on Demand documentation.

Adding a DAST Automated assessment task

You can add the **FoD DAST Automated** assessment task to your pipeline using the classic editor or YAML editor in Azure DevOps. The following instructions describe how to add a DAST Automated assessment to a build pipeline through the YAML editor.

> **Note:** You can use the classic editor or YAML editor to define build pipelines; use the classic editor to define release pipelines.

To add a DAST Automated assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Select **FoD DAST Automated** from the list.

   The DAST Automated assessment task settings appear.
4. Complete the following fields:

Field	Description
Fortify Connection	Select an existing service connection or click **+New** to add a new service connection. For more information, see "Adding Fortify on Demand credentials in Azure DevOps" on page 16.

5. In the **Application/Release Options** section, select the method of identifying the release from the **Pick a Release** list:
   - **Release ID**
   - **New Application and Release**
6. Follow the procedure for the selected method:

Method	Procedure
Release Id	In the **Release ID** field, specify the 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.
New Application and Release	Complete the following fields to create an application and/or release: • **Application Name**: specify the application name. If a unique value is provided, an application will be created. **Note:** If you are working with an existing application, updates to application settings will be applied where applicable. • **Business Criticality**: select the business criticality. • **Application Attributes**: specify required and optional application attributes as `<attributeName1>: <attributeValue1>; <attributeName2>: <attributeValue2>; ...` • **Application Type** (not applicable to existing applications): select the application type. • **Microservice Application** (not applicable to existing applications): select

	the check box to scan the application as a microservice application. The microservice feature must be enabled for the tenant. • **Microservice Name**: If the application consists of microservices, specify the microservice name. If a unique value is provided, a microservice will be created. **Note:** An application can have a maximum of 10 microservices. • **Release Name**: specify the release name. A unique value must be provided. • **SDLC Status**: select the SDLC status. • **Owner ID**: specify the owner ID.

7. In the **Entitlement Options** section, complete the following fields:

Field	**Description**
AssessmentType Id	Specify the DAST Automated assessment type ID.
Entitlement ID	Specify the entitlement ID that the assessment will use.
Entitlement Frequency	Specify the entitlement frequency: **Single Scan**, **Subscription**. Note that microservice applications are restricted to subscriptions.

8. In the **Scan Options** section, complete the following fields:

Field	**Description**
Choose Scan Settings Source	Select how scan settings are specified: • **Create/Override Existing Scan Settings if any** (required if you are creating a release) **Note:** Updates to scan settings are retained for subsequent scans. • **Use Existing Saved Scan Settings**
Scan Type	Select the dynamic scan type: • **Website**: this scan is similar to a Dynamic Website scan.

Field	Description
	- **Workflow Driven**: this scan is similar to a Dynamic Website scan that utilizes a workflow macro. - **API**: this scan is similar to a Dynamic API scan.

9. If you selected **Create/Override Existing Scan Settings if any**, complete the following fields. Otherwise, skip to the next step. Fields are not described in the order of presentation in the UI.

Scan type	Field	Description
All scan types	Environment Facing	Select whether the site is internal or external.
All scan types	Time Zone	Select your location's time zone, which is used to schedule the scan's start time.
All scan types	Request False Positive Removal (optional)	Select the check box to request false positive removal by the testing team once per application. **Important!** Login macro generation and false positive removal are an optional service that is available once per application and consumes 1 additional assessment unit. **Important!** If you want to request both login macro generation and false positive removal, you must select both options together; once a scan that includes either option has completed, both options will be disabled for subsequent scans.
API	API Type	Select the API definition type: **Postman**, **OpenApi**, **Graph QL**, **GRPC**. Perform the relevant task based on your API definition type: **Note:** OpenAPI Specification versions 2.0 and 3.0 are supported.

