Micro Focus
Fortify WebInspect

Software Version: 18.10
Windows® operating systems

Installation Guide

Document Release Date: June 2018
Software Release Date: June 2018

Legal Notices

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

https://www.microfocus.com

Warranty

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

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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.microfocus.com/support-and-services/documentation

Contents

Preface

Contacting Micro Focus Fortify Customer Support

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

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

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

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

About the Documentation Set

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

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

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
18.10 / June 2018	Added: • Information about product activation when licensing is controlled by a Micro Focus AutoPass License Server (APLS). See "Activate Now" on page 23 and "Activating with an AutoPass License Server" on page 27. **Note:** The APLS content applies only to customers who use an APLS to manage licenses acquired from the Micro Focus entitlement portal and who purchased the APLS-enabled version of WebInspect.
18.10	Added: • Cross-reference for instructions on updating installations lacking an Internet connection. See "Updating Fortify WebInspect" on page 30. Updated: • Installation preparations instructions to include Windows Server 2016. See "Installing IIS, ASP.NET, and .NET Framework" on page 36. • Licensing information with details about AutoPass licenses. See "About Licensing" on page 23. • Minor edits to incorporate branding changes. Removed: • References to 32-bit operating systems. • References to Windows Server 2008 R2 with SP1 and Windows Server 2008 with SP2, which are no longer supported.
17.20	Added: • Notice of the prerequisites that must be installed prior to installing Fortify WebInspect. See "Prerequisites" on page 16. • Description of the available installers. See "About the Installer Files" on

Software Release / Document Version	Changes
	page 16. • Contact information for the regional license teams. See "About Licensing" on page 23. Updated: • Procedure for Installing Fortify WebInspect to standardize terminology and specify how to launch the Setup Wizard. See "Installing Fortify WebInspect" on page 17. • LIM installation troubleshooting information with browser-related issues. See "Troubleshooting the LIM Installation" on page 39. • Procedures for configuring LIM services and virtual directories and for configuring Fortify WebInspect to use the LIM with tips to assist in the configuration. See "Initializing the LIM" on page 37 and "Configuring Fortify WebInspect to use the LIM" on page 43. • Requirement to run as administrator with important information about Global Policy security settings. See "Running as Administrator" on page 16. • Installation procedure and directory structure with important information about using the default installation directory when installing Fortify WebInspect as a sensor for Fortify WebInspect Enterprise. See "Installing Fortify WebInspect" on page 17 and "Directory Structure" on page 31.
17.10	Added: • Details about using the WIConfig program to configure Fortify WebInspect as a sensor for Fortify WebInspect Enterprise. See "Syntax " on page 20, "Required Parameters to Configure a Sensor " on page 21, and "Optional Parameters to Configure a Sensor " on page 22. Updated: • Description of LIM to clarify that it does not generate activation tokens. See "About the License and Infrastructure Manager" on page 35.

Chapter 1: Welcome to Micro Focus Fortify WebInspect

Micro Focus 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.

About the Main Features of Fortify WebInspect

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

About 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.

About Reporting

Use Fortify WebInspect reports to gain valuable, organized application information. You can customize report details, deciding what level of information to contain 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.

About 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.

About 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.

About 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.

About 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 allows 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.

About 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.

About Web Services Scan

Fortify WebInspect can provide a comprehensive scan of your Web services vulnerabilities, allowing you to assess applications containing Web services.

About 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.

About 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
- License Wizard
- Log Viewer
- Policy Manager
- Regular Expression Editor
- Server Analyzer
- SQL Injector
- Support Tool
- SWFScan
- Traffic Tool
- Web Discovery
- Web Form Editor

- Web Macro Recorder (Unified)
- Web Proxy
- Web Services Test Designer

Related Documents

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

Note: You can find the Micro Focus Fortify Product Documentation at https://www.microfocus.com/support-and-services/documentation.

