opentext™

OpenText™ Fortify WebInspect

Software Version: 24.2.0
Windows® operating systems

Installation Guide

Document Release Date: May 2024
Software Release Date: May 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

Documentation Updates

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

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

This document was produced for OpenText™ Fortify WebInspect CE 24.2 on May 14, 2024. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface ... 6
Contacting Customer Support ... 6
For More Information ... 6
About the Documentation Set ... 6
Fortify Product Feature Videos ... 6

Change Log ... 7

Chapter 1: Welcome to Fortify WebInspect ... 9
The Main Features of Fortify WebInspect ... 9
Crawling and Auditing ... 9
Reporting ... 9
Manual Hacking Control ... 10
Summary and Fixes ... 10
Scanning Policies ... 10
Sortable and Customizable Views ... 10
Enterprise-Wide Usage Capabilities ... 11
API and Web Services Scans ... 11
API Discovery ... 11
Integration Capabilities ... 11
Export Wizard ... 11
Hacker-level Insights ... 11
Testing Tools ... 12
Related Documents ... 12
All Products ... 13
Fortify ScanCentral DAST ... 13
Fortify WebInspect ... 14
Fortify WebInspect Enterprise ... 16

Chapter 2: Installing WebInspect ... 17
Installation Recommendation ... 17
Prerequisites ... 17

SQL Server Database Privileges ... 17
About the Installer Files ... 17
Installation Options ... 18
Using the Setup Wizard ... 18
Using the msiexec Program ... 19
Normal Installation ... 19
Reboot Message Suppression ... 19
Silent Mode ... 20
Synchronous Installation ... 20
Using the WIConfig Program ... 20
Important Facts About WIConfig ... 21
Syntax ... 21
Parameters ... 21
Required Parameters to Configure a Sensor ... 24
Optional Parameters to Configure a Sensor ... 24
Guidelines When Using Azure SQL Database ... 26
Recommended Process for Configuring Azure SQL Database ... 26
Updating Fortify WebInspect ... 26
Directory Structure ... 27
Disclaimer ... 28

Chapter 3: Licensing WebInspect ... 29
Licensing with the License Wizard ... 29
Activating Your Software ... 29
Connect to OpenText ... 30
License File Activation ... 30
Fortify Activation ... 31
Connect to LIM ... 32
License Revocation ... 33
Licensing with the License Utility ... 34
Syntax for Named Users ... 34
Syntax for Concurrent Users ... 34
Options ... 34
Configuring Fortify WebInspect to use the LIM ... 36
For Existing (Licensed) Fortify WebInspect Installations ... 36
For New (Unlicensed) Fortify WebInspect Installations ... 37

Chapter 4: The WebInspect SDK 38
Installation Recommendation 38
Installing the WebInspect SDK 38
Verifying the Installation 39

Send Documentation Feedback 40

Preface

Contacting Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/application-security

About the Documentation Set

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

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText Fortify Community:

https://community.microfocus.com/cyberres/fortify/w/announcements

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

https://www.youtube.com/c/FortifyUnplugged

Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
24.2.0	Updated: • Licensing information with new LIM URL format. See "Licensing with the License Wizard" on page 29 and "Connect to LIM" on page 32. Removed: • Images from Setup Wizard content.
23.2.0 / January 2024	Updated: • Licensing information to clarify LIM URL. See "Connect to LIM" on page 32.
23.2.0	Updated: • Minor edits to incorporate branding changes. Removed: • 15-day trial option from the License Wizard content. • Content related to the 32-bit installer package for WebInspect SDK.
23.1.0	Added: • Content for accessing Debricked open source health metrics. See "Hacker-level Insights " on page 11 and "Using the WIConfig Program" on page 20. Removed: • Content related to AutoPass licensing. • Content related to Telemetry.
22.2.0 / December 2022	Added:

Software Release / Document Version	Changes
	• Process for configuring an Azure SQL database. See "Guidelines When Using Azure SQL Database" on page 26.
22.2.0	Updated: • Features list with new API scanning functionality. See "The Main Features of Fortify WebInspect" on page 9. • `WIConfig` information with 2FA server and OAST server options. See "Using the WIConfig Program" on page 20.

Chapter 1: Welcome to Fortify WebInspect

OpenText™ Fortify WebInspect is the most accurate and comprehensive automated Web application and Web services vulnerability scanning solution available today. With Fortify WebInspect, security professionals and compliance auditors can quickly and easily analyze the numerous Web applications and Web services in their environment. Fortify WebInspect is the only product that is maintained and updated daily by the world's leading Web security experts. These solutions are specifically designed to assess potential security flaws and to provide all the information you need to fix them.

Fortify WebInspect delivers the latest evolution in scanning technology, a Web application security product that adapts to any enterprise environment. As you initiate a scan, Fortify WebInspect assigns "assessment agents" that dynamically catalog all areas of a Web application. As these agents complete the assessment, findings are reported to a main security engine that analyzes the results. Fortify WebInspect then launches audit engines to evaluate the gathered information and apply attack algorithms to locate vulnerabilities and determine their severity. With this smart approach, Fortify WebInspect continuously applies appropriate scan resources that adapt to your specific application environment.

The Main Features of Fortify WebInspect

The following is a brief overview of what you can do with Fortify WebInspect, and how it can benefit your organization.

Crawling and Auditing

Fortify WebInspect uses two basic modes for determining your security weaknesses:

- A crawl is the process by which Fortify WebInspect identifies the structure of the target Web site. In essence, a crawl runs until no more links on the URL can be followed.
- An audit is the actual vulnerability assessment.

When a crawl and an audit are combined into one function, it is termed a scan. A scan combines application crawl and audit phases into a single fluid process. The scan is refined based on real-time audit findings, resulting in a comprehensive view of an entire Web application's attack surface. Intelligent engines employ a structured, logic-based approach to analyzing an application and then customize attacks based on the application's behavior and environment. Fortify WebInspect combines sophisticated, ground-breaking scanning technologies with a database of known Web application vulnerabilities.

Reporting

Use Fortify WebInspect reports to gain valuable, organized application information. You can customize report details, deciding what level of information to include in each report, and gear the

report for a specific audience. You can save reports in a variety of formats, and you can also include graphic summaries of vulnerability data.

