Micro Focus Fortify Software

Software Version: 18.20

System Requirements

Document Release Date: November 2018
Software Release Date: November 2018

Legal Notices

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

https://www.microfocus.com

Warranty

Restricted Rights Legend

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

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

https://www.microfocus.com/support-and-services/documentation

Contents

Preface

Contacting Micro Focus Fortify Customer Support

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

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

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

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

About the Documentation Set

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

https://www.microfocus.com/support-and-services/documentation

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 Software Security Center Server
- Micro Focus Fortify Static Code Analyzer
- Micro Focus Fortify Audit Workbench and Secure Code Plugins
- Micro Focus Fortify CloudScan
- Micro Focus Fortify Runtime Agent
- Micro Focus Fortify WebInspect
- Micro Focus Fortify WebInspect Enterprise
- License Infrastructure Manager

Software Delivery

Micro Focus Fortify Software is delivered only electronically. It is not available on disc. See "Acquiring Fortify Software" on page 41 for more information.

Software Licenses

Micro Focus Fortify Software products require a license.

For Micro Focus Fortify Software Security Center, Micro Focus Fortify Static Code Analyzer, Micro Focus Fortify Audit Workbench, Micro Focus Fortify Secure Code Plugins, Micro Focus Fortify CloudScan, and Micro Focus Fortify Runtime Agent, you must download the Fortify licenses for your purchases from either the Fortify Customer Portal (https://support.fortify.com) or Micro Focus Fortify Customer Support (https://softwaresupport.softwaregrp.com). To access either location, use the credentials that Micro Focus Fortify Customer Support has provided.

To download the Fortify license from the Fortify Customer Portal:

1. Log onto the Fortify Customer Portal.
2. Click **Download Licenses**, and then click the link for the license you want to use.

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

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
Fortify Software Security Center	Processor	Quad-core	Eight-core
	RAM	8 GB	32 GB
Fortify Software Security Center server	Java heap size	4 GB	24 GB

Database

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:

((<*Total_Issues*>*30 KB) + <*Total_Artifacts*>) ÷ 1,000,000

where:

- <*Total_Issues*> is the total number of issues in the system
- <*Total_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	Architecture	Versions
Windows	64-bit	Server 2012 R2 Server 2016
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12

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 Java 8.

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	Version	Character Set	Driver

MySQL	5.7 (Community Edition)	utf8_bin, latin1_general_cs	5.1.44 or later
			Driver class:
			`com.mysql.jdbc.driver`
			JAR file:
			`mysql-connector-java-<version>-bin.jar`

Database	Version	Character Set	Driver
Oracle	12c Release 2	AL32UTF8 for all languages WE8MSWIN1252 for US English	Oracle Database 12c Release 2 (12.2.x) JDBC Driver Driver class: `oracle.jdbc.OracleDriver` JAR files: `ojdbc8.jar` (for Java 8)

SQL Server	2014
	2016
	2017
		Make sure to use the case-sensitive (CS) option when choosing your collation method. For example:
		`SQL_Latin1_General_CP1_CS_AS`
			Microsoft JDBC Driver 6.0 for SQL Server
			Driver class:
			`com.microsoft.sqlserver.jdbc.SQLServerDriver`
			JAR file:
			`sqljdbc42.jar`

Browsers

Fortify recommends that you use one of the browsers listed in the following table and a screen resolution of 1280 x 1024.

Browser	Version
Google Chrome	65.0 or later
Microsoft Edge	38 or later
Internet Explorer	11
Mozilla Firefox	59.0 or later
Safari	11

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.

- 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 4.4.2.

Service Integrations for Fortify Software Security Center

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

Service	Applications	Versions
Bug tracking	Bugzilla	5.0
	Micro Focus Application Lifecycle Management (ALM)/ Quality Center Enterprise (QC)	12.50
	JIRA	7.4, 7.11
	Team Foundation Server (TFS)	2015, 2017
	Visual Studio Team Services (VSTS) **Note:** Only basic user password authentication is supported.	n/a
Authentication	Active Directory	2008, 2012
Dynamic assessments	Micro Focus Fortify WebInspect Enterprise	18.20

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 *Micro Focus Fortify Static Code Analyzer Performance 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 8. The Fortify SCA and Applications installer installs OpenJDK/JRE 1.8.0_181.

Translating .NET code requires .NET framework version 4.6.1 or later.