All Products

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

Document / File Name	Description
About Micro Focus Fortify Product Software Documentation About_Fortify_Doc_*<version>*.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. **Note:** This document is included only with the product download.
Micro Focus Fortify Software System Requirements Fortify_Sys_Reqs_*<version>*.pdf Fortify_Sys_Reqs_Help_*<version>*	This document provides the details about the environments and products supported for this version of Fortify Software.
Micro Focus Fortify Software Release Notes FortifySW_RN_*<version>*.txt	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 Micro Focus Fortify Software <version> Fortify_Whats_New_*<version>*.pdf Fortify_Whats_New_Help_*<version>*	This document describes the new features in Fortify Software products.
Micro Focus Fortify Open Source and	This document provides open source and third-party

Document / File Name	Description
Third-Party License Agreements Fortify_OpenSrc_<*version*>.pdf	software license agreements for software components used in Fortify Software.

Micro Focus Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
Micro Focus Fortify WebInspect Installation Guide WI_Install_<*version*>.pdf WI_Install_Help_<*version*>	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
Micro Focus 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 formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
Micro Focus 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.
Micro Focus Fortify WebInspect Runtime Agent Installation Guide WI_RT_Agent_Install_<*version*>.pdf WI_RT_Agent_Install_Help_<*version*>	This document describes how to install the Fortify WebInspect Runtime Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.

Document / File Name	Description
Micro Focus Fortify WebInspect Agent Rulepack Kit Guide WI_Agent_Rulepack_Guide_<*version*>.pdf PDF only; no help file	This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify Runtime 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.

Micro Focus Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website.

Document / File Name	Description
Micro Focus Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf WIE_Install_Help_<*version*>	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.
Micro Focus 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.
Micro Focus Fortify WebInspect	This document describes how to use the Fortify WebInspect

Document / File Name	Description
Tools Guide WI_Tools_Guide_<*version*>.pdf	diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Chapter 2: Getting Started

This chapter contains instructions on installing Micro Focus Fortify WebInspect and activating the product license. It also provides information about the WebInspect Software Development Kit (SDK) and instructions for locating and installing the WebInspect SDK Visual Studio extension file.

Installation Recommendation

Fortify recommends that you do not install Fortify WebInspect on the same machine as Micro Focus Fortify WebInspect Enterprise. Doing so may result in known issues that affect the usability of the products.

Running as Administrator

Fortify WebInspect requires administrative privileges for proper operation of all features. Refer to your Windows operating system documentation for instructions on changing the privilege level to run Fortify WebInspect as an administrator.

Important! Group Policy security settings can override Local security settings. Take this possibility into account when modifying permissions.

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 *Micro Focus Fortify Software System Requirements*.

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" below.

Installing Fortify WebInspect

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

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 "About Licensing" on page 23.

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 Micro Focus Fortify WebInspect Enterprise, do *not* make any changes to the default Destination Folder. Click **Next**.

     Important! If you are installing 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\HP\HP 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. 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 Windows account credentials for this sensor.

For important information about installing Fortify WebInspect as a sensor and configuring it to work with Fortify WebInspect Enterprise, see the *Micro Focus 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 Micro Focus Fortify WebInspect from the command line interface or with a script using the `msiexec` program. 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 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 use it in a script:

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

Replace *<directory>* with the location where the `webinspect.msi` file resides on your machine. To install Fortify WebInspect on a 64-bit operating system, use the `webinspect64.msi` file.

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 use it in a script:

```
msiexec /I "<directory>:\webinspect.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:

```
msiexec /I "<directory>:\webinspect.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 or use it in a script:

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

Using the WIConfig Program

The `msiexec` program installs Micro Focus 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.

Note: You must run the `WIConfig` program with administrative privileges.