Manual Hacking Control

With Fortify WebInspect, you can see what's really happening on your site, and simulate a true attack environment. Fortify WebInspect functionality gives you the ability to view the code for any page that contains vulnerabilities, then make changes to server requests and resubmit them instantly.

When using the Web Proxy tool, you can also pause the client-server data flow when Web Proxy receives a request from the client, receives a response from the server, or finds text that satisfies the search rules you create.

Summary and Fixes

Fortify WebInspect provides summary and remediation information for all vulnerabilities detected during a scan. This includes reference material, links to patches, instructions for prevention of future problems, and vulnerability solutions. As new attacks and exploits are formulated, we update our remediation database. Use Smart Update on the Fortify WebInspect toolbar to update your database with the latest vulnerability solution information.

Scanning Policies

You can edit and customize scanning policies to suit the needs of your organization, reducing the amount of time it takes for Fortify WebInspect to complete a full scan.

Fortify WebInspect also lets you extend the product's capabilities to meet your organization's specific needs. You can configure Fortify WebInspect to adapt to any web application environment and use the custom check wizard to create custom attacks.

Sortable and Customizable Views

When conducting or viewing a scan, the navigation pane on the left side of the Fortify WebInspect window includes the Site, Sequence, Search, and Step Mode buttons, which determine the contents (or "view") presented in the navigation pane. The following are descriptions of the views:

- **Sequence** view displays server resources in the order they were encountered by Fortify WebInspect during an automated scan or a manual crawl (Step Mode).
- **Search** view enables you to locate sessions that fulfill the criteria you specify.
- **Site** view presents the hierarchical file structure of the scanned site.
- **Step Mode** is used to navigate manually through the site, beginning with a session you select from either the site view or the sequence view.

Enterprise-Wide Usage Capabilities

The integrated scan process provides a comprehensive overview of your Web presence from an overall enterprise perspective, enabling you to selectively conduct application scans, either individually or scheduled, of all Web-enabled applications on the network.

API and Web Services Scans

Fortify WebInspect supports scanning GraphQL, gRPC, OData, Postman, Swagger (also known as Open API), and SOAP by way of the API Scan Wizard, `WI.exe`, and the WebInspect REST API.

API Discovery

With API discovery, any Swagger or OpenAPI schema that is detected during a scan will have its endpoints added to the existing scan and authentication will be applied to the endpoints using automatic state detection. In addition, probes will be sent to default locations of popular API frameworks to discover schemas.

Integration Capabilities

You can integrate Fortify WebInspect with some of the most widely-used application security development and testing tools, including the following:

- Burp
- Postman
- Selenium WebDriver

Export Wizard

Fortify WebInspect's configurable XML export tool enables users to export (in a standardized XML format) any and all information found during the scan. This includes comments, hidden fields, JavaScript, cookies, Web forms, URLs, requests, and sessions. Users can specify the type of information to be exported. The Export Wizard also includes a "scrubbing" feature that prevents any sensitive data from being included in the export.

Hacker-level Insights

Fortify WebInspect flags libraries that are detected in the application during the scan. This information provides developers and security professionals with context relating to the overall security posture of their application. While these findings do not necessarily represent a security vulnerability, it is important to note that attackers commonly perform reconnaissance of their target in an attempt to identify known weaknesses or patterns.

If the detected library is open source, the hacker-level insights check includes information from the National Vulnerability Database (NVD). If OpenText™ Debricked access is configured, then Debricked health metrics for open source libraries is also included. For more information on configuring access to the Debricked database, see "Using the WIConfig Program" on page 20

Testing Tools

A robust set of diagnostic and penetration testing tools is packaged with Fortify WebInspect. These include:

- Audit Inputs Editor
- Compliance Manager
- Encoders/Decoders
- HTTP Editor
- Log Viewer
- Policy Manager
- Regular Expression Editor
- Server Analyzer
- SQL Injector
- Traffic Tool
- Web Discovery
- Web Form Editor
- Web Fuzzer
- Event-based Web Macro Recorder
- Session-based Web Macro Recorder
- Web Proxy
- Web Services Test Designer

Related Documents

This topic describes documents that provide information about Fortify software products.

Note: You can find the Fortify Product Documentation at https://www.microfocus.com/support/documentation. Most guides are available in both PDF and HTML formats. Product help is available within the Fortify LIM product and the Fortify WebInspect products.

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Product Documentation website.

Document / File Name	Description
About Fortify Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral DAST

The following document provides information about Fortify ScanCentral DAST. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-ScanCentral-DAST.

Document / File Name	Description
OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide SC_DAST_Guide_<*version*>.pdf	This document provides information about how to configure and use Fortify ScanCentral DAST to conduct dynamic scans of Web applications.
OpenText™ Fortify License and Infrastructure Manager Installation	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM),

Document / File Name	Description
and Usage Guide LIM_Guide_<*version*>.pdf	which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Fortify WebInspect and OAST on Docker User Guide WI_Docker_Guide_<*version*>.pdf	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.

Fortify WebInspect

The following documents provide information about Fortify WebInspect. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
OpenText™ Fortify WebInspect Installation Guide WI_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
OpenText™ Fortify WebInspect User Guide WI_Guide_<*version*>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be

Document / File Name	Description
	formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect and OAST on Docker User Guide WI_Docker_Guide_<*version*>.pdf	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.
OpenText™ Fortify WebInspect Agent Installation and Rulepack Guide WI_Agent_Install_<*version*>.pdf	This document describes how to install the OpenText™ Fortify WebInspect Agent and describes the detection capabilities of the Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect-enterprise.

Document / File Name	Description
OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Fortify Software Security Center and Fortify WebInspect, and troubleshooting the installation. It also describes how to configure the components of the Fortify WebInspect Enterprise system, which include the Fortify WebInspect Enterprise application, database, sensors, and users.
OpenText™ Fortify WebInspect Enterprise User Guide WIE_Guide_<*version*>.pdf	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of Fortify WebInspect sensors to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect Enterprise help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Chapter 2: Installing WebInspect

This chapter contains instructions on installing Fortify WebInspect.