Platforms and Architectures

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

Operating System	Architecture	Platforms
Windows	64-bit	Windows Server 2016 Windows Server 2012 R2 Windows 8.1, 10
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12
macOS		10.13
Oracle Solaris	x86, 64-bit	10.5 and later
	SPARC 64-bit	10.5 and later
HP-UX	Itanium 64-bit	11.31
IBM AIX	64-bit	6.1, 7.2

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

Operating System	Architecture	Platforms
Windows	64-bit	Windows 7, 8.1, 10
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12
macOS		10.13

Supported Languages

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

Language	Versions
.NET	2.0–4.7.2
.NET Core	1.x, 2.0, 2.1
ABAP/BSP	6
ActionScript	3.0
Angular	2, 4, 5, 6
AngularJS	1.x
Apex	36
ASP.NET	2.0–4.7
C#	5, 6, 7
C/C++	See "Compilers" on page 15
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 3.4.1 with CICS, IMS, DB2, and IBM MQ
ColdFusion	8, 9, 10
HTML	5 and earlier

Language	Versions
Java (including Android)	5.0, 6, 7, 8, 9
JavaScript	ECMAScript 2015, 2016, 2017
JSP	1.2, 2.1
MXML (Flex)	4
Objective-C/C++	See "Compilers" on the next page
PHP	5.3, 5.4, 5.5, 5.6, 7.0, 7.1
PL/SQL	8.1.6
Python	2.6, 2.7, 3.x (3.6 and earlier)
Ruby	1.9.3
Scala	2.11, 2.12, 2.13
Swift	4.0.3, 4.1, 4.2
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	2.8
VB.NET	11, 14, 15
VBScript	2.0, 5.0
Visual Basic	6
XML	1.0

Build Tools

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

Build Tool	Versions	Notes
Ant	1.9.6	
Bamboo	6.2, 6.3, 6.4	The Fortify App for Bamboo is available from the Atlassian Marketplace.

Build Tool	Versions	Notes
Gradle	2.13	The Fortify Static Code Analyzer Gradle build integration supports the following language/platform combinations: • Java/Windows, Linux, and macOS • C/Linux • C++/Linux
Jenkins	2.121.2	
Maven	3.0.5, 3.5.x	
MSBuild	4.x, 12.0, 14.0, 15.0	
Xcodebuild	9.0, 9.1, 9.2, 9.3, 10.0	

Compilers

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

Compiler	Versions	Platform
gcc	GNU gcc 4.9, 5.x	Windows , Linux, macOS, Solaris, IBM AIX
	GNU gcc 4.2.5 and later	HP-UX
g++	GNU g++ 4.9, 5.x	Windows , Linux, macOS, Solaris, IBM AIX
	GNU g++ 4.2.5 and later	HP-UX
Intel C++ Compiler	icc 8.0	Linux
Oracle javac	7, 8. 9	Windows , Linux, macOS, Solaris, HP-UX, IBM AIX
Oracle Solaris Studio	12	Solaris
cl	2013, 2015, 2017	Windows
Apple LLVM (Clang)	9.x, 10.x	macOS
Swiftc	4.0.3, 4.1, 4.2	macOS

Secure Code Plugins

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

Plugin / Extension	IDE and Version	Notes
Eclipse (Complete and Remediation)	Eclipse 4.6, 4.7, 4.8	
IntelliJ IDEA Analysis	IntelliJ IDEA 2017.x, 2018.x Android Studio 2.3.x, 3.0, 3.1	
IntelliJ IDEA Remediation	IntelliJ IDEA 2017.x Android Studio 2.3.x, 3.0, 3.1 WebStorm 2017.x, 2018.x	
Security Assistant Extension for Visual Studio	Visual Studio 2017 Community, Professional, and Enterprise (version 15.6 and later)	Security Assistant Extension for Visual Studio is available from the Visual Studio Marketplace
Security Assistant Plugin for Eclipse	Eclipse 4.6, 4.7, 4.8	
Visual Studio Extension	Visual Studio 2013 Premium, Professional, and Ultimate Visual Studio 2015 Community, Professional, and Enterprise Visual Studio 2017 Community, Professional, and Enterprise **Note:** Fortify Static Code Analyzer is not compatible with Visual Studio Express.	