Important! 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
/DisableTelemetry –SqlConnString <string>
```

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

Syntax

```
WIConfig.exe /? /AcceptUntrustedCerts /CreateDatabase
/DisableSmartUpdateOnStartup /DisableTelemetry -FipsCompliance <string> -
LicenseFile <string> -LIMPassword <string> -LIMPool <string> -LIMUrl <string>
-RCServerAuthType <string> -RCServerHost <string> -RCServerPort <number>
/RCServerUseHTTPS -SqlConnString <string> -WIEUrl <string> -SensorWIEUsername
<domain>\<user> -SensorWIEPassword <string> -SensorServiceUsername
<domain>\<user> -SensorServicePassword <string> -SensorProxyAddress <string>
-SensorProxyPort <port_number> -SensorProxyUsername <domain>\<user> -
SensorProxyPassword <string> -SensorSqlConnType <SQLExpress or SQLServer> -
SensorSqlConnString Data Source=<SQL Server connection string>
```

Parameters

The following table describes the optional parameters.

Parameter	Description

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

Parameter	Description
/DisableSmartUpdateOnStartup	Prevents SmartUpdate from running automatically when Fortify WebInspect starts.
/DisableTelemetry	Disables Fortify WebInspect Telemetry.
-FipsCompliance	Enables/disables FIPS compliance. The value can be one of the following: {enable|disable}
-LicenseFile	Specifies the path to the Micro Focus license file.
-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.

Required Parameters to Configure a Sensor

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

Parameter	Description
	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 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.
`-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	Description
	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`

About Licensing

The first time you launch Micro Focus Fortify WebInspect, the program displays the License Wizard. The License Wizard prompts you to select one of the following options:

- **Activate Now**: use this option if you have purchased a license or have access to a license through an AutoPass License Server (APLS) or a License Infrastructure Manager (LIM). For more information, see "Activate Now" below.
- **Register 15-day trial**: use this option if you would like to try out Fortify WebInspect for 15 days. After your 15-day trial elapses, you can purchase a license and convert your trial into a fully-licensed version. For more information, see "Register 15-day Trial" on page 29.

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

- North, Central, and South America: mi.licensing-na@microfocus.com
- Europe, the Middle East, and Africa: mi.licensing-emea@microfocus.com
- Asia-Pacific: licensesapac@microfocus.com

Activate Now

Activate Now allows you to activate Fortify WebInspect in one of the following ways:

- Connecting to a Micro Focus corporate license server
- Using a license file for offline installations
- Connecting to an AutoPass License Server (APLS) and using a concurrent (floating) license
- 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. For more information on the LIM requirements, see the *Micro Focus Fortify Software System Requirements* document. For information on installing and managing concurrent licenses using the LIM, see "License Infrastructure Manager" on page 35.

To activate Fortify WebInspect:

1. On the Welcome to Fortify 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 Micro Focus corporate license server** - Select this option if licensing is controlled by a Micro Focus 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 AutoPass License Server** - Select this option if licensing is controlled by your local server running the APLS software.
   - **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 Micro Focus corporate license server**, the License Wizard displays the Named License Activation window. Proceed to "Connect to Micro Focus" below.

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

If you chose **Connect to AutoPass License Server**, the License Wizard displays the APLS License Activation window. Go to "Activating with an AutoPass License Server" on page 27.

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 28.

Connect to Micro Focus

1. In the Activation Token area, enter the 32-digit license token sent to you by email from Micro Focus. 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).
