Micro Focus Fortify Software

Software Version: 21.1.0

System Requirements

Document Release Date: Revision 2: July 30, 2021
Software Release Date: July 2021

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

All trademarks, service marks, product names, and logos included in this document are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on July 29, 2021. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

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

About the Documentation Set

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

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

Change Log

The following table lists revisions made to this document.

Document Revision	Changes
Revision 2: July 30, 2021	Updated: • "Build Tools" on page 16 and "Languages and Build Tools for Fortify ScanCentral SAST Sensor Project Translation" on page 28 - New supported versions of MSBuild available with Fortify Static Code Analyzer and Fortify ScanCentral SAST version 21.1.2
Revision 1: July 15, 2021	Updated: • "Platforms and Architectures" on page 10, "Build Tools" on page 16, and "Compilers" on page 17 - New supported versions of macOS, xcodebuild, Clang, and swiftc that are available with Micro Focus Fortify Static Code Analyzer version 21.1.1

Introduction

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

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

Software Delivery

Micro Focus Fortify Software is delivered only electronically. It is not available on disc. See "Acquiring Fortify Software" on page 58 for more information.

Software Licenses

Micro Focus Fortify Software products require a license.

For Micro Focus Fortify WebInspect, Micro Focus Fortify WebInspect Enterprise, and Micro Focus Fortify ScanCentral DAST you will receive an email with instructions for how to activate your product.

For all other Fortify Software products described in this document, you must download the Fortify license for your purchases from the Micro Focus Software Licenses and Downloads (SLD) portal (https://sld.microfocus.com/mysoftware/index). Use the credentials that Micro Focus Fortify Customer Support has provided for access.

Fortify Static Code Analyzer Requirements

This section describes the system requirements for Micro Focus Fortify Static Code Analyzer, and the Fortify Static Code Analyzer Tools (including the Secure Code Plugins).

Hardware Requirements

Fortify recommends that you install Micro Focus Fortify Static Code Analyzer on a high-end processor with at least 16 GB of RAM. If you plan to scan dynamic languages such as JavaScript, TypeScript, Python, PHP, or Ruby, Fortify recommends that you have 32 GB of RAM. If your software is complex,

you might require more RAM. See the content about improving performance in the *Micro Focus Fortify Static Code Analyzer User Guide* for more information.

Increasing the number of processor cores and increasing memory both result in faster processing.

Software Requirements

Micro Focus Fortify Static Code Analyzer requires Java 11. The Fortify SCA and Applications installer installs OpenJDK/JRE 11.0.10.

Translating .NET and Visual Studio C/C++ projects requires the Windows operating system and .NET Framework 4.7.2 or later.

Translating applications that use the Blazor web framework requires the installation of Visual Studio 2019.

Platforms and Architectures

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

Operating System	Platforms / Versions
Windows	Windows 8.1, 10 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
Linux	CentOS Linux 7.x (7.6 and later) CentOS Linux 8.x (8.2 and later) Red Hat Enterprise Linux 6.x (6.7 and later) Red Hat Enterprise Linux 7.x (7.2 and later) Red Hat Enterprise Linux 8.x (8.2 and later) SUSE Linux Enterprise Server 12, 15 Ubuntu 20.04.1 LTS
macOS	10.14, 10.15, 11

Fortify Static Code Analyzer Tools (including Secure Code Plugins) support the platforms and architectures listed in the following table.

