Hewlett Packard
Enterprise

HPE Security
Fortify Software

Software Version: 17.10

System Requirements

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE 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. Valid license from HPE 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.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

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

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security 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 HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Introduction

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

- HPE Security Fortify Software Security Center Server
- HPE Security Fortify Static Code Analyzer
- HPE Security Fortify Audit Workbench and Secure Code Plugins
- HPE Security Fortify CloudScan
- HPE Security Fortify Runtime
- HPE Security Fortify WebInspect
- HPE Security Fortify WebInspect Enterprise
- License Infrastructure Manager (LIM)

Software Delivery

HPE Security Fortify Software is delivered only electronically. It is not available on disc. See "Acquiring HPE Security Fortify Software" on page 38 for more information.

Software Licenses

Before you can start using HPE Security Fortify Software, you must download the licenses for your purchases from the Fortify Customer Portal (https://support.fortify.com). To access the site, use the credentials that HPE Security Fortify Customer Support has provided.

HPE Security Fortify Software Security Center Server Requirements

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

Hardware Requirements

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

HPE 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
IBM DB2	293,930	1,812,570
MySQL	362,514	2,589,385
Oracle Database	231,392	3,020,950
SQL Server	725,028	3,625,140

Platforms and Architectures

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

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

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

Application Servers

Fortify Software Security Center supports the application servers listed in the following table.

Application Server	Versions	Java Versions
Apache Tomcat	8.0	8
IBM WebSphere 8	8.5.5	8
Oracle WebLogic 12c	12.1.3	8

Fortify Software Security Center Database

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

For a production environment, Fortify Software Security Center supports the databases listed in the following table.

Databases	Supported Character Sets	Drivers
IBM DB2 10.5 fixpack 6	UTF8, IBM-1252	IBM DB2 drivers also require that you add at least one of the following driver license files to the `CLASSPATH` before you load the JDBC driver and seed the database:

Databases	Supported Character Sets	Drivers

		- `db2jcc_license_cisuz.jar`
		- `db2jcc_license_cu.jar`
		IBM DB2 JDBC Driver v10.5
		Driver class:
		`com.ibm.db2.jcc.DB2Driver`
		JAR file:
		`db2jcc4.jar`

MySQL 5.6	utf8_bin, latin1_general_cs	5.1.35 or later
		Driver class:
		`com.mysql.jdbc.driver`
		JAR file:
		`mysql-connector-java-<version>-bin.jar`

Oracle Database 12c	AL32UTF8 for all languages WE8MSWIN1252 for US English	Oracle Database 12c Release 1 (12.1) JDBC Drivers Driver class: `oracle.jdbc.OracleDriver` JAR files: `ojdbc7.jar` (for Java 7 or later)

SQL Server 2014, 2016	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 4.0 for SQL Server
		Driver class:
		`com.microsoft.sqlserver.jdbc.SQLServerDriver`
		JAR file:
		`sqljdbc4.jar`

Note: The Fortify Software Security Center Demonstration Server includes an Apache Derby database for evaluation purposes only. You cannot expand or upgrade the database. Do not use it to store critical data.

Browsers

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

Browser	Version	Adobe Flash Player
Google Chrome	54.0 or later	10.2 or later, 11 (recommended)

Browser	Version	Adobe Flash Player
Internet Explorer	11	10.2 or later, 11 (recommended)
Mozilla Firefox	44.0 or later	10.2 or later, 11 (recommended)
Safari	10	14 **Note:** To access Fortify Software Security Center Flex user interface, you must have Adobe Flash Player version 16 or later installed.

Authentication Systems

Fortify Software Security Center supports the following directory services:

- LDAP: LDAP 3 compatible
- Windows Active Directory Service

Single Sign-On (SSO)

Fortify Software Security Center supports:

- HTTP SSO (Oracle SSO, CA SSO)
- SAML SSO
- SPNEGO/Kerberos SSO
- PKI SSO (X.509)
- CAS SSO

BIRT Reporting

Software Security Center reports support Business Intelligence and Reporting Technology (BIRT) version 4.4.2.

