Micro Focus
Fortify License and Infrastructure Manager

Software Version: 20.2.0
Windows® operating systems

Installation and Usage Guide

MICRO FOCUS®

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

© Copyright 2009-2020 Micro Focus or one of its affiliates

Trademark Notices

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

Documentation Updates

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

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

This document was produced on January 15, 2021. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

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

About the Documentation Set

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

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

Change Log

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

Software Release / Document Version	Changes
20.2.0 / January 2021	Updated: • LimDirectory default setting to correct error in letter case. See "Configuring the Environment File" on page 25 and "Running the Container" on page 27.

20.2.0	Added:
	
	• Chapter to describe accessing and using the LIM on Docker. See "LIM on Docker" on page 23.
	
	• Description of new server-type license. See "Product Licenses" on page 35.
	
	• Procedures for activating and updating the LIM after installation. See the following topics:
	
	   • "Activating or Updating the LIM" on page 30
	
	   • "Accessing the LIM Admin Console" on page 17
	
	   • "Running the Container" on page 27
	
	Removed:
	
	• References to the SmartUpdate and LIM Updates features.

3.30 / September 2020	Updated: • Tasks for transferring the LIM from one server to another to include copying the existing LIM activation token. See "Backing Up and Restoring the LIM" on page 43.
3.30	Initial release of separate LIM Installation and Usage Guide. Updated: • Procedure for installing IIS to include selecting IIS Management Scripts and Tools. See "Installing IIS, ASP.NET, and .NET Framework" on

Software Release / Document Version	Changes
	page 15.

Chapter 1: About the License and Infrastructure Manager

The Fortify 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.

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 Options for Fortify WebInspect

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. Connecting to a corporate license server 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.

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/documentation. All guides are available in both PDF and HTML formats. Product help is available within the Fortify WebInspect products.

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_Docs_*<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	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>*.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 Micro Focus Fortify Software <version> Fortify_Whats_New_*<version>*.pdf	This document describes the new features in Fortify Software products.

Micro Focus Fortify ScanCentral DAST

The following document provides information about Fortify ScanCentral DAST. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center and https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
Micro Focus 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.

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 at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
Micro Focus 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.
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 on Docker User Guide WI_Docker_Guide_*<version>*.pdf	This document describes how to download, configure, and use Fortify WebInspect that is available as a container image on the Docker platform. This full version of the product 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.
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 License and	This document describes how to install, configure, and

Document / File Name	Description
Infrastructure Manager Installation and Usage Guide LIM_Guide_*<version>*.pdf	use the Fortify WebInspect License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
Micro Focus Fortify WebInspect Agent Installation Guide WI_Agent_Install_*<version>*.pdf	This document describes how to install the Fortify WebInspect 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.
Micro Focus Fortify WebInspect Agent Rulepack Kit Guide WI_Agent_Rulepack_Guide_*<version>*.pdf	This document describes the detection capabilities of 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.

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 at https://www.microfocus.com/documentation/fortify-webinspect-enterprise.

Document / File Name	Description
Micro Focus 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.
Micro Focus Fortify WebInspect Enterprise User Guide	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of Fortify

Document / File Name	Description
WIE_Guide_*<version>*.pdf	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 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: Preparing Windows Server and Installing the LIM

This chapter provides procedures for preparing your Windows server for installation of the LIM, installing and initializing the LIM, and accessing the LIM Admin Console. If you experience issues related to installation and configuration, troubleshooting information is also included.

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 sections 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 following check boxes if they are not already selected:

   - **Web Server (IIS)**

   - **IIS Management Scripts and Tools** (under Management Tools)

4. Click **Next**.

5. On the Features window under .NET Framework 4.6 Features, select **.NET Framework 4.6** and **ASP.NET 4.6**.

6. Click **Next**.

7. On the Role Services window under Application Development, select **ASP.NET 4.6**.
8. Click **Install** to install IIS with the features, roles, and role services you selected.

HTTPS Binding Required

You must configure HTTPS binding in IIS before installing the LIM.

To enable binding:

• In the Edit Site Binding dialog box in IIS, add a host name for the HTTPS binding.

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 require SSL during initialization.

> **Tip:** Write down the URL you select as the Root Web Site. You must enter this URL when configuring Fortify WebInspect to use the LIM. The URL is a combination of the web site configured in IIS and the portion of the LIM that you are configuring, such as the limservice. If you select "Default Web Site" and do not know the URL, you will need to browse your default site in IIS to determine the URL.

3. Specify the names of the virtual directories to use 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 eight 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.

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**.

> **Important!** The first time you access the LIM Admin Console after installation, you must activate or update the LIM on the Fortify License Server. For more information, see "Activating or Updating the LIM" on page 30.

Getting Help

For information about configuring the LIM, see the License and Infrastructure Manager help or refer to the *Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide*. To access the help:

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

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 15.
	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 15.
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`	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
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 page 15) 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

Symptom or Error Message	Possible Cause	Possible Solution
		not render the correct page, 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

Symptom or Error Message	Possible Cause	Possible Solution
		documentation for specific instructions.
The Windows Service fails to start, reporting a service timeout in the LIM logs.	HTTPS bindings may not be configured in IIS.	Enable and configure HTTPS bindings in IIS Site Bindings for the default web site. For more information, refer to your IIS documentation.

Chapter 3: LIM on Docker

Micro Focus engineers have created a Fortify License and Infrastructure Manager (LIM) image that is available for download on the Docker container platform. The image includes the full version of Fortify LIM 20.2.0 software. This chapter provides information about setting up Docker, getting the Fortify LIM Docker image, configuring an environment file, and running the Docker container.

What is Docker?