Operating System	Platforms or Versions
Windows	8.1, 10
Linux	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12
macOS	10.14, 10.15, 11

Languages

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

Language / Frameworks	Versions
.NET	5.0
.NET Framework	2.0–4.8
.NET Core	2.0–3.1
ABAP/BSP	6 **Note:** Fortify ABAP Extractor is supported on a system running SAP release 7.02, SP level 0006.
ActionScript	3.0
Apex	36
C#	5, 6, 7, 8, 9
C/C++	C11, C++11 (see "Compilers" on page 17)
Classic ASP (with VBScript)	2.0, 3.0

Language / Frameworks	Versions
COBOL	IBM Enterprise COBOL for z/OS 6.1 (and earlier) with CICS, IMS, DB2, and IBM MQ Micro Focus Visual COBOL 6.0 **Note:** COBOL translation requires that Microsoft Visual C++ 2017 Redistributable (x86) be installed on the system. This is not a requirement for Legacy COBOL Translation.
ColdFusion	8, 9, 10
Go	1.12, 1.13, 1.14, 1.15, 1.16 **Note:** Scanning Go code is supported on Windows and Linux.
HTML	5 and earlier
Java (including Android)	7, 8, 9, 10, 11, 12, 13, 14
JavaScript	ECMAScript 2015–2020
JSP	1.2, 2.1
Kotlin	1.3.50, 1.4.20
MXML (Flex)	4
Objective-C/C++	2.0 (see "Compilers" on page 17)
PHP	7.0, 7.1, 7.2, 7.3, 7.4, 8.0
PL/SQL	8.1.6
Python	2.6, 2.7, 3.x (3.9 and earlier)
Ruby	1.9.3
Scala	2.11, 2.12, 2.13 **Note:** Scanning Scala code requires a standard Lightbend Enterprise Suite license.

Language / Frameworks	Versions
Swift	5 (see "Compilers" on page 17 for supported swiftc versions)
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	2.8, 3.x, 4.0, 4.1
VBScript	2.0, 5.0
Visual Basic (VB.NET)	11, 14, 15.x, 16.0
Visual Basic	6.0
XML	1.0

Libraries

Micro Focus Fortify Static Code Analyzer supports the libraries and frameworks listed in this section with dedicated Fortify Secure Coding Rulepacks and vulnerability coverage beyond the core language.

Java

Adobe Flex Blaze DS
Ajanta
Amazon Web Services (AWS) SDK
Amazon Web Services (AWS) Lambdas
Apache Axiom
Apache Axis
Apache Beehive NetUI
Apache Catalina
Apache Cocoon
Apache Commons
Apache ECS
Apache Hadoop
Apache HttpComponents
Apache Jasper
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
Castor
Display Tag
Dom4j
GDS AntiXSS
IBM MQ
IBM WebSphere
Java Annotations
Jackson
Java Excel API
JavaMail
JAXB
Jaxen
JAX-RS
JBoss
JDesktop
JDOM
Jetty
JGroups
json-simple
JTidy Servlet
JXTA
Netscape LDAP API
OpenCSV
Oracle Application Development Framework (ADF)
Oracle BC4J
Oracle OA Framework
Oracle JDBC
Oracle tcDataSet
Oracle XML Developer Kit (XDK)
Oracle tcDataSet
OWASP Enterprise Security API (ESAPI)
OWASP HTML Sanitizer
OWASP Java Encoder
Plexus Archiver
Spring Data Commons
Spring Data JPA
Spring Data MongoDB
Spring Data Redis
Spring HATEOAS
Spring JMS
Spring JMX
Spring Messaging
Spring Webflow
Spring WebFlux
Spring WebSockets
Spring WS
Spring Security
Stripes
Sun JavaServer Faces (JSF)

Apache Log4J	Google Android	JYaml	Realm	Tungsten
Apache Lucene	Google Cloud Platform	Liferay Portal	Restlet	Weblogic
Apache MyFaces	Google Web Toolkit	Lombok	SAP Web Dynpro	WebSocket
Apache OGNL	Gson	MongoDB	Saxon	XStream
Apache ORO	Hibernate	Mozilla Rhino	SnakeYAML	YamlBeans
Apache POI	iBatis	MyBatis	Spring and Spring MVC	ZeroTurnaround ZIP
Apache SLF4J			Spring Boot	Zip4J

