Micro Focus Fortify Software

Software Version: 23.1.0

System Requirements

Document Release Date: Revision 3: November 2023
Software Release Date: May 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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 03, 2023. 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/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 revisions made to this document.

Document Revision	Changes
Revision 3: November 2023	Updated: • Incorporated changes available with Fortify Software Security Content 2023 Update 3 (see "Libraries, Frameworks, and Technologies" on page 31)
Revision 2: July 2023	Updated: • Supported databases for Fortify ScanCentral DAST (see "Fortify ScanCentral DAST Database Requirements" on page 12) • Supported Fortify WebInspect Enterprise version for Fortify Software Security Center (see "Service Integrations for Fortify Software Security Center" on page 26) • Incorporated changes available with Fortify Software Security Content 2023 Update 2 (see "Libraries, Frameworks, and Technologies" on page 31)
Revision 1: June 2023	Updated: • Reverted LIM software requirements for Windows Server (see "Software Requirements" on page 10) • .NET SDK Core Runtime version for sensor service for Fortify ScanCentral DAST (see "Fortify ScanCentral DAST Sensor" on page 14) • Requirements for translating .NET applications using Fortify ScanCentral SAST (see "Fortify ScanCentral SAST Sensor Languages and Build Tools" on page 20) • SQL Server database driver version (see "Fortify Software Security Center Database" on page 23) • Xcode and swiftc version support (see "Build Tools" on page 36 and "Compilers" on page 36) • Fortify WebInspect required connection for accessing the Certificate Revocation List (see "Required Connections" on page 44)

Introduction

This document provides the details about the environments and products that Fortify supports for this version of Fortify Software, which includes:

- Fortify License and Infrastructure Manager
- Fortify ScanCentral DAST
- Fortify ScanCentral SAST
- Fortify Software Security Center Server
- Fortify Static Code Analyzer
- Fortify Static Code Analyzer Applications and Tools (including Secure Code Plugins)
- Fortify WebInspect
- Fortify WebInspect Agent
- Fortify WebInspect Enterprise

Software Delivery

Micro Focus Fortify Software is delivered electronically. See "Acquiring Fortify Software" on page 61 for more information.

Software Licenses

Fortify Software products require a license. For Fortify ScanCentral DAST, Fortify Static Code Analyzer, Fortify WebInspect, and Fortify WebInspect Enterprise, you will receive an email with instructions for how to activate your product.

For all other Fortify Software products described in this document (including Fortify Static Code Analyzer and Secure Code Plugins), you must download the Fortify license file for your purchase from the Micro Focus Software Licenses and Downloads (SLD) portal (https://sld.microfocus.com). Use the credentials that Micro Focus Fortify Customer Support has provided for access.

Note: Using Fortify License and Infrastructure Manager (LIM) to manage concurrent licenses for Fortify Static Code Analyzer requires LIM version 21.2.0 or later.

Fortify License and Infrastructure Manager Requirements

This section describes the hardware and software requirements for Fortify License and Infrastructure Manager (LIM).

Hardware Requirements

Fortify recommends that you install the LIM on a system that conforms to the supported components listed in following table.

Component	Requirement	Notes
Processor	2.5 GHz single-core or faster	Recommended
	1.5 GHz single-core	Minimum
RAM	2+ GB	Recommended
	1 GB	Minimum
Hard disk	50+ GB	Recommended
	20 GB	Minimum
Display	1280 x 1024	Recommended
	1024 x 768	Minimum

Software Requirements

LIM runs on and works with the software packages listed in the following table. Beta or pre-release versions of operating systems, service packs, and required third-party components are not supported.

Package	Versions	Notes
Windows Server	Windows Server 2016	
	Windows Server 2019	
Web Server	IIS 8.5	Recommended
	IIS 7.5, 8.0, 10	
.NET Platform	.NET Framework 4.8	
	ASP.NET 4.8	

LIM on Docker Requirements

LIM on Docker has the requirements listed in the following table.

Software	Version
Windows	Windows Server 2019
Docker Enterprise	18.09 or later

Fortify ScanCentral DAST Requirements

Before you install Fortify ScanCentral DAST, make sure that your system meets the requirements described in this section. Fortify does not support beta or pre-release versions of operating systems, service packs, or required third-party components.

Architectural Best Practices

The Fortify ScanCentral DAST core components are available as Docker images only. The Fortify WebInspect sensor is either a Docker image or a Windows computer with both Fortify WebInspect and the Fortify ScanCentral DAST sensor service installed.

Follow these best practice guidelines when you configure Fortify ScanCentral DAST:

- Run the DAST API, DAST Global Service, DAST Utility Service, and Fortify License and Infrastructure Manager (LIM) Docker containers on the same VM or on separate VMs.
- Do not run the Fortify WebInspect sensor (container or classic installation) on the same VM as any of the other DAST components.

For more information about the Fortify ScanCentral DAST components, see the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

Fortify ScanCentral DAST Configuration Tool CLI

This topic describes the software and hardware requirements for the machine on which the configuration tool CLI runs to configure settings for the Fortify ScanCentral DAST components.

Software Requirements

The Fortify ScanCentral DAST Configuration Tool CLI runs on and works with the software packages listed in the following table.

Package	Versions
Windows	Windows 10
	Windows Server 2019
.NET Platform	.NET SDK Core Runtime 6.0
Red Hat Enterprise Linux (RHEL)	8.*x* x86_64

Hardware Requirements

Fortify recommends that you use the Fortify ScanCentral DAST Configuration Tool CLI on a system that conforms to the supported components listed in the following table.

Component	Requirement	Notes
RAM	2+ GB	Recommended
	1 GB	Minimum

Fortify ScanCentral DAST Database Requirements

Fortify ScanCentral DAST supports the databases listed in the following table.

Package	Versions	Notes
SQL Server (English-language version only)	SQL Server 2022	Recommended No scan database limit
	SQL Server 2019	No scan database limit
	Azure SQL Server	Using Azure SQL Server outside the Azure infrastructure may cause poor performance for Fortify ScanCentral DAST. Fortify recommends using Azure SQL Server with Fortify ScanCentral DAST inside the Azure infrastructure only.

Package	Versions	Notes
	Amazon RDS for SQL Server	
PostgreSQL	PostgreSQL 15 or later	
	Azure PostgreSQL	
	Amazon RDS for PostgreSQL	

Database Recommendations

Fortify recommends that you configure the database server on a separate machine from either Micro Focus Fortify Software Security Center or any other Fortify ScanCentral DAST components.

The Fortify ScanCentral DAST SQL database requires case-insensitive collation.

Important! This is opposite the requirement for Fortify Software Security Center databases as described in "Fortify Software Security Center Database" on page 23.

Important Recommendation About Disk I/O

Disk I/O encompasses the input/output operations on a physical disk. If you are reading data from a file, the processor must wait for the file to be read (the same applies to writing data to a file). Fortify ScanCentral DAST is a high I/O-intensive application, which affects performance. Make sure that your disk subsystem provides low read/write latency. Fortify recommends that you monitor disk I/O as the database grows.

Fortify ScanCentral DAST Core Components VM

This topic describes the hardware and software requirements to run the DAST API, DAST Global Service, and DAST Utility Service containers.

Software Requirements

The DAST API, DAST Global Service, and DAST Utility Service containers run on and work with the software packages listed in the following table.

Software	Versions
Windows	Windows Server 2019
Red Hat Enterprise Linux (RHEL)	8.*x* x86_64

Follow Docker recommendations for the Docker engine version to use for these versions of Windows and Red Hat images.

Hardware Requirements

Fortify recommends that you use the DAST API, DAST Global Service, and DAST Utility Service containers on a system that conforms to the supported components listed in the following table.

Component	Requirement
RAM	32 GB
Processor	8 Core

Fortify ScanCentral DAST Sensor

The following options are available for a Fortify ScanCentral DAST sensor:

- Use the Fortify WebInspect on Docker image in a container
- Use a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service

Fortify WebInspect on Docker Option

For system requirements for this option, see "WebInspect on Docker" on page 43.

Classic Fortify WebInspect Installation Option

For hardware and software requirements for this option, see "WebInspect Hardware Requirements" on page 40 and "WebInspect Software Requirements" on page 41. Additionally, if you plan to conduct Postman scans, see "Support for Postman" on page 42.

Important! When running a Fortify ScanCentral DAST sensor outside of a container, such as a sensor service on the same machine as a classic Fortify WebInspect installation, you must install the .NET SDK Core Runtime 7.0.0 or later.

Fortify ScanCentral DAST Ports and Protocols

This section describes the ports and protocols that the Fortify ScanCentral DAST components use to make required and optional connections.

DAST API Required Connections

The following table lists the ports and protocols that the DAST API container uses for required connections.

Endpoint	Port	Protocol	Notes
Fortify Software Security Center DAST Global Service DAST Sensor Service	80	HTTP	If SSL is not configured, the port on the host running the container is forwarded to port 80 on the container. Host port mapping is customizable to the container port.
Fortify Software Security Center DAST Global Service DAST Sensor Service	443	HTTPS	If SSL is configured, the port on the host running the container is forwarded to port 443 on the container. Host port mapping is customizable to container port.
SQL Server, Azure SQL Server, or Amazon RDS for SQL Server	1433	TCP	This is the default SQL Server port.
PostgreSQL, Azure PostgreSQL, or Amazon RDS for PostgreSQL	5432	TCP	This is the default PostgreSQL port.

DAST Global Service Required Connections

The DAST Global Service does not expose any ports.

The following table lists the ports and protocols that the DAST Global Service container uses for required connections.

Endpoint	Port	Protocol	Notes
SQL Server, Azure SQL Server, or Amazon RDS for SQL Server	1433	TCP	This is the default SQL Server port.
PostgreSQL, Azure PostgreSQL, or Amazon RDS for PostgreSQL	5432	TCP	This is the default PostgreSQL port.

DAST Sensor Required Connections

The DAST sensor does not expose any ports.