Installation Recommendation

We recommend that you do not install Fortify WebInspect on the same machine as OpenText™ Fortify WebInspect Enterprise. Doing so may result in known issues that affect the usability of the products.

Prerequisites

Before you install Fortify WebInspect, install a supported or recommended version of the following third-party software:

- .NET Framework
- SQL Server or SQL Server Express

For information about the supported versions of these software products and other system requirements, see the *Fortify Software System Requirements*.

SQL Server Database Privileges

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.

About the Installer Files

The following installer files are available for 64-bit operating systems:

- WebInspect64.exe – An executable file that launches an embedded Windows installer file
- WebInspect64.msi – A Windows installer file

Double-clicking any of the installer files launches the Setup Wizard which guides you through the installation. For more information, see "Using the Setup Wizard" on the next page.

Installation Options

You can install Fortify WebInspect using the Setup Wizard or the `msiexec` program. You can use the `WIConfig` program to override Fortify WebInspect configurations after installation.

Tip: You can use a classic Fortify WebInspect installation with the OpenText™ Fortify ScanCentral DAST sensor service. For more information, see the *OpenText™ Fortify ScanCentral DAST Configuration and Usage Guide*.

Using the Setup Wizard

Use the following procedure to install Fortify WebInspect using the Setup Wizard.

Note: After installing Fortify WebInspect, the program will auto launch and require that you license the product before continuing. For information on licensing Fortify WebInspect, see "Licensing with the License Wizard" on page 29.

1. Double-click the .exe or .msi file to start the Setup Wizard.

   The Welcome to the Fortify WebInspect Setup Wizard window appears.
2. Click **Next.**

   The End-User License Agreement window appears.
3. Review the license agreement. If you accept it, select the check box and click **Next**; otherwise click **Cancel**.

   If you accept the license agreement, the Destination Folder window appears.
4. In the Destination Folder window, do one of the following:
   - If you are installing Fortify WebInspect as a sensor for Fortify WebInspect Enterprise, do *not* make any changes to the default Destination Folder. Click **Next**.

     Important! If you are installing Fortify WebInspect as a sensor, you must use the default Destination Folder. Otherwise, SmartUpdates to the sensor will not work. The default Destination Folder is:

     ```
     C:\Program Files\Fortify\Fortify WebInspect
     ```
   - Otherwise, you can accept the default Destination Folder or choose a different folder into which you want to install the software. Click **Next**.

     The Sensor Configuration window appears.
5. Optionally, to install Fortify WebInspect as a sensor:
   a. In the **Configure WebInspect as a Sensor for this installation (optional)** area, select **Configure WebInspect as a Sensor**.
   b. Enter the **Enterprise Manager URL**, that is, the URL of Fortify WebInspect Enterprise manager.

c. In the Sensor Authentication group, enter the following Windows account credentials for this sensor:
   - In the **User Name** box, type the sensor user name.
   - In the **Password** and **Confirm Password** boxes, type the password for the sensor user.

   For important information about installing Fortify WebInspect as a sensor and configuring it to work with Fortify WebInspect Enterprise, see the *OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide*.

6. Click **Next**.

   The Ready to install Fortify WebInspect window appears.

7. Click **Install**.

   When the installation process is complete, the Completed the Fortify WebInspect Setup Wizard window appears.

8. Select **Launch Fortify WebInspect** and click **Finish**.

   The Setup Wizard closes and Fortify WebInspect launches.

Using the msiexec Program

You can install Fortify WebInspect using the `msiexec` program from the command line interface (CLI) or with a script. After installing the product, you can license it from the CLI with the License Utility. For more information, see "Licensing with the License Utility" on page 34.

The following installation methods are supported when installing from the command line interface or with a script:

- Normal Installation
- Reboot Message Suppression
- Silent Mode
- Synchronous Installation

The following paragraphs provide details about these installation methods.

Normal Installation

A normal installation includes a user interface that prompts you to accept or change the default installation options. To run a normal installation, type the following at the command line prompt or in a script:

```
msiexec /I "<directory>:\WebInspect64.msi"
```

Replace <*directory*> with the location where the `WebInspect64.msi` file resides on your machine.

Reboot Message Suppression

If some files that need to be updated are in use during the installation, the installer prompts you that a reboot is required to complete the installation. Using the `msiexec` program, you can suppress these

messages during the installation. To suppress reboot messages, type the following at the command line prompt or in a script:

```
msiexec /I "<directory>:\WebInspect64.msi" REBOOT=Suppress
```

Important! Using this method, the installation completes normally without any messages to reboot. However, if files were in use during the installation and a reboot is required, Fortify WebInspect may not run until you reboot your machine.

Silent Mode

You can suppress the user interface altogether by using the silent mode method. Using this method, all user prompts and messages are suppressed, and the default installation options are used. To use silent mode, type the following at the command line prompt or in a script:

```
msiexec /I "<directory>:\WebInspect64.msi" REBOOT=Suppress /qn
```

Important! There is no way to specify non-default installation options without user interaction. To override the default configurations, use the `WIConfig` program. For information, see "Using the msiexec Program" on the previous page.

Synchronous Installation

Installing Fortify WebInspect from the command line interface or with a script using the commands described above starts the installation as a background task. You can type commands or run other script operations while Fortify WebInspect is installing in the background. If you were to attempt to run the `WIConfig` program immediately after submitting the `msiexec` command, the `WIConfig` program would fail because the Fortify WebInspect installation would not have completed. You can avoid this issue by running a synchronous installation, which means that you cannot further interact with the command prompt or run the next line in a script until the installation is complete.

To run a synchronous installation, type the following at the command line prompt:

```
Start /wait msiexec /I "<directory>:\WebInspect64.msi" REBOOT=Suppress /qn
```

The following sample shows a PowerShell equivalent for a synchronous installation:

```
Start-Process -FilePath 'msiexec.exe' -ArgumentList @('/I', '<directory>:
   \WebInspect64.msi', 'REBOOT=Suppress', '/qn') -Wait
```

Using the WIConfig Program

The `msiexec` program installs Fortify WebInspect, but it does not configure Fortify WebInspect with any non-default configuration settings. You can use the `WIConfig` program after installation to override the default configuration settings.