2. The default URLs are as follows:
   - Fortify Service URL– `https://licenseservice.fortify.hpe.com/`
   - AutoPass Service URL– `https://appas-prd-ellb.itcs.softwaregrp.com/`

   Change these URLs only if directed to do so by Fortify Customer Support personnel.

3. 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.
4. 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 Micro Focus.
5. 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" below.

AutoPass Activation

To activate a license generated by AutoPass:

1. Select **AutoPass Activation**.
2. Copy the device codes from the **Device Codes** field.
3. Write down the URL displayed on the UI.
4. Take the device codes and URL to a machine that is connected to the Internet.
5. In a browser, navigate to the URL you wrote down and follow the instructions online to activate your Fortify WebInspect license.

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.hpe.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:

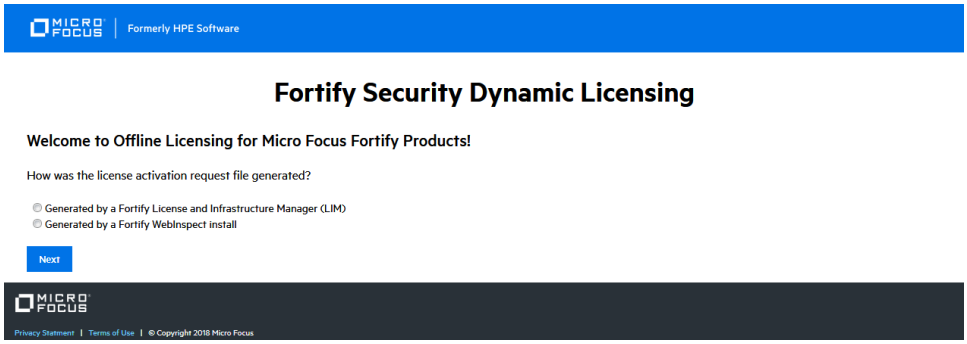
1. Select **Fortify Activation**.
2. In the **Activation Token** field, enter the 32-digit license token sent to you by email from Micro Focus. Omit any hyphens that may appear in the string (or simply copy the token, position your

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.

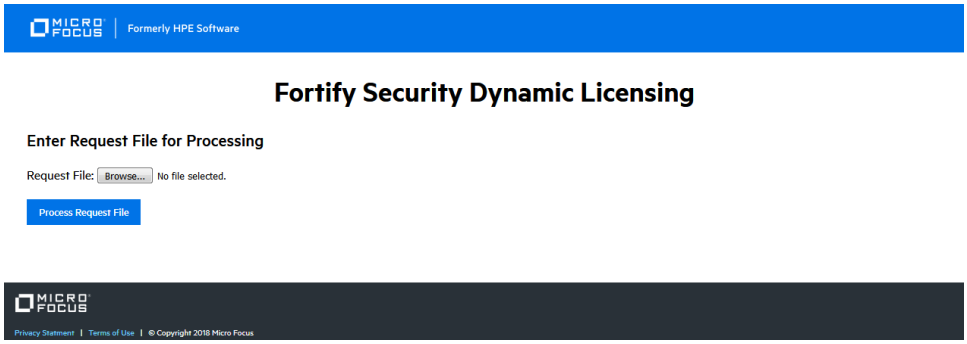
   Tip: Be sure to save this file to a portable device or at a location that is accessible by a machine that has access to the Internet.

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



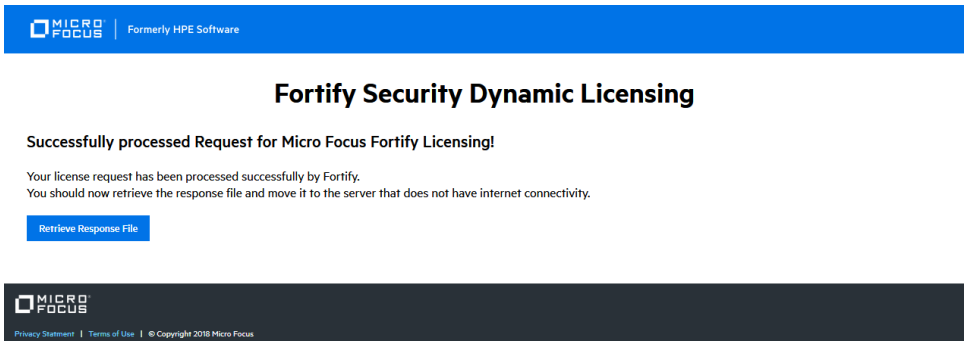
7. Select the option that describes how the license request file was generated and click **Next**.

   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 Micro Focus 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.

Activating with an AutoPass License Server

The AutoPass License Server (APLS) enables you to manage the concurrent (floating) licenses for your software products. A concurrent license is shared dynamically between multiple client users. Using concurrent licenses enables you to purchase the number of licenses equal to the largest number of users likely to be active at any time, instead of the total number of users of a product.

The APLS manages the licenses acquired from the Micro Focus entitlement portal. These licenses are then installed on the APLS. When a client computer needs a license, the client sends a request to the APLS and a license is checked out to this user. After the client user's work session ends (or when the license expires), the license is returned to the APLS for renewal or for use by other users.

For more information, see the *AutoPass License Server User Guide* or help.

Note: Contact your APLS administrator to obtain the information required for configuring Fortify WebInspect to use APLS.

To configure Fortify WebInspect to use APLS:

1. In the **URL** field, enter the URL of the APLS.
2. In the **Username** and **Password** fields, type your user name and password.
3. If connecting to the APLS through a proxy, select **Network Proxy** and choose a setting from the

Proxy Profile list.

- 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.

4. 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 Micro Focus.
5. Click **Next**.

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

   This completes the licensing procedure.

Connect to LIM

The LIM allows 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 Micro Focus's central licensing facility.

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

To configure Fortify WebInspect to use the LIM:

1. In the **URL** field, enter the URL of the License and Infrastructure Manager.
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. This allows 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.

Register 15-day Trial

Use the following procedure to begin a free 15-day trial of Fortify WebInspect.

1. On the Welcome to Fortify Licensing window, click **Register 15 Day Trial**.

   The wizard displays a window prompting you to enter information about you and your company.
2. Enter the requested information.
3. 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.
4. Click **Next**.

   The program attempts to contact Micro Focus servers, which will send an email message to you containing a 32-character activation token.
5. Click **Finish**.
6. When the email arrives, in the Fortify WebInspect menu bar click **Edit > Application Settings**.
