Micro Focus
Fortify WebInspect on Docker

Software Version: 21.1.0
Windows® operating systems

User Guide

Document Release Date: August 2021
Software Release Date: May 2021

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

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 August 18, 2021. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:
https://www.microfocus.com/solutions/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

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

Change Log

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

Software Release / Document Version	Changes
21.1.0 / August 18, 2021	Updated: • Docker image name with current version number. See "About the Docker Image" on page 12 and "Getting a Fortify WebInspect Image" on page 13. Removed: • References to the `latest` image tag.
21.1.0	Added: • Description of the ScanCentral DAST Utility Service mode. See "Understanding the Operation Modes" on page 12. Updated: • Information about requesting access to the Fortify Docker repository. See "Getting a Fortify WebInspect Image" on page 13. • Script name for pulling sensor image for use with Fortify ScanCentral DAST, environment parameter for DAST API root URL, and DAST artifact ZIP file name. See "Running the Container in ScanCentral DAST Mode" on page 20.
20.2.0	Added: • Information for running the Docker image in Fortify ScanCentral DAST mode. See "Running the Container in ScanCentral DAST Mode" on page 20. Updated: • Links to Docker-related websites. See "Setting Up Docker" on page 11. • Description of image naming convention to remove details about version tags. See "About the Docker Image" on page 12. • Instructions for configuring an environment file and running the

Software Release / Document Version	Changes
	container to indicate they apply only to CLI and API modes. See "Configuring the Environment File for CLI and API Modes" on page 14 and "Running the Container in CLI and API Modes" on page 18.
20.1.0	Added: • Information about updating Windows. See "Windows Version Available" on page 12 and "Getting a Fortify WebInspect Image" on page 13. Updated: • Windows versions that are available in the Docker image. See "Windows Version Available" on page 12. • Image naming convention examples and descriptions with current Fortify WebInspect version. See "Image Naming Convention" on page 12.
19.2.0	Added: • Process for using proxy settings for a scan. See "Using Proxy Settings" on page 19 Updated: • Image naming convention examples and descriptions with current Fortify WebInspect version. See "Image Naming Convention" on page 12. • Recommended memory to 16 GB. See "Understanding the Docker CLI Options" on page 19.

Related Documents

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

Note: You can find the Micro Focus Fortify Product Documentation at https://www.microfocus.com/support/documentation. All guides are available in both PDF and HTML formats. Product help is available within the Fortify WebInspect products.

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
About Micro Focus Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. **Note:** This document is included only with the product download.
Micro Focus Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Micro Focus Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Micro Focus Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Micro Focus Fortify ScanCentral DAST

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

Document / File Name	Description
Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide SC_DAST_Guide_<*version*>.pdf	This document provides information about how to configure and use Fortify ScanCentral DAST to conduct dynamic scans of Web applications.

Micro Focus Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
Micro Focus Fortify WebInspect Installation Guide WI_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
Micro Focus Fortify WebInspect User Guide WI_Guide_<*version*>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
Micro Focus Fortify WebInspect on Docker User Guide WI_Docker_Guide_<*version*>.pdf	This document describes how to download, configure, and use Fortify WebInspect that is available as a container image on the Docker platform. This full version of the product is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center.
Micro Focus Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Document / File Name	Description
Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify WebInspect License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
Micro Focus Fortify WebInspect Agent Installation Guide WI_Agent_Install_<*version*>.pdf	This document describes how to install the Fortify WebInspect Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.
Micro Focus Fortify WebInspect Agent Rulepack Kit Guide WI_Agent_Rulepack_Guide_<*version*>.pdf	This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect on Docker

Micro Focus engineers have created a Fortify WebInspect image that is available for download on the Docker container platform. The image includes the full version of Fortify WebInspect 21.1.0 software, but is intended to be used in automated processes as a headless scanner configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center.

What is Docker?

Docker is a platform that facilitates creating, deploying, and running applications. Developers can package their application and all dependencies, including the platform and all its dependencies, into one logical package called a container or image. You can download a Docker image and run the application contained therein on a virtual machine (VM).