Scan type	Field	Description
		Postman Specify the file ID of the uploaded file in the **Postman Collection** field.
		OpenAPI Select **File** or **URL to the OpenAPI specification** and perform the relevant task based on your selection. • **File** i. Specify the file ID of the uploaded file in the **OpenApi Json File** field. ii. If the API requires authentication, provide the API key value in the **API Key** field. **Note:** The supported security scheme is API key. Multiple API keys in requests are not supported. • **URL to the OpenAPI specification** i. Specify the OpenAPI document URL in the **OpenApi Url** field. ii. If the API requires authentication, provide the API key value in the **API Key** field. **Note:** The supported security scheme is API key. Multiple API keys in requests are not supported.
		GraphQL Select **File** or **URL** and perform the relevant task based on your selection. • **File** i. Specify the file ID of the uploaded file in

Scan type	Field	Description
		the **GraphQL Json File** field. ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. iii. Specify the URL or hostname In the **API Host** field. iv. Specify the directory path for the API service in the **API Service Path** field. - **URL** i. Provide the GraphQL introspection endpoint URL in the **GraphQL Url** field. ii. Select the API scheme in the **API Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. iii. Specify the URL or hostname In the **API Host** field. iv. Specify the directory path for the API service in the **API Service Path** field. **Note:** The GraphQL API must have introspection enabled to download the schema contents for the scan.
		gRPC a. Specify the file ID of the uploaded file in the **GRPC Proto File** field. b. Select the API scheme in the **Scheme Type** field: **HTTP**, **HTTPS**, **HTTP and HTTPS**. c. Specify the URL or hostname In the **API Host** field. d. Specify the directory path for the API service in the **API Service Path** field.

Scan type	Field	Description
Website	Dynamic Site URL	Provide your site's URL.
Website	Scope	Select one of the following options: • **Scan entire host (*<URL>*)** (default): the entire host will be scanned **Example**: Given https://foo.com/home, the following URLs will be included: ○ https://foo.com/ ○ https://foo.com/contact-us.html ○ https://foo.com/folder/ ○ https://foo.com/folder/folder2/page.aspx ○ https://foo.com/home/folder/ ○ https://foo.com/home/index.html • **Restrict scan to a URL or sub folder**: only the directory denoted by the last slash in the URL and its subdirectories will be scanned. **If you select this option, make sure the last slash denotes the directory to which you want the scan to be restricted.** **Example**: Given https://foo.com/home/, the following URLs will be excluded: ○ https://foo.com/ ○ https://foo.com/folder/ ○ https://foo.com/contact-us.html ○ https://foo.com/folder/folder2/page.aspx
Website	Redundant Page Direction (optional)	Select the check box to enable comparison of page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources.

Scan type	Field	Description
		Important! Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.
Website	Exclude URLs (optional)	Specify full or partial URLs to exclude URLs matching the strings as `<Url1>; <Url2>; <Url3>; ...`The field is not case-sensitive.
Options depend on scan type	Scan Policy	Select the policy (collection of vulnerability checks and attack methodologies that the sensor deploys against a Web application): **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers. **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers. **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error

Scan type	Field	Description
		messages, and others of a similar nature. **API**: The API policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.
Website API	Timebox Scan Duration (Hours)	Specify the maximum duration of the scan. If the scan is not completed at the end of the specified duration, the scan is terminated and partial results are available. If the scan is completed during the specified duration, then complete results are available. Incremental scanning is not supported.
All scan types	Network Authentication (optional)	Select the check box if network authentication is required. Provide the authentication type, username, and password. **Note:** The scan will be canceled if network authentication fails.
Website	Site Authentication (optional)	Select the check box if site authentication is required. Specify the file ID of the uploaded file in the **Login Macro File for Site Authentication** field. **Note:** Make preparations so that the user credentials remain valid for the scan duration, such as increasing the password expiration duration. The scan will be

Scan type	Field	Description
		canceled if site authentication fails.
Website	RequestForLoginMacroCreation(optional)	Select the check box to request generation of a login macro by the testing team once per application. Upon scan completion, the login macro will be available for download on the Scans page. **Important!** Login macro generation and false positive removal are an optional service that is available once per application and consumes 1 additional assessment unit. **Important!** If you want to request both login macro generation and false positive removal, you must select both options together; once a scan that includes either option has completed, both options will be disabled for subsequent scans.