Docker is a platform that facilitates creating, deploying, and running applications. Developers can package their application and all dependencies, including the platform and all its dependencies, into one logical package called a container or image. You can download a Docker image and run the application contained therein on a virtual machine (VM).

Benefits of Docker

Using a Docker image makes configuring the various prerequisite dependencies unnecessary, and can reduce the time it takes to deploy an instance of the application.

Docker is command-line driven, so it is easy to integrate into build processes, making Docker perfect for automation. As part of an automated build process, you can download a Fortify LIM image from the Docker repository, configure licenses as needed, and then remove the image from your VM.

For more information about Docker, visit https://www.docker.com.

Supported Version

Fortify LIM on Docker runs on Docker Enterprise Edition version 18.09 or later.

Audience

This chapter is intended for users who are familiar with Fortify LIM. Users should also have experience installing, configuring, and using Docker.

Setting Up Docker

Before you can run Docker containers, you must set up Docker according to the process described in the following table.

Stage	Description
1.	Download and install Docker for Windows.
2.	Configure your machine for Docker containers.
3.	Register and start the Docker service.

For information about Docker Engine Enterprise, see https://docs.mirantis.com/docker-enterprise/v3.0/dockeree-products/docker-ee/windows.html.

For additional Docker documentation, see http://docs.docker.oeynet.com/.

Process for Getting and Starting a LIM Docker Image

After setting up Docker, you can download a copy of the Fortify LIM Docker image, configure an environment file, and run the Docker container. The following table describes this process.

Stage	Description
1.	Create a directory on the host machine that is easily identifiable . For example: `d:\lim`
2.	Pull a LIM Docker image to the host machine. For more information, see: • "About the Docker Image" below • "Downloading a Fortify LIM Docker Image" on the next page
3.	To use an SSL Certificate, copy the certificate into the directory you created in Stage 1. **Note:** If you are not using SSL, you can configure the environment file to not use a certificate.
4.	Configure an environment file. For more information, see "Configuring the Environment File" on the next page.
5.	Run the Docker container. For more information, see "Running the Container" on page 27.

About the Docker Image

Images available on the Fortify Docker repository use the following naming convention:

`<repository>/<image>`

For Fortify LIM images, the *<repository>*/*<image>* is `fortifydocker/lim`.

Downloading a Fortify LIM Docker Image

After starting the Docker service, you can download a Fortify LIM image from the Fortify Docker repository.

To download a Fortify LIM image:

- In PowerShell, type the following command:

  ```
  docker pull fortifydocker/lim
  ```

Configuring the Environment File

After you download a Fortify LIM image from the Docker repository, you must configure an environment (`.env`) file that defines how the image will operate. An environment file is a text file that contains variables that provide settings that will be used when the image is run. For more information, see https://docs.docker.com/compose/env-file.

In the environment file, configure the variables as described in the following sections.

Variables to Set

The following table describes the variables that must be set in the environment file. Where applicable, default values are provided. You can override these default values with those that are specific to your installation.

Variable	Description
`LimUseSSL`	Specifies whether the LIM will use an SSL certification. The options are: • `true` – Use an SSL certificate. **Important!** With this setting, you must copy the certificate into the directory you created for the LIM on the host machine. For more information, see "Process for Getting and Starting a LIM Docker Image" on the previous page. • `false` – Do not an SSL certificate.
`LimAdminWebSiteName`	Specifies the name of the LIM web site where you perform administrative tasks. This is the same as the Admin Virtual Directory Name. You will use this name to access the LIM to add product licenses, create and maintain license pools, and manage license-

Variable	Description
	related activities.
	The default setting is `\LimAdmin`.
`LimServiceSiteName`	Specifies the site on which the LIM services will run. This is the same as the Service Virtual Directory Name. This is the site from which Fortify WebInspect will get a license.
	The default setting is `LimService`.
`LimDirectory`	Identifies the client directory in the container. When you run the Docker container, the `-v` option binds the local host directory to this client directory. For more information, see "Understanding the Docker CLI Options" on page 28.
	The default setting is `c:\lim`.
`certpath`	Specifies the directory path to the certificate used for SSL.
`certpassword`	Specifies the password for the SSL certificate.
`LimAdminUsername`	Specifies the LIM administrator user name.
`LimAdminPassword`	Specifies the LIM administrator user password.
`LimAdminEmail`	Identifies the email address to which notifications regarding the LIM administration will be sent.
`LimAdminFriendlyName`	Specifies the full name for the LIM administrator. This name appears rather than the administrator user name in certain places in the LIM user interface.

Sample LIM Environment File

The following is a sample environment file for the Fortify LIM:

```
#!-- LIM Docker env file. --!
LimUseSSL=true
LimAdminWebSiteName=LimAdmin
LimServiceSiteName=LimService
LimDirectory=c:\lim
certpath=c:\lim\limcert.pfx
certpassword=limcert
```

```
LimAdminUsername=limuser
LimAdminPassword=limuser!1
LimAdminEmail=limadmin@limadmin.com
LimAdminFriendlyName=LimAdmin!
```

What's next?

After you have configured and saved your environment file, you can run the image in a container. Go to Running the Container.

Running the Container

This topic provides a sample Docker run command for the Fortify LIM container. The Docker run command uses CLI options that define the container's resources at runtime. To understand how the Docker CLI options used in the samples determine how the container is run, see "Understanding the Docker CLI Options" on the next page.

Sample Docker Run Command

The following example uses Docker CLI options to run the container:

```
docker run -v d:/lim:c:/lim -d -p 80:80 --restart always --env-file
d:\lim\LimDocker.env --memory=8g --cpus=2 --name lim fortifydocker/lim
```

Upon successful execution of the container, an IP address appears in the PowerShell console. Use this IP address to access the Fortify LIM container user interface.

Accessing the Container UI

You can perform administration tasks using the Fortify LIM container.