Important Facts About WIConfig

Keep the following facts in mind when using the `WIConfig` program:

- You must run the `WIConfig` program with administrative privileges.
- Before running commands in the `WIConfig` program, make sure that all instances of `WebInspect.exe` are closed. Otherwise, changes made using `WIConfig` commands will be overridden by the `WebInspect.exe` process that is currently running.
- If one of the parameters fails, the configuration will be left in an unknown state. You must re-run `WIConfig.exe` with a configuration that will succeed to ensure the setup is in a known state.

  For example, if you were to run `WIConfig.exe` using the following options:

  ```
  WIConfig.exe /CreateDatabase /DisableSmartUpdateOnStartup –SqlConnString
  <string>
  ```

  Where you specified a connection string, but the Create Database option failed, you would not know if SmartUpdate on Startup had been disabled.

Syntax

```
WIConfig.exe [/?] [/AcceptUntrustedCerts] [/CreateDatabase]
[-DebrickedAccessToken <string>] [/DisableSmartUpdateOnStartup]
[/EnableAzureDatabaseSupport] [-FipsCompliance <string>]
[-LicenseFile <string>] [/LIMDeactivate] [-LIMPassword <string>] [-LIMPool
<string>] [-LIMUrl <string>] [-RCServerAuthType <string>] [-RCServerHost
<string>] [-RCServerPort <number>] [/RCServerUseHTTPS]
[-SensorID <string>] [-SensorProxyAddress <string>]
[-SensorProxyPassword <string>] [-SensorProxyPort <number>]
[-SensorProxyUsername <string>] [-SensorServicePassword
<string>] [-SensorServiceUsername <string>] [-SensorSqlConnString
<string>] [-SensorSqlConnType <string>] [-SensorWIEPassword <string>]
[-SensorWIEUsername <string>] [-SqlConnString <string>]
[-TwoFAListenerAddress <string>] [-TwoFAListenerPort <number>]
[-WIEUrl <string>] [-WIOASTServerAddress <string>] [-WISECluster <string>]
[-WISEClusterAuthToken <string>] [-WISEClusterMaxPoolSize <number>]
```

Parameters

The following table describes the optional parameters.

Parameter	Description
`-optionsFile`	Specifies file name to use for command line arguments.

Parameter	Description

	Command line arguments take precedence over those specified in the file. An options file is an XML file where each XML element corresponds to a case-insensitive switch name and flags are defined as attributes on the main tag.
	
	Example:
	
	`<options flag1="true" flag2="true">`
	`  <switch1>value</switch1>`
	`  <switch2>value</switch2>`
	`</options>`

`/?`	Displays the help information.
`/AcceptUntrustedCerts`	Accepts untrusted SSL certificates and suppresses warnings. **Caution!** This option can be insecure. Use this option only with self-signed certificates from parties you trust.
`/CreateDatabase`	Creates the database specified by `SqlConnString` if the database does not exist. If the database exists and the schema is correct, this option will have no effect. If the database exists, but the schema is the wrong version, this command will fail.
`-DebrickedAccessToken`	Specifies the Debricked access token to use for retrieving open source client-side library health metrics and correlated GitHub Security Advisory (GHSA) information from the Debricked database. To disable Debricked integration, run this parameter with empty double quotation marks (`""`) to remove the access token and return the configuration to the default state. For example: `WIConfig -DebrickedAccessToken ""`
`/DisableSmartUpdateOnStartup`	Prevents SmartUpdate from running automatically when Fortify WebInspect starts.

Parameter	Description
`/EnableAzureDatabaseSupport`	Enables support for Azure SQL database. For more information, see "Guidelines When Using Azure SQL Database" on page 26. **Tip:** After configuring support for Azure SQL database, you can add the connection to your Fortify WebInspect database configuration in the same way as a remote SQL Server. For more information, see the *OpenText™ Fortify WebInspect User Guide*.
`-FipsCompliance`	Enables/disables FIPS compliance. The value can be one of the following: `{enable|disable}`
`-LicenseFile`	Specifies the path to the OpenText license file.
`/LIMDeactivate`	Deactivates the LIM license.
`-LIMPassword`	Specifies the LIM pool password.
`-LIMPool`	Specifies the LIM pool name.
`-LIMUrl`	Specifies the LIM URL.
`-RCServerAuthType`	Specifies the WebInspect API Server authentication type. The value can be one of the following: `{None|Basic|NTLM|ClientCert}`
`-RCServerHost`	Specifies the hostname the WebInspect API Server should listen on. Use + for all.
`-RCServerPort`	Specifies the WebInspect API Server port to listen on.
`/RCServerUseHTTPS`	Runs the WebInspect API Server over HTTPS.
`-SqlConnString`	Specifies the SQL Server database connection string.
`-TwoFAListenerAddress`	Internal use only.
`-TwoFAListenerPort`	Internal use only.

Parameter	Description
`-WIOASTServerAddress`	Specifies the WebInspect out-of-band application security testing (OAST) server address to configure local DNS service (for use in networks that lack an Internet connection).
`-WISECluster`	Internal use only.
`-WISEClusterAuthToken`	Internal use only.
`-WISEClusterMaxPoolSize`	Internal use only.

Required Parameters to Configure a Sensor

The following table describes the required parameters for configuring Fortify WebInspect as a sensor for Fortify WebInspect Enterprise.

Note: To configure a sensor, you must first install WebInspect to run as a sensor.

Parameter	Description
`-WIEUrl`	Specifies the URL for the WebInspect Enterprise server. Untrusted certificates will be accepted. Example: `-WIEUrl <https://server.domain.com/WIE/>`
`-SensorWIEUsername`	Specifies the domain and user account for the sensor when connecting to the WebInspect Enterprise server. The values must be in the format of *<domain>**<user>*.
`-SensorWIEPassword`	Specifies the password for the sensor when connecting to the WebInspect Enterprise server.

Optional Parameters to Configure a Sensor

The following table describes the optional parameters for configuring Fortify WebInspect as a sensor.