10. In the **Poll Options** section, complete the following fields:

Field	Description
Polling Interval	Specify the length of time in minutes between polling for static and open source scan statuses and results. The default value is 1. A value of 0 disables polling. **Note:** Polling stops once either the static or open source scan is canceled, paused, or completed.
Action if Failing Policy	Select whether to complete the task and throw a warning or fail the task based on the application security policy set by your organization.

11. Click **Add**.

    The YAML code for the task is added to your build pipeline. The YAML code specifies the latest version of the extension.

12. Save the settings.

If a scan is successfully submitted during the pipeline run, the task will be marked as succeeded. If the scan is rejected, the build logs will display the appropriate error message.

Troubleshooting Fortify on Demand tasks

Task fails with error "SyntaxError: Use of const in strict mode"

Problem: The task fails with the following error:

```
const tl = require('vsts-task-lib/task');
^^^^^
SyntaxError: Use of const in strict mode
```

Cause: The version of `node.exe` in the VSO agent folder is earlier than 5.0. To check the version of `node.exe` installed for the agent, search for "node.exe" in the VSO agent folder, then run `[path to node.exe]\node -v`.

Solution: Manually update the node in the VSO agent folder to version 5.0 or later.

Static Assessment task fails with error "The process 'C:\hostedtoolcache\windows\scancentral\21.1.2\x64\bin\scancentral.bat' failed with exit code 1"

Issue: The Static Assessment task fails with the following error: `The process 'C:\hostedtoolcache\windows\scancentral\21.1.2\x64\bin\scancentral.bat' failed with exit code 1`. The ScanCentral log contains the following error: `java.io.IOException: Cannot run program "msbuild.exe": CreateProcess error=2, The system cannot find the file specified`.

Cause: The MSBuild executable was not added to the PATH environment variable.

Solution: Set the environment variable by running the Batch Script task. For more information, see "Adding a Static Assessment task" on page 18.

Getting started with Fortify ScanCentral SAST

You can submit your project to Fortify ScanCentral SAST for remote static analysis (translation and scan). You can also upload and view the results in Fortify Software Security Center. See "Adding a Fortify ScanCentral SAST Assessment task" on page 36. With this task, you do not need to install Fortify Static Code Analyzer on the Azure DevOps agent.

> **Note:** To run the translation locally and offload only the scan phase to Fortify ScanCentral SAST, use the Fortify Static Code Analyzer Install task and the Fortify Static Code Analyzer Assessment task (see "Getting started with Fortify Static Code Analyzer" on page 9).

Requirements for the Fortify ScanCentral SAST task

Make sure that your environment meets the requirements described in this section to use Fortify ScanCentral SAST task in your build. This section also includes preparation steps and information required to have on hand to use the task.

- The Fortify ScanCentral SAST task is available with Fortify ScanCentral SAST versions 20.2.0 or later.
- To trigger a build failure based on the scan results, you must use Fortify ScanCentral SAST version 22.1.0 or later (see "Upload results to SSC" on page 37).
- Fortify ScanCentral SAST runs on a Java Virtual Machine. Make sure that you have a Java Virtual Machine installed on the agent. You can use the Java tool installer task in your pipeline to install it.

  > **Note:** You can run the Fortify ScanCentral SAST Assessment task on a Microsoft-hosted agent that might already have a Java Virtual Machine installed.