The DAST sensor communicates with the DAST API over the port that is exposed on the host running the DAST API container.

DAST Utility Service Required Connections

The following table lists the ports and protocols that the DAST Utility Service container uses for required connections.

Endpoint	Port	Protocol	Notes
DAST API	5000	HTTP	If SSL is not configured, the port on the host running the container is forwarded to port 5000 on the container. Host port mapping is customizable to the container port.
DAST API	5001	HTTPS	If SSL is configured, the port on the host running the container is forwarded to port 5001 on the container. Host port mapping is customizable to container port.
SQL Server, Azure SQL	1433	TCP	This is the default SQL Server port.

Endpoint	Port	Protocol	Notes
Server, or Amazon RDS for SQL Server			
PostgreSQL, Azure PostgreSQL, or Amazon RDS for PostgreSQL	5432	TCP	This is the default PostgreSQL port.

Fortify ScanCentral DAST Browsers

For Fortify ScanCentral DAST browser requirements, see "Browsers" on page 25 for Fortify Software Security Center.

Standalone Web Macro Recorder Requirements

Fortify ScanCentral DAST allows you to download and use a standalone version of the Web Macro Recorder tool. The Web Macro Recorder tool runs on and works with the software packages listed in the following table.

Package	Version
Windows	Windows 10
	Windows Server 2019

Running as Administrator

The standalone Web Macro Recorder tool requires administrative privileges for proper operation of all features. Refer to the Windows operating system documentation for instructions on changing the privilege level to run the Web Macro Recorder tool as an administrator.

Software Integrations for Fortify ScanCentral DAST

The following table lists products that you can integrate with Fortify ScanCentral DAST.

Product	Versions
Micro Focus Fortify Software Security Center	23.1.0
Kubernetes on Azure	1.19 or later

Fortify ScanCentral SAST Requirements

Fortify ScanCentral SAST has three major components: a ScanCentral Controller, ScanCentral clients, and ScanCentral sensors.

Fortify ScanCentral SAST Controller Requirements

This section describes the hardware and platform requirements for the Fortify ScanCentral SAST Controller.

Fortify ScanCentral SAST Controller Hardware Requirements

Fortify recommends that you install the Fortify ScanCentral SAST Controller on a high-end 64-bit processor running at 2 GHz with at least 8 GB of RAM.

To estimate the amount of disk space required on the machine that runs the Fortify ScanCentral SAST Controller, use one of the following equations:

Intended Use	Equation
Remote scan only	*<num_jobs_per_day>* x (*<size_avg_MBS>* + *<size_avg_FPR>* + *<size_avg_SCA_log>*) x *<number_days_data_is_persisted>*
Remote translation and scan	*<num_jobs_per_day>* x (*<size_avg_archived_project_with_dependencies>* + *<size_avg_FPR>* + *<size_avg_SCA_log>*) x *<num_days_data_is_persisted>*

By default, data is persisted for seven days.

Fortify ScanCentral SAST Controller Platforms and Architectures

The Fortify ScanCentral SAST Controller supports the platforms and architectures listed in the following table.

Operating System	Versions
Windows	Server 2016 Server 2019 Server 2022

Operating System	Versions
Linux	Red Hat Enterprise Linux 7.x, 8 SUSE Linux Enterprise Server 15

Fortify ScanCentral SAST Controller Application Server

The Micro Focus Fortify ScanCentral SAST Controller supports Apache Tomcat version 9.x running on JRE 11.

Fortify ScanCentral SAST Client and Sensor Requirements

This section describes the requirements for the Fortify ScanCentral SAST clients and sensors.

Fortify ScanCentral SAST Client and Sensor Hardware Requirements

Micro Focus Fortify ScanCentral SAST clients and sensors run on any machine that supports Micro Focus Fortify Static Code Analyzer. Fortify ScanCentral SAST clients and sensors are installed on build machines that run Micro Focus Fortify Static Code Analyzer. See "Fortify Static Code Analyzer Requirements" on page 27 for hardware, platform, and architecture requirements.

Sensor Disk Space Requirements

To estimate the amount of disk space required on the machine that runs a Fortify ScanCentral SAST sensor, use one of the following equations:

Intended Use	Equation
Remote scan only	*<num_of_scans>* x (*<size_avg_MBS>* + *<size_avg_FPR>* + *<size_avg_SCA_log>*) x *<num_days_data_is_persisted>*
Remote translation and scan	*<num_jobs_per_day>* x (*<size_avg_archived_project_with_dependencies>* + *<size_avg_project_with_dependencies>* + *<size_avg_FPR>* + *<size_avg_SCA_log>*) x *<number_days_data_is_persisted>*

By default, data is persisted for seven days.

Fortify ScanCentral SAST Client and Sensor Software Requirements

Fortify ScanCentral SAST clients and sensors are installed on build machines that run Micro Focus Fortify Static Code Analyzer. See "Software Requirements" on page 27 for the software requirements.

Fortify ScanCentral SAST standalone clients require Java 11.

Fortify ScanCentral SAST Sensor Languages and Build Tools

Micro Focus Fortify ScanCentral SAST supports offloading the translation phase of the analysis to ScanCentral SAST sensors for the languages and build tools described in this section.

Languages

Fortify ScanCentral SAST supports offloading translation to ScanCentral sensors for the following languages. See "Languages" on page 28 for specific supported versions.

- .NET applications in C# and Visual Basic (VB.NET) (.NET Core, .NET Standard, ASP.NET)

  Note:

  - Packaging of .NET applications is supported only on Windows systems.
  - Translation of .NET applications requires .NET Framework version 4.7.2 or later *and* .NET 6.0.

- ABAP
- Apex
- Classic ASP
- ColdFusion
- Dockerfiles
- Go
- Java
- JavaScript
- Kotlin
- PHP
- PL/SQL
- Python
- Ruby
- T-SQL
- TypeScript
- Visual Basic 6.0

Build Tools

Fortify ScanCentral SAST supports the build tools listed in the following table.

Build Tool	Versions
Gradle	5.0–7.3

Build Tool	Versions
Maven	3.5.x, 3.6.x, 3.8.x, 3.9.x
MSBuild	14.0, 15.x, 16.x, 17.0, 17.1, 17.2

Fortify Software Security Center Server Requirements

This section describes the system requirements for the Fortify Software Security Center server.

Hardware Requirements

Fortify Software Security Center requires the hardware specifications listed in the following table.

	Component	Minimum Required	Minimum Recommended
Application server	Java heap size	4 GB	24 GB
Database server	Processor	Quad-core	Eight-core
	RAM	8 GB	64 GB

Database Hardware Requirements

Fortify recommends an eight-core processor with 64 GB of RAM for the Fortify Software Security Center database. Using less than this recommendation can impact Fortify Software Security Center performance.

Use the following formula to estimate the size (in GB) of the Fortify Software Security Center database disk space:

((<*num_issues*>*30 KB) + <*size_of_artifacts*>) ÷ 1,000,000

where:

- <*num_issues*> represents the total number of issues in the system
- <*size_of_artifacts*> represents the total size in KB of all uploaded artifacts and analysis results

Note: This formula produces only a rough estimate for database disk space allocation. Do not use it to estimate disk space requirements for long-term projects. Disk requirements for Fortify Software Security Center databases increases in proportion to the number of projects, scans, and issues in the system.

Database Performance Metrics for Minimum and Recommended Hardware Requirements

The following table shows performance metrics (number of issues discovered per hour) for Fortify Software Security Center configured with the minimum and the recommended hardware requirements.

Database	Issues per Hour Minimum Configuration	Issues per Hour Recommended Configuration
MySQL	362,514	2,589,385
Oracle	231,392	3,020,950
SQL Server	725,028	3,625,140

Platforms and Architectures

Fortify Software Security Center supports the platforms and architectures listed in the following table.

Operating System	Versions
Windows	Server 2016 Server 2019 Server 2022
Linux	Red Hat Enterprise Linux 7.x, 8 SUSE Linux Enterprise Server 15

Note: Although Fortify Software Security Center has not been tested on all Linux variants, most distributions are not known to have issues.

Application Servers

Fortify Software Security Center supports Apache Tomcat version 9.x for the following JDK versions:

- Oracle JDK 11
- Red Hat OpenJDK 11
- SUSE OpenJDK 11
- Zulu OpenJDK 11 from Azul

Fortify only supports the deployment of a single Fortify Software Security Center instance. Furthermore, that instance must not be behind a load balancer.

Fortify Software Security Center Database

Fortify Software Security Center requires that all database schema collations are case-sensitive.

Caution! Fortify Software Security Center does not support MySQL or Oracle in the cloud.

Important! Disk I/O encompasses the input/output operations on a physical disk. If you are reading data from a file on a disk, the processor must wait for the file to be read (the same applies to writing data to a file). Fortify Software Security Center is a high I/O-intensive application, which affects performance. Make sure that your disk subsystem provides low read/write latency. Fortify recommends that you monitor disk I/O as the database grows.

Fortify Software Security Center supports the databases listed in the following table.

Database	Versions	Collation / Character Sets	Driver
MySQL	8.0 (Community Edition)	latin1_general_cs and utf8_bin	The driver is included in the Fortify Software Security Center WAR file.
Oracle	12c Release 2 19c (18.3)	AL32UTF8 for all languages WE8MSWIN1252 for US English	The Oracle Database 21c JDBC driver is included in the Fortify Software Security Center WAR file.
SQL Server	2017 2019 AWS SQL Server Azure SQL Server	SQL_Latin1_ General_CP1_CS_ AS	The Microsoft JDBC Driver 11.2.1 for SQL Server is included in the Fortify Software Security Center WAR file.

Note: Fortify does not support the direct conversion from one database server type to another, such as converting from MySQL to Oracle. To do this, you must use the Server API to move data from your current Fortify Software Security Center instance to a new Fortify Software Security Center instance that uses the database server type you want to use going forward. Professional Services can assist you with this process.