Single Sign-On (SSO)

The Eclipse Complete plugin and the Visual Studio extension support the following SSO methods to connect with Fortify Software Security Center:

- SPNEGO/Kerberos SSO
- X.509 SSO

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
Bugzilla	5.0	Audit Workbench, Eclipse Plugin, Visual Studio Extension
Micro Focus Application Lifecycle Management (ALM)/ Quality Center Enterprise (QC)	12.50	Audit Workbench, Eclipse Plugin
Team Foundation Server (TFS)	2013	Visual Studio Extension
	2015, 2017	Audit Workbench, Eclipse Plugin, Visual Studio Extension
Visual Studio Team Services (VSTS) **Note:** Only basic user password authentication is supported.	n/a	Audit Workbench, Eclipse Plugin
JIRA	7.4, 7.11	Audit Workbench, Eclipse Plugin
Fortify Software Security Center Bug Tracker	18.20	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 Rulepacks updates do not break any working Fortify Software installation.

Fortify CloudScan Requirements

Micro Focus Fortify CloudScan has three major components: a CloudScan Controller, CloudScan clients, and CloudScan sensors. This section describes the requirements for each component.

CloudScan Controller Hardware Requirements

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

CloudScan Controller Disk Space Requirements

To estimate the amount of disk space required on the machine that runs the CloudScan Controller, use the following equation:

<Number_Jobs_Per_Day> x (*<Average_MBS_Size>* + *<Average_FPR_Size>* + *<Average_SCA_Log_Size>*) x *<Number_Days_Data_is_Persisted>*

By default, data is persisted for seven days.

CloudScan Controller Platforms and Architectures

The CloudScan Controller supports the platforms and architectures listed in the following table.

Operating System	Architecture	Versions
Windows	64-bit	Server 2012 R2 Server 2016
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x SUSE Linux Enterprise Server 12

CloudScan Client and Sensor Hardware Requirements

CloudScan clients and sensors run on any machine that supports Micro Focus Fortify Static Code Analyzer. Because CloudScan 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 11 for hardware, software, and platform and architecture requirements.

CloudScan Sensor Disk Space Requirements

To estimate the amount of disk space required on the machine that runs a CloudScan sensor, use the following equation:

<Number_of_Scans> x (*<Average_MBS_Size>* + *<Average_FPR_Size>* + *<Average_SCA_Log_Size>*) x *<Number_Days_Data_is_Persisted>*

By default, data is persisted for seven days.

Fortify Runtime Agent Requirements

Micro Focus Fortify Runtime Agent technology is delivered for production application logging and protection with the Application Defender platform, and for Interactive Application Security Testing (IAST) with Fortify WebInspect Agent.

Platforms and Architectures

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

Java Runtime Environments

Fortify Runtime 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: Runtime for Java is supported on Unix, Linux, and Windows.

Java Application Servers

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

Application Server	Versions
Apache Tomcat	6.0, 7.0, 8.0
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	5.1.2, 5.2.0, 6.0.1, 6.1.1, 6.2.0, 6.3.0, 6.4.0
Jetty	9.3
WildFly	10.1

.NET Frameworks

Fortify Runtime Agent supports .NET framework versions 2.0, 3.0, 3.5, 4.0, 4.5, and 4.5.1.

Cloud Platforms

Fortify Runtime Agent supports the cloud platforms listed in the following table.

Cloud Platform	Service
Amazon Web Services	Virtual machines without a sandboxed environment
Microsoft Azure	Virtual machines and cloud services **Note:** Microsoft Azure platform as a service (PaaS) is not supported.

IIS for Windows Server

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

Cipher Suites for Fortify Runtime Agent

Fortify Runtime Agent supports the following cipher suites for communicating with an external syslog server:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

To run Fortify Runtime Agent on a Windows 2003 machine with IIS 6.0, you must install the Advanced Encryption Standard (AES) cipher suites in the `Schannel.dll` module for Windows server 2003. Download the hotfix from Microsoft support (https://support.microsoft.com/en-us/kb/948963).

Fortify WebInspect Requirements

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

Running as Administrator

Micro Focus Fortify WebInspect 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 Fortify WebInspect as an administrator.

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	Recommended
	2.0 GHz dual-core	Minimum
RAM	16 GB	Recommended
	8 GB	Minimum
Hard disk	100+ GB	Recommended
	40 GB	Minimum
Display	1980 x 1080	Recommended
	1280 x 1024	Minimum

Important! If you are running a Fortify WebInspect sensor with SQL Express, Fortify recommends that you use at least a 4-core CPU with at least 16 GB of RAM.