To access the user interface:

- In a browser, navigate to:

  `https://<IP_Address>/limadmin`
  The *<IP_Address>* is the IP address that appeared in the PowerShell console after the Docker run command executed.

  You must log in using the LIM administrator user name and password you configured in the environment file. For instructions on using the Fortify LIM, see "Using the LIM" on page 30.

  > **Important!** The first time you access the LIM Admin Console after installation, you must activate or update the LIM on the Fortify License Server. For more information, see "Activating or Updating the LIM" on page 30.

Understanding the Docker CLI Options

The following table describes the Docker CLI options used in the Docker run command.

Option	Description
`--cpus`	Specifies the number of CPUs to allocate to the container. Fortify recommends 2 CPUs.
`-d`	Runs the container in the background and displays the container ID.
`--env-file`	Identifies the `.env` file to use. For more information, see "Configuring the Environment File" on page 25.
`-i`	Keeps the standard input (STDIN) stream open for data input. Use this option for diagnostic purposes. **Tip:** You can combine the `-t` and `-i` options to make `-ti`, which creates a pseudo-terminal driver.
`--memory`	Specifies the amount of memory to allocate to the container. Fortify recommends 16 GB.
`--name`	Specifies the container name to be run.
`-p`	Maps a port inside the container to a port on the host system.
`--restart`	Configures the restart policy for the container. Options are: • `no` – Do not automatically restart the container. This is the default option. • `on-failure` – Restart the container if it exits due to an error. • `always` – Always restart the container if it stops. • `unless-stopped` – Always restart the container unless it is manually stopped. **Important!** Fortify recommends that you use `always` as the restart policy for your LIM container.
`-t`	Allocates a pseudo-terminal or pseudo-TTY. Use this option for diagnostic purposes. **Tip:** You can combine the `-t` and `-i` options to make `-ti`, which creates a pseudo-terminal driver.

Option	Description
–v	Maps the volume (or folder) from the container to a folder on the host system. Separate multiple folder names with a colon.

Tip: For more information and a complete list of Docker run options, see
https://docs.docker.com/engine/reference/commandline/run.

Chapter 4: Using the LIM

The Fortify License and Infrastructure Manager (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 WebInspect 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 Micro Focus central licensing facility.

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.

Getting Started

To get started, perform the following tasks:

1. Activate or update the LIM as described in "Activating or Updating the LIM" below.
2. Configure the LIM as described in "Server Configuration" below.
3. Add administrators as described in "Administrative Users" on page 34.
4. Add a product license to the database as described in "Product Licenses" on page 35.
5. Create a license pool, add a license to the pool, and add/delete license pool seats as described in "License Pools" on page 37.

Server Configuration

You can review and configure the following items for the server on the Server Configuration page:

*   Activation (see "Activating or Updating the LIM" below)
*   Proxy (see "Configuring a Proxy Server" on the next page)
*   E-mail (see "Configuring Email Notifications" on page 32)

To access the page, click **ADMIN** > **SERVER CONFIGURATION**.

Activating or Updating the LIM

When you install the LIM and create a new database, you must activate the new installation on the Fortify License Server. When you install the LIM and use an existing database, you must update the application on the Fortify License Server. You can activate or update the LIM on the Server Configuration page.

Activating a New Installation

To activate a new installation:

1. Select **ADMIN** > **SERVER CONFIGURATION** > **Activation**.
2. Click **Activate**.

Updating the Application

To update the application:

1. Select **ADMIN** > **SERVER CONFIGURATION** > **Activation**.
2. Click **Update**.

Activating Offline

If this computer does not have Internet access, clear the check box next to **Server has internet connection**. The screen will repopulate and display instructions for offline activation. For more information, see "Offline Activation" on page 33.

Configuring a Proxy Server

To configure a proxy server:

1. Click **ADMIN** > **SERVER CONFIGURATION**.
2. Select the **Proxy** tab.

3. Select an option as described in the following table.

Option	Description
Direct Connection	Select this option if you are not using a proxy server. Proxy is disabled.
Configure Proxy using a PAC file URL	Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file in the location that you specify in the URL field.
Explicitly configure proxy	Select this option to configure a proxy. Provide the following information: a. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080). b. From the **Type** list, select a protocol type for handling TCP traffic through a proxy server: Socks4, Socks5, or Standard. c. If authentication is required, select an authentication type from the **Authentication** list. d. Type the required credentials in the **User Name** and **Password** fields.

4. Click **OK**.

Configuring Email Notifications

You can receive email notices for a variety of events, such as notification that a license pool has been exhausted.

To review and configure the Simple Mail Transfer Protocol (SMTP) server information for email notification:

1. Click **ADMIN** > **SERVER CONFIGURATION**.
2. Select **E-mail**.
3. Enter the **SMTP Server address** (IP address) and **SMTP Port** (port number) of your e-mail server.
4. Enter your **SMTP Server User ID** and **SMTP Server Password**.
5. For the **SMTP Authentication Type**, select either **None**, **Basic**, or **NTLM**.
6. If the SMTP server requires a secure link, select **SMTP Requires SSL**.
7. Enter an **Email Address to be used as From**. This email address will appear as the originator of the message in the "From" field.
8. Click **OK**.

Offline Activation

Use the following procedure to activate your license if you have installed the License and Infrastructure Manager (LIM) on a computer that is not connected to the Internet.

You will create a file containing information about the computer and the application, and then transfer the file to a portable device (diskette or flash drive) or to a location on your intranet. You will then access that file with an Internet-connected computer and run a program that transmits the file to a Micro Focus server, which will download a license file that you can copy and install on the computer that is not connected to the Internet.