Deploying Fortify Software Security Center to a Kubernetes Cluster (Optional Deployment Strategy)

If you plan to deploy Fortify Software Security Center on a Kubernetes cluster, you must make sure that the following requirements are met.

Kubernetes Cluster Requirements

The following are the *minimum* requirements for the default installation.

- Kubernetes versions 1.23, 1.24, 1.25, 1.26
- Kubernetes Persistent Volumes with optional support for Pod Security Context fsGroup option (fsGroup support is required for using a non-default container user ID.)
- Kubernetes LoadBalancer Service Type (Recommended)
- 28 GB of available RAM and 8 CPUs on a single Kubernetes node
- 4 GiB of storage for persistent volume

Locally-Installed Tools Required

- A kubectl command-line tool - Fortify recommends that you use the same kubectl command-line tool version as the Kubernetes cluster version (1.23, 1.24, 1.25, 1.26), or follow the Kubernetes version skew policy (see https://kubernetes.io/releases/version-skew-policy).
- Helm command-line tool, versions 3.9, 3.10, 3.11. To determine which Helm command-line tool version matches your Kubernetes cluster version, see the Helm Version Support Policy (https://helm.sh/docs/topics/version_skew).
- (Recommended) A Docker client and server installation (any version)

Additional Requirements

- Kubeconfig file for the Kubernetes cluster
- Docker Hub account with access to Fortify Software Security Center images

  Note: If you need access to Fortify Docker Organization on Docker Hub, contact fortifydocker@microfocus.com with your first name, your last name, and your Docker account name. Fortify will then give you access to the Fortify Docker organization that contains the Fortify Software Security Center images.

- DNS name for the Fortify Software Security Center web application (address used to access the service)

- Java keystore for setting up HTTPS (For details, see the *Fortify Software Security Center User Guide*.) The keystore must contain a CA certificate and a server certificate for the Fortify Software Security Center DNS name with an associated private key.
  - Keystore password
  - Private key password
- An installed MySQL, Oracle, or SQL Server for the database server
  - Database server host name
  - Name of the Fortify Software Security Center database
  - Username and password for an account that has permission to manage the Fortify Software Security Center schema and data
- Fortify Software Security Center license

Browsers

Fortify recommends that you use one of the browsers listed in the following table and a screen resolution of 1400 x 800.

Browser	Version
Google Chrome	90 or later
Microsoft Edge	90 or later
Mozilla Firefox	91 or later
Safari	14 or later

Authentication Systems

Fortify Software Security Center supports the following directory services:

- LDAP: LDAP 3 compatible

  Important! Although Fortify supports the use of multiple LDAP servers, it does not support the use of multiple LDAP servers behind a load balancer unless they are exact copies.

- Windows Active Directory Service

Single Sign-On (SSO)

Fortify Software Security Center supports:

- Central Authentication Service (CAS) SSO
- HTTP Headers SSO (Oracle SSO, CA SSO)

- SAML 2.0 SSO
- SPNEGO/Kerberos SSO
- X.509 SSO

BIRT Reporting

Fortify Software Security Center custom reports support BIRT Report Designer version 4.9.0.

(Linux with OpenJDK only) Installing Required Fonts

If your Fortify Software Security Center server is installed on a Linux system, and you are running OpenJDK, you must install the fontconfig library, DejaVu Sans fonts, and DejaVu serif fonts on the server to enable users to successfully generate reports. Otherwise, report generation will fail. If you need to, you can download these fonts from https://github.com/dejavu-fonts/dejavu-fonts.

(Non-GUI Linux Operating System only) Installing Required Libraries

If you are using a non-GUI Linux operating system, you must install the GTK and X Window System (X11) libraries to successfully generate reports.

Service Integrations for Fortify Software Security Center

Fortify Software Security Center supports the service integrations listed in the following table.

Service	Application	Versions
Bug tracking	Application Lifecycle Management (ALM)/ Quality Center Enterprise (QC)	12.50
	Azure DevOps **Note:** Only basic user password authentication is supported.	n/a
	Azure DevOps Server	2019, 2020
	Bugzilla	5.0.x
	Jira	8.13
	Jira Cloud	n/a
Dynamic assessments	Fortify WebInspect Enterprise	22.2.x
	Fortify ScanCentral DAST	23.1.x

Fortify Static Code Analyzer Requirements

This section describes the system requirements for Fortify Static Code Analyzer.

Hardware Requirements

Fortify recommends that you install Fortify Static Code Analyzer on a high-end processor with the hardware requirements described in the following table.

RAM	Processor	Programming Language to Analyze
16 GB	Quad-core	Non-dynamic languages
32 GB	Eight-core	Dynamic languages such as JavaScript, TypeScript, Python, PHP, and Ruby

Increasing the number of processor cores and RAM both result in faster processing. If your software is complex, you might require more RAM or processors. See the information about improving performance in the *Micro Focus Fortify Static Code Analyzer User Guide* for recommendations.

Software Requirements

Fortify Static Code Analyzer requires Java 11. The Fortify Static Code Analyzer installation includes an embedded OpenJDK/JRE version 11.0.18.

Language	Requirement	Operating System
Visual Studio, MSBuild, or .NET projects	.NET Framework 4.8 or later	Windows
	.NET 6.0	Windows Linux
ABAP/BSP	Fortify ABAP Extractor is supported on a system running SAP release 7.02, SP level 0006.	
COBOL	Microsoft Visual C++ 2017 Redistributable (x86) **Note:** This is not a requirement for Legacy COBOL analysis.	Windows

Language	Requirement	Operating System
Scala	Scala Fortify compiler plugin available in the Maven Central Repository	All

Platforms and Architectures

Fortify Static Code Analyzer supports the platforms and architectures listed in the following table.

Operating System	Platforms / Versions
Windows	Windows 10, 11 Windows Server 2016, 2019, 2022
Linux	CentOS Linux 7.x (7.6 or later) Red Hat Enterprise Linux 7.x (7.2 or later), 8.x (8.2 or later), 9.x SUSE Linux Enterprise Server 15 Ubuntu 20.04.1 LTS, 22.04.1 LTS
macOS	12, 13
AIX	7.1 **Important!** You must have the IBM XL C/C++ for AIX 16.1 Runtime environment package installed.
Solaris SPARC	11.3
Solaris x64	11.4

Languages

Fortify Static Code Analyzer supports the programming languages listed in the following table.

Language / Framework	Versions
.NET	5.0, 6.0, 7

Language / Framework	Versions
.NET Core	2.0–3.1
.NET Framework	2.0–4.8
ABAP/BSP	6
ActionScript	3.0
Apex	55, 56, 57
C#	5, 6, 7, 8, 9, 10, 11
C/C++	C11, C++11, C++14, C++17, C++20 (see "Compilers" on page 36)
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 6.1 (or earlier), 6.2, and 6.3 with CICS, IMS, DB2, and IBM MQ Visual COBOL 6.0, 7.0, 8.0
ColdFusion	8, 9, 10
Dart	2.12–2.18
Docker (Dockerfiles)	any
Flutter	2.0–3.3
Go	1.12–1.19 **Note:** Fortify Static Code Analyzer supports analyzing Go code on Windows and Linux.
HCL	2.0 **Note:** HCL language support is specific to Terraform and supported cloud provider Infrastructure as Code (IaC) configurations.
HTML	5 or earlier
Java	7, 8, 9, 10, 11, 12, 13, 14, 17

Language / Framework	Versions
(including Android)	
JavaScript	ECMAScript 2015–2022
JSON	ECMA-404
JSP	1.2, 2.1
Kotlin	1.3, 1.4, 1.5, 1.6, 1.7
MXML (Flex)	4
Objective-C/C++	2.0 (see "Compilers" on page 36)
PHP	7.3, 7.4, 8.0, 8.1, 8.2
PL/SQL	8.1.6
Python	2.6, 2.7, 3.0–3.11
Ruby	1.9.3
Scala	2.11, 2.12, 2.13
Swift	5 (see "Compilers" on page 36 for supported swiftc versions)
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	2.8, 3.x, 4.x
VBScript	2.0, 5.0
Visual Basic (VB.NET)	11, 14, 15.x, 16.0
Visual Basic	6.0
XML	1.0
YAML	1.2

Libraries, Frameworks, and Technologies

Fortify Static Code Analyzer supports the libraries, frameworks, and technologies listed in this section with dedicated Fortify Secure Coding Rulepacks and vulnerability coverage beyond core supported languages.

Java

- Adobe Flex Blaze DS
- Ajanta
- Amazon Web Services (AWS) SDK
- Android
- Android Jetpack
- Apache Axiom
- Apache Axis
- Apache Beam
- Apache Beehive NetUI
- Apache Catalina
- Apache Cocoon
- Apache Commons
- Apache ECS
- Apache Hadoop
- Apache HttpComponents
- Apache Jasper
- Apache Log4j
- Apache Lucene
- Apache MyFaces
- Apache OGNL
- Apache ORO
- Apache POI
- Apache SLF4J
- Apache Slide
- Apache Spring Security (Acegi)
- Apache Struts
- Apache Tapestry
- Apache Tomcat
- Apache Torque
- Apache Util
- Apache Velocity
- Apache Wicket
- Apache Xalan
- Apache Xerces
- ATG Dynamo
- Azure SDK
- Castor
- Display Tag
- Dom4j
- GDS AntiXSS
- Google Cloud
- Google Dataflow
- Google Guava
- Google Web Toolkit
- gRPC
- Gson
- Hibernate
- iBatis
- IBM MQ
- IBM WebSphere
- Jackson
- Jakarta Activation
- Jakarta EE (Java EE)
- Java Annotations
- Java Excel API
- JavaMail
- JAX-RS
- JAXB
- Jaxen
- JBoss
- JDesktop
- JDOM
- Jetty
- JGroups
- json-simple
- JTidy Servlet
- JXTA
- JYaml
- Liferay Portal
- MongoDB
- Mozilla Rhino
- MyBatis
- Netscape LDAP API
- OpenCSV
- Oracle Application Development Framework (ADF)
- Oracle BC4J
- Oracle JDBC
- Oracle OA Framework
- Oracle tcDataSet
- Oracle XML Developer Kit (XDK)
- OWASP Enterprise Security API (ESAPI)
- OWASP HTML Sanitizer
- OWASP Java Encoder
- Plexus Archiver
- Realm
- Restlet
- SAP Web Dynpro
- Saxon
- SnakeYAML
- Spring
- Spring MVC
- Spring Boot
- Spring Data Commons
- Spring Data JPA
- Spring Data MongoDB
- Spring Data Redis
- Spring HATEOAS
- Spring JMS
- Spring JMX
- Spring Messaging
- Spring Security
- Spring Webflow
- Spring WebSockets
- Spring WS
- Stripes
- Sun JavaServer Faces (JSF)
- Tungsten
- Weblogic
- WebSocket
- XStream
- YamlBeans
- ZeroTurnaround ZIP
- Zip4J

Kotlin

Kotlin support includes all libraries covered for Java and the following Kotlin libraries.