Parameter	Description
`-SensorServiceUsername`	Specifies the user account for the WebInspect Sensor

Parameter	Description
	Windows service. If no user name is provided, `LOCAL SYSTEM` will be used.
`-SensorServicePassword`	Specifies the password for the user account to be used for the WebInspect Sensor Windows service.
`-SensorID`	A GUID that indicates the sensor ID.
`-SensorProxyAddress`	Specifies the proxy address if required to access the WebInspect Enterprise server.
`-SensorProxyPort`	Specifies the proxy port if required to access the WebInspect Enterprise server.
`-SensorProxyUsername`	Specifies the proxy user name if required to access the WebInspect Enterprise server.
`-SensorProxyPassword`	Specifies the proxy password if required to access the WebInspect Enterprise server.
`-SensorSqlConnType`	Specifies the SQL connection type. The value can be one of the following: `{SQLServer|SQLExpress}` If this parameter is not provided, the connection type defined for Fortify WebInspect will be used. If this parameter is defined, validation will occur to ensure the connection.
`-SensorSqlConnString`	Specifies the SQL Server database connection string for the sensor. If none is provided, SQL Express will be used. The connection string must be in the standard format. Example: `Data Source=<server>;Initial Catalog=<database>;Integrated Security=False;User ID=<DB user>;Password=<password>;User Instance=False`

Guidelines When Using Azure SQL Database

Follow these guidelines when using Azure SQL database:

- Fortify WebInspect requires a SQL Server Admin user for database creation. Ensure that this account exists in Azure SQL prior to using the `/EnableAzureDatabaseSupport` parameter.
- External clients connect to Azure SQL database through a gateway with a public IP address. This type of connection results in latency that can significantly affect scan performance. We recommend that you use Azure SQL database only when Fortify WebInspect is installed inside the Azure Infrastructure.

Recommended Process for Configuring Azure SQL Database

We recommend using the following process to configure an Azure SQL database.

Stage	Description
1.	Run the following command only: `wiconfig /EnableAzureDatabaseSupport`
2.	Open Fortify WebInspect.
3.	In Fortify WebInspect, configure the database connection and create a new database. For more information, see the *OpenText™ Fortify WebInspect User Guide*.

Updating Fortify WebInspect

OpenText security engineers uncover new vulnerabilities nearly every day. They develop attack agents to search for these malicious threats, and then update our corporate database so that you will always be on the leading edge of Web application security.

To ensure that you have up-to-date information about the Fortify WebInspect catalog of vulnerabilities, you can use the Smart Update feature of Fortify WebInspect to contact the OpenText knowledgebase server each time you start the application. If vulnerability or program updates are available, Fortify WebInspect informs you and asks if you want to install them.

For complete information about updating Fortify WebInspect, including how to update installations lacking an Internet connection, see the Update SecureBase topic in the *OpenText™ Fortify WebInspect User Guide* or the Fortify WebInspect help.

Directory Structure

The following table describes the directories created and used by Fortify WebInspect, assuming that the main drive is "C" and the user accepts the default directories suggested by the installation program. This information can assist customers and Customer Support in troubleshooting.

Purpose	Path	Comments
Installation Directory	`C:\Program Files\Fortify\Fortify WebInspect` **Note:** If you are updating from an earlier version, the default installation directory is `C:\Program Files\HP\HP WebInspect`	Can be set by the user during installation. SmartUpdate of full Fortify WebInspect version will override everything that exists in this directory. **Important!** When Fortify WebInspect is installed as a sensor for Fortify WebInspect Enterprise, you must use the default Destination Folder. Otherwise, SmartUpdates to the sensor will not work.
	`<Installation Directory>\ComplianceTemplates`	Compliance template directory; can be modified by Smart Update.
	`<Installation Directory>\Samples`	Contains subdirectories for sample scans, and a login macro and a WSDL file for zero.webappsecurity.com.
	`C:\ProgramData\HP\HP WebInspect`	Subdirectories include Policies, Schedule, SecureBase database, Server Analyzer, Settings, and SupportChannel.
	`C:\ProgramData\HP\Licenses\WebInspect`	Licenses activated on the

Purpose	Path	Comments
		local machine.
	`C:\ProgramData\HP\SmartUpdate`	SmartUpdate directory where new patches are downloaded. Security checks are copied and inserted into the database; other artifacts are copied into installation directory (for example, Compliance Template).
Application Data Directory	`%localappdata%\HP` [1]	All data required for Fortify WebInspect that is not user-specific.
User Data Directory	`%localappdata%\HP\HP WebInspect` [1]	All data created by the user and not global for the application. Subdirectories include ComplianceTemplates, Exports, Logs, Plugins, Reporting, ScanData, and Tools.

[1] **%localappdata%** represents the location of local application data for your operating system. For example, for Windows 10 (using the default **C:** drive), **%localappdata%** is **C:\Users\<**username**>\AppData\Local**.

Disclaimer

Certain versions of Fortify WebInspect may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company.

This software was acquired by Micro Focus on September 1, 2017, and is now offered by OpenText, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Chapter 3: Licensing WebInspect

This chapter contains information on the options for activating the product license, including licensing with the License Wizard and licensing with the License Utility. It also includes information about configuring Fortify WebInspect to use a Fortify License Infrastructure Manager (LIM).

Licensing with the License Wizard

The first time you launch Fortify WebInspect, the program displays the License Wizard. The License Wizard prompts you to activate your software.

If you have questions about your licensing, contact the license team for your region.

- North, Central, and South America: mfi-milicensingna@opentext.com
- Europe, the Middle East, and Africa: mfi-milicensingemea@opentext.com
- Asia-Pacific: mfi-licensesapac@opentext.com

Activating Your Software

You can activate Fortify WebInspect in one of the following ways:

- Connecting to an OpenText corporate license server
- Using a license file for offline installations
- Connecting to a License Infrastructure Manager (LIM) server and using a concurrent license

Note: To connect to a LIM, you must first install the LIM on a Windows server or run the LIM Docker image. For more information on the LIM requirements, see the *Fortify Software System Requirements* document. For information on installing and managing concurrent licenses using the LIM, see *OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide*.

To activate Fortify WebInspect:

1. On the Welcome to OpenText Licensing window, click **Activate Now**.

   The wizard displays the Configure WebInspect Licensing window.
2. In the Licensing Method group, choose one of the following:
   - **Connect directly to OpenText corporate license server** - Select this option if licensing is controlled by an OpenText server and the installation is connected to the Internet.
   - **Install License File** - Select this option for an installation that is not connected to the Internet. This option is for offline product activation.