Service Integrations

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

Service	Applications	Versions
Bug tracking	Bugzilla	5.0
	HPE Application Lifecycle Management (HPE ALM)/ HPE Quality Center	12.50
	JIRA	6.4, 7.1
	Team Foundation Server (TFS)	2015
	Visual Studio Team Services (VSTS) **Note:** Only basic user password authentication is supported.	n/a
Authentication	Active Directory	2008, 2012
Dynamic assessments	HPE Security Fortify WebInspect Enterprise	17.10

Fortify Software Security Center Configuration Wizard Requirements

This section describes the system requirements for the Fortify Software Security Center Configuration Wizard (Configuration wizard).

Hardware Requirements

The Configuration wizard requires the following:

Component	Requirement
Processor	2.0 GHz or faster, 64-bit
RAM	4 GB or higher (minimum 3 GB available)

Platforms and Architectures

The Configuration wizard supports the same platforms and architectures as Fortify Software Security Center. For details, see "Platforms and Architectures" on page 9.

Java Virtual Machine

The Configuration wizard supports Oracle JVM version 8.

Graphical User Interface

The Configuration wizard supports the following graphical user interfaces:

- X Window System for Linux
- Desktop UI for Windows

> **Note:** The system from which you run the Configuration wizard must also have network access to the database and infrastructure servers.

HPE Security Fortify Static Code Analyzer Requirements

This section describes the system requirements for HPE Security Fortify Static Code Analyzer (Fortify Static Code Analyzer), Audit Workbench, and Secure Code Plugins.

Hardware Requirements

HPE recommends that you install Fortify Static Code Analyzer on a high-end processor with at least 8 GB of RAM. If your software is complex, you might require more RAM. See the *HPE Security Fortify Static Code Analyzer Performance Guide* for more information.

The minimum requirements for running Fortify Static Code Analyzer in parallel analysis mode are:

- 16 GB RAM *per core*
- 4 cores

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

Software Requirements

Fortify Static Code Analyzer requires Java 8. The HPE Security Fortify SCA and Applications installer installs JRE 1.8.0_121.

Platforms and Architectures

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

Operating System	Architectures	Platforms
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x Oracle Linux 6 update 5 and later Oracle Linux 7.x SUSE Linux Enterprise Server 12
Windows	64-bit	Windows Server 2012 R2 Windows 8.1 Windows 10
Oracle Solaris	x86, 64-bit	10.5 and later 11.3
Oracle Solaris	SPARC 64-bit	10.5 and later 11.3
HP-UX	Itanium 64-bit	11.31
AIX	64-bit	6.1 7.2
Mac OS X macOS		10.11 10.12

Note: If the previous table does not list an operating system that you require, contact HPE Security Fortify Support.

Note: Audit Workbench, Process Designer, Custom Rules Editor, and Scan Wizard are not supported on AIX, HP-UX, or Oracle Solaris systems.

Supported Languages

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

Language	**Versions**
ABAP/BSP	6
ActionScript	3.0
Apex	36
ASP.NET	4.6
C# (.NET)	6
C/C++	See "Compilers" on the next page
Classic ASP (with VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL for z/OS 3.4.1 with CICS, IMS, DB2 embedded SQL, and IBM MQ
ColdFusion CFML	8, 9, 10
HTML	5 and earlier
Java (including Android)	5.0, 6, 7, 8
JavaScript	1.7
JSP	1.2, 2.1
MXML (Flex)	4
Objective-C/C++	See "Compilers" on the next page
PHP	5.3
PL/SQL	8.1.6
Python	2.6, 2.7
Ruby	1.9.3
Swift	2.2, 3.0
T-SQL	SQL Server 2005, 2008, 2012
VB.NET	14

Language	Versions
VBScript	2.0, 5.0
Visual Basic	6
XML	1.0

Build Tools

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

Build Tool	Versions	Notes
Ant	1.9.6	
Gradle	2.13	The Fortify Static Code Analyzer Gradle build integration supports the following language/platform combinations: • Java/Windows, Linux, and Mac OS X • C/Linux • C++/Linux
Jenkins	1.6	
Maven	3.0.5, 3.3.x	
MSBuild	4.x, 12.0, 14.0	
Xcodebuild	7.x, 8.0, 8.1, 8.2.1	

Compilers

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

Compiler	Versions	Platform
gcc	GNU gcc 4.9, 5.x	AIX, Linux, HP-UX, Mac OS X, Solaris, Windows
g++	GNU g++ 4.9, 5.x	AIX, Linux, HP-UX, Mac OS X, Solaris, Windows
Intel C++ Compiler	icc 8.0	Linux
Oracle javac	7, 8	AIX, Linux, HP-UX, Mac OS X, Solaris, Windows
Oracle Solaris Studio	12	Solaris

Compiler	Versions	Platform
cl	VS 2012, 2013, 2015	Windows
Apple LLVM (Clang)	7.x, 8.0, 8.1	Mac OS X, macOS
Swiftc	2.2, 3.0.2	Mac OS X, macOS

Secure Code Plugins

The following table lists the supported IDE environments for Secure Code Plugins.