- Kotlin standard library

Scala

Scala support includes all libraries covered for Java and the following Scala libraries.

Akka HTTP	Scala Slick
Scala Play	

.NET

.NET Framework, .NET Core, and .NET Standard	ASP.NET Web API	Hot Chocolate	MongoDB	SharePoint Services
.NET WebSockets	Azure SDK	IBM Informix .NET Provider	MySQL Connector/NET	SharpCompress
ADO.NET Entity Framework	Castle ActiveRecord	Json.NET Log4Net	NHibernate	SharpZipLib
ADODB	CsvHelper	Microsoft ApplicationBlocks	NLog	SQLite .NET Provider
Amazon Web Services (AWS) SDK	Dapper	Microsoft My Framework	Npgsql	SubSonic
ASP.NET MVC	DB2 .NET Provider	Microsoft Practices Enterprise Library	Open XML SDK	Sybase ASE ADO.NET Data Provider
ASP.NET SignalR	DotNetZip	Microsoft Web Protection Library	Oracle Data Provider for .NET	Xamarin
	Entity Framework		OWASP AntiSamy	Xamarin Forms
	Entity Framework Core		Saxon	YamlDotNet
	fastJSON			

C

ActiveDirectory LDAP	CURL Library	MySQL	OpenSSL	Sun RPC
Apple System Logging (ASL)	GLib	Netscape LDAP	POSIX Threads	WinAPI
	JNI	ODBC	SQLite	

C++

Boost Smart Pointers	STL
MFC	WMI

SQL

Oracle ModPLSQL

PHP

ADOdb	PHP Debug	PHP Mcrypt	PHP OpenSSL	PHP Smarty
Advanced PHP Debugging	PHP DOM	PHP Mhash	PHP PostgreSQL	PHP XML
CakePHP	PHP Extension	PHP Mysql	PHP Reflection	PHP XMLReader
	PHP Hash	PHP OCI8	PHP SimpleXML	PHP Zend

JavaScript/TypeScript/HTML5

Angular	Helmet	Node.js Azure Storage	React Native Async Storage	Underscore.js
Apollo Server	iOS JavaScript Bridge	Node.js Core	React Router	Vue
Express	jQuery	React	SAPUI5/OpenUI5	
GraphQL.js	JS-YAML	React Native	Sequelize	
Handlebars	Mustache			

Python

aiopg	Graphene	memcache-client	psycopg2	requests
Amazon Web Services (AWS) Lambda	gRPC	_mysql	pycrypto	simplejson
Azure Functions	httplib2	MySQL Connector/Python	pycurl	six
Django	Jinja2	MySQLdb	pylibmc	Twisted Mail
Flask	libxml2	oslo.config	PyMongo	urllib3
Google Cloud	lxml		PyYAML	WebKit

Ruby

MySQL	Rack	Thor
pg	SQLite	

Objective-C

AFNetworking	Apple CoreFoundation	Apple LocalAuthentication	Apple WatchConnectivity	SBJson
Apple AddressBook	Apple CoreLocation	Apple MessageUI	Apple WatchKit	SFHFKeychainUtils
Apple AppKit	Apple CoreServices	Apple Security	Apple WebKit	SSZipArchive
Apple CFNetwork	Apple CoreTelephony	Apple Social	Hpple	ZipArchive
Apple ClockKit	Apple Foundation	Apple UIKit	Objective-Zip	ZipUtilities
Apple CommonCrypto	Apple HealthKit		Realm	ZipZap
Apple CoreData				

Swift

Alamofire	Apple CoreFoundation	Apple MessageUI	Apple WatchKit	Zip
Apple AddressBook	Apple CoreLocation	Apple Security	Apple WebKit	ZipArchive
Apple CFNetwork	Apple Foundation	Apple Social	Hpple	ZIPFoundation
Apple ClockKit	Apple HealthKit	Apple SwiftUI	Realm	ZipUtilities
Apple CommonCrypto	Apple LocalAuthentication	Apple UIKit	SQLite	ZipZap
Apple CoreData		Apple WatchConnectivity	SSZipArchive	

COBOL

Auditor	Micro Focus COBOL Run-time System	POSIX
CICS	MQ	SQL
DLI		

Go

GORM
logrus
gRPC

Configuration

.NET Configuration	Docker Configuration (Dockerfiles)	Java Apache Struts	Java OWASP AntiSamy	OpenAPI Specification
Adobe Flex (ActionScript) Configuration	GitHub Actions	Java Apache Tomcat Configuration	Java Spring and Spring MVC	Oracle Application Development Framework (ADF)
Ajax Frameworks	Google Android Configuration	Java Blaze DS	Java Spring Boot	PHP Configuration
Amazon Web Service (AWS)	iOS Property List	Java Hibernate Configuration	Java Spring Mail	PHP WordPress
Ansible	J2EE Configuration	Java iBatis Configuration	Java Spring Security	Silverlight Configuration
AWS CloudFormation	Java Apache Axis	Java IBM WebSphere	Java Spring WebSockets	Terraform (AWS, Azure, GCP)
Azure Resource Manager (ARM)	Java Apache Log4j Configuration	Java MyBatis Configuration	Java Weblogic	WS-SecurityPolicy
Build Management	Java Apache Spring Security (Acegi)		Kubernetes	XML Schema
			Mule	

Secrets

.netrc	Defined	HashiCorp (Terraform, Vault)	New Relic	Sendbird
1Password	DES		npm	SendGrid

- Actually Good Encryption (AGE)
- Adafruit
- Adobe
- Airtable
- Algolia
- Alibaba (Aliyun)
- Amazon (AWS, MWS)
- Apple (macOS)
- Apache HTTP
- Asana
- Atlassian
- Authress
- Basic access authentication
- bcrypt
- Beamer
- Bearer token
- Bitbucket
- Bittrex
- Brevo (Sendinblue)
- Clojars
- Code Climate
- Codecov
- Coinbase
- Confluent
- Contentful
- Databricks
- Datadog
- DigitalOcean
- Docker
- Doppler
- Droneci
- Dropbox
- Duffel
- Dynatrace
- EasyPost
- Encryption key
- Etsy
- Facebook
- Fastly
- Finicity
- Finnhub
- Flickr
- Flutterwave
- Frame.io
- Freshbooks
- Git
- GitHub
- GitLab
- Gitter
- GNOME
- GNU (Bash)
- GoCardless
- Google (API, Google Cloud, OAuth)
- Grafana
- Heroku
- HexChat
- HubSpot
- Intercom
- Java
- JFrog (Artifactory)
- JSON Web Token
- KDE Wallet (Kwallet)
- KeePass
- Kraken
- Kucoin
- LaunchDarkly
- Linear
- LinkedIn
- Lob
- Mailchimp
- Mailgun
- Mapbox
- Mattermost
- MD5
- MessageBird
- Microsoft (Azure App Storage, Cosmos DB, Functions and Bitlocker, PowerShell, RDP, VBScript)
- Microsoft (Outlook)
- Mutt
- MySQL
- Netlify
- NuGet
- Okta
- OpenVPN
- Password in comment
- Password in connection string
- Password in PowerShell script
- Password in URI
- Password Safe
- PayPal (Braintree)
- Pidgin
- Plaid
- Planetscale
- PostgreSQL
- Postman
- Prefect
- Pulumi
- PuTTY
- PyPI
- RapidAPI
- Readme
- RSA Security
- Ruby (Ruby on Rails, RubyGems)
- Sauce Labs
- Secret key
- Secure Shell Protocol (SSH)
- Sentry
- SHA1
- SHA256
- SHA512
- Shippo
- Shopify
- Sidekiq
- Slack
- SonarQube
- Square
- Squarespace
- StackHawk
- Stripe
- Sumologic
- Telegram
- Travis
- Trello
- Twilio
- Twitch
- Twitter
- Typeform
- Yandex
- Zendesk

Build Tools

Fortify Static Code Analyzer supports the build tools listed in the following table.

Build Tool	Versions	Notes
Ant	1.10.x or earlier	
Gradle	5.0–7.4.x, 8.0.x	The Fortify Static Code Analyzer Gradle build integration supports the following language/platform combinations: • Java/Windows, Linux, and macOS • Kotlin/Windows and Linux • C/Linux • C++/Linux
Maven	3.0.5, 3.5.x, 3.6.x, 3.8.x, 3.9.x	
MSBuild	14.0, 15.x, 16.x, 17.0–17.5	The MSBuild integration is supported on Windows and Linux.
Xcodebuild	13.2, 13.2.1, 13.3, 13.3.1, 13.4, 13.4.1, 14, 14.0.1, 14.1, 14.2, 14.3, 14.3.1	

Compilers

Fortify Static Code Analyzer supports the compilers listed in the following table.