- **Connect to Fortify License and Infrastructure Manager** - Select this option if licensing is controlled by your local server running the LIM software.

3. Click **Next**.

If you chose **Connect directly to OpenText corporate license server**, the License Wizard displays the Named License Activation window. Proceed to "Connect to OpenText" below.

If you chose **Install License File**, the License Wizard displays the License File Activation window. Go to "License File Activation" below.

If you chose **Connect to Fortify License and Infrastructure Manager**, the License Wizard displays the Concurrent License Activation window. Go to "Connect to LIM" on page 32.

Connect to OpenText

1. In the Activation Token area, enter the 32-digit license token sent to you by email from OpenText. Omit any hyphens that may appear in the string (or copy the token, position your cursor in the first block of the **Activation Token** field, and press **Ctrl + V** to paste the token).

   Important! The default Fortify Service URL is https://licenseservice.fortify.microfocus.com/. Change this URL only if directed to do so by Customer Support personnel.

2. If this computer accesses the Internet through a proxy, select the **Network Proxy** option and select a setting from the **Proxy Profile** drop-down list. Click **Edit** and complete the Proxy Profile dialog box as necessary.
   - If you select **Use PAC file** to load proxy settings from a Proxy Automatic Configuration (PAC) file, you must click **Edit**, enter the URL of the PAC file in the **Configure proxy using PAC File URL** field, and click **Save** on the Proxy Profile dialog box.
   - If you select **Use Explicit Proxy Settings**, you must click **Edit**, configure a proxy by entering the requested information for the **Explicitly configure proxy** option, and click **Save** on the Proxy Profile dialog box.
3. Enter the information requested in the User Information group. The information you provide is kept in strict confidence and is not shared with anyone outside of OpenText.
4. Click **Next**.

The Congratulations window appears and Fortify WebInspect is activated.

License File Activation

If your WebInspect is installed on a computer that is not connected to the Internet, select an option for file activation.

If the activation instructions in your welcome email indicate that you must generate a License Request file from within WebInspect to start the process, follow the steps listed under "Fortify Activation" on the next page.

Fortify Activation

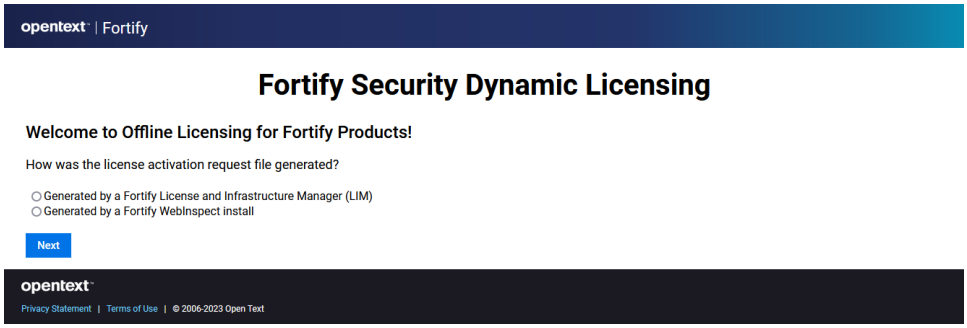
For this option, you must create a license request file containing information about the computer where Fortify WebInspect is installed. Then, using a separate Internet-connected computer, access a web site (https://licenseservice.fortify.microfocus.com/OfflineLicensing.aspx) to transmit the file to a server, which will download a license file that you can copy and install on the computer that is not connected to the Internet.

To activate a license generated by the Fortify license server:

1. Select **Fortify Activation**.
2. In the **Activation Token** field, enter the 32-digit license token sent to you by email from OpenText. Omit any hyphens that may appear in the string (or simply copy the token, position your cursor in the first block of the **Activation Token** field, and press **Ctrl** + **V**).
3. Click **File** to the right of the **License Request File** field.
4. Select a location where the license request file will be saved. The name of the request file is formatted as WebInspectLicenseReq.xml.

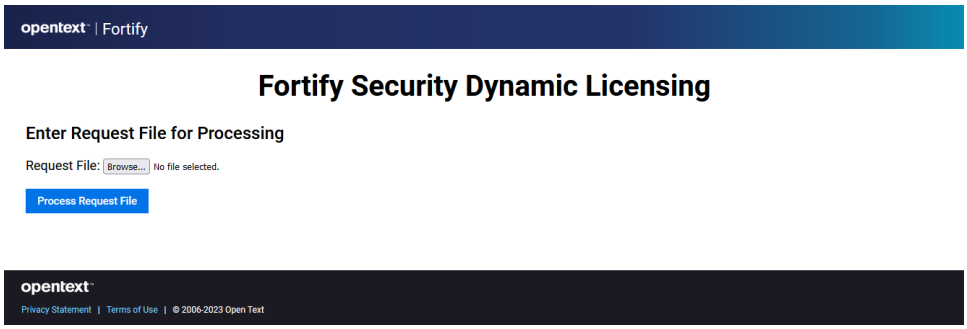
   Tip: Be sure to save this file to a portable device or in a location that is accessible by a machine that has access to the Internet.

5. Click **Save**.
6. On a computer that is connected to the Internet, open a browser and navigate to https://licenseservice.fortify.microfocus.com/OfflineLicensing.aspx.



7. Select the option that describes how the license request file was generated and click **Next**.

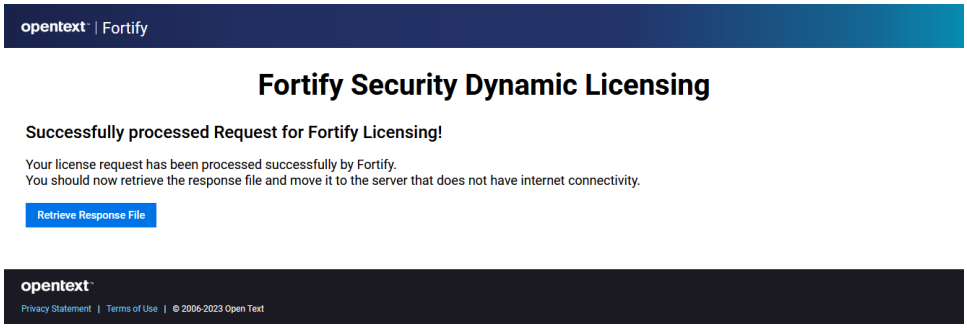
   The Enter Request File for Processing page appears.