7. On the Application Settings window, select **License** from the left pane.
8. Enter the 32-digit license token, omitting 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).

9. Click **OK**.

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 using 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 Fortify Customer Support or your LIM administrator.

Updating Fortify WebInspect

Micro Focus 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 Micro Focus Fortify WebInspect catalog of vulnerabilities, you can use the Smart Update feature of Fortify WebInspect to contact the Micro Focus 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 *Micro Focus Fortify WebInspect User Guide* or the Fortify WebInspect help.

About WebInspect Telemetry

The first time Micro Focus Fortify WebInspect is started, the WebInspect Telemetry window appears. Telemetry provides an automated process for collecting and sending Fortify WebInspect usage information to Fortify, where software developers use this information to help improve the product.

Note: The information collected contains no personally identifiable data.

Configuring Telemetry

Do one of the following:

- To enable telemetry, click **Yes**.

  Use the **Application Settings > Telemetry** page to configure the type of information you want sent to Fortify and other Telemetry settings. Once enabled, the WebInspect Telemetry window will no longer appear upon starting Fortify WebInspect.
- To disable telemetry, click **No**.

  The WebInspect Telemetry window will continue to appear each time Fortify WebInspect is started. To disable the window, select the **Don't show this again** check box.

Directory Structure

The following table describes the directories created and used by Micro Focus 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 Fortify Customer Support in troubleshooting.

Purpose	Path	Comments
Installation Directory	`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 Micro Focus 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

Purpose	Path	Comments
		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 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 (e.g., Compliance Template).
Application Data Directory	`%localappdata%\HP` [1]	All data required for Fortify WebInspect that are 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 7 (using the default **C:** drive), **%localappdata%** is **C:\Users\<**username**>\AppData\Local**.

About 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! Fortify recommends that the WebInspect SDK be used only by qualified software developers who have expertise in developing code using Visual Studio.

For more information about the WebInspect SDK, see the *WebInspect Help* in Micro Focus 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, Fortify recommends 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 *Micro Focus 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 one of the following:

- `C:\Program Files\HP\HP WebInspect\Extensions`
- `C:\Program Files (x86)\HP\HP 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 2013 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" on the next page.

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.

Chapter 3: License Infrastructure Manager

Introduction

This chapter contains information on using an License Infrastructure Manager (LIM) to manage concurrent Micro Focus Fortify WebInspect product licenses.

About the License and Infrastructure Manager

The License and Infrastructure Manager (LIM) allows you to centrally manage your Micro Focus Fortify WebInspect concurrent product licenses. The LIM is required when using concurrent licenses.

The LIM does not generate activation tokens. Micro Focus generates activation tokens that specify the number of licenses purchased. You add your activation token to the LIM database, and then use the LIM to assign and release license seat leases to users.

The LIM uses SmartUpdate to download updates to the software, keeping it up to date.

About Concurrent Licenses

Concurrent licenses allow you to maximize resources by assigning more than one user account to a license. If you have five concurrent licenses, five users can potentially be logged on through the LIM at one time though you have many more than five users with access. A concurrent license enables a one-to-many relationship, allowing you to maximize resources.