Compiler	Versions	Operating Systems
gcc	GNU gcc 6.x–10.4, 11	Windows, Linux, macOS
	GNU gcc 4.9, 5.x	Windows, Linux, macOS, AIX, Solaris
g++	GNU g++ 6.x–10.4, 11	Windows, Linux, macOS
	GNU g++ 4.9, 5.x	Windows, Linux, macOS, AIX, Solaris
OpenJDK javac	9, 10, 11, 12, 13, 14, 17	Windows, Linux, macOS, AIX, Solaris

Compiler	Versions	Operating Systems
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
Clang	13.0.0[1], 13.1.6, 14.0.0, 14.0.3	macOS
Swiftc	5.5.2, 5.6, 5.6.1, 5.7, 5.7.1, 5.8, 5.8.1[2]	macOS

[1]Clang 13.0.0 is only supported when used with Xcode 13.2 and 13.2.1 as part of an Xcode project.

[2]Fortify Static Code Analyzer supports applications built in the following Xcode versions: 13.2, 13.2.1, 13.3, 13.3.1, 13.4, 13.4.1, 14, 14.0.1, 14.1, 14.2, 14.3, 14.3.1.

Fortify Software Security Content

Fortify Secure Coding Rulepacks are backward compatible with all supported Fortify Software versions. This ensures that Rulepack updates do not break any working Fortify Software installation.

Fortify Static Code Analyzer Applications and Tools Requirements

This section describes the system requirements for Fortify Static Code Analyzer applications and tools.

Hardware Requirements

Fortify Static Code Analyzer applications and tools require a system with at least 8 GB of RAM. In addition, Fortify Static Code Analyzer applications used to perform code analysis have the same hardware requirements as Fortify Static Code Analyzer (see "Hardware Requirements" on page 27).

Software Requirements

Fortify Static Code Analyzer applications and tools require Java 11. The Fortify Applications and Tools installation includes an embedded OpenJDK/JRE version 11.0.18.

To run Fortify Audit Workbench, Fortify Custom Rules Editor, or Fortify Scan Wizard remotely from a local server, you must use a remote desktop connection such as Virtual Network Computing (VNC) or Windows Remote Desktop Connection. Do not use X Window System (X11) forwarding to access these Fortify Static Code Analyzer applications from a remote server.

Platforms and Architectures

Fortify Static Code Analyzer applications and tools support the platforms and architectures listed in the following table.

Operating System	Platforms / Versions
Windows	10, 11
Linux	Red Hat Enterprise Linux 7.x, 8 SUSE Linux Enterprise Server 15 **Important!** Fortify Audit Workbench, Fortify Custom Rules Editor, and Fortify Scan Wizard require GTK version 3.22 or later. Some platform versions include this requirement such as Red Hat Enterprise Linux 7.4 and later.
macOS	11, 12, 13

Service Integrations for Fortify Applications and Tools

The following table lists the supported service integrations for Fortify Audit Workbench and the Fortify Secure Code Plugins.

Service	Versions	Supported Application
Application Lifecycle Management (ALM)/ Quality Center	12.50	Fortify Audit Workbench Fortify Plugin for Eclipse
Azure DevOps Server	2019, 2020	Fortify Audit Workbench Fortify Plugin for Eclipse Fortify Extension for Visual Studio
Azure DevOps **Note:** Only basic user password authentication is supported.	n/a	Fortify Audit Workbench Fortify Plugin for Eclipse
Bugzilla	5.0.x	Fortify Audit Workbench

Service	Versions	Supported Application
		Fortify Plugin for Eclipse Fortify Extension for Visual Studio
Jira	8.13	Fortify Audit Workbench Fortify Plugin for Eclipse
Jira Cloud	n/a	Fortify Audit Workbench Fortify Plugin for Eclipse
Fortify Software Security Center Bug Tracker	23.1.0	Fortify Audit Workbench Fortify Plugin for Eclipse Fortify Extension for Visual Studio

Secure Code Plugins

The following table lists the supported integrated development environments (IDE) for the Fortify Secure Code Plugins.

Secure Code Plugin	IDE	Versions	Notes
Fortify Plugin for Eclipse	Eclipse	2020-x 2021-x, 2022-x 2023-03	
Fortify Analysis Plugin for IntelliJ IDEA and Android Studio	IntelliJ IDEA	2020.x 2021.x 2022.x 2023.1	
	Android Studio	2020.x 2021.x 2022.1	
Fortify Extension for Visual Studio	Visual Studio	2017 2019	Visual Studio Community, Professional, and Enterprise editions for Windows are supported.

Secure Code Plugin	IDE	Versions	Notes
		2022	For supported MSBuild versions, see "Build Tools" on page 36.

Single Sign-On (SSO)

Fortify Audit Workbench, the Fortify Plugin for Eclipse, and the Fortify Extension for Visual Studio support the following SSO methods to connect with Fortify Software Security Center:

- SPNEGO/Kerberos SSO

  Supported on Windows only.
- X.509 SSO

Note: Fortify Audit Workbench and the Secure Code Plugins can use token-based authentication with Fortify Software Security Center, which removes the requirement to configure SSO directly.

BIRT Reports

To generate BIRT reports on a Linux system from the Secure Code Plugins or the BIRTReportGenerator utility, you must install fontconfig, DejaVu Sans fonts, and DejaVu serif fonts on the server.

To run the BIRTReportGenerator utility in a Linux Docker container, you must have the X Window System (X11) libraries installed in the image. The X11 libraries provide the graphical user interface API that BIRT requires for data visualization.

Red Hat Enterprise and CentOS Example:

```
yum -y install xorg-x11-xauth xorg-x11-fonts-* xorg-x11-utils
```

Ubuntu Example:

```
apt-get install x11-apps
```

Fortify WebInspect Requirements

Before you install Micro Focus Fortify WebInspect, make sure that your system meets the requirements described in this section. Fortify does not support beta or pre-release versions of operating systems, service packs, or required third-party components.

WebInspect Hardware Requirements

Fortify recommends that you install Micro Focus Fortify WebInspect on a system that conforms to the supported components listed in the following table.

Component	Requirement	Notes
Processor	2.5 GHz quad-core or faster	Complex applications might benefit from additional cores.
RAM	16 GB	Complex applications might benefit from additional memory. Fortify recommends 32 GB of memory to scan with single-page application (SPA) support.
Hard disk	40 GB	Using SQL Express and storing scans locally requires additional disk space per scan.
Display	1280 x 1024	

WebInspect Software Requirements

Micro Focus Fortify WebInspect runs on and works with the software packages listed in the following table.

Package	Versions	Notes
Windows	Windows 10	Recommended **Important!** Not all builds of Windows 10 support .NET Framework 4.8. Refer to Microsoft's website to identify Windows 10 builds that support .NET Framework 4.8.
	Windows 11	This version is required for conducting scans of gRPC APIs.
	Windows Server 2019	
	Windows Server 2022	
.NET Platform	.NET Framework 4.8	
SQL Server (English-language versions only)	SQL Server 2019	Recommended No scan database limit
	SQL Server 2022	No scan database limit
	Azure SQL Server	Using Azure SQL Server outside the Azure

Package	Versions	Notes
		infrastructure may cause poor performance for Fortify WebInspect. Fortify recommends using Azure SQL Server with Fortify WebInspect inside the Azure infrastructure only.
SQL Server Express (English-language versions only)	SQL Server 2019 Express	Recommended 10 GB scan database limit
	SQL Server 2022 Express	10 GB scan database limit
	SQL Server 2017 Express	10 GB scan database limit
	SQL Server 2016 Express SP2	10 GB scan database limit
Portable Document Format	Adobe Acrobat Reader 11	Recommended
	Adobe Acrobat Reader 8.1.2	Minimum

Support for Postman

A Postman collection version 2.0 or 2.1 is required to conduct scans in Fortify WebInspect.

Additionally, you must install the following third-party software on the machine where Fortify WebInspect is installed:

- Newman command-line collection runner 4.5.1 or later

Important! You must install Newman globally rather than locally. You can do this by adding a `-g` option to the installation command, as follows:

```
npm install -g newman
```

When you install Newman, a path variable for Newman is automatically added to the user variables. The path variable is similar to the following:

<directory_path>\AppData\Roaming\npm

You must manually add the same Newman path variable to the system environment variables. Ensure that the variable is in both the user variables and system environment variables before proceeding.

System variables are read only when the machine boots, so after manually adding the path variable, you must restart your machine. See your Windows documentation for specific instructions on how to add a system environment variable.

- Node.js and the included Node Package Manager (NPM)

Note: Install the Node.js version that is required for the version of Newman that you install. For more information, see https://www.npmjs.com/package/newman.

Notes on SQL Server Editions

When using the Express edition of SQL Server:

- Scan data must not exceed the database size limit. If you require a larger database or you need to share your scan data, use the full version of SQL Server.
- During the installation you might want to enable "Hide advanced installation options." Accept all default settings. Micro Focus Fortify WebInspect requires that the default instance is named SQLEXPRESS.

When using the full edition of SQL Server:

- You can install the full version of SQL Server on the local host or nearby (co-located). You can configure this option in Fortify WebInspect Application Settings (**Edit > Application Settings > Database**).
- The account specified for the database connection must also be a database owner (DBO) for the named database. However, the account does not require sysadmin (SA) privileges for the database server. If the database administrator (DBA) did not generate the database for the specified user, then the account must also have the permission to create a database and to manipulate the security permissions. The DBA can rescind these permissions after Fortify WebInspect sets up the database, but the account must remain a DBO for that database.

WebInspect on Docker

Fortify WebInspect on Docker has the software requirements listed in the following table.

Package	Versions	Notes
Windows	Windows Server 2019	The Windows version supports the process isolation runtime mode.
Red Hat Universal Base Image (UBI)	8.*x* x86_64	The Linux version supports conducting scans of gRPC APIs.

Follow Docker recommendations for the Docker engine version to use for these versions of Windows and Red Hat images.