Plugin	IDE Versions
Eclipse (Complete and Remediation)	Eclipse 4.6
IntelliJ IDEA (Analysis and Remediation)	IntelliJ IDEA 15, 2016.x
Android Studio (Analysis and Remediation)	Android Studio 2.1.2
JDeveloper (Remediation)	JDeveloper 12c
Visual Studio Package	Visual Studio 2012 Premium, Professional, and Ultimate Visual Studio 2013 Premium, Professional, and Ultimate Visual Studio 2015 Community, Professional, and Enterprise **Note:** Fortify Static Code Analyzer is not compatible with Visual Studio Express.
Security Assistant (for Java code only)	Eclipse 4.6
Xcode (Scanning)	Xcode 7.x

Service Integrations for Fortify Static Code Analyzer Tools

The following table lists the supported service integrations for the Fortify Static Code Analyzer Tools.

Bug Tracker Application	Versions	Supported Tools
Bugzilla	5.0	Audit Workbench, Eclipse Plugin, Visual Studio Package

Bug Tracker Application	Versions	Supported Tools
HPE Application Lifecycle Management (HPE ALM)/ HPE Quality Center	12.50	Audit Workbench, Eclipse Plugin
Team Foundation Server (TFS)	2012, 2013	Visual Studio Package
	2015	Audit Workbench, Eclipse Plugin, Visual Studio Package
Visual Studio Team Services (VSTS) **Note:** Only basic user password authentication is supported.	n/a	Audit Workbench, Eclipse Plugin
JIRA	6.4, 7.1	Audit Workbench, Eclipse Plugin
Fortify Software Security Center Bugtracker	17.10	Audit Workbench, Eclipse Plugin, Visual Studio Package

Security Content

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

HPE Security Fortify CloudScan Requirements

HPE Security Fortify CloudScan has three major components: CloudScan Controller, CloudScan client, and CloudScan sensor. This section describes the requirements for each component.

CloudScan Controller Hardware Requirements

HPE recommends that you install 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 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	Architectures	Versions
Linux	64-bit	Red Hat Enterprise Linux 6 update 5 and later Red Hat Enterprise Linux 7.x Oracle Linux 6 update 5 and later Oracle Linux 7.x SUSE Linux Enterprise Server 12
Windows Server	64-bit	Server 2012 R2

CloudScan Client and Sensor Hardware Requirements

CloudScan client and sensor run on any machine that supports Fortify Static Code Analyzer. Because CloudScan client and sensor are installed on build machines running Fortify Static Code Analyzer, the hardware requirements are met.

See "HPE Security Fortify Static Code Analyzer Requirements" on page 13 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 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.

HPE Security Fortify Runtime Requirements

HPE Security Fortify Runtime is delivered as separate install images for HPE Security Fortify Runtime Application Protection, HPE Security ArcSight Application View, and HPE Security Fortify WebInspect Agent.

Platforms and Architectures

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

Java Runtime Environments

HPE Security Fortify Runtime 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

HPE Security Fortify Runtime 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, 6.30, 6.40
Jetty	9.3
WildFly	10.1

.NET Frameworks

HPE Security Fortify Runtime supports .NET frameworks versions 2.0, 3.0, 3.5, 4.0, 4.5, and 4.5.1.

IIS for Windows Server

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

Cipher Suites for HPE Security Runtime Agent

HPE Security 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 HPE Security 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).

HPE Security Fortify WebInspect Requirements

Before you install HPE Security Fortify WebInspect (Fortify WebInspect), ensure that your system meets the requirements described in this section.

Running as Administrator

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

HPE recommends that you install Fortify WebInspect on a system that conforms to the supported components listed in the 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 quad-core or faster	Recommended
	2.0 GHz dual-core	Minimum
RAM	8+ GB (2 GB per core)	Recommended
	4 GB	Minimum
Hard disk	100+ GB	Recommended
	40 GB	Minimum

Component	Requirement	Notes
Display	1980 x 1080	Recommended
	1280 x 1024	Minimum

Important: If you are running a Fortify WebInspect sensor with SQL Express, HPE recommends that you use at least a 4-core CPU and a 64-bit operating system with at least 8 GB of RAM.

