Micro Focus
Fortify Azure DevOps Extension

Software Version: 8.9

User Guide

Document Release Date: November 2022
Software Release Date: November 2022

MICRO FOCUS®

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 2019 - 2022 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 November 02, 2022. 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-and-services/documentation

Contents

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/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 Micro Focus Product Documentation website:

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

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

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

Fortify Product Feature Videos

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

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

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
8.9	Updated: "Adding a Static Assessment Task" on page 25 - Added information on packaging files required for Debricked open source scans.
8.8	Updated: • "Adding a Static Assessment Task" on page 25 - Updated polling to poll for static and Sonatype scan statuses and results; removed support for release pipelines
8.6	Updated: • "Adding a Fortify Static Code Analyzer Scan as a Build Step" on page 12 and "Adding a Fortify ScanCentral SAST Assessment as a Build Step" on page 47 - Changes made for uploading scan results to Fortify Software Security Center including the ability to trigger a build failure based on the scan results
8.5	Updated: • "Adding a Static Assessment Task" on page 25 - Removed requirement to use the Fortify ScanCentral SAST client to package .NET, Go, and PHP projects
8.4	Added: • "Adding a Static Assessment Task" on page 25 - New option to specify the Fortify ScanCentral SAST client path and support for packaging Go projects with the Fortify ScanCentral SAST client • "Downloading and Installing the Fortify ScanCentral SAST Client" on page 21 - Instructions for downloading and installing the Fortify ScanCentral SAST client
8.0	Added:

Software Release / Document Version	Changes
	• "Adding a Static Assessment Task" on page 25 - New options to create an application and release, specify an entitlement, configure scan settings, and invoke Fortify ScanCentral SAST to package application files Updated: • "Adding a Fortify ScanCentral SAST Assessment as a Build Step" on page 47 - New option to specify a sensor pool
7.0.0	Added: • "Getting Started with Fortify ScanCentral SAST and Fortify ScanCentral DAST" on page 45 - Descriptions of the tasks to run static and dynamic scans with Fortify ScanCentral SAST and Fortify ScanCentral DAST, respectively
6.0.1	Added: • "Adding a Static Assessment Task" on page 25 - Added the option to queue a new scan if a scan is in progress

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 provides instructions for 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	Description	More information
Fortify Static Code Analyzer Install	The Fortify Static Code Analyzer Installation task automatically installs and configures Fortify Static Code Analyzer.	"Getting Started with Fortify Static Code Analyzer" on page 10
Fortify Static Code Analyzer Assessment	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 an existing Fortify Software Security Center server for enterprise vulnerability management.	"Getting Started with Fortify Static Code Analyzer" on page 10
Fortify on Demand Static	The Fortify on Demand Static	"Getting Started with

Task	Description	More information
Assessment	Assessment task submits a static scan request and uploads code to Fortify on Demand as a build step. The scan results are available in Fortify on Demand.	Fortify on Demand" on page 17
Fortify on Demand Dynamic Assessment	The Fortify on Demand Dynamic Assessment task submits a 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 17
Fortify ScanCentral SAST Assessment	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 and Fortify ScanCentral DAST" on page 45
Fortify ScanCentral DAST Assessment	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 SAST and Fortify ScanCentral DAST" on page 45
Fortify WebInspect Dynamic Assessment	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 53

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 the *Micro Focus 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. Fortify 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 (formerly Fortify CloudScan). 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 Scan as a Build Step" on page 12).
- 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 *Micro Focus 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). Fortify 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 Scan as a Build Step

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 Fortify Support log file.
Enable debug logging	(Optional) Select whether to include debug information in the Fortify Support log file, which is useful for Micro Focus Fortify 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 the *Micro Focus Fortify Static Code Analyzer User Guide* in Fortify Static Code Analyzer and Tools Documentation for more detailed 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 10.

   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 10.

      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 the *Micro Focus 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.

Setting Up Fortify on Demand Credentials in Azure DevOps

Before adding a static assessment task or dynamic assessment task to your pipeline, you need to obtain appropriate Fortify on Demand credentials and add them in Azure DevOps. Perform the following tasks to set up Fortify on Demand credentials in Azure DevOps:

- Create an API key pair (Security Leads only) or personal access token with the `api-tenant` scope in Fortify on Demand. See "Creating an API Key" below or "Creating a Personal Access Token" on the next page.