- Java 17 must be installed on the agent for Fortify ScanCentral SAST client version 23.2.0 or later.
- To connect to Fortify ScanCentral SAST, you must have one of the following:
  - The Fortify ScanCentral SAST Controller URL
  - The Fortify Software Security Center URL and a Fortify Software Security Center authentication token of type CIToken (the task determines the Controller information from Fortify Software Security Center)

    Define an Azure DevOps variable that contains the decoded value of this token. By default, the extension uses a variable with the name `ScanCentral.SscCiToken`.
- If the Fortify ScanCentral SAST Controller or Fortify Software Security Center URL uses SSL with a self-signed or untrusted certificate, you might need to add the certificate to the trusted certificates as follows:
  - On the agent's certificate store—To allow the Fortify Azure DevOps Extension to download and install the Fortify ScanCentral SAST client. See the Azure DevOps documentation for how to run with a self-signed certificate.
  - In the Java keystore—To allow the Fortify ScanCentral SAST client to connect to Fortify ScanCentral SAST Controller and Fortify Software Security Center. Use the Java keytool to import a trusted certificate.
- Define an Azure DevOps variable that contains value of the Fortify ScanCentral SAST `client_auth_token` property for the Controller. By default, the extension uses a variable with the name `ScanCentral.ClientToken`.
- Your project must be in one of the supported languages. For a list of languages that are supported for project translation, see the *Fortify Software System Requirements* in Fortify Software Security Center Documentation.

Adding a Fortify ScanCentral SAST Assessment task

Use the **Fortify ScanCentral SAST Assessment** task to perform a remote Fortify Static Code Analyzer analysis using Fortify ScanCentral SAST as part of your build. The project is automatically packaged and then uploaded to Fortify ScanCentral SAST for security analysis. You can also upload the scan results to Fortify Software Security Center.

This task automatically installs a Fortify ScanCentral SAST client from the Fortify ScanCentral SAST Controller on the agent if it is not already installed. In addition, if the Controller version you are using is newer than the Fortify ScanCentral SAST client already installed on the agent, then the task automatically installs the newer version. Make sure that you have enabled auto-updates of Fortify ScanCentral SAST clients from the Controller. The Fortify ScanCentral SAST client is installed in the Azure DevOps Pipelines tool cache.

For detailed information about how to use Fortify ScanCentral SAST, see *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* in Fortify Software Security Center Documentation.

To configure a Fortify ScanCentral SAST Assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Find and add the **Fortify ScanCentral SAST Assessment** task.
4. In the **Server Information** section, provide the information described in the following table.

Field	Description
ScanCentral Controller URL	(Optional) Type the URL for the Fortify ScanCentral SAST Controller. The correct format for the Controller URL is: `<protocol>://<controller_host>:<port>/scancentral-ctrl` (for example: `https://myControllerHost.com:8443/scancentral-ctrl`). **Note:** If you do not provide the Controller URL, then you must provide the SSC URL and the SSC continuous integration token.
ScanCentral client authentication token	Type a defined variable that contains the value of the `client_auth_token` property for the Fortify ScanCentral SAST Controller. This secures the Controller for authorized clients only. See *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* in Fortify Software Security Center Documentation for more information.
SSC URL	(Optional) Type the URL for the Fortify Software Security Center server. **Note:** The **SSC URL** is required if you are uploading the scan results to

Field	**Description**
	Fortify Software Security Center and if you do not provide a Fortify ScanCentral SAST Controller URL.
SSC continuous integration token	Type a defined variable that contains the decoded value of a Fortify Software Security Center authentication of type CIToken. **Note:** The **SSC continuous integration token** is required if you provide an **SSC URL** and if you are uploading scan results to Fortify Software Security Center.
Upload results to SSC	(Optional) To upload the scan results (FPR file) to Fortify Software Security Center, do the following: a. Select **Upload results to SSC**. b. Specify an application version that exists in Fortify Software Security Center by providing one of the following: ○ An application name and an application version name. ○ A Fortify Software Security Center application version ID. **Note:** If you provide both application name and version and an application ID, the extension uses the application ID for the upload regardless of the selected application version type. c. (Optional) To trigger a build failure based on the scan results, type a search query in the **Build failure criteria** box. For example, the following search query causes the build to fail if any critical issues exist in the scan results: `[fortify priority order]:critical` See *OpenText™ Fortify Software Security Center User Guide* in Fortify Software Security Center Documentation for a description of the search query syntax. By default, the task returns a warning when the build failure criteria is met. To fail the build instead, select **FAIL** from the **Task results when build failure criteria is met** list. d. (Optional) To specify how long to poll Fortify Software Security Center to determine if FPR processing is finished, type the time in minutes in