Scala

Akka HTTP	Scala Slick
Scala Play	

.NET

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

C

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

C++

Boost Smart Pointers	STL
MFC	WMI

SQL

Oracle ModPLSQL

PHP

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

JavaScript/TypeScript/HTML5

Angular	iOS JavaScript Bridge	Node.js Core	React Router
Express JS	jQuery	Node.js Azure Storage	Underscore.js
Helmet	JS-YAML	React	

Python

aiopg	Jinja2	MySQLdb	PyMongo	six
Amazon Web Services (AWS) Lambdas	libxml2	psycopg2	PyYAML	Twisted Mail
Django	lxml	pycrypto	requests	urllib3
httplib2	memcache-client	pycurl	simplejson	WebKit
	_mysql	pylibmc		

Ruby

MySQL	SQLite	Thor
pg	Rack	

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

Configuration

Adobe Flex (ActionScript) Configuration	iOS Property List	Java Apache Tomcat Configuration	Java OWASP AntiSamy	Microsoft .NET Configuration
Ajax Frameworks	J2EE Configuration	Java Blaze DS	Java Spring and Spring MVC	Microsoft Silverlight Configuration
Azure Resource Manager Templates	Java Apache Axis	Java Hibernate Configuration	Java Spring Boot	Oracle Application Development Framework (ADF)
Build Management	Java Apache Log4j Configuration	Java iBatis Configuration	Java Spring Mail	PHP Configuration
Docker Configuration (Dockerfiles)	Java Apache Spring Security (Acegi)	Java IBM WebSphere	Java Spring Security	WS-SecurityPolicy
Google Android Configuration	Java Apache Struts	Java MyBatis Configuration	Java Spring WebSockets	XML Schema
			Java Weblogic	

COBOL

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

Go

GORM
logrus

Build Tools

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

Build Tool	Versions	Notes
Ant	1.10.x and earlier	

Build Tool	Versions	Notes
Bamboo	(see the Atlassian Marketplace for supported versions)	The Fortify App for Bamboo is available from the Atlassian Marketplace.
Gradle	6.6.x and earlier	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
Jenkins	(see the Jenkins Plugin Index for supported versions)	The Fortify Jenkins plugin is available from the Jenkins Plugins Index.
Maven	3.0.5, 3.5.x, 3.6.x	
MSBuild	15.x, 16.4, 16.6, 16.8, 16.9, 16.10	
Xcodebuild	11.4.1, 11.5, 11.6, 11.7, 12, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5	

Compilers

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

Compiler	Versions	Operating Systems
gcc	GNU gcc 4.9, 5.x	Windows, Linux, macOS
g++	GNU g++ 4.9, 5.x	Windows, Linux, macOS
OpenJDK javac	9, 10, 11, 12, 13, 14	Windows, Linux, macOS
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl	2017, 2019	Windows

Compiler	Versions	Operating Systems
Clang	11.0.0, 11.0.3, 12.0.0, 12.0.5[1]	macOS
Swiftc	5.2.2, 5.2.4, 5.3, 5.3.1, 5.3.2, 5.4[1]	macOS

[1]Fortify Static Code Analyzer supports applications built in the following Xcode versions: 11.4.1, 11.5, 11.6, 11.7, 12, 12.0.1, 12.1, 12.2, 12.3, 12.4, 12.5.

Secure Code Plugins

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

Plugin / Extension	IDEs and Versions	Notes
Fortify Eclipse Plugins (Complete and Remediation)	Eclipse 2020-x, 2021-x	Supports Java 11
Fortify Analysis Plugin	Android Studio 4.x IntelliJ IDEA 2020.x	Supports Java 11
Fortify Remediation Plugin	Android Studio 4.x IntelliJ IDEA 2020.x PyCharm 2020.x WebStorm 2020.x	Supports Java 11
Fortify Visual Studio Extension	Visual Studio 2017 Community, Professional, and Enterprise Visual Studio 2019 Community, Professional, and Enterprise	For supported MSBuild versions, see "Build Tools" on page 16.
Security Assistant Plugin for Eclipse	Eclipse 2020-x, 2021-x	Supports Java 11

Plugin / Extension	IDEs and Versions	Notes
Security Assistant Extension for Visual Studio	(see the Visual Studio Marketplace for supported versions)	Security Assistant Extension for Visual Studio is available from the Visual Studio Marketplace.