Creating the Request File

1. Click **ADMIN** > **SERVER CONFIGURATION**.
2. Click the **Activation** tab.
3. Clear the **Server has Internet connection** check box.

   The screen will repopulate and display instructions for offline activation.
4. Enter the License Server Activation Token string.
5. (Optional) You can activate other products in addition to the LIM:
   a. Click **Add Product Token**.
   b. On the pop-up dialog, enter the product's activation token and a brief description of the product.
   c. Click **Save**.
   d. Repeat Steps 5a - 5c for additional products.
6. Click **Generate Offline Request** and save the request file to a portable medium or to a location that is accessible by a computer with an Internet connection.

   Note: Do not close the LIM. You will return to this application to complete the process.

Sending the Request to Micro Focus

1. Use a computer with an Internet connection to access the request file.
2. Open an Internet browser and connect to the following URL:

   https://licenseservice.fortify.microfocus.com/OfflineLicensing.aspx
3. Select **Generated by a Fortify License and Infrastructure Manager**.
4. Click **Next**.
5. In the **Request File** box, enter the full path to and name of the request file you created, or click **Browse** to use a standard file-selection window to identify the file.
6. Click **Process Request File**.

7. Click **Retrieve Response File** and save the file to a portable medium or to a location that the LIM can access.

Submitting the Response File to the LIM

1. Return to the LIM.
2. Click **Browse** (next to the **License Response File** box).
3. On the Choose File dialog, select the response file you retrieved from Micro Focus and click **Open**.
4. Click **Activate**.

Administrative Users

The License and Infrastructure Manager (LIM) administrators are authorized to add product licenses, create and maintain license pools, and manage license-related activities.

Adding an Administrator

To add an administrator:

1. Click **ADMIN** > **USERS**.
2. Click **ADD**.
3. Type a **User Name**.
4. Type a **Login Name**.

   > **Note:** This is the name the user will type at the Log In page.

5. Type an **Email Address** for the administrator.
6. To enable the LIM to send email notification of certain events to the administrator, select **Receives Email**.
7. Enter and confirm a **Password**.
8. To send the administrator email notification of the new account, select **Send Welcome Email**.

Editing an Administrator's Account

To edit an administrator's account, including the user's password:

1. Click **ADMIN** > **USERS**.
2. Click **EDIT** next to the user name.
3. Make changes as needed and click **OK**.

Removing an Administrator

To remove a user:

1. Click **ADMIN** > **USERS**.
2. Click **DELETE** next to the user name.
3. Click **OK** to confirm the deletion.

Editing Your LIM Administrator Account

You can modify the following attributes of your License and Infrastructure Manager (LIM) administrator account:

- User Name
- Email Address
- Receive Emails or not
- Password

Note: There are no restrictions on the password.

Editing Your Account

To edit your account:

1. Click **ADMIN** > **USERS**, and then click **EDIT** next to your user name.
2. Make changes as needed.
3. When finished, click **OK**.

Product Licenses

You can view all Micro Focus product licenses currently associated with the License and Infrastructure Manager (LIM) on the Product Licenses page. From this page, you can view product license details or delete the license by clicking the associated button next to the product name. On this page, you can also:

- Add a product license (see "Adding a License" on the next page)
- Add a license pool (see "Adding a License Pool" on the next page)
- Force a license refresh (see "Forcing a License Refresh" on the next page)

Server-type Licenses

Server-type licenses are used to activate certain products, such as components that are used in Fortify ScanCentral DAST environments. You cannot use a server-type license to activate sensors, and you cannot add server-type licenses to license pools.

Adding a License

To add a license to the LIM database:

1. On the Product Licenses page, click **ADD LICENSE**.
2. Enter (type or paste) the **Activation Token** associated with the product license sent to you by Micro Focus.

   > **Note:** The token is a 36-character string formatted as in the following example: 0xx1111e-a5a6-1234-a123-490abcdef801

3. (Optional) Enter a **Description** of the license.
4. Click **OK**.

Adding a License Pool

To create a license pool, click **ADD LICENSE POOL**.

1. Enter the **POOL NAME**.
2. Enter a **POOL DESCRIPTION**.
3. Enter and confirm the **POOL PASSWORD**.

   There are no restrictions on the password.
4. If you want to allow detached licenses, select the **ALLOW DETACHED LEASES** check box.

   A detached lease allows the computer to run WebInspect anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only for the number of days you specify. This allows users to take a laptop to a remote site and run WebInspect. When users reconnect to the corporate intranet, they can access the program's Application License settings and reconfigure from Detached to Connected.
5. If you elect to allow detached leases, in the **DETACHED LEASE DURATION LIMIT** box, enter the number of days that the lease may be detached. Also enter, in the **DETACHED LEASE LIMIT** box, the number of seats that may be assigned a detached lease.
6. Click **OK**.

Forcing a License Refresh

If you renew the concurrent license for your product, you must refresh the license to update the license information in the LIM database.

To refresh your licenses:

- On the Product Licenses page, click **FORCE LICENSE REFRESH** to initiate communication with the Micro Focus global license server.

  The latest information regarding each license in your system is downloaded.

Product License Details

You can view detailed license information on the Product License Detail page. The page also lists the license pool (or pools) to which seats associated with this license have been assigned.

Viewing Product License Details

To view detailed license information:

1. Click **LICENSES > PRODUCT LICENSES**.

   The Product Licenses page appears.

2. Click **DETAILS** for the license you want to view.

   The Product License Detail page appears for the selected product license.

Editing a Pool

To edit pool information or to modify the number of seats currently assigned to a pool:

1. Click **EDIT** next to the pool name.

2. Make changes as needed.

3. When complete, click **OK**.

License Pools

The License Pools page lists all license pools currently defined within the License and Infrastructure Manager (LIM). You can view the license pool details or delete the pool by clicking the associated button next to the pool name.