- Add Fortify on Demand credentials in Azure DevOps. See "Adding Fortify on Demand Credentials in Azure DevOps" on page 20.

Creating an API Key

To create a dedicated API key:

1. Select the **Administration** view.

   The User Management page appears.

2. Click **Settings**.

   The **Attributes** tab of the Settings page appears.

3. Select the **API** tab.

4. Click **+Add Key**.

   The **Add/Edit Key for Application** window opens.

5. Complete the fields. Fields are required unless otherwise noted.

Field	Description
Application Name	Name of your application.
Role	Select the role that has the appropriate API Key permissions. See API Key Roles.
Authorize app to use API	Select **Yes** to enable the key. Select **No** to disable key if it is not in use.

6. Click **Save**.

   The Secret Key window opens.

7. Copy your Base64 encoded secret code. The secret code is only shown once.

8. Click **Close**.

   The new API key appears in the API key list.

Creating a Personal Access Token

To create a personal access token:

1. Click your account name and select **Personal Access Tokens**.

   The Personal Access Tokens page appears.

2. Click **+Add Personal Access Token**.

The Add/Edit Personal Access Token window opens.

3. Complete the fields. Fields are required unless otherwise noted.

Field	Description
Name	Type a name for the token.
Authorize to use API	The token is enabled by default. Move the slider to **No** to disable the token.
Secret Expiration Date, **Secret Expiration Days**	Use the calendar to select an expiration date or type the number of days after which a secret expires. The token will expire at 00:00 PT of the date you set. The expiration date cannot exceed the maximum lifetime as set by the portal.
Allowed Scopes	Select the allowed scopes for the token. For more information on scopes, see API Scopes.

4. Click **Save**.

   The Secret Key window opens.

5. Copy your Base64 encoded secret. The secret is only shown once.

6. Click **Close**.

The new token appears in the personal access token list.

Adding Fortify on Demand Credentials 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** or **Token Based Authentication**.
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 • FedRAMP: https://api.fed.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.
API Key, API Secret Username, Personal Access Token, Tenant ID	• If you selected **Basic Authentication**, Specify the account username, personal access token, and tenant ID. • 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 Micro Focus 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 in Fortify on Demand. See "Configuring a Static Scan" below. This part is optional if you are configuring static scan settings from the Fortify on Demand Static Assessment task.

- Add the Fortify on Demand Static Assessment task to an Azure DevOps pipeline. See "Adding a Static Assessment Task" on page 25.

Downloading and Installing the Fortify ScanCentral SAST Client

Fortify offers a stand-alone Micro Focus Fortify ScanCentral SAST client for automatically packaging the source code and necessary dependencies required for static and Debricked open source scans. The following languages are supported for packaging: .NET and .NET Core (MSBuild projects), Go, Java (Gradle and Maven projects), PHP, and Python.

> **Note:** Packaging of files for Debricked scans is available in the Fortify ScanCentral SAST client 22.1.2 or later.

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

For more information about using the Fortify ScanCentral SAST client, see the following links at Fortify Software Security Center Documentation:

- Fortify ScanCentral SAST client software requirements
- Supported build tools for Fortify ScanCentral SAST (see the "Build Tools" section)
- Fortify ScanCentral SAST command-line options (see the "Package Command" section)

> **Note:** 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 on Demand only uses the packaging feature of the Fortify ScanCentral SAST client.

Configuring a Static Scan

After preparing your application files for a static assessment, you need to configure the static scan settings. You only need to configure the static scan settings once per release as your settings are carried over to the next scan. You can edit settings as needed for subsequent assessments.

To configure a static scan:

1. Select the **Applications** view.

   Your Applications page appears.

2. Click the name of the application.

   The Application Overview page appears.

3. Click **Start Scan** for the release that you want to have assessed and select **Static**.

   The Static Scan Setup page appears.