Software Requirements

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

Note: Fortify WebInspect is available in both 32-bit and 64-bit installation versions.

Package	Versions	Notes
Windows	Windows 10	Recommended
	Windows 7 with SP1	
	Windows 8 or 8.1	
	Windows Server 2012, 2012 R2	
	Windows Server 2016	
.NET	.NET Framework 4.6.1	
SQL Server	SQL Server 2012 with SP2	Recommended No scan database limit
	SQL Server 2008 R2 with SP2	
	SQL Server 2012 with SP1	No scan database limit
	SQL Server 2014 with SP1	No scan database limit
	SQL Server 2016	No scan database limit
SQL Server Express	SQL Server 2014 Express with SP1	Recommended 10 GB scan database limit
	SQL Server 2012 Express with SP1 or SP2	10 GB scan database limit
	SQL Server 2016 Express	10 GB scan database limit
Browser	Internet Explorer 11	Recommended
	Internet Explorer 10	

Package	Versions	Notes
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. 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 the Fortify WebInspect Application Settings (**Edit > Application Settings > Database**).

Ports and Protocols

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

Required Connections

The following table lists the ports and protocols 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 for maintaining the scan data and generating 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 HPE recommends regularly repeating this CRL download process as part of regular maintenance.

Optional Connections

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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Fortify WebInspect to HPE License activation server	Remote HPE Licensing Service	https://licenseservice.fortify.hpe.com/	443	HTTPS over SSL	For one-time activation of a Fortify WebInspect Named User license. 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.hpe.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 HPE	Remote HPE Support Channel	https://supportchannel.fortify.hpe.com/	443	HTTPS over SSL	Used to retrieve product marketing

Direction	Endpoint	URL or Details	Port	Protocol	Notes
Support Channel server	service				messages as well as to upload Fortify WebInspect data or product suggestions to HPE Security Fortify 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 HPE Telemetry server	Remote HPE 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 HPE. HPE software developers use this information to help improve the product.
Fortify WebInspect to License and Infrastructure Manager (LIM)	HPE 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 client license from LIM once activated 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

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					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 as well as 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, the local installation may be configured as a remote scan engine for use by the enterprise security solution community. This is done through a Windows Service. This constitutes a different product from Fortify WebInspect desktop and is recommended to be run on its own, non-user-focused machine.
Browser to Fortify WebInspect	localhost	Manual Step-Mode Scan	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	Fortify WebInspect serves as a web proxy to the browser, enabling manual testing of the target web server through Fortify WebInspect.
Fortify WebInspect to HPE Quality Center (HPE ALM)	HPE QC server	User-specified HPE QC server	Server-specified	HTTP or HTTPS over SSL	Permits submission of findings as defects to the HPE ALM defect management system.
Fortify WebInspect to IBM Rational ClearQuest	IBM CQ server	User-specified IBM CQ server	Server-specified	HTTP or HTTPS over SSL	Permits submission of findings as defects to the ClearQuest defect management system.

Connections for Tools

The following table lists the ports and protocols that the 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)

HPE Security Fortify WebInspect Agent

For system requirements, see "HPE Security Fortify Runtime Requirements" on page 19.

WebInspect Software Development Kit (SDK)

The WebInspect SDK requires the following software:

- Visual Studio 2013 or Visual Studio 2015
- .NET Framework 4.6.1

Important: Visual Studio Express versions do not support third-party extensions such as the WebInspect SDK. Therefore, these versions do not meet the software requirements for using the SDK.

Software Integrations

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

Product	Versions
HPE Security Fortify WebInspect Enterprise	17.10

Product	Versions
HPE Application Lifecycle Management (HPE ALM) **Note:** You must also install the HPE ALM Connectivity tool to connect Fortify WebInspect to HPE ALM.	11.5, 12.01
HPE Security Fortify Software Security Center	17.10
HPE Unified Functional Testing	11.5

HPE Security Fortify WebInspect Enterprise Requirements

Before you install HPE Security Fortify WebInspect Enterprise (Fortify WebInspect Enterprise), ensure that your systems meet the requirements described in this section.