Notes on Image Databases

SQL Server Express is the default database for the Fortify WebInspect images. There is a 10 GB scan database limit.

Hardware Requirements

Fortify recommends that you install Micro Focus Fortify WebInspect on Docker on a host that conforms to the supported components listed in the following table and configure the container to use these resources. Fortify does not support beta or pre-release versions of operating systems, service packs, and required third-party components.

Component	Requirement	Notes
Processor	2.5 GHz quad-core or faster	Complex applications might benefit from additional cores.
RAM	16 GB	Complex applications might benefit from additional memory. Fortify recommends 32 GB of memory to scan with single-page application (SPA) support.
Hard disk	40 GB	Using SQL Express and storing scans locally requires additional disk space per scan.

Fortify WebInspect Ports and Protocols

This section describes the ports and protocols Micro Focus Fortify WebInspect uses to make required and optional connections.

Required Connections

The following table lists the ports and protocols Micro Focus Fortify WebInspect uses to make required connections.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect to target host	Target host	Scan target host	Any	HTTP	Fortify WebInspect must connect to the web application or web service to be scanned.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect to SQL database	SQL Server Express, SQL Server Standard/Enterprise, or Azure SQL Server	SQLEXPRESS service on localhost or SQL TCP service locally installed or remote host	1433	SQL TCP	Used to maintain the scan data and to generate reports within the Fortify WebInspect application.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect to Certificate Revocation List (CRL)	Sectigo CRL	http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl	80	HTTP	Offline installations of Fortify WebInspect or Fortify WebInspect Enterprise require you to manually download and apply the CRL from Verisign. Fortify WebInspect products prompt for these lists from Windows and their absence can cause problems with the application. A one-time download is sufficient, however Fortify recommends that you download the CRL as part of regular maintenance.

Optional Connections

The following table lists the ports and protocols Micro Focus Fortify WebInspect uses to make optional connections.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect to Fortify License activation server	Remote Fortify Licensing Service	https://licenseservice.fortify.microfocus.com	443	HTTPS over SSL	For one-time activation of a Fortify WebInspect Named User license. You may optionally use the following: • An offline activation process instead of using this direct connection • Upstream proxy with authentication instead of a direct connection
Fortify WebInspect to SmartUpdate server	Remote SmartUpdate service	https://smartupdate.fortify.microfocus.com	443	HTTPS over SSL	Used to automatically update the Fortify WebInspect product. SmartUpdate is automatic when opening the product UI, but can be disabled and run manually. Can optionally use upstream proxy with authentication instead of a direct connection.
Fortify WebInspect to Fortify Support Channel server	Remote Fortify Support Channel service	https://supportchannel.fortify.microfocus.com	443	HTTPS over SSL	Used to retrieve product marketing messages and to upload Fortify WebInspect data or product suggestions to Micro Focus Fortify Customer Support. Message check is automatic when opening the product UI, but can be disabled and run manually. Can optionally use upstream proxy with authentication instead of a direct connection.
Fortify WebInspect to Fortify License and Infrastructure Manager (LIM)	Fortify WebInspect LIM (Local Licensing Service)	Lease Concurrent User license	443	Web services over SSL	Required for Fortify WebInspect client to lease and use a Concurrent User license maintained in a LIM license pool. You can detach the client license from LIM after activation to avoid a constant connection.
Fortify WebInspect API	Local machine API, or network	http://localhost:8083/webinspect/api	8083 or user-	HTTP	Use to activate a Fortify WebInspect API Windows

Direction	Endpoint	URL or Details	Port	Protocol	Notes
listener	IP address		specified		Service. This opens a listening port on your machine, which you can use locally or remotely to generate scans and retrieve the results programmatically. This API can be SSL enabled, and supports Basic or Windows authentication.
Fortify WebInspect to Fortify WebInspect Enterprise	Fortify WebInspect Enterprise server	User-specified Fortify WebInspect server	443 or user-specified	HTTP or HTTPS over SSL	The Enterprise Server menu connects Fortify WebInspect as a client to the enterprise security solution to transfer findings and user role and permissions management.
Fortify WebInspect sensor service to Fortify WebInspect Enterprise	Fortify WebInspect Enterprise server	User-specified Fortify WebInspect server	443 or user-specified	HTTP or HTTPS over SSL	Separate from the Fortify WebInspect UI, you can configure the local installation as a remote scan engine for use by the enterprise security solution community. This is done through a Windows Service. This constitutes a different product from Fortify WebInspect desktop and is recommended to be run on its own, non-user-focused machine.
Browser to Fortify WebInspect	localhost	Manual Step-Mode Scan	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	Fortify WebInspect serves as a web proxy to the browser, enabling manual testing of the target web server through Fortify WebInspect.
Fortify WebInspect to Quality Center Enterprise (ALM)	QC server	User-specified ALM server	Server-specified	HTTP or HTTPS over SSL	Permits submission of findings as defects to the ALM bug tracker.

Connections for Tools

The following table lists the ports and protocols that the Micro Focus Fortify WebInspect tools use to make connections.

Tool	Direction	Endpoint	Port	Protocol	Notes
Web Proxy	To target host	localhost	8080 or user-specified	HTTP or HTTPS over SSL	Intercepts and displays web traffic
Web Form Editor	To target host	localhost	Dynamic, 8100, or user-specified	HTTP or HTTPS over SSL	Intercepts web traffic and captures submitted forms
Login or Workflow Macro Recorders	To target host	localhost	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	Records browser sessions for replay during scan
Web Discovery	Fortify WebInspect machine to targeted IP range	Target host network range	User-specified range	HTTP and HTTPS over SSL	Scanner for identifying rogue web applications hosted among the targeted scanned IP and port ranges Use to provide targets to Fortify WebInspect (manually)

Fortify WebInspect Agent

For system requirements, see "Fortify WebInspect Agent Requirements" on the next page.

WebInspect Software Development Kit (SDK)

The WebInspect SDK requires the following software:

- Visual Studio 2019 (version 16.9.0)
- .NET Framework 4.8

Important! Visual Studio Express versions do not support third-party extensions. Therefore, these versions do not meet the software requirements to use the WebInspect SDK.

Software Integrations for Fortify WebInspect

The following table lists products that you can integrate with Micro Focus Fortify WebInspect.

Product	Versions
Micro Focus Fortify WebInspect Enterprise	22.2.0
Application Lifecycle Management (ALM) **Note:** You must also install the ALM Connectivity tool to connect Fortify WebInspect to ALM.	11.5, 12.01, 12.21, 12.53
Micro Focus Fortify Software Security Center	23.1.0
Micro Focus Unified Functional Testing	11.5

Fortify WebInspect Agent Requirements

Micro Focus Fortify WebInspect Agent technology is delivered for production application logging and protection.

Platforms and Architectures

Fortify WebInspect Agent supports 32-bit and 64-bit applications written in Java 5, 6, 7, 8, and 10.

Java Runtime Environments

Fortify WebInspect Agent supports the Java runtime environments listed in the following table.

JRE	Major Versions
IBM J9	5 (SR10 or later) 6 (SR6 or later)
Oracle HotSpot	5, 6, 7, 8
Oracle JRockit	5, 6 (R27.6 or later)

Note: The Java agent is supported on Windows, Linux, and Unix.

Java Application Servers

Fortify WebInspect Agent supports the Java application servers listed in the following table.

Application Server	Versions
Apache Tomcat	6.0, 7.0, 8.0, 9.0
IBM WebSphere	7.0, 8.0, 8.5, 8.5.5
Oracle WebLogic	10.0, 10.3, 11g, 11gR1, 12c
Red Hat JBoss Enterprise Application Platform	7.3.0 or earlier
Jetty	9.3
WildFly	20.0.1 or earlier

.NET Frameworks

Fortify WebInspect Agent supports .NET Framework versions 2.0, 3.0, 3.5, 4.0, and 4.5–4.8.

IIS for Windows Server

Fortify WebInspect Agent supports Internet Information Services (IIS) versions 6.0, 7.0, 7.5, 8, 8.5, and 10.0.

Fortify WebInspect Enterprise Requirements

Before you install Micro Focus Fortify WebInspect Enterprise, make sure that your systems meet the requirements described in this section. Fortify does not support beta or pre-release versions of operating systems, service packs, or required third-party components.

Note: Product versions that are not specifically listed in this document are not supported.

Important Information About This Release

Micro Focus Fortify WebInspect Enterprise was not updated for the 23.1.0 release. However, Fortify WebInspect Enterprise 22.2.0 is compatible with Fortify Software Security Center 23.1.0 and the Fortify WebInspect 23.1.0 sensor.

Integrations for Fortify WebInspect Enterprise

You can integrate Micro Focus Fortify WebInspect Enterprise with the following components:

- Micro Focus Fortify WebInspect sensors 23.1.0
- Micro Focus Fortify WebInspect Agent 23.1.0

Fortify WebInspect Enterprise Database

Fortify recommends that you configure the database server on a separate machine from either Micro Focus Fortify Software Security Center or Micro Focus Fortify WebInspect Enterprise.

The Fortify WebInspect Enterprise Server SQL database requires case-insensitive collation.

Important! This is opposite the requirement for Fortify Software Security Center databases as described in "Fortify Software Security Center Database" on page 23.

WebInspect Enterprise Hardware Requirements

The following table lists the hardware requirements for the Micro Focus Fortify WebInspect Enterprise server.

Component	Requirement
Processor	3.0 GHz quad-core
RAM	16 GB
Hard disk	100+ GB
Display	1920 x 1080

WebInspect Enterprise Software Requirements

Micro Focus Fortify WebInspect Enterprise server runs on and works with the software packages listed in the following table.