Single Sign-On (SSO)

Fortify Audit Workbench, the Eclipse Complete plugin, and the Fortify Visual Studio Extension 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.

Service Integrations for Fortify Static Code Analyzer Tools

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

Service	Versions	Supported Tools
Micro Focus Application Lifecycle Management (ALM)/ Quality Center Enterprise (QC)	12.50	Audit Workbench, Eclipse Plugin
Azure DevOps Server	2019, 2020	Audit Workbench, Eclipse Plugin, Visual Studio Extension
Azure DevOps **Note:** Only basic user password authentication is supported.	n/a	Audit Workbench, Eclipse Plugin
Bugzilla	5.0.x	Audit Workbench, Eclipse Plugin, Visual Studio Extension
Jira	7.13 and later, 8.x	Audit Workbench, Eclipse Plugin

Service	Versions	Supported Tools
Jira Cloud	n/a	Audit Workbench, Eclipse Plugin
Fortify Software Security Center Bug Tracker	21.1.0	Audit Workbench, Eclipse Plugin, Visual Studio Extension

Fortify Software Security Content

Micro Focus 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 Software Security Center Server Requirements

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

Hardware Requirements

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

	Component	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*> is the total number of issues in the system
- <*size_of_artifacts*> is the total size in KB of all uploaded artifacts and scan results

Note: This equation produces only a rough estimate for database disk space allocation. Do not use this formula 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

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

Operating System	Versions
Windows	Server 2012 R2 Server 2016 Server 2019
Linux	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x, 8 SUSE Linux Enterprise Server 12, 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

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

- Red Hat OpenJDK 11
- SUSE OpenJDK 11
- Oracle JDK 11
- Zulu OpenJDK 11 from Azul (Installation of the fontconfig library, DejaVu Sans fonts, and DejaVu Serif fonts are required on the server.)

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

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

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

Database	Versions	Collation / Character Set	Driver
MySQL	8.0 (Community Edition)	latin1_general_cs / latin1	The driver is included in the Fortify Software Security Center WAR file. MariaDB Connector/J 2.7.1 Driver class: `org.mariadb.jdbc.driver`
Oracle	12c Release 2 19c (18.3)	AL32UTF8 for all languages WE8MSWIN1252 for US English	The driver is included in the Fortify Software Security Center WAR file. Driver class: `oracle.jdbc.OracleDriver` JAR file: `ojdbc8.jar` (for Java 11) version 19.9.0.0

Database	Versions	Collation / Character Set	Driver
SQL Server	2017 2019	You must use the case-sensitive (CS) option when choosing your collation method. For example: `SQL_Latin1_General_CP1_CS_AS`	The driver is included in the Fortify Software Security Center WAR file. Microsoft JDBC Driver 8.4.1.jre8 for SQL Server Driver class: `com.microsoft.sqlserver.jdbc.SQLServerDriver`

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. Micro Focus 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 Micro Focus Fortify Software Security Center on a Kubernetes cluster, you must make sure that the following requirements are met.

Kubernetes Requirements

- Versions 1.16–1.20
- Persistent volume support
- A load balancer service (Recommended)
- At least 7 GB of RAM and 1 CPU on a single node (with default configuration)
- Maximum usage: 28 GB of RAM and 8 CPUs on a single node (with default configuration)
- 4 GiB of storage for persistent volume (with default configuration)

Locally-Installed Tools Required

- A kubectl command-line tool (Recommended) - Use the same version as the Kubernetes cluster version (1.16–1.20)
- Helm command-line tool, versions 3.0–3.5
- Air-gapped installation only (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. Micro Focus 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 *Micro Focus 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 Oracle, SQL Server, or MySQL 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
Microsoft Edge	90
Mozilla Firefox	88
Safari	14

Authentication Systems

Micro Focus 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 Authorization Server (CAS) SSO
- HTTP Headers SSO (Oracle SSO, CA SSO)
- SAML 2.0 SSO
- SPNEGO/Kerberos SSO
- X.509 SSO

BIRT Reporting

Micro Focus Fortify Software Security Center custom reports support Business Intelligence and Reporting Technology (BIRT) Designer version 4.7.