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
	Windows 7 with SP1	
	Windows 8, 8.1	
	Windows Server 2012, 2012 R2	
	Windows Server 2016	
.NET	.NET Framework 4.6.1	
SQL Server	SQL Server 2014 with SP2	Recommended No scan database limit
	SQL Server 2012 with SP4	No scan database limit
	SQL Server 2016 with SP2	No scan database limit
	SQL Server 2017	No scan database limit
SQL Server Express	SQL Server 2014 Express with SP2	Recommended 10 GB scan database limit
	SQL Server 2012 Express with SP4	10 GB scan database limit
	SQL Server 2016 Express with SP2	10 GB scan database limit
	SQL Server 2017 Express	10 GB scan database limit
Browser	Internet Explorer 11	Recommended
	Internet Explorer 10	
Portable Document Format	Adobe Acrobat Reader 11	Recommended
	Adobe Acrobat Reader 8.1.2	Minimum

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.

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	MS SQL Express or MS SQL 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.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
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, but Fortify recommends regularly repeating this CRL download process 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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					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.
Fortify WebInspect to 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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					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.

Direction	Endpoint	URL or Details	Port	Protocol	Notes
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 Runtime Agent Requirements" on page 19.

WebInspect Software Development Kit (SDK)

The WebInspect SDK requires the following software:

- Visual Studio 2013 or 2015
- .NET Framework 4.6.1

Important: Visual Studio Express versions do not support third-party extensions. Therefore, these versions do not meet the software requirements for using 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	18.20
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	18.20
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 18.10 to Fortify WebInspect Enterprise 18.20. 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 18.20 before you install a new instance of Fortify WebInspect Enterprise or upgrade from Fortify WebInspect Enterprise 18.10. 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 18.20
- Fortify WebInspect Agent 18.4

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 9.

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	
Display	1920 x 1080	Recommended
	1280 x 1024	Minimum

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 2012 R2	Recommended
	Windows Server 2012	
	Windows Server 2016	

Package	Versions	Notes
.NET	.NET Framework 4.6.1	
Platform	IIS 8.5	Recommended
	IIS 7.5	
	IIS 8.0	
	IIS 10	
SQL Server	SQL Server 2014 with SP2	Recommended No scan database limit
	SQL Server 2012 with SP4	No scan database limit
	SQL Server 2016 with SP2	No scan database limit
	SQL Server 2017	No scan database limit
Browser	Internet Explorer 11	Recommended
	Mozilla Firefox 51.0 or 56.0[1]	Recommended
	Mozilla Firefox[1] 47.0	
Plugins for Enterprise Servers	Silverlight 5.0 or 5.1	

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.

[1]You cannot perform a Guided Scan or create reports using the Mozilla Firefox browser. This browser no longer supports the .NET Framework Assistant plugin.

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 7 with SP1	
	Windows 8 or 8.1	
	Windows Server 2016	
	Windows Server 2012 or 2012 R2	
.NET	.NET Framework 4.6.1	

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	MS SQL 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 MS SQL 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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					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 usability of the product.
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.

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 updates for the product 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.

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.
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
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 20 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.

License Infrastructure Manager Requirements

This section describes the hardware and software requirements for License 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 or 2012 R2	
	Windows Server 2016	
Internet Information Services (IIS)	Version 7 or later	
.NET Framework	4.6.1	
	4.5	
ASP.NET	4.6	
	4.5	
Browser	Internet Explorer 11	Recommended
	Mozilla Firefox 51.0	Recommended
	Mozilla Firefox 44.0 or 47.0	

Version Compatibility Matrix

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

Fortify Software Component Compatibility

Micro Focus Fortify Software version 18.20 works with the component versions listed in the following table.

Component	Versions
Micro Focus Fortify Software Security Center	18.20
Micro Focus Fortify Static Code Analyzer Tools (Micro Focus Fortify Audit Workbench, Fortify Secure Code Plugins, and Fortify Custom Rules Editor)	18.20
Micro Focus Fortify Runtime Agent	18.4
Micro Focus Fortify WebInspect Agent	18.4
Micro Focus Fortify WebInspect	18.20
Micro Focus Fortify WebInspect Enterprise	18.20

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 17.10 cannot read 18.20 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 18.20 can open and read version 17.10 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 18.20 also has the version number 18.20.
- 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 17.10 FPR with a version 18.20 FPR, the resulting FPR has the version number 18.20.