Package	Versions	Notes
Windows	Windows Server 2016	Recommended
	Windows Server 2019	

Package	Versions	Notes
.NET Platform	.NET Framework 4.8	
Web Server	IIS 10	Recommended
	IIS 7.5, 8.0, 8.5	
SQL Server (English-language versions only)	SQL Server 2019	Recommended No scan database limit
	SQL Server 2017	No scan database limit
	SQL Server 2016 SP2	No scan database limit

Administrative Console Requirements

This section describes the hardware and software requirements for the Micro Focus Fortify WebInspect Enterprise Administrative Console.

You do not need to install the Fortify WebInspect Enterprise Administrative Console on the same machine as the Web Console of the Fortify WebInspect Enterprise server. The two consoles have different system requirements. In addition, you can install multiple Administrative Consoles on different machines connected to the same Fortify WebInspect Enterprise server.

Hardware Requirements

The following table lists the hardware requirements for Fortify WebInspect Enterprise Administrative Console.

Component	Requirement	Notes
Processor	2.5 GHz dual-core	Minimum
RAM	4 GB	Minimum
Hard disk	2 GB	
Display	1980 x 1080	Recommended
	1280 x 1024	Minimum

Software Requirements

The Fortify WebInspect Enterprise Administrative Console runs on and works with the software packages listed in the following table.

Package	Versions	Notes
Windows	Windows 10	Recommended
	Windows 8.1	
	Windows Server 2016	
	Windows Server 2019	
.NET	.NET Framework 4.8	

Fortify WebInspect Enterprise Ports and Protocols

This section describes the ports and protocols Micro Focus Fortify WebInspect Enterprise uses to make required and optional connections.

Required Connections

The following table lists the ports and protocols Micro Focus Fortify WebInspect Enterprise uses to make required connections.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect Enterprise Manager server to SQL database	SQL Server Standard/Enterprise	SQL TCP service on locally installed or remote host	1433 or user-specified	SQL TCP	Used to maintain the scan data and full Enterprise environment. Custom configurations of SQL Server are permitted, including port changes and encrypted communication.
Fortify WebInspect Enterprise Manager machine to Fortify Software Security Center server	Fortify Software Security Center server	User-specified Fortify Software Security Center server	8180 or user-specified	HTTP or HTTPS over SSL	As a modular add-on, Fortify WebInspect Enterprise requires a connection to its core Fortify Software Security Center server. **Note:** This connection is required only if you integrate Fortify WebInspect Enterprise

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					with Fortify Software Security Center.
Sensor machines to Fortify WebInspect Enterprise Manager server	Fortify WebInspect Enterprise server	User-specified Fortify WebInspect Enterprise server	443 or user-specified	HTTPS over SSL	Communication is two-way HTTP traffic, initiated in-bound by the Fortify WebInspect sensor machine.
Browser users to Fortify WebInspect Enterprise server UI	Fortify WebInspect Enterprise server	User-specified Fortify WebInspect Enterprise server	443 or user-specified	HTTPS over SSL	You can configure Fortify WebInspect Enterprise not to use SSL, but tests indicate that it might affect the product usability.
Browser user to Fortify Software Security Center UI	Fortify Software Security Center server	User-specified Fortify Software Security Center server	8180 or user-specified	HTTP or HTTPS over SSL	You can configure the Fortify Software Security Center server on any available port during installation.

Optional Connections

The following table lists the ports and protocols Micro Focus Fortify WebInspect Enterprise uses to make optional connections.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect desktop machines to Fortify WebInspect Enterprise Manager server	Fortify WebInspect Enterprise server	User-specified Fortify WebInspect Enterprise server	443 or user-specified	HTTPS over SSL	Communication is two-way HTTP traffic, initiated in-bound by the Fortify WebInspect desktop machine.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect Enterprise Manager machine to Fortify License activation server	Fortify Licensing Service	https://licenseservice.fortify.microfocus.com	443	HTTPS over SSL	For one-time activation of the Fortify WebInspect Enterprise server license as well as periodic checks during an update. You may optionally use the following: • An offline activation process instead of using this direct connection • Upstream proxy with authentication instead of a direct Internet connection **Important!** If you use the offline activation process, then you must also use the offline SmartUpdate process. For more information, see the *Micro Focus Fortify WebInspect Enterprise User Guide* or the WebInspect Enterprise Administrative Console help.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect Enterprise Manager machine to SmartUpdate server	SmartUpdate	https://smartupdate.fortify.microfocus.com	443	HTTPS over SSL	Used to acquire product updates as well as all connected clients (Fortify WebInspect sensors and Fortify WebInspect desktop). The administrator manually runs SmartUpdate, however Fortify recommends that you set up an automated schedule. New client releases are held in reserve until the Fortify WebInspect Enterprise administrator marks them as Approved, at which time they are automatically distributed from the Fortify WebInspect Enterprise Manager server. Can support the use of an upstream proxy with authentication instead of a direct Internet connection. **Important!** Access to the SmartUpdate server also requires access to the licensing server. If you have restrictions on outgoing traffic, you must add both the SmartUpdate server and the licensing server to your allow list.
Fortify WebInspect Enterprise Manager machine to mail server	User's mail server	Email alerts	25 or user-specified	SMTP	Used for SMTP alerts for administration team. To enable mobile TXT alerts, you can use an SMTP-to-SMS gateway address.
Fortify WebInspect Enterprise Manager machine to SNMP Community	User's SNMP Community	SNMP alerts	162 or user-specified	SNMP	Used for SNMP alerts for administration team.

Connections for Tools

The following table lists the ports and protocols that the Micro Focus Fortify WebInspect Enterprise tools use to make connections.

Tool	Direction	Endpoint	Port	Protocol	Notes
Web Proxy	To target web application	localhost	8080 or user-specified	HTTP or HTTPS over SSL	Intercepts and displays web traffic
Web Form Editor	To target web application	localhost	Dynamic, 8100, or user-specified	HTTP or HTTPS over SSL	Intercepts web traffic and captures submitted forms
Login or Workflow Macro Recorders	To target web application	localhost	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	Records browser sessions for replay during scan
Web Discovery	To targeted IP range	localhost	User-specified range	HTTP and HTTPS over SSL	Scanner for identifying rogue web applications hosted among the targeted scanned IP and port ranges Use to provide targets to Fortify WebInspect (manually)

Fortify WebInspect Enterprise Sensor

A Micro Focus Fortify WebInspect Enterprise sensor is a Micro Focus Fortify WebInspect sensor that runs scans on behalf of Fortify WebInspect Enterprise. See "Fortify WebInspect Requirements" on page 40 for more information.

To run a scan from Fortify WebInspect Enterprise, you must have at least one instance of Fortify WebInspect connected and configured as a sensor.

Fortify WebInspect Enterprise Notes and Limitations

- You can connect any instance of Micro Focus Fortify Software Security Center to only one instance of Micro Focus Fortify WebInspect Enterprise, and you can connect any instance of Fortify WebInspect Enterprise to only one instance of Fortify Software Security Center.
- For a Fortify WebInspect Enterprise environment to support Internet Protocol version 6 (IPv6), you must deploy the IPv6 protocol on each Fortify WebInspect Enterprise Administrative Console, each Fortify WebInspect Enterprise sensor, and the Fortify WebInspect Enterprise server.

Fortify Project Results (FPR) File Compatibility

Earlier versions of Micro Focus Fortify Software products cannot open and read FPR files generated by later versions of Fortify Software products. For example, Micro Focus Fortify Audit Workbench 22.1.0 cannot read 23.1.0 FPR files. However, later versions of Fortify Software products can open and read FPR files generated by earlier versions of Fortify Software products. For example, Fortify Audit Workbench version 23.1.0 can open and read version 22.2.0 FPR files.

The FPR file version is determined as follows:

- The FPR version is the same as the version of the analyzer that initially generated it. For example, an FPR generated by Fortify Software version 23.1.0 also has the version 23.1.0.
- The FPR version is the same as the version of the Fortify Software Security Center server or Fortify Applications and Tools used to change or audit the FPR.
- If you merge two FPRs, the resulting FPR has the version of the more recently generated FPR. For example, if you merge a version 22.2.0 FPR with a version 23.1.0 FPR, the resulting FPR has the version 23.1.0.

You can only open 23.1.0 FPR files with Fortify Software Security Center or Fortify Static Code Analyzer applications and tools versions 23.1.0 or later.

Caution Regarding Uploading FPR Files to Fortify Software Security Center

Fortify Software Security Center keeps a project file that contains the latest scan results and audit information for each application. Fortify Audit Workbench and the Secure Code Plugins also use this project file for collaborative auditing.

Each time you upload an FPR to Fortify Software Security Center, it is merged with the existing project file. If the FPR has a later version number than the existing project file, the existing project file version changes to match the FPR. For Fortify Audit Workbench and the Secure Code Plugins to work with the updated FPR, they must be at least the same version as the FPR. For example, Fortify Audit Workbench 22.2.0 cannot open and read a 23.1.0 FPR.

Virtual Machine Support

You can run Micro Focus Fortify Software products on an approved operating system in virtual machine environments. You must provide dedicated CPU and memory resources that meet the minimum hardware requirements. If you find issues that cannot be reproduced on the native environments with the recommended processing, memory, and disk resources, you must work with the provider of the virtual environment to resolve them.

Note: If you run Fortify Software products in a VM environment, Fortify strongly recommends that you have CPU and memory resources fully committed to the VM to avoid performance degradation.

Technologies no Longer Supported in this Release

The following technologies are no longer supported in Fortify Software:

- Build Tools:
  - xcodebuild 13, 13.1
- Compilers:
  - Swiftc 5.5, 5.5.1
- Kubernetes Cluster Deployment (Fortify Software Security Center):
  - Kubernetes 1.22
  - Helm 3.8
- Operating Systems (Fortify Static Code Analyzer):
  - macOS 11
- Platforms and Architectures (Fortify Static Code Analyzer applications and tools):
  - SUSE Linux Enterprise Server 12

Technologies to Lose Support in the Next Release

The technologies listed in this topic are scheduled for deprecation in the next Micro Focus Fortify Software release.