Installation of the fontconfig library, DejaVu Sans fonts, and DejaVu Serif fonts on the server is required for reporting.

Service Integrations for Fortify Software Security Center

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

Service	Application	Versions
Bug tracking	Bugzilla	5.0.x
	Micro Focus Application Lifecycle Management (ALM)/ Quality Center Enterprise (QC)	12.50
	Jira	7.13 and later, 8.x
	Jira Cloud	n/a
	Azure DevOps Server	2019, 2020
	Azure DevOps **Note:** Only basic user password authentication is supported.	n/a
Authentication	Active Directory	2008, 2012
Dynamic assessments	Micro Focus Fortify WebInspect Enterprise	21.1.0

Fortify ScanCentral SAST Requirements

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

Fortify ScanCentral SAST Application Server

Micro Focus Fortify ScanCentral SAST supports Apache Tomcat version 9.x for Java 11.

Fortify ScanCentral SAST Controller Requirements

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

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 equation:

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.

Controller Platforms and Architectures

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

Operating System	Versions
Windows	Server 2012 R2 Server 2016 Server 2019
Linux	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x, 8 SUSE Linux Enterprise Server 12, 15

Fortify ScanCentral SAST Client and Sensor Hardware Requirements

Fortify ScanCentral SAST clients and sensors run on any machine that supports Micro Focus Fortify Static Code Analyzer. Because ScanCentral SAST clients and sensors are installed on build machines running Micro Focus Fortify Static Code Analyzer, the hardware requirements are met.

See "Fortify Static Code Analyzer Requirements" on page 9 for hardware, software, and platform and architecture requirements.

Sensor Disk Space Requirements

To estimate the amount of disk space required on the machine that runs a ScanCentral 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.

Languages and Build Tools for Fortify ScanCentral SAST Sensor Project Translation

Micro Focus Fortify ScanCentral SAST supports offloading project translation to ScanCentral SAST sensors for the following languages and build tools.

Languages

Fortify ScanCentral SAST supports offloading project translation to ScanCentral sensors for the following languages. See "Languages" on page 11 for specific supported versions.

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

  Note: Translation of .NET applications require .NET Framework version 4.7.2 or later.

- ABAP
- Apex
- Classic ASP
- ColdFusion
- Java
- JavaScript
- 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	5.0–6.8.3
Maven	3.x
MSBuild	15.x, 16.4, 16.6, 16.8, 16.9, 16.10

Fortify ScanCentral DAST Requirements

Before you install Micro Focus Fortify ScanCentral DAST, make sure that your system meets the requirements described in this section.

Architectural Best Practices

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

- Install the DAST API, DAST Global Service, DAST Utility Service, and Fortify License and Infrastructure Manager (LIM) on the same VM or on separate VMs.
- Do not install 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

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

Software Requirements

The Fortify ScanCentral DAST Configuration Tool 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 5.0.202

Hardware Requirements

Fortify recommends that you use the Fortify ScanCentral DAST Configuration Tool 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 requires the database server listed in the following table.

Package	Versions	Notes
SQL Server (English-language version only)	SQL Server 2019	No scan database limit

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 22.

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
Docker	18.09 or later

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 39.

Classic Fortify WebInspect Installation Option

For hardware and software requirements for this option, see "WebInspect Hardware Requirements" on page 36 and "WebInspect Software Requirements" on page 37. Additionally, if you plan to conduct Postman scans, see "Support for Postman" on page 38.

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 5.0.202.

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.

Endpoints	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	1433	TCP	This is the default SQL Server 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	1433	TCP	This is the default SQL Server 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.