Note: Deleting a pool does not delete the licenses or the seats assigned to that pool. Those licenses/seats simply become unassigned.

Creating a License Pool

To create a license pool, click **ADD LICENSE POOL**.

1. Enter the **POOL NAME**.

2. Enter a **POOL DESCRIPTION**.

3. Enter and confirm the **POOL PASSWORD**.

   There are no restrictions on the password.

4. If you want to allow detached licenses, select the **ALLOW DETACHED LEASES** check box.

   A detached lease allows the computer to run WebInspect anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only for the number of days you specify. This allows users to take a laptop to a remote site and run WebInspect. When users reconnect to the corporate intranet, they can access the program's Application License settings and reconfigure from Detached to Connected.

5. If you elect to allow detached leases, in the **DETACHED LEASE DURATION LIMIT** box, enter the number of days that the lease may be detached. Also enter, in the **DETACHED LEASE LIMIT** box, the number of seats that may be assigned a detached lease.

6. Click **OK**.

Adding a License to a Pool

To add a license to a pool:

1. Click **DETAILS** next to a pool name.

2. On the Edit License Pool window, click **ADD LICENSE**.

   A pop-up window appears, requesting a license number and a seat count.

3. Select a license from the **LICENSE** list.

4. In the **SEAT COUNT** box, enter the number of seats to be assigned to this pool.

5. Click **OK**.

6. On the Edit License Pool window:

   a. If you want to allow detached licenses, select the **ALLOW DETACHED LEASES** check box.

      A detached lease allows the computer to run the WebInspect software product anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only for the number of days you specify. This allows users to take a laptop to a remote site and run the WebInspect software. When users reconnect to the corporate intranet, they can access the program's Application License settings and reconfigure from Detached to Connected.

   b. If you elect to allow detached leases, in the **DETACHED LEASE DURATION LIMIT** box, enter the number of days that the lease may be detached. Also enter, in the **DETACHED LEASE LIMIT** box, the number of seats that may be assigned a detached lease.

7. Click **OK**.

Editing a License Pool

To add a license to a pool:

1. Click **DETAILS** next to a pool name.

2. On the Edit License Pool window, make changes as needed.

3. When finished, click **OK**.

Modifying Number of Seats for a License

To modify the number of seats assigned to this pool from a specific license:

1. On the Edit License Pool window, click **DETAILS** next to the product name associated with the license.
2. On the pop-up window that appears, select a license from the **LICENSE** list.
3. In the **SEAT COUNT** box, enter the number of seats to be assigned to this pool.
4. Click **OK**.

Current Product Usage

You can view the product seats currently in use on the Current Product Usage page. To access the page, click **ACTIVITY** > **CURRENT PRODUCT USAGE**.

The following table describes the information shown on this page for each product.

Field	Description
PRODUCT	The name of the product
SEATS	The total number of seats available
IN USE	The number of seats in use
# LICENSES	The number of licenses associated with the product

To assure that you are viewing the most recent information available, click **REFRESH**.

Viewing License Details

To view license details for a product (and to add a product license, add a license pool, or force a license refresh), click the associated **LICENSE GUIDS** hyperlink.

Viewing Current Activity for a Product

To view the current activity for a product, click the value in the **IN USE** column.

Current Activity

You can view the current activity involving licenses on the Current Activity page. To access the page, select **ACTIVITY** > **CURRENT ACTIVITY DETAIL**.

Information Displayed

The following table describes the information shown on the Current Activity page about each instance of a product that is currently in use.

Field	Description
USER NAME	The Windows account using the product
MACHINE NAME	The name of the user's workstation machine
PRODUCT	The name of the product
POOL	The license pool containing the seat allocation for the user
ACTIVE SINCE	The date and time when the current instance of the product was started
PROCESS COUNT	The number of products sharing a single lease
CONNECTION MODE	The current status of the machine, either "Detached" or "Connected" to the License and Infrastructure Manager (LIM)
DETACHED EXPIRATION DATE	If detached, the date by which the machine is scheduled to be reconnected to the LIM

Available Actions

Three actions are available on the Current Activity page:

- Releasing a Seat (see "Releasing a Seat" below)
- Revoking a Seat (see "Revoking a Seat" on the next page)
- Releasing All Seats (see "Releasing All Seats" on the next page)

Releasing a Seat

This action applies to connected concurrent licenses. It is used to disconnect a connected LIM client that has a seat lease refreshed through a regular five-minute heartbeat. Release can be performed singlehandedly by the LIM administrator. Once released, the seat becomes available to be leased by another client. The next time it polls the LIM, the client that held the seat receives a notification that it no longer has a license and the application stops working.

To release a seat and return it to a license pool, click the **RELEASE** link associated with that seat.

Revoking a Seat

This action applies to detached leases. Revocation also frees up seats, but because clients with detached seat leases do not poll the LIM, the client cannot be stopped. To revoke a lease, Fortify Customer Support must be involved. The inclusion of support is a control measure designed to discourage concurrent license theft.

To revoke a seat:

1. Contact Fortify Customer Support and identify the lease that needs to be revoked.
2. Click the **REVOKE** link associated with that seat.

> **Note:** Steps 1 and 2 may be reversed.

3. Support logs into the license portal processes the revoke request.
4. Click **REFRESH**.

Releasing All Seats

To release all seats:

- Click **RELEASE ALL LICENSES**.

Lease History

A lease is defined as the period of time during which a product licensed through the License and Infrastructure Manager (LIM) is active. You can view lease history on the Lease History page. To access the page, select **ACTIVITY** > **LEASE HISTORY**.

Information Displayed

The following table describes the information shown on the Lease History page for each lease.