Benefits of Docker

Using a Docker image makes configuring the various prerequisite dependencies unnecessary, and can reduce the time it takes to deploy an instance of the application.

Docker is command-line driven, so it is easy to integrate into build processes, making Docker perfect for automation. As part of an automated build process, you can download a Fortify WebInspect image from the Docker repository, conduct a scan, and then remove the image from your VM.

For more information about Docker, visit https://www.docker.com.

Supported Version

Fortify WebInspect on Docker runs on Docker Enterprise Edition version 18.09 or later.

Audience

This document is intended for users who are familiar with Fortify WebInspect, in particular its CLI and API, and the License and Infrastructure Manager (LIM). Users should also have experience installing, configuring, and using Docker.

Setting Up Docker

Before you can run Docker containers, you must set up Docker according to the process described in the following table.

Stage	Description
1.	Download and install Docker for Windows.
2.	Configure your machine for Docker containers.
3.	Register and start the Docker service.

For information about Docker Engine Enterprise, see https://docs.mirantis.com/docker-enterprise/v3.0/dockeree-products/docker-ee/windows.html.

For additional Docker documentation, see http://docs.docker.oeynet.com/.

About the Docker Image

The following paragraphs describe the Windows versions, database version, and naming convention of the Fortify WebInspect image on Docker.

Image Naming Convention

The Fortify Docker repository uses the following naming convention for the Fortify WebInspect image:

`fortifydocker/webinspect:<version>`

The current version is:

`fortifydocker/webinspect:21.1`

For more information about the version that is available, refer to the Readme file in the fortifydocker/webinspect repository.

Windows Version Available

This release of Fortify WebInspect 21.1 image is available in Windows version 1809.

Important! Before you can run the Fortify WebInspect image, you must install Microsoft update KB4561608 on the host machine. For more information, see https://support.microsoft.com/en-us/topic/june-9-2020-kb4561608-os-build-17763-1282-437af506-e3ef-a8a1-09e7-26cc94e509c7.

Database Version

The Fortify WebInspect 21.1 image includes the SQL Server 2017 Express edition database.

Understanding the Operation Modes

The Fortify WebInspect image can run in one of four operation modes in a container as described in the following table.

Mode	Description
1	**WebInspect CLI mode.** Use this mode to conduct scans using options available in the

Mode	Description
	command-line interface. For an entire list of CLI options, see the "Command Line Execution" topic in the *Micro Focus Fortify WebInspect User Guide*.
2	**WebInspect API mode.** Use this mode to conduct scans using the endpoints available in the Fortify WebInspect REST API. After the Docker container starts, you can navigate to the following URL to browse the Swagger documentation from your local machine: http://<*hostname*>:8083/webinspect/swagger/docs/v1 If you map ports from the container to the host machine as shown in the Docker run command, you can access it using localhost as <*hostname*>. Otherwise, use the IP address of the Docker host machine.
3	**ScanCentral DAST mode.** Use this mode to conduct scans from the ScanCentral DAST user interface in Fortify Software Security Center. For more information about Fortify ScanCentral DAST, see *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*. **Note:** This description is provided for informational purposes only. You do not configure an environment file for this mode. For more information, see "Running the Container in ScanCentral DAST Mode" on page 20.
4	**ScanCentral DAST Utility Service mode.** Use this mode to run the Fortify WebInspect image as a ScanCentral DAST Utility Service container. **Note:** This description is provided for informational purposes only. You do not configure an environment file for this mode. You pull this image and start the container using either the Docker compose file or one of the PowerShell scripts that the Fortify ScanCentral DAST Configuration Tool generates. For more information, see *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

Getting a Fortify WebInspect Image

After starting the Docker service, request access to the private Fortify WebInspect repository on the Docker Hub and download an image of Fortify WebInspect from the Fortify Docker repository as described in this topic.