Endpoints	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	1433	TCP	This is the default SQL Server port.

Fortify ScanCentral DAST 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
Microsoft Edge	90
Mozilla Firefox	88
Safari	14

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	Versions
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	21.1.0
Kubernetes on Azure (for scan scaling support)	1.19 or later

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 and later) 6 (SR6 and later)
Oracle HotSpot	5, 6, 7, 8
Oracle JRockit	5, 6 (R27.6 and 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 and earlier
Jetty	9.3
WildFly	20.0.1 and 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 Requirements

Before you install Micro Focus Fortify WebInspect, make sure that your system meets the requirements described in this section.

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. 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.
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 8.1	
	Windows Server 2016	
	Windows Server 2019	
.NET Platform	.NET Framework 4.8	
SQL Server (English-language versions only)	SQL Server 2017	Recommended No scan database limit
	SQL Server 2014 SP3	No scan database limit
	SQL Server 2016 SP2	No scan database limit
	SQL Server 2019	No scan database limit
SQL Server Express (English-language versions only)	SQL Server 2017 Express	Recommended 10 GB scan database limit
	SQL Server 2014 Express SP3	10 GB scan database limit
	SQL Server 2016 Express SP2	10 GB scan database limit
	SQL Server 2019 Express	10 GB scan database limit

Package	Versions	Notes
Browser	Internet Explorer 11	Recommended
	Internet Explorer 10	
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
Docker Enterprise	18.09 or later	
Windows	Windows Server 2019	This Windows version supports the process isolation runtime mode.

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.
Fortify WebInspect to SQL database	SQL Server Express or SQL Server Standard/Enterprise	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.
Fortify WebInspect to Certificate Revocation List (CRL)	Verisign CRL	http://crl.verisign.com/pca3.crl or http://csc3-2004-crl.verisign.com/CSC3-2004.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	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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
activation server					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 WebInspect Telemetry server	Remote Fortify WebInspect Telemetry and performance reporting service	https://telemetry.fortify.com **Note:** Accessing this URL in a browser does not display any content.	443	HTTPS over SSL	The Telemetry service provides an automated process for collecting and sending Fortify WebInspect usage information to Micro Focus. Our software developers use this information to help improve the product.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
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 listener	Local machine API, or network IP address	http://localhost:8083/webinspect/api	8083 or user-specified	HTTP	Use to activate a Fortify WebInspect API Windows 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.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
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 page 34.

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	21.1.0
Micro Focus 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	21.1.0
Micro Focus Unified Functional Testing	11.5

Fortify WebInspect Enterprise Requirements

Before you install Micro Focus Fortify WebInspect Enterprise, make sure that your systems meet the requirements described in this section.

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

Installation and Upgrade Requirements

You can upgrade directly from Micro Focus Fortify WebInspect Enterprise 20.2.0 to Fortify WebInspect Enterprise 21.1.0. You cannot upgrade directly from any other versions of Fortify WebInspect Enterprise. For detailed information about upgrades, see the *Micro Focus Fortify WebInspect Enterprise Installation and Implementation Guide*.

Integration with Micro Focus Fortify Software Security Center is optional. If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, then you must install and run Fortify Software Security Center 21.1.0 before you install a new instance of Fortify WebInspect Enterprise or upgrade from Fortify WebInspect Enterprise 20.2.0. You can install Fortify Software Security Center and Fortify WebInspect Enterprise on the same or different machines. Using separate machines might improve performance.

Integrations for Fortify WebInspect Enterprise

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

- Micro Focus Fortify WebInspect sensors 21.1.0
- Micro Focus Fortify WebInspect Agent 21.1.0

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 22.