4. Complete the fields as needed. Fields are required unless otherwise noted.

Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed. The SLO of the selected assessment type appears below the field.
Entitlement	Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. Note that microservice applications are restricted to subscriptions. If the release has an active subscription, only options that do not consume entitlements are displayed. **Note:** If you select an entitlement offered through a Dynamic Premium or Mobile Premium assessment, the assessment is activated and the full cost of the entitlement is deducted.
Source or Compiled Code/Files	Select the method of uploading the payload. • **Manual Upload** (default): Manually upload the payload from your local system. • **Source Control**: Upload the payload from a version control platform. This option is only available if source control has been configured.
Technology Stack	Select the application's technology stack. The languages available for selection depends on the application type (web/thick client or mobile) and whether the application is a microservice application.
Language Level	If applicable, select the technology stack's language level from the list.
Open Source Component Analysis by Sonatype	(Optional) Select the check box to include a Sonatype analysis of open source components and associated security issues.
Scan Binary	**Note:** Contact support to enable the option. (Optional) Select the check box to have compiled and source code files scanned. This option is available for Java and .NET technology stacks. **Note:** If the source code inclusion requirement is enabled and this

	option is not selected, the scan will be cancelled if the payload does not contain source code. **Note:** Scanning binary files is not supported for ScanCentral-packaged payloads.
Audit Preference	Select the audit preference. • **Manual**: A security expert manually reviews the scan results and removes false positives. • **Automated**: False positives identified by Fortify Scan Analytics with high confidence are automatically suppressed and results are published without manual review. **Note**: Fortify Scan Analytics is only applied to new issues found in a scan using automated audit. The ability to select audit preference depends on the assessment type: • A Static single scan allows Automated only. • A Static subscription allows one Manual audit per application (not per release or microservice). • A Static+ single scan allows Manual only. • A Static+ subscription allows Automated or Manual audit for each assessment.
Scan third-party libraries for static security assessment	**Note:** Contact support to enable the option. (Optional) Select the check box to have third party libraries scanned for vulnerabilities, which will be included in the scan results. This significantly increases the turnaround time. This option is not available for microservice applications. **Note:** Selecting this option infers that your organization has received consent from all third-party vendors to scan their libraries.
Release ID	Once the static scan settings have been saved, the release ID can be used to submit a static scan using CICD tools. The release ID serves as a token that retrieves the most recently saved scan settings in the portal.

	Important! The release ID replaces the BSI token. Migrate build configurations to the release ID at your earliest convenience.
Build Server Integration	Once the static scan settings (assessment type, technology stack, language level, audit preference, open source component analysis, and include third party libraries) have been configured, a token is automatically populated in the **Build Server Integration** field. The token can be used to submit a static assessment using external tools. **Note:** The BSI token is persistent across assessments of a release.

5. Click **Save**.

   Your static scan settings are saved.

6. If you have the Consume Entitlements permissions and selected a subscription entitlement, click **Start Subscription** to start the static assessment subscription and consume the entitlement without starting a scan.

   Note: Contact support to enable the option.

   Note: The assessment cost is deducted from the entitlement when a user starts the initial scan.

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 will fail. For more information, see Fortify ScanCentral SAST Client and Sensor Requirements.
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 20.

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	Complete the following fields to create an application and/or release:

Method	Procedure

Application and 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
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.

Field	Description
	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

Field	Description
	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] • **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.
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.

Field	Procedure
	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 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) select the check box to disable the project preparation build step before packaging. Note: **Skip Build** is not valid with 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.

Field	Procedure
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, Fortify 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. If you are not using the Fortify ScanCentral SAST client 22.1.2 or later, 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.

Adding a FedRamp Static Assessment Task (Deprecated)

If you are a FedRAMP user and you want to use the basic scan options, add the **FedRamp - FOD Static Assessment** task to your pipeline. The following instructions describe how to add a FedRamp static assessment task to a build pipeline using the YAML editor.

> **Note:** Build pipelines can be defined using the classic editor or YAML editor; release pipelines can be defined using the classic editor.

To add a FedRamp static assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Select **FedRamp - FOD Static Assessment** in the **Tasks** list.

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

Field	Description
Source code location	Provide the path on the agent where the source code files are located. You can also use predefined variables to specify the source code directory. Do not use `$(Build.ArtifactStagingDirectory)` or `$(Build.ArtifactDirectory)`, as these locations can cause errors when compressing the source code prior to transmission.
Build Server Integration Token	Provide the BSI token.

5. In the **Authentication Methods** section, complete the following fields:

Field	Description
API Authentication Type	a. Select the method of authentication: **API Key/Secret** or **Personal Access Token**. b. Provide the API key and secret or your account username, personal access token, and tenant ID. Fortify recommends using secret build variables to specify the Fortify on Demand credentials.
Proxy host	(Optional) Type the URL of the proxy server.
Proxy port	(Optional) Type the port of the proxy server.