Field	Description
ACQUIRED DATE	The date and time when the product was activated
LICENSE GUID	The license used to activate this instance of the WebInspect software product
USER NAME	The identifier used for authenticating to system services
MACHINE NAME	The name of the computer as it appears on a network

Field	Description
PRODUCT	The WebInspect software product
POOL	The named collection of seats, associated with one or more licenses, to which this application instance is assigned
LEASE LENGTH	The amount of time during which the product is or was in use, formatted as HH:MM:SS, where • HH = hours • MM = minutes • SS = seconds
RELEASE STATUS	The condition under which the product became inactive. Possible values are: • **Released**: A product using a connected concurrent license shut down normally. The seat was returned to the pool; the client is no longer licensed. • **Revoked**: A LIM administrator initiated a revoke on the lease, Fortify Customer Support processed the revoke, and the LIM connected and received the approved revocation. The seat was made available in the pool. The client still has a functioning license because it does not connect to the LIM on a regular basis. • **Expired**: A detached lease reached the end of the user-defined lease period and expired. The seat was returned to the pool. The client is no longer licensed.

Refreshing the Page

To assure that you are viewing the most recent information available:

• Click **REFRESH**.

Data Migration

The following procedure is recommended for installations that currently use Microsoft SQL Server Compact Edition, but would like to use Microsoft SQL Server Enterprise Edition.

1. Open the installed version of the License and Infrastructure Manager (LIM) Admin Console.

2. Return all detached licenses to the LIM.

3. For each license pool, save a record of all licenses and seats assigned to the pool.

4. Detach all licenses from the original database. Be sure to keep a record of each license token before removing it.

5. Deactivate all LIM licenses.

6. Exit the LIM Admin Console.

7. Install the latest version of the LIM and be sure to select Microsoft SQL Server Enterprise Edition during LIM initialization.

> **Note:** If you have already installed a version of the LIM that accommodates Enterprise Edition, simply run the LIM initialization program. The application name is **License and Infrastructure Manager Initialize**.

8. Open the LIM Admin Console.

9. Click **ADMIN** > **SERVER CONFIGURATION** and activate the LIM license.

10. Use the **Proxy** and **E-mail** tabs to add or verify information.

11. Add all licenses.

12. Recreate all pools.

13. Attach licenses to pools.

14. If your previous installation had multiple administrators, click **ADMIN** > **USERS** and define administrator accounts.

Backing Up and Restoring the LIM

Read this document in its entirety before backing up your License and Infrastructure Manager (LIM) investment.

Task 1: Copy the LIM

Make a back-up copy of the LIM database and other files. The easiest back-up process tested by Fortify is to stop the Web server and save the entire LIM directory to a ZIP file. Essential files to restore are:

- `x:\<install-path>\DB\*.*`
- `x:\<install-path>\logs\*.*`

Task 2: Restore the LIM onto Another Server

1. Deactivate the existing LIM installation.

   a. Click **ADMIN** > **SERVER CONFIGURATION**.

   b. On the **Activation** tab, copy the LIM activation token. You will use this token on the new LIM server.

   c. Click **Release**. This releases the LIM token and all of the associated product tokens.

2. Install the LIM on the new server, but do not initialize the application.

3. Restore the LIM database and logs to the new server.

4. Run the initialization. The application name is **License and Infrastructure Manager Initialize**.

Task 3: Activate the Restored Application

1. Log in to the admin console.
2. Click **ADMIN** > **SERVER CONFIGURATION**.
3. On the **Activation** tab, enter the LIM activation token that you copied from the previous server, and then click **Activate**.
4. Was activation successful?
   - If *yes*, go to Task 4.
   - If *no*, contact Fortify Customer Support for assistance.

Task 4: Refresh Product Licenses

1. Click **LICENSES** > **PRODUCT LICENSES**.
2. Click **FORCE LICENSE REFRESH**.

Task 5: Verify License Pools and Tokens

1. View product tokens and execute forced license refresh.
2. View License pools – verify token associations, etc.

Task 6: Configure Clients to Use New Server

For security purposes, client applications configured to use a LIM do not accept responses that redirect the lease request to a new LIM. This action prevents compromise of an organization's legitimately purchased license.

When a LIM has failed, you can use either of two option to ensure that the products can use the LIM replacement.

- Option A: Name the rebuilt LIM exactly the same as its predecessor. This tactic ensures minimal reconfiguration of client products, some of which may be virtualized and used only rarely.
- Option B: Rebuild the LIM with a new name. Then update each installed product configured for concurrent license use to direct requests to the new LIM URL at runtime (i.e., change the locally installed license server URL from the old LIM URL to the new LIM URL).

Alternative Back-Up Strategy

1. Run the LIM on a virtual machine.
2. Back up the virtual machine.
3. Restore the virtual machine on new hardware if the virtual server fails.

The LIM supports virtualized Windows server environments.

LIM Troubleshooting

This section addresses some of the problems or malfunctions that may occur when using the License and Infrastructure Manager (LIM).

Required components not installed

See the *Micro Focus Fortify Software System Requirements* for a list of required modules.

If any module is not installed, the installer will report the problem and terminate. To continue, provide the missing components and restart the installation.

Consult your Windows server documentation for assistance with the following:

- Adding IIS
- Enabling ASP.Net on a Web site
- Enabling/restoring the network services account

LIM installer appears to stop responding

After completing the installation, the Installer program launches the Initializer program. On some systems, the Initializer window opens behind the Installer window and is effectively hidden. The Installation cannot complete until the initialize window has closed.

1. Move the installer window to check for initialize window.
2. Click on initialize to bring to foreground.
3. Complete or cancel initialize.
4. Click **Finish** on install wizard.

LIM initializer appears to stop responding

After completing the installation, the Installer program launches the Initializer program. On systems where the initialize fails to open, error dialogs may also fail to open and be hidden behind other Windows.