WebInspect Enterprise Hardware Requirements

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

Component	Requirement	Notes
Processor	3.0 GHz quad-core or faster	Recommended
	2.5 GHz dual-core	Minimum
RAM	16 GB	Recommended
	8 GB	Minimum
Hard disk	100+ GB	Recommended
	20+ GB if using a local database	
	5 GB if using a remote database	

Component	Requirement	Notes
Display	1920 x 1080	Recommended
	1280 x 1024	Minimum

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	
.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 2017	Recommended No scan database limit
	SQL Server 2014 SP3	No scan database limit
	SQL Server 2016 SP2	No scan database limit
	SQL Server 2019	No scan database limit
Browser	Mozilla Firefox 75 or later	Recommended
	Google Chrome 81 or later	
	Microsoft Edge 81 or later	
	Internet Explorer 11	

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 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.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
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 36 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 License and Infrastructure Manager Requirements

This section describes the hardware and software requirements for Micro Focus 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. Beta or pre-release versions of operating systems, service packs, and required third-party components are not supported.

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.

Package	Versions	Notes
Windows Server	Windows Server 2012, 2012 R2	The default .NET Framework that is installed on this operating system is earlier than 4.6.1. You might need to manually update the .NET Framework by using Windows Update or downloading it from Microsoft.

Package	Versions	Notes
	Windows Server 2016	
	Windows Server 2019	
Web Server	IIS 8.5	Recommended
	IIS 7.5, 8.0, 10	
.NET Platform	.NET Framework 4.5, 4.6.1	When configuring Roles and Features in Windows Server Manager, you might see .NET Framework 4.6 rather than 4.6.1 even though you have installed 4.6.1. You can confirm the installed version in the Command Prompt using the `.\MSBuild.exe -version` command in the following directory: `%windir%\Microsoft.NET\Framework\<version>`
	ASP.NET 4.5, 4.6	
Browser	Internet Explorer 11	Recommended
	Mozilla Firefox 51.0	Recommended
	Mozilla Firefox 44.0, 47.0, 69.0	

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

Version Compatibility Matrix

This section provides compatibility information for Micro Focus Fortify Software components.

Fortify Software Component Compatibility

Micro Focus Fortify Software version 21.1.0 works with the component versions listed in the following table.

Component	Version
Micro Focus Fortify Software Security Center	21.1.0
Micro Focus Fortify Static Code Analyzer Tools (Micro Focus Fortify Audit Workbench, Fortify Secure Code Plugins, and Fortify Custom Rules Editor)	21.1.0
Micro Focus Fortify WebInspect Agent	21.1.0
Micro Focus Fortify WebInspect	21.1.0
Micro Focus Fortify WebInspect Enterprise	21.1.0

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 19.1.0 cannot read 21.1.0 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 21.1.0 can open and read version 19.1.0 FPR files.

FPR version numbers are 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 21.1.0 also has the version number 21.1.0.
- The FPR version is the same as the version of the Micro Focus Fortify Software Security Center or Micro Focus Fortify Static Code Analyzer Tool used to modify 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 19.1.0 FPR with a version 21.1.0 FPR, the resulting FPR has the version number 21.1.0.

You can only open 21.1.0 FPR files with Fortify Software Security Center or Fortify Static Code Analyzer Tools version 21.1.0 or later.

Caution Regarding Uploading FPRs 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 19.1.0 cannot open and read a 21.1.0 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 possible performance degradation.

Technologies no Longer Supported in this Release

The following technologies and features are no longer supported in Fortify Software:

- Build Tools:
  - Xcodebuild 11, 11.1, 11.2.1, 11.3, and 11.3.1
- Compilers:
  - Intel C++ Compiler
  - cl 2015
  - Swiftc 5.1, 5.1.2, 5.1.3
- Integrated Development Environments (Secure Code Plugins):
  - Android Studio 3.x
  - Eclipse 2018-x, 2019-x
  - JetBrains IntelliJ IDEA, WebStorm, and PyCharm 2019.x
  - Visual Studio 2015 (Fortify Visual Studio Extension)
- Language Support (Fortify Static Code Analyzer):
  - Analysis of Java 5 and 6