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

Field	Description
Entitlement Preference	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.
Purchase Entitlements	Select the check box 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 build logs will display an error message.
Prefer Remediation	Select the check box to run a remediation scan if one is available.

7. Click **Add**.

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

8. Save the settings.

If a scan is successfully submitted during the pipeline run, the task is marked as succeeded and the Fortify on Demand Scans pages display a new scan for the release.

Setting Up a Fortify on Demand Dynamic Assessment

Perform the following tasks to set up a Fortify on Demand dynamic assessment:

- In Fortify on Demand, configure dynamic scan settings. See "Configuring a Dynamic Scan" below.
- In an Azure DevOps project, configure a Fortify on Demand dynamic assessment task. See "Adding a Dynamic Assessment Task" on page 43.

Configuring a Dynamic Scan

After preparing your website for a dynamic assessment, you need to complete the Dynamic Scan Setup page. You only need to configure the dynamic scan settings once per release as the settings are carried over to the next scan. You can edit settings as needed for subsequent assessments.

To configure a dynamic scan:

1. Select the Applications view.

   Your Applications page appears.

2. Click the name of the application.

   The Application Overview page appears.
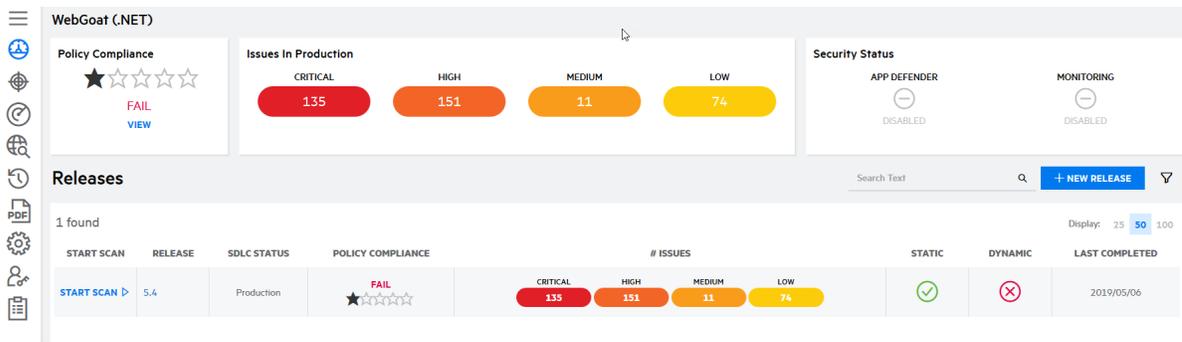
3. Click **Start Scan** for the release that you want to have assessed and select **Dynamic**.

   The Dynamic Scan Setup page appears.
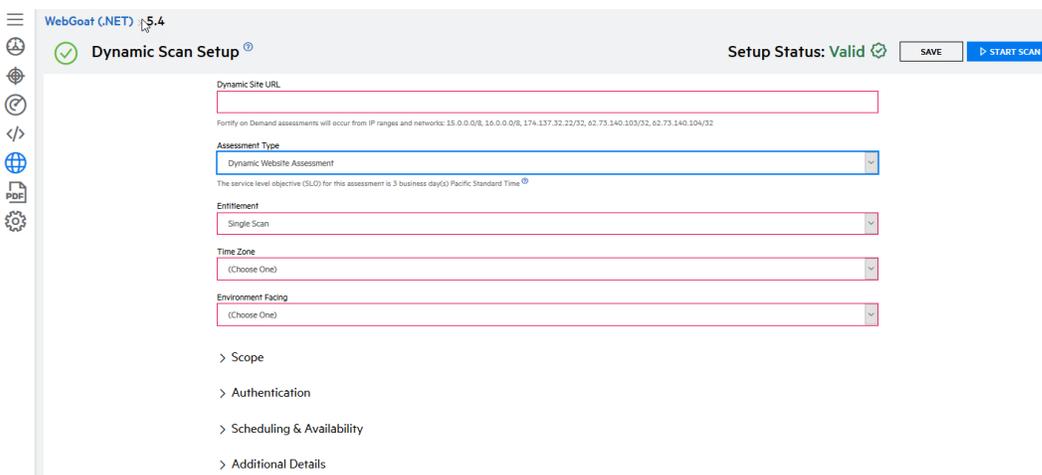
4. Complete the required fields. All other fields are optional or set to default values.

Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed. The SLO of the selected assessment type appears below the field. **Note:** The **Dynamic+ Web Services** assessment is used for testing web services where an OpenAPI definition or Postman collection is not available.
Dynamic Site URL	Type your site's URL. This field is available for Dynamic Website, Dynamic+ Website, and Dynamic+ Web Services assessments.
Entitlement	Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. If the release has an active subscription, only options

Field	Description
	that do not consume entitlements are displayed.
Time Zone	Select your location's time zone, which is used to schedule the scan's start time.
Environment Facing	Select whether the site is internal or external.

5. If needed, you can configure additional scan settings in the sections appearing below the required fields. The sections that are available depend on the assessment type selected.

Scope (Dynamic Website, Dynamic+ Website, Dynamic+ Web Services)

  a. To edit the scope of the scan, click **Scope**.

  ∨ Scope

  Fortify on Demand may scan the entire host of the designated URL. Other domains and subdomains will not be scanned during the assessment.

  ● Scan entire host (zero.webappsecurity.com)   ○ Restrict scan to URL directory and subdirectories ⑦

  ■ Allow HTTP (:80) and HTTPS (:443)

  ■ Allow form submissions during crawl ⑦

  Exclude URLs which contain

  [   ] +

  b. Complete the fields as needed.

Field	Description
Scan entire host (*<URL>*)	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 the scan to the URL directory and subdirectories**: only the directory denoted by the last slash in the URL and its

Field	Description
	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.**
Restrict scan to URL directory and subdirectories	**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
Allow HTTP (:80) and HTTPS (:443)	Select the check box to allow both HTTP and HTTPS scanning of the site (default). **Example**: Given https://foo.com/home, if the **Scan entire host** option is selected, http://foo.com/ and its subdirectories will be included. If the **Restrict scan to URL directory and subdirectories** option is selected, only http://foo.com/home and its subdirectories will be included.
Allow form submissions during crawl	Select this option to allow form submissions during the crawl of the site (default). This uncovers additional application surface area that can then be examined for a more thorough scan. Deselecting this option does **not** prevent form submissions during the vulnerability checks. Detection of many critical vulnerabilities, such as SQL injection and cross-site scripting, requires form submissions. To exclude specific web functionalities from form submissions, specify those URLS in the **Exclude URLS that contain** field.
Exclude URLS that contain	(Optional) Type a full or partial URL and click + to exclude URLs matching the string from testing. Add a new entry for each string. The field is not case-sensitive. By default, Fortify Azure DevOps Extension does not scan URLs outside the provided hostname, such as subdomains (https://www.foo.com, https://dev.foo.com) or offsite domain (https://bar.com).

Field	Description
	Example: https://foo.com/login.html, login.html

(Authentication (Dynamic Website, Dynamic+ Website, Dynamic+ Web Services)

a. To edit the authentication settings, click **Authentication**.

b. Complete the fields as needed.

Field	Description
Form Authentication	(Optional) Select the check box if form authentication is required. Provide user names and passwords for at least two users. To add more credentials, use the **Additional Notes** field at the bottom of this form.
Network Required	(Optional) Select the check box if network authentication is required and provide a username and password.
Additional Authentication Instructions	(Optional) Select the check box if additional authentication is required, such as an account number or tenant code, and type instructions. **Important!** Fortify Azure DevOps Extension does not support multi-factor authentication. Examples include authentication controls involving SMS messages, email verifications, CAPTCHA, OATH Tokens, and physical tokens.

Web Services (Dynamic Web Services)

For information on preparing web services project files suitable for automated testing, see Preparing Web Services Project Files.

a. To add instructions for scanning web services utilized by the site, click **Web Services**.

b. Select the API definition type: **Postman Collection (File)**, **Postman Collection (URL)**, **OpenAPI (File)**, **OpenAPI (URL)**.