8. Click **Browse**, and then locate and select `WebInspectLicenseReq.xml`.

9. Click **Process Request File**.

   If the request is processed successfully, the Successfully processed Request for Fortify Licensing page appears.



10. Click **Retrieve Response File**.
11. In the File Download window, click **Save** and specify the location on the portable device where you want to download the response file `LicenseResp.xml`.
12. Return to the computer where you are installing Fortify WebInspect. Copy the `LicenseResp.xml` file from the portable device to a location on this computer.
13. In the Complete Offline License Activation window, click the **File** button next to the **License Response File** field, and then locate and select the `LicenseResp.xml` file.
14. Click **Next**.

    Information pertaining to your installed license appears in the License Details section.
15. Click **Finish**.

    This completes the licensing procedure.

Connect to LIM

The LIM enables you to manage concurrent licenses for Fortify WebInspect in a manner that best suits your organization's development and testing environment. For example, your company may have Fortify WebInspect software installed on 25 machines, but holds a concurrent license that permits a maximum of 10 instances to be active at any one time. Using the LIM, you can allocate and deallocate those 10 seats in any way you like, without coordinating or negotiating through the OpenText central licensing facility.

Note: Contact your LIM administrator to obtain the information required to complete this procedure.

To configure Fortify WebInspect to use the LIM:

1. In the **URL** field, type the URL of the LIM server in the format `https://<server-url>:<port>`.

   Note: If using a version of the LIM prior to 24.2.0, the format is `https://<server-url>:<port>/<service-directory>` where:

- *server-url* is the site specified during LIM initialization as the root web site.
- *service-directory* is the directory specified during LIM initialization as the Service Virtual Directory name (the default is “LIM.Service” or "LIM.API").

2. Enter the name of the license pool and its password in the **Pool Name** and **Password** fields.
3. If authorization is required to access the LIM, select **Network Authorization** and then enter your user name and password.
4. If this computer accesses the Internet through a proxy:
   a. Select the **Network Proxy** option.
   b. Select a setting from the **Proxy Profile** drop-down list.
   c. Click **Edit** and complete the Proxy Profile dialog box as necessary.
      - If you select **Use PAC file** to load proxy settings from a Proxy Automatic Configuration (PAC) file, you must click **Edit** and enter the URL of the PAC file in the **Configure proxy using PAC File URL** field.
      - If you select **Use Explicit Proxy Settings**, you must click **Edit** and configure a proxy by entering the requested information for the **Explicitly configure proxy** option.
   d. Click **Save** on the Proxy Profile dialog box.
5. Click **Next**.
6. On the Complete on-site License Activation window, select the manner in which you want the License and Infrastructure Manager to handle the license associated with Fortify WebInspect.
   - **Connected License** - The computer can run the product only when the computer is able to contact the LIM. Each time you start the software, the LIM allocates a seat from the license pool to this installation. When you close the software, the seat is released from the computer and allocated back to the pool, allowing another user to consume the license.
   - **Detached License** - The computer can run the product anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only until the expiration date you specify. A detached license enables you to take your laptop to a remote site and run the software. When you reconnect to the corporate intranet, you can access the Application License settings and reconfigure from Detached to Connected.
7. Click **Next**.
   Information pertaining to your installed license appears in the License Details section.
8. Click **Finish**.
   This completes the licensing procedure.

License Revocation

If your Fortify WebInspect license expires, or if your facility is managing licenses through the LIM and the administrator releases your license, you will not be able to conduct or schedule scans.

To regain a license if you use the LIM:

1. In the Fortify WebInspect menu bar, click **Edit > Application Settings**.
2. On the Application Settings window, select **License** from the left pane.
3. Verify your license data.
4. Click **OK**.

If necessary, contact Customer Support or your LIM administrator.

Licensing with the License Utility

If you installed Fortify WebInspect from the command line interface (CLI) or with a script using the `msiexec` program, you can use the `LicenseUtility.exe` application to license your product. The License Utility application is installed in the Fortify WebInspect installation directory. For more information, see "Directory Structure" on page 27.

Syntax for Named Users

Use the following syntax for a named user and an activation token:

```
LicenseUtility.exe [-? | -notrial | -p <product> -token <token> | -
   deactivate | -serviceURL <url>]
```

Syntax for Concurrent Users

Use the following syntax for concurrent users and a Fortify License & Infrastructure Manager (LIM):

```
LicenseUtility.exe [-? | -limURL <limURL> -limPool <limPool> -limPswd
   <password>]
```

Options

The following table describes the options and the type of license to which the option applies.

Option	Description	License Type
`-?`	Displays the usage notes for the License Utility.	Both
`-deactivate`	If used with the `-p` option, deactivates product license and exits using the command line arguments.	Named User
`-limAuth`	Sets network authentication using the format `user:password`. The user can be passed in as	Concurrent User

Option	Description	License Type
	domain\username to support a domain account.	
`-limPacFile`	Configures the proxy using a PAC file URL.	Concurrent User
`-limPool`	Specifies the LIM pool name. If used with the `-p`, `-limURL`, and `-limPswd` options, configures the product to use a LIM for licensing.	Concurrent User
`-limProxy`	Sets an explicit proxy using the format `user:password@host:port` or `user:password@ip:port`. **Tip:** The user can be passed in as `domain\username` to support a domain account.	Concurrent User
`-limPswd`	Specifies the LIM Pool password.	Concurrent User
`-limURL`	Specifies the LIM service URL.	Concurrent User
`-p`	Indicates the Fortify product you are licensing. If used alone, skips the product selection step.	Named User
`-serviceURL`	Specifies the OpenText Fortify License Service URL. **Tip:** This is *not* the URL the LIM administrator uses to access the LIM web interface. This is the URL you selected as the Root Web Site during LIM initialization. The URL is a combination of the website configured in IIS and the limservice in the format `https://<server-url>/<service-directory>`.	Named User
`-silent`	Suppresses all popups and answers 'no' to interactive prompts. See `-y` option for more information.	Both
`-token`	Specifies the Fortify Product Activation Token GUID. If used with the `-p` option, licenses the product and exits using the command line arguments.	Named User
`-topMost`	Places the application as the top window on the desktop.	Both
`-y`	When running in silent mode, answers 'yes' to interactive prompts.	Both

Configuring Fortify WebInspect to use the LIM

You can configure existing (licensed) and new (unlicensed) Fortify WebInspect installations to use the License and Infrastructure Manager (LIM). This section describes how to configure Fortify WebInspect to use the LIM.