Field	Description
	the **Polling timeout** box. If no value or a value of 0 is specified, polling continues until FPR processing finishes or stops due to errors. The valid values are 0–10080. e. (Optional) To specify how frequently to poll Fortify Software Security Center to determine if the FPR processing is finished, in the **Polling interval** box, specify an interval (in minutes). The valid values are 1–60 and the default value is 1 minute.

5. In the **Translation Options** section, select the name of the build tool used to build the project.
   a. For Gradle, Maven, or MSBuild, provide the information described in the following table.

Field	Description
Build command	(Optional) Type any custom build commands to prepare and build the project. If not specified, the default build command is used.
Build file	(For Gradle or Maven) Type the name of the build file if it is different than the default of `build.gradle` or `pom.xml`. (For MSBuild) Type the name of the build file.
Skip build	Select whether to skip the build invocation that prepares the generated sources and libraries before the project information is packaged for submission to Fortify ScanCentral SAST. **Note:** This setting is only valid with Gradle and Maven in Fortify ScanCentral SAST versions 21.1.2 and later.
Include test	(For Gradle and Maven projects only) Select whether to include the test source set (Gradle) or a test scope (Maven) with the scan.
Exclude disabled projects	(For MSBuild projects only) Select whether to skip projects that are either explicitly excluded from the build in the solution or skipped during the build due to platform and configuration settings. **Note:** This setting is only valid with Fortify ScanCentral SAST versions 21.1.2 and earlier.

   b. If you selected **none** for the build tool, provide the information described in the following table.

Field	**Description**
Include node_modules dependencies	(Optional) Select whether to restore dependencies to the node_modules directory before the scan.
Python version	(Optional) Select the Python version for Python projects.
Python requirements file	(Optional) Type the name of the Python project requirements file used to install and collect dependencies. Use only this Python field if you have no preference for the Python version used or there is only one Python version installed and on the PATH.
Python virtual environment	(Optional) Type the location (directory) of the Python virtual environment. Specify this together with the Python requirements file to have dependencies restored before the scan.
PHP version	(Optional) Type the PHP version used in the project.
Translate Apex project	Select this option if your project consists of Apex and Visualforce code.
Translate SQL project	Select this option if your project is an SQL project and then select if your project is **PL/SQL** or **T-SQL**.

6. (Optional) In the **Scan Options** section, provide the information described in the following table.

Field	**Description**
Filter file	Type the name of a filter file to filter out specific vulnerability categories, rules, and vulnerability instances from the analysis. For more information, see *OpenText™ Fortify Static Code Analyzer User Guide* in Fortify Static Code Analyzer and Tools Documentation.
Issue template	Type an issue template to include for the scan. An issue template determines how issues uncovered in your project are filtered and sorted.
Custom Rulepacks	Specify any custom rules files (`*.xml`) separated by spaces or specify a directory that contains custom rules.

7. (Optional) In the **Advanced Options** section, provide the information described in the following table.