Activate Now

When licensing Fortify WebInspect, the Activate Now option allows you to activate Fortify WebInspect by connecting to a Micro Focus corporate license server or by connecting to a LIM server and using a concurrent license. The former option requires an activation token provided by Micro Focus.

The LIM allows you to use concurrent licenses. Concurrent licenses allow multiple instances of Fortify WebInspect to share a single, concurrent license. Only one user can use a concurrent license at a time; if you find users getting locked out, use the LIM to manage your license pool.

To connect to a LIM, you will need to first install the LIM on a Windows server. See the *Micro Focus Fortify Software System Requirements* for the minimum and recommended hardware and software requirements.

Preparing to Install the LIM

Before installing the LIM on your Windows server, you must install and configure Internet Information Services (IIS), ASP.NET, and the Microsoft .NET Framework, if applicable. The following paragraphs provide guidance for installing and configuring these components. Refer to your Windows server documentation for specific details pertaining to your software version.

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

Note: When you select role services to add, some or all of their subordinate role services might be automatically selected as well. Leave any automatic selections as is. If a message appears indicating that other particular role services must also be installed, click the button to add them and they will be automatically selected for installation.

Installing IIS, ASP.NET, and .NET Framework

To install IIS and configure the required features and role services:

1. In the Server Manager, click **Manage** and then **Add Roles and Features**.

   The Add Roles and Features Wizard appears.
2. Follow the wizard to select the installation type and destination server.
3. On the Server Roles window, select the **Web Server (IIS)** check box, if it is not already selected, and click **Next**.
4. On the Features window, select the following:
   - For Windows Server 2012 / 2012 R2, under .NET Framework 4.5 Features, select **.NET Framework 4.5** and **ASP.NET 4.5**.
   - For Windows Server 2016, under .NET Framework 4.6 Features, select **.NET Framework 4.6** and **ASP.NET 4.6**.
5. Click **Next**.

6. On the Role Services window, continue according to the following table:

For...	Then...
Windows Server 2012 / 2012 R2	a. Under Application Development, select **ASP.NET 3.5** (which will subsequently require the dependent role services ISAPI Filters, ISAPI Extensions and .NET Extensibility 3.5) and select **ASP.NET 4.5** (which will subsequently require the dependent role .NET Extensibility 4.5). b. Under Management Tools, select **IIS 6 Management Compatibility**.
Windows Server 2016	a. Under Application Development, select **ASP.NET 4.6**. b. Under Management Tools, select **IIS 6 Management Compatibility**.

7. Click **Install** to install IIS with the features, roles, and role services you selected.

Installing the LIM

The License and Infrastructure Manager (LIM) software is part of the Micro Focus Fortify WebInspect electronic download. The LIM installation file, `LocalLicenseServer64.msi`, is located in the directory where you installed Fortify WebInspect.

To install the LIM:

1. Navigate to the Fortify WebInspect installation directory.
2. Locate and copy the `LocalLicenseServer64.msi` file to the Windows Server where you want to run the LIM.
3. Double-click the `LocalLicenseServer64.msi` file.
4. On the Welcome window, click **Next**.
5. Review the license agreement. If you agree with the terms, select the check box and click **Next**; otherwise, click **Cancel**.
6. Specify the destination folder or accept the default location.
7. Click **Next**.
8. Click **Install** and follow the prompts to complete the installation.
9. Click **Finish** to launch the initialization program.

Initializing the LIM

After installing the software, the License and Infrastructure Manager (LIM) installation program calls the initialization program which adds and configures required services to the Web Application.

To initialize the LIM:

1. On the Welcome screen, click **Next**.

   The Setup Web Service window appears.
2. From the **Root Web Site** list, select the site on which the LIM services will be installed.