For Existing (Licensed) Fortify WebInspect Installations

To configure Fortify WebInspect installations that are already licensed:

1. Start Fortify WebInspect.
2. Click **Edit > Application Settings**.
3. On the Application Settings window, in the **WebInspect** group, select **License**.
4. In the **License Details** group, click **Configure Licensing...**.

   The License Wizard appears.
5. In the **Licensing Method** group, click **Connect to local License and Infrastructure Manager** and click **Next**.
6. In the **URL** field, type the URL of the LIM server in the format `https://<server-url>:<port>`.

   Note: If using a version of the LIM prior to 24.2.0, the format is `https://<server-url>:<port>/<service-directory>` where:

   - *server-url* is the site specified during LIM initialization as the root web site.
   - *service-directory* is the directory specified during LIM initialization as the Service Virtual Directory name (the default is “LIM.Service” or "LIM.API").
7. In the **Pool Name** field, type the pool name from which to extract a license for this instance of Fortify WebInspect.
8. In the **Password** field, type the password that will allow access to the specified license pool.
9. If network authentication is required, select the **Network Authentication** check box, and in the **User Name** and **Password** fields, enter a valid user name and password.
10. Click **Next**.
11. Do one of the following:
    - To allow others to use this license when Fortify WebInspect closes, select **Concurrent License**.
    - To allow Fortify WebInspect to disconnect from the LIM for an extended period of time, select **Detached Lease** and enter an **Expiration Date**.
12. Click **Next**.
13. Click **Finish** and **OK**.

For New (Unlicensed) Fortify WebInspect Installations

To configure new Fortify WebInspect installations:

1. Start Fortify WebInspect.

   The License Wizard appears.
2. Select **Activate Now**.
3. In the **Licensing Method** group, click **Connect to local License and Infrastructure Manager** and click **Next**.
4. In the **URL** field, type the URL of the LIM server in the format `https://<server-url>:<port>`.

   Note: If using a version of the LIM prior to 24.2.0, the format is `https://<server-url>:<port>/<service-directory>` where:

   - *server-url* is the site specified during LIM initialization as the root web site.
   - *service-directory* is the directory specified during LIM initialization as the Service Virtual Directory name (the default is “LIM.Service” or "LIM.API").
5. In the **Pool Name** field, type the pool name from which to extract a license for this instance of Fortify WebInspect.
6. In the **Password** field, type the password that will allow access to the specified license pool.
7. If network authentication is required, select the **Network Authentication** check box, and in the **User Name** and **Password** fields, enter a valid user name and password.
8. Click **Next**.
9. Do one of the following:
   - To allow others to use this license when Fortify WebInspect closes, select **Concurrent License**.
   - To allow Fortify WebInspect to disconnect from the LIM for an extended period of time, select **Detached Lease** and enter an **Expiration Date**.
10. Click **Next**.
11. Click **Finish** and **OK**.

Chapter 4: The WebInspect SDK

The WebInspect Software Development Kit (SDK) is a Visual Studio extension that enables software developers to create an audit extension to test for a specific vulnerability in a session response.

Caution! We recommend that the WebInspect SDK be used only by qualified software developers who have Visual Studio expertise.

For more information about the WebInspect SDK, see the WebInspect Help in Fortify WebInspect or the WebInspect SDK Help which is available in Visual Studio after the SDK installation.

Installation Recommendation

The WebInspect SDK does not need to be installed on the same machine as a Fortify WebInspect product. In most cases, it will be installed on the software developer's development machine. However, if you are developing new extensions that will require debugging, we recommend that you install Fortify WebInspect on the development machine where you will be creating the extension. Doing so will allow you to test your extension locally. For existing extensions that do not require debugging, you do not need to install Fortify WebInspect locally.

For minimum requirements for installing and using the WebInspect SDK, see the *Fortify Software System Requirements*.

Installing the WebInspect SDK

To use the WebInspect SDK, the developer must install a Visual Studio extension file named `WebInspectSDK.vsix`.

During installation of Fortify WebInspect, a copy of the `WebInspectSDK.vsix` file is installed in the Extensions directory in the Fortify WebInspect installation location. The default location is:

```
C:\Program Files\Fortify\Fortify WebInspect\Extensions
```

To install the SDK where Fortify WebInspect is installed on the developer's machine:

1. Navigate to the `Extensions` folder and double click the `WebInspectSDK.vsix` file.
   The VSIX Installer is launched.
2. When prompted, select the Visual Studio product(s) to which you want to install the extension and click **Install**.
   The WebInspect Audit Extension project template is created in Visual Studio. Continue with "Verifying the Installation" on the next page.

To install the SDK where Fortify WebInspect is *not* installed on the developer's machine:

1. Navigate to the `Extensions` folder and copy the `WebInspectSDK.vsix` file to portable media, such as a USB drive.
2. Insert the drive into the development box that has Visual Studio installed, as well as the other required software and hardware.
3. Navigate to the USB drive and double click the `WebInspectSDK.vsix` file.
   The VSIX Installer is launched.
4. When prompted, select the Visual Studio product(s) for which you want to install the extension and click **Install**.
   The WebInspect Audit Extension project template is created in Visual Studio. Continue with "Verifying the Installation" below.

Verifying the Installation

To verify that the extension was successfully installed:

1. In Visual Studio, select **Tools > Extensions and Updates**.
2. Scroll down the list of extensions.
   If you see WebInspect SDK in the list, the extension was installed successfully.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Fortify WebInspect 24.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!