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

Fortify WebInspect Enterprise Installation and Upgrade Requirements

You can upgrade directly from Fortify WebInspect Enterprise 16.20 to Fortify WebInspect Enterprise 17.10. You cannot upgrade directly from any other versions of Fortify WebInspect Enterprise. For detailed information about upgrades, see the *HPE Security Fortify WebInspect Enterprise Installation and Implementation Guide*.

Integration with HPE Security 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 17.10 before you install a new instance of Fortify WebInspect Enterprise or upgrade from Fortify WebInspect Enterprise 16.20. 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

HPE Security Fortify supports integration of Fortify WebInspect Enterprise with the following components:

- HPE Security Fortify WebInspect sensors 17.10
- HPE Security Fortify WebInspect Agent 17.3

Fortify WebInspect Enterprise Database

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

Component	Requirement	Notes
Processor	3.0 GHz quad-core or faster	Recommended
	2.5 GHz dual-core	Minimum
RAM	8+ GB (2 GB per core)	Recommended
	4 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	Minimum
	1280 x 1024	Recommended

Software Requirements

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	
.NET	.NET Framework 4.6.1	

Package	Versions	Notes
Platform	IIS 8.5	Recommended
	IIS 7.5	
	IIS 8.0	
	IIS 10	
SQL Server	SQL Server 2014 with SP1	Recommended No scan database limit
	SQL Server 2012 with SP1 or SP2	No scan database limit
	SQL Server 2016	No scan database limit
Browser	Internet Explorer 11	Recommended
	Mozilla Firefox 51.0[1]	Recommended
	Mozilla Firefox[1] 44.0 or 47.0	
Plugins for Enterprise Servers	For Fortify Software Security Center: Flash	
	For Fortify WebInspect Enterprise: Silverlight 5.0 or 5.1	

Fortify WebInspect Enterprise Administrative Console Requirements

This section describes the hardware and software requirements for the 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.

Note: The Fortify WebInspect Enterprise Administrative Console is available in both 32-bit and 64-bit installation versions.

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 Fortify WebInspect Enterprise uses to make required and optional connections.

Required Connections

The following table lists the ports and protocols 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.
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 usability of the product.
Browser users to Fortify Software Security Center server 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.hpe.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 HPE 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 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 HPE License activation server	HPE Licensing Service	https://licenseservice.fortify.hpe.com	443	HTTPS over SSL	For one-time activation of Fortify WebInspect Enterprise server license as well as periodic checks during an update. You may optionally use the following:

Direction	Endpoint	URL or Details	Port	Protocol	Notes
					- 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. If you want mobile TXT alerts, then 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 Fortify WebInspect 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 Fortify WebInspect Enterprise sensor is a Fortify WebInspect sensor that runs scans on behalf of Fortify WebInspect Enterprise. See "HPE Security Fortify WebInspect Requirements" on page 21 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 Fortify Software Security Center to only one instance of 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 (LIM) Requirements

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

Hardware Requirements

HPE recommends that you install the License Infrastructure Manager (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

License Infrastructure Manager (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 2008 R2 with SP1	
	Windows Server 2008 with SP2	
Internet Information Server (IIS)	Version 7 or later	
.NET Framework	4.6.1	
Browser	Internet Explorer 11	Recommended
	Internet Explorer 10	
	Mozilla Firefox 33.0	Recommended
	Mozilla Firefox 30.0	

Version Compatibility Matrix

This section provides compatibility information for HPE Security Fortify Software components.

HPE Security Fortify Software Component Compatibility

HPE Security Fortify Software version 17.10 works with the component versions listed in the following table.

Component	Versions
Fortify Software Security Center	17.10
Fortify Software Security Center Tools (Audit Workbench, Secure Code Plugins, Custom Rules Editor, Process Designer, and fortifyclient)	17.10
HPE Security Fortify Runtime	17.3
HPE Security Fortify WebInspect Agent	17.3
HPE Security Fortify WebInspect	17.10
HPE Security Fortify WebInspect Enterprise	17.10

FPR File Compatibility

Earlier versions of HPE Security Fortify products cannot open and read FPR files generated by later versions of HPE Security Fortify products. For example, Audit Workbench 4.40 cannot read 17.10 FPR files. However, later versions of HPE Security Fortify products can open and read FPR files generated by earlier versions of HPE Security Fortify products. For example, Audit Workbench version 17.10 can open and read version 4.40 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 HPE Security Fortify Software version 17.10 also has the version number 17.10.
- The FPR version is the same as the version of the Fortify Software Security Center or 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 4.40 FPR with a version 17.10 FPR, the resulting FPR has the version number 17.10.