Field	Description
Notification email	Type the email address to which the Fortify ScanCentral SAST Controller will send notifications.
Sensor pool UUID	To target a specific sensor pool for the scan, specify the sensor pool UUID. You can obtain the UUID for sensor pools from the ScanCentral SAST **Sensor Pools** page in Fortify Software Security Center. By default, Fortify ScanCentral SAST uses the default sensor pool as defined in Fortify Software Security Center.
Wait for scan to finish	Select whether to have this task wait until the scan is complete and the results are downloaded to the DevOps agent. If selected, then you can provide the following: • In the **Results file** box, type a name for the Fortify results file (FPR). For example, `MyProjectA.fpr`. The file is saved in the working folder unless you specify an absolute path. • In the **Log file** box, type a name for the local log file. The file is saved in the working folder unless you specify an absolute path. • Select **Overwrite** to replace any existing results file (*.fpr) or log file with new data. Otherwise, existing files are not overwritten and the results are not downloaded to the agent. A message will indicate if this happens.
Quiet	Select this option to prevent execution statements from being written to stdout during the build.

Troubleshooting the Fortify ScanCentral SAST task

Unable to open the FPR file in the email notification from Fortify ScanCentral SAST

You can use Postman or cURL (available on Windows 10) to download the FPR or log file mentioned in the email notification from Fortify ScanCentral SAST.

To use Postman to download the FPR or log file:

1. Copy the URL for the FPR or the log file from the notification email.
2. Paste the URL in the Postman URL text field and then add `fortify-client` in the HTTP header.

3. Click **Send and Download**.
4. Save the file.

Unsupported class version error

If Fortify ScanCentral SAST client is run with an unsupported Java version (see "Requirements for the Fortify ScanCentral SAST task" on page 35), the following message appears in the log file:

```
java.lang.UnsupportedClassVersionError:
com/fortify/scancentral/launcher/Launcher has been compiled by
a more recent version of the Java Runtime...
```

If you are using Fortify ScanCentral SAST client version 22.2.0 and later, set the SCANCENTRAL_JAVA_HOME environment variable to point to the supported Java version. Alternatively, make sure that the correct Java version is installed on the agent. If multiple Java versions are available on the agent, make sure the pipeline that runs the Fortify ScanCentral SAST task has PATH or JAVA_HOME environment variables that point to the supported Java version.

Failure with a self-signed certificate error

You are connecting to Fortify ScanCentral SAST Controller or Fortify Software Security Center using SSL with a self-signed or untrusted certificate. Add the certificate to to both the agent certificate store and the Java keystore (see "Requirements for the Fortify ScanCentral SAST task" on page 35).

Getting started with Fortify ScanCentral DAST

You can submit your Web application to Fortify ScanCentral DAST for a dynamic scan and view the results in Fortify Software Security Center. See "Adding a Fortify ScanCentral DAST Assessment task" on the next page.

Requirements for the Fortify ScanCentral DAST task

Make sure that your environment meets the requirements described in this section to use Fortify ScanCentral DAST task in your build. This section also includes preparation steps and information required to have on hand to use the task.

Fortify ScanCentral DAST Requirements

- You must use Fortify Software Security Center and Fortify ScanCentral DAST version 20.2.0 or later.
- You must have the Fortify ScanCentral DAST API URL.
- If the ScanCentral DAST API uses SSL with a self-signed or untrusted certificate, verify that the ScanCentral DAST API URL is accessible from the Azure DevOps agent. You might need to add the

certificate to the trusted certificates on the agent.

- You must have a CI/CD identifier for the Web application you want to scan.

Adding a Fortify ScanCentral DAST Assessment task

Use the **Fortify ScanCentral DAST Assessment** task to perform a scan of your Web application as part of your build. After you run the build and the scan is complete, the scan results are available in Fortify Software Security Center. For more information about configuring and using Fortify ScanCentral DAST, see *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide* in Fortify ScanCentral DAST Documentation for versions 20.2.0 and later.

To configure a Fortify ScanCentral DAST Assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Find and add the **Fortify ScanCentral DAST Assessment** task.
4. Provide the information described in the following table.

Field	**Description**
ScanCentral DAST API URL	Specify the URL and port where the DAST API service runs in the format `<protocol>://<DAST_API_hostname>:<port>/api` or `<protocol>://<DAST_API_IP_address>:<port>/api`.
CI/CD identifier	Specify a scan settings identifier GUID. This is also known as the Settings Identifier.
SSC continuous integration token	Specify an Azure DevOps variable that contains the decoded value of a Fortify Software Security Center authentication token of type CIToken.
Overrides	(Optional) Fortify ScanCentral DAST scan setting overrides (JSON format).