Note: A deprecated technology is no longer recommended for use. Typically, the deprecated item will be removed from the product in a future release. When a technology is deprecated, Fortify recommends that you remove it from your workflow at your earliest convenience.

- Fortify Static Code Analyzer support for all Swift, Xcode, and Objective-C/C++ versions follows the deprecation path Apple Inc. adopts.
- Integrated Development Environments (Fortify Secure Code Plugins):
  - Eclipse 2020-x
  - IntelliJ IDEA 2020.x
  - Android Studio 2020.x
- Kubernetes Cluster Deployment (Fortify Software Security Center):
  - Kubernetes 1.23–1.25
  - Helm 3.9–3.10

Acquiring Fortify Software

Micro Focus Fortify Software is available as an electronic download. For instructions on how to download the software from the Micro Focus Software Licenses and Downloads (SLD) portal (https://sld.microfocus.com), click **Contact Us / Self Help** to review the videos and the *Quick Start Guide*.

The following table lists the available packages and describes their contents.

File Name	Description

Fortify_SCA_<*version*>_ Windows.zip	Fortify Static Code Analyzer package for Windows
	This package includes:
	• Fortify Static Code Analyzer installer, which includes the following components:
	  • Fortify Static Code Analyzer
	  • Fortify ScanCentral SAST client
	• Fortify License and Infrastructure Manager installer
	• Fortify Custom Rules Guide bundle
	• About Fortify Software Documentation
	Note: Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation.

Fortify_SCA_<*version*>_ Windows.zip.sig	Signature file for the Fortify Static Code Analyzer package for Windows

Fortify_SCA_<*version*>_ Linux.tar.gz	Fortify Static Code Analyzer package for Linux
	This package includes:
	• Fortify Static Code Analyzer installer, which includes the following components:
	  • Fortify Static Code Analyzer
	  • Fortify ScanCentral SAST client
	• Fortify Custom Rules Guide bundle
	• About Fortify Software Documentation

File Name	Description
	Note: Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation.
Fortify_SCA_<*version*>_ Linux.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Linux
Fortify_SCA_<*version*>_ Mac.tar.gz	Fortify Static Code Analyzer package for macOS This package includes: • Fortify Static Code Analyzer installer • Fortify Custom Rules Guide bundle • About Fortify Software Documentation **Note:** Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation.
Fortify_SCA_<*version*>_ Mac.tar.gz.sig	Signature file for the Fortify Static Code Analyzer package for macOS
Fortify_SCA_<*version*>_ Solaris.tar.gz	Fortify Static Code Analyzer for Solaris This package includes: • Fortify Static Code Analyzer installer • Fortify Custom Rules Guide bundle • About Fortify Software Documentation
Fortify_SCA_<*version*>_ Solaris.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Solaris
Fortify_SCA_<*version*>_ AIX.tar.gz	Fortify Static Code Analyzer for AIX This package includes: • Fortify Static Code Analyzer installer • Fortify Custom Rules Guide bundle • About Fortify Software Documentation
Fortify_SCA_<*version*>_ AIX.tar.gz.sig	Signature file for Fortify Static Code Analyzer for AIX

File Name	Description
Fortify_SCA_Samples_<version>.zip	Code samples to help you learn to use Fortify Static Code Analyzer
Fortify_SCA_Samples_<version>.zip.sig	Signature file for Fortify Samples

Fortify_Tools_<version>_Windows.zip	Fortify Static Code Analyzer Applications and Tools package for Windows
	This package includes:
	• Fortify Applications and Tools installer, which includes the following components:
	  • Fortify Audit Workbench
	  • Fortify Custom Rules Editor
	  • Fortify Plugin for Eclipse (Eclipse Complete Plugin)
	  • Fortify Analysis Plugin for IntelliJ IDEA and Android Studio
	  • Fortify Extension for Visual Studio
	  • Fortify Scan Wizard
	• Fortify Security Assistant Plugin for Eclipse
	• About Fortify Software Documentation

Fortify_Tools_<*version*>_Windows.zip.sig	Signature file for the Fortify Applications and Tools package for Windows

Fortify_Tools_<*version*>_Linux.tar.gz	Fortify Static Code Analyzer Applications and Tools package for Linux
	This package includes:
	• Fortify Applications and Tools installer, which includes the following components:
	  • Fortify Audit Workbench
	  • Fortify Custom Rules Editor
	  • Fortify Plugin for Eclipse (Eclipse Complete Plugin)
	  • Fortify Analysis Plugin for IntelliJ IDEA and Android Studio

File Name	Description
	• Fortify Extension for Visual Studio • Fortify Scan Wizard • Fortify Security Assistant Plugin for Eclipse • About Fortify Software Documentation
Fortify_Tools_<*version*>_Linux.tar.gz.sig	Signature file for Fortify Applications and Tools for Linux
Fortify_Tools_<*version*>_Mac.tar.gz	Fortify Static Code Analyzer Applications and Tools package for macOS This package includes: • Fortify Applications and Tools installer, which includes the following components: • Fortify Audit Workbench • Fortify Custom Rules Editor • Fortify Plugin for Eclipse (Eclipse Complete Plugin) • Fortify Analysis Plugin for IntelliJ IDEA and Android Studio • Fortify Extension for Visual Studio • Fortify Scan Wizard • Fortify Security Assistant Plugin for Eclipse • About Fortify Software Documentation
Fortify_Tools_<*version*>_Mac.tar.gz.sig	Signature file for the Fortify Applications and Tools package for macOS
Fortify_SSC_Server_<*version*>.zip	Fortify Software Security Center package This package includes: • Fortify Software Security Center WAR file • Fortify seed bundles • About Fortify Software Documentation
Fortify_SSC_Server_<*version*>.zip.sig	Signature file for Fortify Software Security Center

File Name	Description
Fortify_ScanCentral_Controller_<*version*>.zip	Fortify ScanCentral SAST Controller package This package includes: • Fortify ScanCentral SAST • ScanCentral standalone client • About Fortify Software Documentation
Fortify_ScanCentral_Controller_<*version*>.zip.sig	Signature file for Fortify ScanCentral SAST Controller
ScanCentral_DAST_<*version*>.zip	Fortify ScanCentral DAST package This package includes: • DAST.ConfigurationToolCLI.exe • scancentral-dast-config.tar (Docker container with the DAST.ConfigurationToolCLI.exe and SecureBase) • SampleSettingsFile.json • SampleSettingsFile.yaml • ScanCentral DAST - Sensor Service.zip (sensor service and supporting bits) • appsettings.json (configures the sensor service) • Dynamic_Addons.zip (installers for optional FAST and Scan Scaling components) • About Fortify Software Documentation
ScanCentral_DAST_<*version*>.zip.sig	Signature file for Fortify ScanCentral DAST
SecurityToolkit_<*version*>.zip	Fortify WebInspect Toolkit package for use with Fortify WebInspect Enterprise
WebInspect_64_<*version*>.zip	Fortify WebInspect 64-bit package This package includes: • Installer • About Fortify Software Documentation
WebInspect_Agent_	Fortify WebInspect Agent package

File Name	Description
<version>.zip	
WI_Enterprise_ *<version>*.zip	Fortify WebInspect Enterprise package This package includes the following components: • Fortify WebInspect Enterprise server • Fortify WebInspect Enterprise Administrative Console • About Fortify Software Documentation

About Verifying Software Downloads

This topic describes how to verify the digital signature of the signed file that you downloaded from the Micro Focus Fortify Customer Support site. Verification ensures that the downloaded package has not been altered since it was signed and posted to the site. Before proceeding with verification, download the Fortify Software product files and their associated signature (`*.sig`) files. You are not required to verify the package to use the software, but your organization might require it for security reasons.

Preparing Your System for Digital Signature Verification

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To prepare your system for electronic media verification:

1. Navigate to the GnuPG site (http://www.gnupg.org).
2. Download and install GnuPG Privacy Guard.
3. Generate a private key, as follows:
   a. Run the following command (on a Windows system, run the command without the `$` prompt):
      ```
      $ gpg --gen-key
      ```
   b. When prompted for key type, select `DSA and Elgamal`.
   c. When prompted for a key size, select `2048`.
   d. When prompted for the length of time the key should be valid, select `key does not expire`.
   e. Answer the user identification questions and provide a passphrase to protect your private key.
4. Download the Micro Focus GPG public keys (compressed tar file) from https://mysupport.microfocus.com/documents/10180/0/MF_public_keys.tar.gz.
5. Extract the public keys.

6. Import each downloaded key with GnuPG with the following command:

   ```
   gpg --import <path_to_key>/<key_file>
   ```

Verifying Software Downloads

To verify that the signature file matches the downloaded software package:

1. Navigate to the directory where you stored the downloaded package and signature file.
2. Run the following command:

   ```
   gpg --verify <file>.sig <filename>
   ```
   For example:

   ```
   gpg --verify Fortify_SSC_Server_23.1.0.zip.sig Fortify_SSC_Server_
   23.1.0.zip
   ```

3. Examine the output to make sure that you receive verification that the software you downloaded is signed by Micro Focus Group Limited and is unaltered. Your output will include something similar to the following:

   ```
   gpg: Signature made Wed, November 10, 2022 12:05:20 AM PDT using RSA
   key ID AB42A5CF
   gpg: Good signature from "Micro Focus Group Limited RS A2048 1"
   ```

Note: A warning message might indicate that the public key is not known to the system. You can ignore this warning or set up your environment to trust these public keys.

Assistive Technologies (Section 508)

In accordance with section 508 of the Rehabilitation Act, Micro Focus Fortify Audit Workbench has been engineered to work with the JAWS screen reading software package from Freedom Scientific. JAWS provides text-to-speech support for use by the visually impaired. With JAWS, labels, text boxes, and other textual components can be read aloud, providing greater access to these technologies.

Micro Focus Fortify Software Security Center works well with the ChromeVox screen reader.

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 System Requirements (Fortify Software 23.1.0)

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!