You can only open 17.10 FPR files with Fortify Software Security Center or Fortify Static Code Analyzer Tools version 17.10 or later.

Caution Regarding Uploading FPRs to Fortify Software Security Center

HPE Security Fortify Software Security Center keeps a project file that contains the latest scan results and audit information for each application. 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 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, Audit Workbench 4.40 cannot open and read a 17.10 FPR.

Fortify Software Security Center Support for Runtime Configuration Bundle and Template

Fortify Software Security Center 17.10 supports Runtime Configuration Bundle and Template 17.3.

Virtual Machine Support

You can run HPE Security 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 HPE Security 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

The following technologies are no longer supported in Fortify Software:

- Android Studio 1.5 (Fortify Static Code Analyzer Tools)
- HPE ALM 12.01 (Fortify Software Security Center and Fortify Static Code Analyzer Tools)
- Fortify Static Code Analyzer utility `rulepackupdate` (replaced by the `fortifyupdate` utility)
- IBM WebSphere 8 with Java 7 (Fortify Software Security Center)
- Internet Explorer 10 (Fortify Software Security Center)
- MSBuild 2 and 3.5
- Oracle Solaris (Fortify Software Security Center)
- Safari 9
- SOAP web-service API (Fortify Software Security Center)

Technologies and Features to Lose Support in the Next Release

The following technologies are scheduled for deprecation in the next Fortify Software release:

- Mac OS X 10.11 (Fortify Static Code Analyzer and Tools)
- Mac OS X Apple LLVM (clang) compiler version 7.x (Fortify Static Code Analyzer)
- Swift compiler version 2.2 (Fortify Static Code Analyzer)
- JIRA 6.4
- MS SQL Server 2014 (Fortify Software Security Center)

Acquiring HPE Security Fortify Software

HPE Security Fortify Software is available as an electronic download. You must have a SAID access account number to download HPE Security Fortify Software from the HPE Security Software Support site. The following table lists the available packages and describes their contents.

File Name	**Description**
HPE_Security_Fortify_17.10_Windows.iso	(For Windows operating systems) Disc image of the entire HPE Security Fortify Software product line. After downloading, you must either mount the ISO image or burn it to a DVD before installation.

File Name	Description
HPE_Security_Fortify_17.10_Windows.iso.sig	(For Windows operating systems) Signature file for the HPE Security Fortify Software product line ISO
HPE_Security_Fortify_17.10_Linux_Unix_Mac.iso	(For Linux, Unix, and Mac operating systems) Disc image of the entire HPE Security Fortify Software product line. After downloading, you must either mount the ISO image or burn it to a DVD before installation.
HPE_Security_Fortify_17.10_Linux_Unix_Mac.iso.sig	(For Linux, Unix, and Mac operating systems) Signature file for the HPE Security Fortify Software product line ISO
HPE_Security_Fortify_SSC_Server_17.10.zip	Fortify Software Security Center
HPE_Security_Fortify_SSC_Server_17.10.zip.sig	Signature file for Fortify Software Security Center
HPE_Security_Fortify_CloudScan_Controller_17.10.zip	HPE Security Fortify CloudScan Controller
HPE_Security_Fortify_CloudScan_Controller_17.10.zip.sig	Signature file for HPE Security Fortify CloudScan Controller
HPE_Security_Fortify_Runtime_17.3.zip	HPE Security Fortify Runtime
HPE_Security_Fortify_Runtime_17.3.zip.sig	Signature file for HPE Security Fortify Runtime
HPE_Security_Fortify_SCA_and_Apps_17.10_Windows.zip	HPE Security Fortify SCA and Applications package for Windows This package includes the following components: • Fortify Static Code Analyzer • Audit Workbench • Custom Rules Editor • Process Designer • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Package for Visual Studio • Scan Wizard • Product documentation (PDF) • Sample applications **Note:** • Security content (Rulepacks and external metadata) can be downloaded during the