Important! Before you can run the Fortify WebInspect image, you must install Microsoft update KB4561608 on the host machine. For more information, see https://support.microsoft.com/en-us/topic/june-9-2020-kb4561608-os-build-17763-1282-437af506-e3ef-a8a1-09e7-26cc94e509c7.

Requesting Access to Fortify Docker Repository

Access to the Fortify Docker repository requires credentials and is granted through your Docker ID. To access the Fortify Docker repository, email your Docker ID to fortifydocker@microfocus.com.

Downloading an Image for API and CLI Modes

Note: Instructions for downloading an image apply only when running the container in API and CLI modes. To download an image when running the container in ScanCentral DAST Mode, see "Running the Container in ScanCentral DAST Mode" on page 20.

To download the current version of the Fortify WebInspect image:

- In PowerShell, enter the following command:

```
docker pull fortifydocker/webinspect:21.1
```

Configuring the Environment File for CLI and API Modes

After you download a Fortify WebInspect image from the Docker repository, you must configure an environment (`.env`) file that defines how the image will operate. For more information, see https://docs.docker.com/compose/env-file.

In the environment file, configure the operation mode, licensing (if required), and options as described in the following sections.

Configuring the Operation Mode (Required)

You must specify a mode for the image. For more information about the modes, see "Understanding the Operation Modes" on page 12.

In the environment file, specify the operation mode as follows:

```
# WebInspect Container Mode

mode=<number>
```

The following example sets the image to run in WebInspect CLI mode:

```
# WebInspect Container Mode
mode=1
```

Configuring Licensing (Required for CLI and API Modes)

You must configure licensing for the image when running in CLI and API modes. Currently, licensing must be handled by a License and Infrastructure Manager (LIM). In the environment file, type the following information for your LIM installation to configure licensing for this instance of Fortify WebInspect:

```
# Licensing
limURL=<LIM_URL>
limPool=<LIM_pool>
limPswd=<LIM_password>
```

For more information about using the LIM, see the *Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide*.

Configuring CLI Mode Options

You must configure CLI options to use WebInspect CLI mode. You can configure any of the available CLI options as scan arguments in the environment file. For the complete list of CLI options, see the "Command Line Execution" topic in the *Micro Focus Fortify WebInspect User Guide*.

In the environment file, type the following to configure the CLI options to use in the scan. Substitute *<options>* with your specific options:

```
# WebInspect CLI scan options
scanArgs=<options>
```

The following example performs a crawl-only scan of zero.webappsecurity.com and exports the results to the `zero.scan` file:

```
# WebInspect CLI scan options
scanArgs=-u http://zero.webappsecurity.com -c -es zero.scan
```

Sample CLI Environment File

The following is a sample environment file for WebInspect CLI mode to run a full audit:

```
#!-- WebInspect Docker Mode. --!
#!-- Sample configuration for CLI mode. --!

# 1 = CLI mode
mode=1

# Licensing
limURL=http://xxx.xx.xxx.xxx/limservice/
limPool=xxxxxx
limPswd=******

# WebInspect options - for use in scan mode
# Full audit
scanArgs=-u http://zero.webappsecurity.com -es c:\host\zero.scan

# Full audit with macro
#scanArgs=-u http://zero.webappsecurity.com -xd -es c:\host\zero.scan -
macro c:\host\zero_macro.webmacro

# Crawl only
#scanArgs=-u http://zero.webappsecurity.com -es c:\host\zero.scan -c

# Full audit with settings file and reporting
#scanArgs=-u http://zero.webappsecurity.com -s c:\host\Settings.xml -r
Vulnerability -y Standard -f c:\host\Report -gp -es c:\host\zero.scan
```

The full audit with macro, crawl only, and full audit with settings file and reporting examples are commented out in this sample file.

Configuring API Mode Options

You must configure API options to use WebInspect API mode. To conduct a scan that uses the Fortify WebInspect API, you must provide the host, port, and authentication type parameters for the API server as described in the following table.