You can only open 18.20 FPR files with Fortify Software Security Center or Fortify Static Code Analyzer Tools version 18.20 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 17.10 cannot open and read an 18.20 FPR.

Virtual Machine Support

You can run Micro Focus Fortify Software products in 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 sufficient processing, memory, and disk resources, you need to work with the provider of the virtual environment to get them resolved.

Note: Running Fortify software products in a VM environment with shared CPU and memory resources is not supported.

Technologies and Features no Longer Supported in this Release

Customers who are currently using Micro Focus Fortify Runtime are encouraged to upgrade to Fortify Application Defender, a Runtime Application Self Protection (RASP) solution that helps mitigate risk from homegrown or third-party applications. Fortify Application Defender provides visibility into application abuse while protecting software vulnerabilities from exploits in real time. Application Defender is available as a SaaS offering or it can be installed on-premises. For more information, see https://software.microfocus.com/software/application-defender.

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

- Application Servers: Apache Tomcat 8.5 (Fortify Software Security Center)
- Build Tools: Xcodebuild 8.x
- Compilers:
  - Apple LLVM (clang) 8.x
  - Swiftc 3.1
- Databases: MySQL 5.6 (Fortify Software Security Center)
- Integrated Development Environments (IDEs): IntelliJ IDEA 2016.x
- Operating Systems: macOS 10.12

- Fortify Software Security Center features:
  - Legacy (4.30) user interface
  - Legacy Parsers:
    - Whitehat
    - Runtime
    - Real-Time Analyzer (RTA)
    - PenTest Analysis
    - Program Trace Analyzer (PTA)
    - AppScan
    - AppDetective
  - Process Designer

Technologies and Features to Lose Support in the Next Release

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

- Databases: SQL Server 2014 (Fortify Software Security Center)
- Browsers: Internet Explorer 11 (Fortify Software Security Center)
- Build Tools:
  - Bamboo 6.2
  - Xcodebuild 9.x
- Compilers (Fortify Static Code Analyzer):
  - All compilers on HP-UX, IBM AIX, Solaris
  - Swiftc 4.0.3, 4.1
- Integrated Development Environments (IDEs):
  - Android Studio 2.3.x
  - Eclipse 4.6, 4.7
  - IntelliJ IDEA 2017.x
  - WebStorm 2017.x
- Operating Systems:
  - HP-UX, IBM AIX, and Solaris
  - Windows 7 (Fortify Static Code Analyzer Tools and Secure Code Plugins)
- Service Integrations: JIRA 7.4

Acquiring Fortify Software

Micro Focus Fortify Software is available as an electronic download. The following table lists the available packages and describes their contents.

File Name	Description
Fortify_SSC_ Server_18.20.zip	Fortify Software Security Center
Fortify_SSC_ Server_ 18.20.zip.sig	Signature file for Fortify Software Security Center
Fortify_CloudScan_ Controller_ 18.20.zip	Fortify CloudScan Controller
Fortify_CloudScan_ Controller_ 18.20.zip.sig	Signature file for Fortify CloudScan Controller
Fortify_SCA_and_ Apps_ 18.20_Linux.tar.gz	Fortify SCA and Applications installer for Linux The installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench • 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 `Fortify_SCA_and_Apps_18.20_Linux.tar.gz` package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, the Fortify Remediation Plugin for IntelliJ, Android Studio, and WebStorm, and the Fortify Jenkins Plugin.
Fortify_SCA_and_ Apps_ 18.20_ Linux.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Linux

File Name	Description
Fortify_SCA_and_Apps_18.20_Mac.tar.gz	Fortify SCA and Applications installer for macOS This installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench • 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 `Fortify_SCA_and_Apps_18.20_Mac.tar.gz` package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, the Fortify Remediation Plugin for IntelliJ, Android Studio and WebStorm, and the Fortify Jenkins Plugin.
Fotify_SCA_and_Apps_18.20_Mac.tar.tz.sig	Signature files for the Fortify SCA and Applications package for macOS
Fortify_SCA_and_Apps_18.20_Windows.zip	Fortify SCA and Applications installer for Windows This installer includes the following components: • Fortify Static Code Analyzer • Fortify Audit Workbench • Custom Rules Editor • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Extension for Visual Studio • Scan Wizard • Sample applications **Note:** • Fortify Software Security Content (Rulepacks and external metadata) can be downloaded during the installation. • The `Fortify_SCA_and_Apps_18.20_Windows.zip` package includes the Fortify Remediation Plugin for Eclipse, the Fortify Security Assistant Plugin for Eclipse, the Fortify Remediation Plugin for IntelliJ, Android Studio, and WebStorm, and the Fortify Jenkins Plugin.