File Name	Description
	installation. - Fortify Remediation Extension for JDeveloper, Fortify Remediation Plugin for Eclipse, Fortify Security Assistant Plugin for Eclipse, Fortify Remediation Plugin for IntelliJ and Android Studio, and Fortify Jenkins Plugin are included as part of the `HPE_Security_Fortify_17.10_Windows` disc image.
HPE_Security_Fortify_SCA_and_Apps_17.10_Windows.zip.sig	Signature files for the HPE Security Fortify SCA and Applications package for Windows
HPE_Security_Fortify_SCA_and_Apps_17.10_Mac.tar.gz	HPE Security Fortify SCA and Applications package for Mac OS This package includes the following components: - Fortify Static Code Analyzer - Audit Workbench - Custom Rules Editor - Process Designer - Fortify Plugin for Eclipse - Fortify Analysis Plugin for IntelliJ and Android Studio - Fortify Scan Wizard - Fortify Scanning Plugin for Xcode - Product documentation (PDF) - Sample applications **Note:** - Security content (Rulepacks and external metadata) can be downloaded during the installation. - Fortify Remediation Extension for JDeveloper, Fortify Remediation Plugin for Eclipse, Fortify Security Assistant Plugin for Eclipse, Fortify Remediation Plugin for IntelliJ and Android Studio, and Fortify Jenkins Plugin are included as part of the `HPE_Security_Fortify_17.10_Linux_Unix_Mac` disk image.
HPE_Security_Fortify_SCA_and_Apps_17.10_Linux.tar.gz	HPE Security Fortify SCA and Applications package for Linux The package includes the following components: - Fortify Static Code Analyzer

File Name	Description
	• Audit Workbench • Custom Rules Editor • Process Designer • Fortify Plugin for Eclipse • Fortify Analysis Plugin for IntelliJ and Android Studio • Fortify Scan Wizard • Product documentation (PDF) • Sample applications **Note:** • Security content (Rulepacks and external metadata) can be downloaded during the installation. • Fortify Remediation Extension for JDeveloper, Fortify Remediation Plugin for Eclipse, Fortify Security Assistant Plugin for Eclipse, Fortify Remediation Plugin for IntelliJ and Android Studio, and Fortify Jenkins Plugin are included as part of the `HPE_Security_Fortify_17.10_Linux_Unix_Mac` disk image.
HPE_Security_Fortify_SCA_and_Apps_17.10_Linux.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Linux
HPE_Security_Fortify_SCA_17.10_HPUX.tar.gz	Fortify Static Code Analyzer for HP-UX
HPE_Security_Fortify_SCA_17.10_HPUX.tar.gz.sig	Signature file for Fortify Static Code Analyzer for HP-UX
HPE_Security_Fortify_SCA_17.10_Solaris.tar.gz	Fortify Static Code Analyzer for Solaris
HPE_Security_Fortify_SCA_17.10_Solaris.tar.gz.sig	Signature file for Fortify Static Code Analyzer for Solaris
HPE_Security_Fortify_SCA_17.10_AIX.tar.gz	Fortify Static Code Analyzer for AIX
HPE_Security_Fortify_SCA_17.10_AIX.tar.gz.sig	Signature file for Fortify Static Code Analyzer for AIX
HPE_Security_Fortify_Scan_Wizard_17.10_Windows.zip	Fortify Scan Wizard for Windows
HPE_Security_Fortify_Scan_Wizard_17.10_Windows.zip.sig	Signature file for Fortify Scan Wizard for Windows

File Name	Description
HPE_Security_Fortify_Scan_Wizard_17.10_MacOSX.tar.gz	Fortify Scan Wizard for Mac OS X
HPE_Security_Fortify_Scan_Wizard_17.10_MacOSX.tar.gz.sig	Signature file for Fortify Scan Wizard for Mac OS X
HPE_Security_Fortify_Scan_Wizard_17.10_Linux.tar.gz	Fortify Scan Wizard for Linux
HPE_Security_Fortify_Scan_Wizard_17.10_Linux.tar.gz.sig	Signature file for Fortify Scan Wizard for Linux
HPE_Security_Fortify_SSC_Demo_Suite_17.10_Windows_x64.zip	HPE Security Fortify Demo Suite for Windows (x64)
HPE_Security_Fortify_SSC_Demo_Suite_17.10_Windows_x64.zip.sig	Signature file for HPE Security Fortify Demo Suite for Windows (x64)
HPE_Security_Fortify_SSC_Demo_Suite_17.10_Unix.tar.gz	HPE Security Fortify Demo Suite for Unix
HPE_Security_Fortify_SSC_Demo_Suite_17.10_Unix.tar.gz.sig	Signature file for HPE Security Fortify Demo Suite for Unix
WebInspect_32_17.10.zip	Fortify WebInspect 32-bit version package This package includes product documentation (PDF)
WebInspect_64_17.10.zip	Fortify WebInspect 64-bit version package This package includes product documentation (PDF)
WebInspect_Agent_17.3.zip	Fortify WebInspect Agent package
HPSecurityToolkit_17.10.zip	HPE Security Toolkit package for use with Fortify WebInspect Enterprise
WI_Enterprise_17.10.zip	Fortify WebInspect Enterprise package The package includes the following components: • Fortify WebInspect Enterprise server • Fortify WebInspect Enterprise Administrative Console • Product documentation (PDF)