Technologies to Lose Support in the Next Release

The following technologies and features are scheduled for deprecation in the next Micro Focus Fortify Software release:

- Fortify Static Code Analyzer support for all Swift, Xcode, and Objective-C/C++ versions will follow the deprecation path Apple Inc. adopts.
- Build Tools:
  - Xcodebuild 11.4.1, 11.5, 11.6, 11.7
- Compilers:
  - Clang 11.0.0 and 11.0.3
  - Swiftc 5.2.x
- Kubernetes Cluster Deployment (Fortify Software Security Center):
  - Kubernetes 1.16, 1.17
  - Helm 3.0, 3.1
- Language Support (Fortify Static Code Analyzer):
  - Analysis of PHP 7.0, 7.1, and 7.2
- Operating Systems (Fortify Static Code Analyzer and Tools):
  - Red Hat Enterprise Linux version 6.x
- Platforms and Architectures:
  - Windows Server 2012 R2
  - macOS 10.14
- Service Integrations (Fortify Software Security Center and Fortify Static Code Analyzer Tools):
  - Bugzilla 5.0.x
  - Micro Focus Application Lifecycle Management (ALM)/Quality Center Enterprise (QC) 12.50

Acquiring Fortify Software

Micro Focus Fortify Software is available as an electronic download. For instructions on how to download the software from Micro Focus Fortify Customer Support (https://www.microfocus.com/support), click **Contact Us / Self Help** from the Software Licenses and Downloads page 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_and_Apps_<*version*>_Windows.zip	Fortify SCA and Applications installer for Windows This installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench • Fortify Custom Rules Editor • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Extension for Visual Studio • Fortify Scan Wizard • Sample applications **Note:** • Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation. • The package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, and the Fortify Remediation Plugin for JetBrains and Android Studio IDEs.
Fortify_SCA_and_Apps_<*version*>_Windows.zip.sig	Signature file for the Fortify SCA and Applications package for Windows
Fortify_SCA_and_Apps_<*version*>_Linux.tar.gz	Fortify SCA and Applications installer for Linux The installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench

File Name	Description
	• Fortify Custom Rules Editor • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Scan Wizard • Sample applications **Note:** • Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation. • The package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, and the Fortify Remediation Plugin for JetBrains and Android Studio IDEs.
Fortify_SCA_and_Apps_<*version*>_Linux.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Linux
Fortify_SCA_and_Apps_<*version*>_Mac.tar.gz	Fortify SCA and Applications installer for macOS This installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench • Fortify Custom Rules Editor • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Scan Wizard • Sample applications **Note:** • Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation. • The package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, and the Fortify Remediation Plugin for JetBrains and Android Studio IDEs.
Fotify_SCA_and_Apps_<*version*>_Mac.tar.gz.sig	Signature file for the Fortify SCA and Applications package for macOS

File Name	Description
Fortify_SSC_Server_<*version*>.zip	Fortify Software Security Center
Fortify_SSC_Server_<*version*>.zip.sig	Signature file for Fortify Software Security Center
Fortify_ScanCentral_Controller_<*version*>.zip	Fortify ScanCentral SAST Controller
Fortify_ScanCentral_Controller_<*version*>.zip.sig	Signature file for Fortify ScanCentral SAST Controller
ScanCentral_DAST_<*version*>.zip	Fortify ScanCentral DAST package This package includes: • Configuration Tool EXE • Scanner service and supporting bits • About Fortify Software Documentation (PDF)
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 (PDF)
WebInspect_Agent_<*version*>.zip	Fortify WebInspect Agent package
WI_Enterprise_<*version*>.zip	Fortify WebInspect Enterprise package The package includes the following components: • Fortify WebInspect Enterprise server • Fortify WebInspect Enterprise Administrative Console • About Fortify Software Documentation (PDF)

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_21.1.0.zip.sig Fortify_SSC_Server_
21.1.0.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 Fri, Oct 06, 2017 10:37:56 PM PDT using RSA key ID
AA71A9CF
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 21.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!