1. Move the initialize and installer Windows to check for error dialogs.
2. Note the error message and acknowledge the dialog.
3. Address the cause of error.

Service fails to start at initialize

Always check the logs to determine the reason. Logs are located in *X*:*installdir*\Logs , where *X* is the drive and *installdir* is the directory in which the LIM was installed. The logs are:

- HP.AppSec.Lim.Initialize.log (Initialization log)
- HP.AppSec.Lim.Service.log (Service log)
- HP.AppSec.Lim.Agent.log (Agent log)

Service may fail to start for the following reasons:

Pre-existing Secure Sockets Layer (SSL) and/or Authentication required by the Web site prior to LIM installation and initialization may prevent the LIM Windows service from starting.

1. Using IIS site configuration, modify the Web site:
   a. Remove the SSL required setting.
   b. Enable Anonymous access.
   c. Save the site settings and apply them to all child nodes.
   d. Restart the site.
2. Launch the LIM initializer from the Windows Programs menu (**Start > All Programs > Fortify > License and Infrastructure Manager Initialize**).
3. Rerun the LIM initialize.
   a. Select the SSL certificate from list in initialize.
   b. Set the SSL required bit in initialize.
   c. Complete the initialize workflow.
4. When Initialize is complete, verify that SSL required is set in IIS manager site configuration.
5. Verify that `{drive}:\installpath\Bin\HP.AppSec.Lim.Agent.exe.config` has been updated to require SSL on the three lines specifying URLs:
   - LeaseServiceUrl
   - HP.AppSec.Lim.Agent.Properties.Settings - HP_AppSec_Lim_Agent_AgentTaskService
   - HP.AppSec.Lim.Agent.Properties.Settings - HP_AppSec_Lim_Agent_AgentTaskService_AgentTaskService
6. Verify that the web.config element used by the Menu control and the Help file has been updated to require HTTPS:
   a. On the LIM server, go to the {drive}:\\Installpath\ directory.
   b. Open the web.config file.
   c. Update the line add key="Http Protocol" to change the value from https to http.
7. Using IIS site configuration, modify the website as follows:
   a. Restore the SSL required setting.
   b. Disable Anonymous access.

    c. Save the site settings and apply them to all child nodes.

    d. Restart the site.

8. In Windows Services Management, do the following:

    a. Locate the Fortify License and Infrastructure Manager Agent Service.

    b. Attempt to start the service.

Dependencies removed after installation prevent services from starting or functioning properly.

1. Verify the presence of the dependencies. Consider rerunning the LIM installation program.

2. Install any missing dependencies.

Service originally installed to a directory that no longer exists but is still referenced in original configuration file and registry setting, preventing service from starting (reinstall/reinitialize issue).

1. Open Windows Service Manager: **Start > All Programs > Administrative Tools > Services**.

2. Double-click the **Fortify License and Infrastructure Manager Agent Service** in the list of services.

3. Verify that the path to the executable (HP.AppSec.LIM.Agent.exe) is valid: open the referenced directory and confirm that the file exists.

4. If not valid, consult Windows documentation for instructions on changing the path.

LIM Windows Service does not have permissions to access the site.

This could occur for either of two reasons:

- The site was created and set with authenticated access prior to the LIM installation. The underlying site has been configured with a restrictive set of users and does not allow the LIM Windows service account access.
- The Network Service account was not installed or does not have permissions.

To correct this issue:

1. Verify the existence of the network service account and its activity status.

2. One possible solution is to enable permission to the service account to access the LIM virtual directories or the underlying Web site. Consult your Windows documentation for assistance in adding users or groups to a site .

3. Another possible solution is to update the Windows service to run with an account allowed by the site. This can be an account specifically created to access the LIM site virtual directories and no others. The account will need to be added to the allowed list for the virtual directories.

LIM cannot activate its license (manual process)

This occurs if the LIM fails to connect to the Micro Focus license service.

1. Check your proxy settings. You may need to enter network credentials for the web service to use when connecting to Micro Focus for license activation and recurring license checks.

2. After updating proxy settings, retry license activation.

3. Use the command line to verify that the activation URL resolves to an IP address.

4. Use a browser on the LIM server to visit a public Web site such as Google or Yahoo.

For machines without Internet access, see instructions for offline activation in the LIM help.

LIM receives message during activation that all instances are in use

LIM tokens are issued with a maximum active instance count of 1. This means a single license token GUID cannot be used to activate multiple LIMs. If the token has been used to activate a previous LIM, the token can be deactivated and exchanged, or the active instance can be deactivated allowing reuse of the existing token.

- If the LIM has been reinstalled, contact Fortify Customer Support and ask to have the previous instance deactivated for that specific activation token.

- If the LIM was not reinstalled, contact Fortify Customer Support and inquire about other installations of the LIM for that specific activation token. Discuss deactivation and exchange options with the Support representative.

Error message indicates that the token is not valid for the product

The activation token is a unique string of characters. Mistyping the string will prevent activation. An activation token is unique for a specific product.

Re-enter or paste the LIM token from the original Micro Focus email and resubmit. Make sure there are no trailing spaces.

Use the command line interface to resolve the IP address of the license service URL and verify that the address is correct.

Contact Fortify Customer Support and verify that the license token exists in the license database and is intended for the product being activated. Also verify that the token is configured to be a concurrent license.

LIM cannot activate a concurrently licensed product

There are several possible reasons:

- The LIM manager is unable to connect to the Internet to complete the activation action.
- The license token entered is incorrect.
- The license token was incorrectly created and did not have the concurrent flag enabled.
- The license token was already activated and associated with another LIM.

