Micro Focus
Fortify WebInspect on Docker

Software Version: 18.20
Windows® operating systems

User Guide

Document Release Date: January 2019
Software Release Date: November 2018

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

Adobe™ is a trademark of Adobe Systems Incorporated.

Docker® and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

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

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.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-and-services/documentation

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-and-services/documentation. Apart from the Release Notes, 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*>.txt	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 Open Source and Third-Party License Agreements Fortify_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in Fortify Software.

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.

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 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.
Micro Focus Fortify WebInspect Runtime Agent Installation Guide WI_RT_Agent_Install_<*version*>.pdf	This document describes how to install the Fortify WebInspect Runtime 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 Runtime Agent, allowing it to monitor your code for

Document / File Name	Description
	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 18.20 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).

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 Version 18.09 Enterprise Edition (EE).

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 more information, see https://docs.docker.com/install/windows/docker-ee.

Getting a Fortify WebInspect Image

After starting the Docker service, download an image of Fortify WebInspect from the Fortify Docker repository as described in this topic.

Windows Versions Available

Fortify WebInspect images are available in two Windows versions:

- Windows Server 2016
- Windows Server version 1709

Image Naming Convention

Images available on the Fortify Docker repository use the following naming convention:

<repository>/*<image>*:*<WebInspect_version>*-*<SecureBase_version>*-*<optional_Windows_version>*

For Fortify WebInspect images, the *<repository>*/*<image>* is `fortifydocker/webinspect`. The tags following the colon indicate specific versions. If *<optional_Windows_version>* is not specified, Windows Server 2016 is assumed. The following table provides examples and descriptions to help you understand the naming convention.

Tip: Using the image named `fortifydocker/webinspect:latest` downloads the latest version of the Fortify WebInspect image, including the latest SecureBase update that is available in a Docker image.

Image Name	Description
`fortifydocker/webinspect:1820-sb2018u4`	Fortify WebInspect version 18.20 with SecureBase update 4 for the year 2018 on Windows Server 2016
`fortifydocker/webinspect:1820-sb2018u4-win1709`	Fortify WebInspect version 18.20 with SecureBase update 4 for the year 2018 on Windows Server version 1709
`fortifydocker/webinspect:1820-sb2018u3`	Fortify WebInspect version 18.20 with SecureBase update 3 for the year 2018 on Windows Server 2016

Image Name	Description
`fortifydocker/webinspect:1820-sb2018u3-win1709`	Fortify WebInspect version 18.20 with SecureBase update 3 for the year 2018 on Windows Server version 1709

Downloading an Image

To download a specific version of Fortify WebInspect:

- In PowerShell, type the following command:

  `docker pull fortifydocker/webinspect:<WebInspect_version>-<SecureBase_version>-<optional_Windows_version>`

To download the latest version of Fortify WebInspect that is available on Docker:

- In PowerShell, type the following command:

  `docker pull fortifydocker/webinspect:latest`

Configuring the Environment File

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, and options as described in the following sections.

Configuring the Mode (Required)

You must specify a mode for the image. The Fortify WebInspect image can run in the following modes:

- `1` – WebInspect CLI mode: Use this mode to conduct scans using options available in the 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.

In the environment file, type 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)

You must configure licensing for the image. 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 WebInspect Installation Guide* and the *Micro Focus Fortify WebInspect User 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" on the next page.

Running the Container

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 "Docker CLI Options Explained" 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=8g
--cpus=2 --name webinspect fortifydocker/webinspect:<tags>
```

Substitute *<tags>* with the specific version that you downloaded. The following example runs the latest version available on Docker:

```
docker run -d --rm -v c:/scans:c:/host --env-file ScanMode.env --memory=8g
--cpus=2 --name webinspect fortifydocker/webinspect:latest
```

For more information about image filenames and version numbers, see "Image Naming Convention" on page 11.

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=8g --
cpus=2 --name webinspect_api fortifydocker/webinspect:<tags>
```

Substitute *<tags>* with the specific version that you downloaded. The following example runs the latest version available on Docker:

```
docker run -d --rm -p 8083:8083 --env-file APIMode.env --memory=8g --
cpus=2 --name webinspect_api fortifydocker/webinspect:latest
```

For more information about image filenames and version numbers, see "Image Naming Convention" on page 11.

Docker CLI Options Explained

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 two CPUs.
`--env-file`	Identifies the `.env` file to use. For more information, see "Configuring the Environment File" on page 13.
`--memory`	Specifies the amount of memory to allocate to the container. Fortify recommends four 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.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify WebInspect on Docker 18.20)

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!