   The Web site you select must be running, must have anonymous access enabled during initialization, and must not requires SSL during initialization.

   Tip: Write down the URL you select as the Root Web Site. You must enter this URL when configuring Micro Focus Fortify WebInspect to use the LIM.
3. Specify the names of the virtual directories to be used for the LIM's Web site and Web service.

   Tip: Write down the virtual directory that you specify for the Web service. You must enter this service virtual directory when configuring Fortify WebInspect to use the LIM.
4. (Optional) To associate an SSL certificate with the site, select **Require Secure Channel (SSL)** and select an available certificate (or click **Add** to add a certificate).
5. Click **Next**.

   The Setup LIM Administrator window appears.
6. Type in the requested information and click **Next**.

   Note: The password should contain at least 8 characters and include at least three of the following four character groups:

   - Uppercase characters (A through Z)
   - Lowercase characters (a through z)
   - Numerals (0 through 9)
   - Non-alphabetic characters (such as !, $, #, %)
7. On the Setup Authentication window, if your IIS requires authentication, provide a valid user name and password. Otherwise, select **Use anonymous access**.
8. Click **Next**.
9. If the settings displayed on the Summary window are correct, click **Next**; otherwise, click **Back** and correct the settings.
10. After the initialization program installs Web services, creates a database, and adds the LIM Admin Console shortcut to the desktop, click **Finish** to terminate the program.

Troubleshooting the LIM Installation

The following table provides possible causes and solutions for issues related to the LIM installation and configuration.

Symptom or Error Message	Possible Cause	Possible Solution
The LIM Installer completes but the LIM Initialize Wizard does not appear.	You are not running the executable files with Administrator rights.	Do the following: 1. Navigate to the `Bin` subfolder in the LIM installation directory. 2. Right-click the `LimInitialize.exe` file and select **Run as Administrator**.
The LIM Initialize Wizard displays the following error: "Couldn't read IIS Configuration. Make sure IIS is installed on this machine and permissions to read are allowed."	IIS is not installed on the system.	Install IIS. See "Installing IIS, ASP.NET, and .NET Framework" on page 36.
	The IIS 6 Management Compatibility role is missing.	Add the IIS 6 Management Compatibility role. See "Installing IIS, ASP.NET, and .NET Framework" on page 36.
The LIM Initialize Wizard displays the following error: "Failed to start agent service" **Note:** You can find details of the specific error in the `HP.AppSec.Lim.Agent` log file in the `Logs` subfolder in the LIM installation directory. However, the quickest resolution might be to return to the installation directions ("Preparing to Install the LIM" on	ISAPI and CGI Restrictions settings are not set to **Allowed** at the server level.	In the IIS Manager, open the **ISAPI and CGI Restrictions** feature settings at the server level and ensure that all entries are set to **Allowed**.

Symptom or Error Message	Possible Cause	Possible Solution
page 36) and ensure that you followed all the requisite steps.		

Symptom or Error Message	Possible Cause	Possible Solution
	The Fortify License and Infrastructure Manager application pool is not configured properly.	In the IIS Manager, ensure that the Fortify License and Infrastructure Manager application pool shows **v4.0** as the .NET Framework and **Integrated** as the Managed Pipeline Mode.
	The default timeout of 30 seconds set by the operating system is insufficient.	Modify the registry key at **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control** to increase the value of the **ServicesPipeTimeout** to **180000**. The value is in ms, so this setting allows 3 minutes. If the ServicesPipeTimeout value does not exist in that key, add it to the key as a `DWORD` value.
	The Agent Task Service URL is invalid.	Do the following: 1. Navigate to the `Bin` subfolder in the LIM installation directory. 2. Open the `HP.AppSec.Lim.Agent.exe.config` file. 3. Copy the Agent Task Service URL specified in the **appSettings** section and paste it into a browser. A page listing the AgentTaskService web service endpoints should appear. If browsing to that URL does not render the correct page,