Parameter	Description
RCServerHost	Specifies the hostname that the WebInspect API Server should listen on. Use + for all.
RCServerPort	Specifies the WebInspect API Server port to listen on.
RCServerAuthType	Specifies the WebInspect API Server authentication type. The value can be one of the following: • None • Basic • NTLM • ClientCert

In the environment file, provide the details for your Fortify WebInspect REST API using the following parameters:

```
# WebInspect API
RCServerHost=<hostname>
RCServerPort=<port_number>
RCServerAuthType=<auth_type>
```

Sample API Environment File

The following is a sample environment file for WebInspect API mode:

```
#!-- WebInspect Docker Mode. --!
#!-- Example configuration for API mode. --!

# 2 = WebInspect API mode
mode=2

# Licensing
limURL=http://xxx.xx.xxx.xxx/limservice/
limPool=xxxxxx
limPswd=*****

# WebInspect API settings
RCServerHost=+
RCServerPort=8083
```

```
# RCServerAuthType: None, Basic, NTLM, ClientCert
RCServerAuthType=None
```

What's next?

After you have configured and saved your environment file, you can run the image in a container. Go to "Running the Container in CLI and API Modes" below.

Running the Container in CLI and API Modes

This topic provides a sample Docker run command for the WebInspect CLI and API modes. The Docker run command uses CLI options that define the container's resources at runtime. To understand how the Docker CLI options used in the samples determine how the container is run, see "Understanding the Docker CLI Options" on the next page.

Note: If proxy settings are required, see "Using Proxy Settings" on the next page.

Sample Docker Run Command for CLI Mode

The following example uses Docker CLI options to run the container in CLI mode:

```
docker run -d --rm -v c:/scans:c:/host --env-file ScanMode.env --memory=16g
--cpus=4 --name webinspect fortifydocker/webinspect:21.1
```

For more information about image filenames and version numbers, see "Getting a Fortify WebInspect Image" on page 13.

Sample Docker Run Command for API Mode

The following example uses Docker CLI options to run the container in API mode:

```
docker run -d --rm -p 8083:8083 --env-file APIMode.env --memory=16g --
cpus=4 --name webinspect_api fortifydocker/webinspect:21.1
```

For more information about image filenames and version numbers, see "Getting a Fortify WebInspect Image" on page 13.

Understanding the Docker CLI Options

The following table describes the Docker CLI options used in "Sample Docker Run Command for CLI Mode" on the previous page and "Sample Docker Run Command for API Mode" on the previous page.

Option	Description
`-d`	Runs the container in the background and displays the container ID.
`--cpus`	Specifies the number of CPUs to allocate to the container. Fortify recommends 2 CPUs.
`--env-file`	Identifies the `.env` file to use. For more information, see "Configuring the Environment File for CLI and API Modes" on page 14.
`--memory`	Specifies the amount of memory to allocate to the container. Fortify recommends 16 GB.
`-p`	Maps a port inside the container to a port on the host system. **Important!** This is required to use WebInspect API mode.
`--rm`	Automatically removes the container when it exits.
`-v`	Maps the volume (or folder) from the container to a folder on the host system. Separate multiple folder names with a colon.

Tip: For more information and a complete list of Docker run options, see https://docs.docker.com/engine/reference/commandline/run.

Using Proxy Settings

You cannot pass proxy settings directly to the WebInspect image through command line arguments or in the .env file. However, you can use the following process to use proxy settings for a scan.

Stage	Description
1.	Create a custom WebInspect settings file that includes the proxy settings.
2.	Save the file on the Docker host machine.
3.	Use the following options:

Stage	Description

	• The `-s` WebInspect CLI option as a scan argument (`scanArgs`) in the .env file to pass the settings file, as shown in the following example:
	`scanArgs=-u http://zero.webappsecurity.com/ -s c:\host\CustomSettings.xml -es c:\host\zero.scan -xd`
	• The `-v` Docker CLI option in the Docker run command to map the folder with the settings to a folder in the container, as shown in the following example:
	`docker run -v c:/widocker:c:/host --env-file config.env fortifydocker/webinspect`

Running the Container in ScanCentral DAST Mode

The ScanCentral DAST Configuration Tool creates and downloads the following PowerShell scripts that you can use to pull and start a new sensor container:

- `pull-and-start-sensor-container.ps1` - This PowerShell script pulls the Fortify WebInspect image from Docker Hub, and then starts the container.
- `pull-sensor-image.ps1` - This PowerShell script pulls the Fortify WebInspect image from Docker Hub, but does not start the container.
- `start-sensor-container.ps1` - This PowerShell script starts the Fortify WebInspect container, but does not pull the image.