Use the following procedure to investigate:

1. Verify that the computer hosting the LIM is connected to the Internet.

2. If the network configuration has changed, bring your computer into compliance.

3. If using a proxy that requires a password, make sure you provide the correct password.

4. Re-enter the token included in the original Micro Focus e-mail and resubmit. Make sure there are no trailing spaces.

5. Contact Fortify Customer Support and verify that the license token exists in the license database and is intended for the product being activated. Also verify that the token is configured to be a concurrent license.

LIM does not release expired leases automatically

The LIM Windows service is unable to communicate with the LIM web services.

Verify that the Windows service is running.

1. Launch the LIM and click **LIM** in the menu bar.

   You should see the following message:

   The Fortify License and Infrastructure Manager Agent Service is running.

2. If the Windows service is not running, use **Windows Control Panel > Administrative tools > Services** to locate the LIM service and attempt to start the service.

   Windows service may not be able to connect to LIMservice. Check the service log for entries stating that the Windows service could not connect.

LIM does not refresh licenses automatically

There are several possible reasons:

- The LIM is unable to connect to the Internet to complete the activation action.
- The license token is no longer active or available in the Micro Focus database.
- The Windows service is not executing automated tasks.

Use the following procedure to investigate:

1. Attempt a manual refresh of the licenses.
2. Verify proxy settings.
3. Use a browser on the Windows server running LIM to contact a site on the Internet.
4. See also **LIM does not refresh licenses manually** and **Windows service not executing automated tasks**.

If unsuccessful, contact Fortify Customer Support and verify that the license token exists in the license database and is intended for the product being activated. Also verify that the token is configured to be a concurrent license

LIM does not refresh licenses manually

The LIM may be unable to connect to the Internet to complete the activation action, or the license token has been deactivated on the Micro Focus license server.

The following test requires physical or remote access to the Windows server running the LIM. The LIM uses a web console. A machine that can access the LIM may also be able to access the license service, even if the LIM cannot.

1. Verify that the computer hosting the LIM is connected to the Internet: open a browser and visit a site such as https://software.microfocus.com.

2. If the network configuration has changed, bring your computer into compliance.

3. If using a proxy that requires a password, make sure you provide the correct password.

If unsuccessful, contact Fortify Customer Support and verify that the license token exists in the license database and is intended for the product being activated. Also verify that the token is configured to be a concurrent license.

Windows service not executing automated tasks

Physical or remote desktop access to the LIM server is required for diagnosis and issue resolution. Always check the logs to determine the reason for the issue. Possible reasons include:

- The site was created and set with authenticated access prior to the LIM installation. The underlying site has been configured with a restrictive set of users and does not allow the LIM Windows service account access.

- The site was configured to require SSL after the LIM was installed and initialized.

- The Network Service account is not installed or does not have permissions.

Verify the existence of the network service account and its activity status.

One possible solution is to enable permission to the service account to access the LIM virtual directories or the underlying website. Consult your Windows documentation for assistance in adding users or groups to a site.

Another possible solution is to update the Windows service to run with an account allowed by the site. This can be an account specifically created to access the LIM site virtual directories and no others. The account will need to be added to the allowed list for the virtual directories.

On the machine where the LIM is installed:

1. Open Windows Service Manager: **Start > All Programs > Administrative Tools > Services**.

2. Identify the **Fortify License and Infrastructure Manager Agent Service**.

3. Check the service status.

4. If the service is not running, try to start the service. If it doesn't start, verify that the path to the executable (`HP.AppSec.LIM.Agent.exe`) is valid.

5. Open the referenced directory and confirm that the file exists. If not valid, consult Windows documentation for instructions on changing the path.

6. If the service is running, open the LIM agent and LIM service logs and look for recent entries stating that the service cannot be contacted (scheme incorrect, site not available, access denied, etc). If the site requires SSL, verify that the web-config file specifies the correct protocol (HTTPS and not HTTP):

    a. Verify the `{drive}:\installpath\Bin\HP.AppSec.Lim.Agent.exe.config` has been updated to require SSL on the three lines specifying URLs:

- ○ LeaseServiceUrl
- ○ HP.AppSec.Lim.Agent.Properties.Settings - HP_AppSec_Lim_Agent_AgentTaskService
- ○ HP.AppSec.Lim.Agent.Properties.Settings - HP_AppSec_Lim_Agent_AgentTaskService_AgentTaskService

b. Update the LIM's web.config file to require HTTPS:

    i. On the LIM server, go to the directory where LIM is installed.

    ii. Open the web.config file.

    iii. Update the line add key="Http Protocol" to change "http" to "https" (or reverse).

Help File errors on open – message specifies HTTPS required

During initialization or post-initialization, the LIM administration site was configured to require HTTPS and required changes were not made to the Help file configuration. Simply changing the URL to use https:// from http:// will overcome the problem short term.

For a longer term solution:

1. On the LIM server, go to the directory where LIM is installed.
2. Open the web.config file.
3. Update the line add key="Http Protocol" to change "http" to "https" (or reverse).

Note: On sites where SSL is enabled but not required, the pop-up will always occur with one scheme http or https.

Annoying message bar pops up from IE every time LIM menu is moused over

The menu expects either SSL or non-SSL connectivity, depending upon the site setup. This can be changed by editing the LIMadmin page's web.config. By default the web.config expects an SSL connection for the menu. This typically occurs on sites where SSL was not required and users are connecting to the Admin pages using HTTP.

1. On the LIM server, go to the directory where LIM is installed.
2. Open the web.config file.
3. Update the line add key="Http Protocol" to change "http" to "https" (or reverse).

Note: On sites where SSL is enabled but not required, the popup will always occur with one scheme http or https.

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 and Usage Guide (Fortify License and Infrastructure Manager 20.2.0)

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@microfocus.com.

We appreciate your feedback!