> **Note:** OpenAPI Specification versions 2.0 and 3.0 are supported.

c. Perform the relevant task based on your API definition type:

API Definition Type	Procedure

Postman Collection (File)	**Web Services**
	
	To help ensure quality results and avoid paused scans, please review the detailed instructions for web services assessments. ⑦
	
	Web Service Type
	`Postman Collection (File)`
	
	Please upload the Postman collection
	`...` `UPLOAD`
	
	i. Click **...** and browse to and select the Postman collection file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file.

Postman Collection (URL)	**Web Services**
	
	To help ensure quality results and avoid paused scans, please review the detailed instructions for web services assessments. ⑦
	
	Web Service Type
	`Postman Collection (URL)`
	
	Please provide a URL to the postman collection
	
	Must use SSL with hostname
	
	Header Name Header Value (Leave Empty If Unchanged)
	
	i. Provide the Postman collection URL.
	
	ii. If authentication is needed to access the URL, provide the header name in the **Header Name** and the credentials in **Header Value** fields. For example, provide `Authorization` in **Header Name** and `Bearer <token>` in **Header Value**. Not that this is separate from the credentials used to authenticate requests.
	
	Examples:
	
	`X-API-Key: <apikey>`
	`Authorization: <apikey>`
	`Authorization: Bearer <token>`
	
	Note: If the credentials are passed as a query parameter, include

	it in the URL.
OpenAPI (File)	∨ Web Services To help ensure quality results and avoid paused scans, please review the detailed instructions for web services assessments. ⊘ Web Service Type OpenAPI (File) ⌄ Please upload your OpenApi specification json file [...] [⬆ UPLOAD] API Key [ ] i. Click ... and browse to and select the OpenAPI document file. The JSON file format is accepted. If a file already exists, you can use the existing file or upload a new file. 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.
OpenAPI (URL)	∨ Web Services To help ensure quality results and avoid paused scans, please review the detailed instructions for web services assessments. ⊘ Web Service Type OpenAPI (URL) ⌄ Please provide a URL to your OpenApi specification [ ] Must use SSL with hostname API Key [ ] i. Provide the OpenAPI document URL. 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.

d. In the **Additional Instructions** field, type additional instructions.

Web Services (Dynamic+ Web Services)

For information on preparing web services project files suitable for automated testing, see Preparing Web Services Project Files.

a. To add instructions for scanning web services utilized by the site, click **Web Services**.

b. Complete the fields as needed.

Field	Description
Web Service Type	i. Select the web service type: **SOAP**, **REST**. ii. Upload a project file, such as a WSDL file or API definition file, that contains working sample data. The JSON, WSDL, TXT, and XML file formats are accepted.
Additional Instructions	(Optional) Type additional instructions, such as required headers, tokens, or authentication mechanisms.
Username, Password API Key, Password	(Optional) Provide the username and password or API key and password.

Scheduling & Availability (all assessments)

a. To edit the scan frequency and site availability settings, click **Scheduling & Availability**.

b. Complete the fields as needed.

Field	Description
Repeat Frequency	Select the scan's repeat frequency: **Do not repeat** (default), **2 weeks**, **1 month**, **2 months**, **3 months**, **4 months**, **6 months**, **12 months**. If you are requesting a single scan, keep the default value. Scheduled recurring scans are automated and subjected to the following stipulations: ◦ Scheduling of a scan occurs seven days before the calculated scan date, which is determined by the start date of the previous scan and the repeat frequency. For example, if a monthly scheduled scan starts on the 5th of the month, the next scan will be scheduled for the 5th of the next month. ◦ The entitlement is deducted at the time of scheduling. ◦ A scan will only be scheduled if a valid entitlement for the selected assessment type exists at the time of the scheduling. ◦ If a scan is canceled, no further scans will be scheduled. ◦ If a scan is still in progress when the next scan is to be scheduled, Fortify Azure DevOps Extension will attempt once a day to reschedule the next scan until the scan date has passed. For example, if a monthly scheduled scan that starts on the 5th of the month is still in progress by the 5th of the next month, the next rescheduling attempt will take place seven days before the 5th of the month after that.
Site Availability	Select the check boxes to indicate when the environment is available for testing. Use the local time of the time zone specified above. You must provide a minimum of a four hour window of availability during the week. Pausing and resuming testing causes the scan to take longer than the standard SLO. Contact the support team for more information if you have site availability constraints.

Additional Details (Dynamic Website, Dynamic+ Website, Dynamic+ Web Services)

a. To add additional details about the scan, click **Additional Details**.

b. Complete the fields as needed.