File Name	Description
Fortify_SCA_and_Apps_18.20_Windows.zip.sig	Signature files for the Fortify SCA and Applications package for Windows
Fortify_SCA_18.20_AIX.tar.gz	Fortify Static Code Analyzer for AIX
Fortify_SCA_18.20_AIX.tar.gz.sig	Signature file for Fortify Static Code Analyzer for AIX
Fortify_SCA_18.20_HPUX.tar.gz	Fortify Static Code Analyzer for HP-UX
Fortify_SCA_18.20_HPUX.tar.gz.sig	Signature file for Fortify Static Code Analyzer for HP-UX
Fortify_SCA_18.20_Solaris.tar.gz	Fortify Static Code Analyzer for Solaris
Fortify_SCA_18.20_Solaris.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Solaris
Fortify_Scan_Wizard_18.20_Linux.tar.gz	Fortify Scan Wizard for Linux
Fortify_Scan_Wizard_18.20_Linux.tar.gz.sig	Signature file for Fortify Scan Wizard for Linux
Fortify_Scan_Wizard_18.20_MacOSX.tar.gz	Fortify Scan Wizard for macOS
Fortify_Scan_Wizard_18.20_MacOSX.tar.gz.sig	Signature file for Fortify Scan Wizard for macOS
Fortify_Scan_Wizard_18.20_Windows.zip	Fortify Scan Wizard for Windows

File Name	Description
Fortify_Scan_ Wizard_ 18.20_ Windows.zip.sig	Signature file for Fortify Scan Wizard for Windows
WebInspect_64_ 18.20.zip	Fortify WebInspect 64-bit version package This package includes product documentation (PDF)
WebInspect_ Agent_18.4.zip	Fortify WebInspect Agent package
WebInspectToolkit_ 18.20.zip	Fortify WebInspect Toolkit package for use with Fortify WebInspect Enterprise
WI_Enterprise_ 18.20.zip	Fortify WebInspect Enterprise package The package includes the following components: • Fortify WebInspect Enterprise server • Fortify WebInspect Enterprise Administrative Console • Product documentation (PDF)

Downloading Fortify Software

To download Micro Focus Fortify Software:

1. Open a browser window and go to https://softwaresupport.softwaregrp.com.
2. Click **Sign In**.
3. Sign in with your Micro Focus Passport credentials.
4. Select **Licensing & Downloads**.
5. Select either **Commercial Customer** or **US Government**.
6. Select an account, and then click **Manage Entitlements**.

   If you do not see your account listed, click **Search Account**, and provide your SAID or Order Number.
7. Find the product you want to download, and then click **Download**.
8. Select the version you want, and then click **Download**.

   Note: If your organization requires that you verify the download, you must also download the like-named signature file. For example, if you download `Fortify_SCA_and_Apps_18.20_Windows.zip`, you must also download the associated signature file `Fortify_SCA_and_Apps_18.20_Windows.sig`.

If you encounter any difficulties with the download process, click **Contact Us / Self Help** from the Software Licenses and Downloads page and review the *Quick Start Guide* for more information.

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

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 version 1.4.x or 2.0.x.
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 the following location:
   https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do
5. Extract the public keys.
6. Import each downloaded key with GnuPG, as follows:
   - Run `gpg --import <Path_to_Key>/<File_Name_of_Key>`

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 <Signature_File_Name> <Downloaded_File_Name>`

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 should include something similar to the following:

```
gpg: Signature made Fri, Oct 06, 2017 10:37:56 PM PDT using RSA key ID
AA71A9CF
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   3  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 3u
gpg: next trustdb check due at 2025-12-07
gpg: Good signature from "Micro Focus Group Limited RSA-2048-12"
```

Note: A warning message might be displayed because 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. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on System Requirements (Fortify Software 18.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!