Getting started with Fortify WebInspect

- Install an agent on a Virtual Machine.
- Install an instance of Fortify WebInspect on the agent.
- Configure and start the Fortify WebInspect API on the agent.
- Create a Scan Settings file on the agent to be used during the scan.

For more information about how to install and configure Fortify WebInspect, see the installation and the user guide in Fortify WebInspect Documentation.

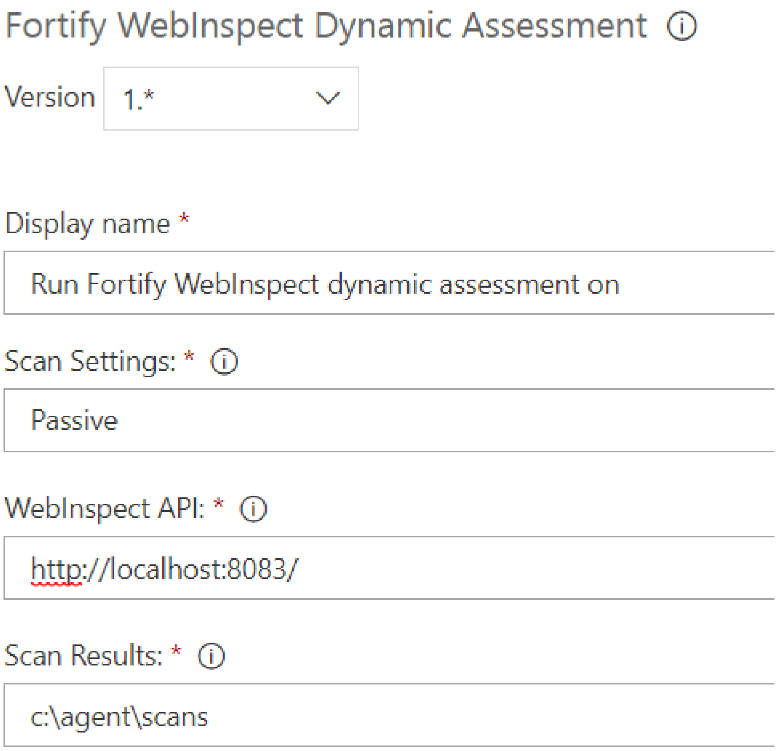
Setting up a Fortify WebInspect Dynamic Assessment

To configure a Fortify WebInspect Dynamic Assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Find and add the **Fortify WebInspect Dynamic Assessment** task.
4. In the **Scan Settings** box, type the name of the settings file to use in the scan.
5. In the **WebInspect API** box, type `http://<hostname>:<port>/`, where *<hostname>* and *<port>* identify where the WebInspect API is installed.

   > **Important!** You must specify the WebInspect API location. The task will not start without this information.

6. In the **Scan Results** box, type the location where you want the scan results written.



Fortify WebInspect Dynamic Assessment ⓘ

Version: 1.*

Display name *: Run Fortify WebInspect dynamic assessment on

Scan Settings: * ⓘ: Passive

WebInspect API: * ⓘ: http://localhost:8083/

Scan Results: * ⓘ: c:\agent\scans

For more information about the WebInspect API, see the API documentation at `http://<hostname>:<port>/webinspect/api` on the agent where Fortify WebInspect is installed. If you used the default settings when configuring the Fortify WebInspect API, then type `http://localhost:8083/webinspect/api`.

Troubleshooting the Fortify WebInspect Dynamic Assessment task

If the Fortify WebInspect Dynamic Assessment task fails to start, you might need to stop the Fortify Monitor program on the agent and restart it with Administrator privileges.

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 Azure DevOps Extension 9.4)

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!