You can find these files in the `DAST-start.zip` file along with the other ScanCentral DAST launch artifacts. For more information about the ScanCentral DAST Configuration Tool, see the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

Sample Script

The script you use should be similar to the following example:

```
docker run -d --restart always --name scancentral-dast-sensor
   -e "mode=3" -e "RCServerHost=+" -e "RCServerPort=8089"
   -e "RCServerUseHTTPS=false" -e "RCServerAuthType=none"
```

```
    -e "DASTApiRootUrl=http://<IP_Address>:<Port>/api"
    -e "AllowNonTrustedServerCertificate=true"
    -e "ServiceToken=QgitxRErVP5Eh7hr2Bnuig=="
    -e "ScannerPoolId=0" --memory=8g --cpus=2 fortifydocker/webinspect:21.1
```

About the ServiceToken

The `ServiceToken` is the encrypted "Sensor Service Token" that is set by the administrator using the ScanCentral DAST Configuration tool. This value should be protected.

Caution! A change to the `ServiceToken` value by the configuration tool requires all sensor containers to be updated with the new value.

About the ScannerPoolId

The `ScannerPoolId` is the sensor pool ID number in Fortify Software Security Center. If you need to hand-edit the `ScannerPoolId` in your script, you can find the sensor pool ID number in Fortify Software Security Center on the **SCANCENTRAL** > **DAST** > **Sensor Pools** page. Select the sensor pool in the list and view the Pool ID in the detail panel.

Tip: Setting `ScannerPoolId` to `0` automatically allocates the sensor to the Default pool.

Using PowerShell Scripts

These PowerShell scripts offer the following options:

- Use one script to pull the Fortify WebInspect image and then start the container.
- Use two scripts: one to pull the image, and then another to start the container.

You use the script or scripts on the host where you want to run the Fortify WebInspect container.

Using One Script

Use the following process to use a single PowerShell script to pull the image and start the container.

Stage	Description
1.	Copy the `pull-and-start-sensor-container.ps1` file to the host where you want to run the Fortify WebInspect container.
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information

Stage	Description
	about using PowerShell, refer to your Windows PowerShell documentation.
3.	To avoid errors regarding non-digitally signed scripts, run the contents of the `pull-and-start-sensor-container.ps1` script: 1. Copy the contents from the `pull-and-start-sensor-container.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-and-start-sensor-container.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The Fortify WebInspect image is pulled and the container is started.

Using Two Scripts

Use the following process to use separate pull and start PowerShell scripts.

Stage	Description
1.	Copy the following files to the host where you want to run the Fortify WebInspect container: • `pull-sensor-image.ps1` • `start-sensor-container.ps1`
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information about using PowerShell, refer to your Windows PowerShell documentation.
3.	Pull the image. To avoid errors regarding non-digitally signed scripts, run the contents of the `pull-sensor-image.ps1` script: 1. Copy the contents from the `pull-sensor-image.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon.

Stage	Description
	Note: Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-sensor-image.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The Fortify WebInspect image is pulled.
4.	Start the container. To avoid errors regarding non-digitally signed scripts, run the contents of the `start-sensor-container.ps1` script: 1. Copy the contents from the `start-sensor-container.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, if you set the execution policy to allow all scripts as described in Stage 3, you can run the script as follows: `& "<drive>:<path_to_script>\start-sensor-container.ps1"` The Fortify WebInspect container is started.

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 WebInspect on Docker 21.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!