Symptom or Error Message	Possible Cause	Possible Solution
		the LIM Initialize Wizard did not update the URL in the configuration file with the correct pathname or hostname. Edit the file to correct the URL, and then manually start the service named **Fortify License and Infrastructure Manager Agent Service** in the Windows Service Manager.
When logging into the LIM Admin Console your login fails with the following error: "Your login attempt has failed. Please try again or check with your LIM administrator and ensure that the IIS identity for this site has permissions to the Machine Keys folder."	The LIM application pool does not have access to the Machine Keys folder on the machine located at `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys`.	Do one of the following: • Give the built-in IIS_IUSRS group Read permission to the Machine Keys folder. • Change the identity of the Fortify License and Infrastructure Manager application pool to a user with permission to the Machine Keys folder (for example, LocalSystem).
When logging into the LIM Admin Console your login fails with the following error: "Your login attempt has failed. Please try again."	If you previously had access, you forgot your LIM Admin Console credentials. Otherwise, you do not have LIM Admin Console credentials.	Re-run the LIM Initialize Wizard to create a new admin user.
After logging into the LIM, the Admin, License Management, Activity Management, and My Account tabs are not clickable.	Scripting may be disabled in your browser.	Enable scripting in your browser's settings. See your browser documentation for specific instructions.
	Internet Explorer Enhanced Security Configuration may be preventing access to the LIM.	Add the LIM host to the list of trusted sites in Internet Explorer. See your browser documentation for specific

Symptom or Error Message	Possible Cause	Possible Solution
		instructions.

Accessing the LIM Admin Console

To access the LIM Admin Console:

1. Double-click the **Fortify License and Infrastructure Manager Admin Console** shortcut.
2. Type the **Login Name** and **Password** you specified during the LIM initialization.
3. Click **Log In**.

Getting Help

For information about configuring the LIM, see the License and Infrastructure Manager help. To access the help:

- Click **Help** in the footer of any page in the License and Infrastructure Manager Admin Console.

Configuring Fortify WebInspect to use the LIM

You can configure existing (licensed) and new (unlicensed) Micro Focus 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. Type the **URL** of the LIM server in the format `https://<server-url>/<service-directory>`
   where

   server-url is the site you specified during installation as the root Web site.

   service-directory is the directory you specified during installation as the Service Virtual Directory name (the default is "limservice").

   Example:

   `http://<LIMServer_IP_Address>/limservice`

   Tip: This is *not* the URL the LIM administrator uses to access the LIM web interface.
7. Type the **Pool Name** from which a license should be extracted for this instance of Fortify WebInspect.
8. 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 enter a valid **User Name** and **Password**.
10. Click **Next**.
11. Do one of the following:
    - To allow this license to be used by others 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. Type the **URL** of the LIM server in the format `https://<server-url>/<service-directory>`
   where

   server-url is the site you specified during installation as the root Web site.

   service-directory is the directory you specified during installation as the Service Virtual Directory name (the default is "limservice").

Tip: This is *not* the URL the LIM administrator uses to access the LIM web interface.

5. Type the **Pool Name** from which a license should be extracted for this instance of Fortify WebInspect.
6. 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 enter a valid **User Name** and **Password**.
8. Click **Next**.
9. Do one of the following:
   - To allow this license to be used by others 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**.

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 Installation Guide (Fortify WebInspect 18.10)

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 FortifyDocTeam@microfocus.com.

We appreciate your feedback!