Downloading HPE Security Fortify Software

To download HPE Security Fortify software:

1. Open a browser window and go to https://softwaresupport.hpe.com.
2. Click **My Software Support Sign-in**, and then provide your login credentials.

3. From the HPE menu, select **Product Information > Downloads**.

   The **My software updates** page opens and lists the software support contracts (SAIDs) linked to your HPE Passport Profile with their associated products.

   Note: If you do not have SAID access to HPE Security products associated with your HPE Passport, select the **Directly enter an SAID** option, and then type in your HPE SAID account number.

4. Select (or provide) your SAID.
5. View the terms and conditions, and then click the **Yes, I accept these terms and conditions** check box.
6. Click **View available products**.

   The **My software updates - product list** page opens in a new browser tab.

7. To see the HPE Security products available for download, expand the **Fortify Software Security Center** node.
8. Select the check boxes for the products and versions to download, and then click **Get software updates**.

   The **My software updates - downloads** page opens.

9. On the **Selected Products** tab, in the **Deliverables** column, click **Get Software** to download the product.
10. On the **Get Software** tab, follow the instructions to complete the 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 the `HPE_Security_Fortify_SCA_and_Apps_17.10_Windows.zip` file, you must also download the associated signature file `HPE_Security_Fortify_SCA_and_Apps_17.10_Windows.sig`. In rare cases, the signature file you download might have the wrong extension (either `.zip` or `.gz`). If this is the case, change the final extension to `sig`.

About Verifying Software Downloads

This topic describes how to verify the digital signature of the signed file that you downloaded from the HPE Security Software Support site. Verification ensures that the downloaded package has not been altered since it was signed by HPE and posted to the site. Before proceeding with verification, download the HPE Security 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 HPE public keys (compressed tar file) from the following location:

   https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning
5. Extract the public keys using WinZip.
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 ensure you receive verification that the software you downloaded is signed by HPE and is unaltered.

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 the HPE public keys.

HPE Assistive Technologies (Section 508)

In accordance with section 508 of the Rehabilitation Act, 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.

Using JAWS with HPE Security Products

When using JAWS to generate text-to-speech translations of the text in the Audit Workbench graphical user interface, you can use several keyboard combinations to help you get the most out of the interaction. These are described in the following table.

Task	**Keyboard Combination**
To read values in combo boxes.	Press **Ctrl** + down arrow key to turn on Form mode or press **Enter**.
Tab through multiple line text boxes.	Press **Ctrl** + **Tab** to move from one multiple line text box to another.
Read multiple line labels.	Press **Insert** + down arrow to read all lines in label.
Read disabled (grayed-out) items.	Press **Insert** + **b** or **Insert** + down arrow.
Read disabled check boxes.	Press **Insert** to exit Forms mode and enter Virtual Cursor mode.
Enable reading table headings.	Press **Insert** + **F2**. The Run JAWS Manager dialog box opens. Click **OK**.
Switch between pods or panels.	Press and hold **Ctrl**+ **F7** as you select a different pane.
Return focus to the application (JAWS is reading the web browser application rather than the content of the browser).	Press **Ctrl**+ **R** to refresh the display. **Note:** If you refresh the display, your session is aborted and any data you have typed in the page is lost.

For more information about using JAWS, see the JAWS documentation.

For more information about the accessibility of HPE products, visit the Hewlett Packard Enterprise Accessibility site at http://www8.hp.com/us/en/hpe/hp-information/accessibility-aging/index.html.

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 (HPE Security Fortify Software 17.10)

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 HPFortifyTechpubs@hpe.com.

We appreciate your feedback!