Field	Description
User agent	Select the user agent type that will be used for the site: **Desktop browser** (default), **Mobile browser**
Concurrent request threads	Select the number of concurrent requests that will be used for the scan: ○ **Standard** (default): 5 crawl requestor threads, 10 audit requestor threads, 20 second request timeout ○ **Limited**: 2 crawl requestor threads, 3 audit requestor threads, 5 second request timeout Selecting the **Limited** option will reduce the scan load but will also cause the scan to take longer than the standard SLO.
Additional Notes	(Optional) Type additional information that the testing team needs to know before starting the assessment. **Note**: Free form exclusions and whitelist notes have been migrated to this field.

Field	Description
Additional Documentation	(Optional) Upload documentation (30 MB limit) that facilitates testing of the application. Uploaded files are displayed in the **Uploaded Files** section below. Supported file types: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX, CSV.
Generate WAF Virtual Patch	**Note:** Contact support to enable the option. (Optional) Select the check box to request a WAF virtual patch from Fortify WebInspect. Once the assessment is complete, you can download the file on the Scans page
Request pre-assessment conference call	(Optional, Dynamic Premium and Dynamic+ assessments only) Select the check box to request a pre-assessment conference call. The check box is cleared after the assessment is completed. **Note**: You cannot request a pre-assessment conference call for a scan scheduled within 72 hours.

6. Once you have configured the scan settings, click **Save**.
   - If the form is complete, the **Setup Status** is marked as **Valid**.
   - If the form is incomplete, the **Setup Status** is marked as **Incomplete**. A list of the issues appears at the top of the page. You can hover over the **x** icon next to **Setup Status** to display the list.

Adding a Dynamic Assessment Task

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

Note: Build pipelines can be defined using the classic editor or YAML editor; release pipelines can be defined using the classic editor.

To add a dynamic assessment task:

1. In an Azure DevOps project, navigate to your existing build pipeline.
2. Click **Edit**.
3. Select **Fortify on Demand Dynamic Assessment** from the list.
   The dynamic assessment task settings appear.

4. Complete the following fields:

Field	Description
Display name	Type a name for the task.
The root API Url	Type the API root URL of your Fortify on Demand data server.
Release Id	Type the release ID.

5. In the **Authentication Methods** section, complete the following fields:

Field	Description
API Authentication Type	a. Select the method of authentication: **API Key/Secret** or **Personal Access Token**. b. Provide the API key and secret or your account username, personal access token, and tenant ID. Fortify recommends using secret build variables to specify the Fortify on Demand credentials.
Proxy host	(Optional) Type the URL of the proxy server.
Proxy port	(Optional) Type the port of the proxy server.

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

Field	Description
Entitlement Preference	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.
Purchase Entitlements	(Optional) 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.
Prefer Remediation	Select the check box to run a remediation scan if one is available.

7. Click **Add**.

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

8. 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 25.

Getting Started with Fortify ScanCentral SAST and Fortify ScanCentral DAST

Use Fortify ScanCentral to run a static scan or a dynamic scan. You can:

- Submit your project to Fortify ScanCentral SAST for 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 as a Build Step" on page 47. 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 10).

- 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 Scan as a Build Step" on page 52.

Requirements for the Fortify ScanCentral Tasks

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

Fortify ScanCentral SAST Requirements

- Use with Fortify ScanCentral SAST versions 20.2.0 or later.
- Fortify ScanCentral SAST client version 21.2.0 or later requires that Java 11 be installed on the agent.
- 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 48).
- 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.

- To connect to Fortify ScanCentral SAST, you must have one of the following:
  - The 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`.
- 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 *Micro Focus Fortify Software System Requirements* in Fortify Software Security Center Documentation.

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 SAST Assessment as a Build Step

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 the *Micro Focus 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 the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* in Fortify Software Security Center Documentation for more information.

Field	Description
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 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 the *Micro Focus 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.

Field	Description
	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 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.

Field	Description
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 the *Micro Focus 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.

Field	Description
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 Assessment 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.

Adding a Fortify ScanCentral DAST Scan as a Build Step

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 the *Micro Focus 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 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 Azure DevOps Extension 8.9)

Just add your feedback to the email and click send.

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

We appreciate your feedback!