

Fortify License and Infrastructure Manager

Software Version: 23.2.0

Windows® and Linux® operating systems

Installation and Usage Guide

Document Release Date: January 2024

Software Release Date: December 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2009-2024 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks 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 03, 2024. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface	8
Contacting Fortify Customer Support	8
For More Information	8
About the Documentation Set	8
Fortify Product Feature Videos	8
Change Log	9
Chapter 1: About the License and Infrastructure Manager	11
Understanding Concurrent Licenses	11
Understanding License Seats and Leases	11
Understanding Detached Leases	11
Understanding License Pools	12
Sensor Licenses May Be Shared Between Products	12
Related Documents	12
All Products	12
Fortify ScanCentral DAST	13
Fortify Static Code Analyzer	14
Fortify WebInspect	15
Chapter 2: Preparing Windows Server and Installing the LIM	17
Locating the Installation File	17
Preparing to Install the LIM	17
Installing IIS, ASP.NET, and .NET Framework in Server Manager	18
Installing IIS, ASP.NET, and .NET Framework in PowerShell	18
HTTPS Binding Required	18
Installing the LIM	19
Initializing the LIM	19
Accessing the LIM Admin Console	21
Getting Help	21

Troubleshooting the LIM Installation	22
Chapter 3: Using the LIM Docker Images	27
What is Docker?	27
Benefits of Docker	27
Supported Docker Versions	27
Audience	27
Requesting Access	28
Setting Up Docker	28
About the Docker Images	28
Using the Windows Version	28
Process for Getting and Starting a Windows Image	29
Pulling a Windows Image	29
Configuring the Environment File	29
Variables to Set	30
Sample LIM Environment File	32
What's next?	32
Running the Windows Container	32
Sample Docker Run Commands	33
Accessing the Windows Container UI	33
Understanding the Docker CLI Options	33
Using the Linux Version	34
Process for Getting and Starting a Linux Image	35
Editing the Docker Compose File for Linux	35
Unused Optional Environment Variables	35
Understanding the Kestrel Variables	35
Understanding the Database Variable	36
Understanding the Signing Certificate Variables	36
Understanding the JSON Web Token Variables	37
Understanding the Default Administrator Variables	37
Understanding the Proxy Variables	38
Understanding the Miscellaneous Variables	39
Understanding the Licensing URL Variable	39
Running the Linux Container	39
Accessing the Linux Container UI	40
Important Information for Configuring Fortify Products	40

Accessing LIM Log Files on Docker	41
Upgrading LIM on Docker	41
Chapter 4: Using the LIM	43
Getting Started	43
Server Configuration	43
Activating or Updating the LIM	43
Activating a New Installation	44
Updating the Application	44
Activating Offline	44
Configuring a Proxy Server	44
Configuring Email Notifications	45
Offline Activation	46
Creating the Request File	46
Sending the Request to OpenText	46
Submitting the Response File to the LIM	47
Administrative Users	47
Adding an Administrator	47
Editing an Administrator's Account	47
Removing an Administrator	48
Logging Out	48
Editing Your LIM Administrator Account	48
Editing Your Account	48
Product Licenses	49
Server-type Licenses	49
Adding a License	49
Adding a License Pool	49
Forcing a License Refresh	50
Removing a License	50
Product License Details	50
Viewing Product License Details	50
Editing a Pool	51
License Pools	51
Creating a License Pool (Windows Version)	51
Creating a License Pool (Linux Version)	52
Adding a License to a Pool	52

Editing a License Pool	52
Modifying Number of Seats for a License	53
Current Product Usage	53
Viewing License Details	53
Viewing Current Activity for a Product	53
Current Activity	54
Information Displayed	54
Available Actions	55
Releasing a Seat	55
Revoking a Seat	55
Releasing All Seats	55
Lease History	56
Information Displayed	56
Refreshing the Page	57
Data Migration	57
Backing Up and Restoring the LIM	58
Task 1: Copy the LIM	58
Task 2: Restore the LIM onto Another Server	58
Task 3: Activate the Restored Application	58
Task 4: Refresh Product Licenses	59
Task 5: Verify License Pools and Tokens	59
Task 6: Configure Clients to Use New Server	59
Alternative Back-Up Strategy	59
LIM Troubleshooting	59
Required components not installed	59
LIM installer appears to stop responding	60
LIM initializer appears to stop responding	60
Service fails to start at initialize	60
LIM cannot activate its license (manual process)	62
LIM receives message during activation that all instances are in use	62
Error message indicates that the token is not valid for the product	63
LIM cannot activate a concurrently licensed product	63
LIM does not release expired leases automatically	64
LIM does not refresh licenses automatically	64
LIM does not refresh licenses manually	64
Windows service not executing automated tasks	65
Help File errors on open – message specifies HTTPS required	66

Annoying message bar pops up from IE every time LIM menu is moused over66

Send Documentation Feedback67

Preface

Contacting 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/cyberres/application-security>

About the Documentation Set

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

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

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

<https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements>

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	Changes
23.2.0 / January 2024	Updated: <ul style="list-style-type: none">• SmartUpdate URL for Docker compose file. See "Process for Getting and Starting a Linux Image" on page 35 and "Upgrading LIM on Docker" on page 41.• Docker compose file content with information about unused optional environment variables. See "Unused Optional Environment Variables" on page 35.• Tip for accessing the Linux container UI to include the Docker Hostname and Docker Host IP address. See "Accessing the Linux Container UI" on page 40.• URL samples to use when configuring Fortify products to get licenses from the Linux version of LIM. See "Important Information for Configuring Fortify Products" on page 40.
23.2.0	Added: <ul style="list-style-type: none">• Content for Linux version. See "Using the Linux Version" on page 34. Updated: <ul style="list-style-type: none">• Detached lease content to indicate not supported on Linux. See "About the License and Infrastructure Manager" on page 11.• License pool content with procedure for creating a license pool for the Linux version. See "License Pools" on page 51.
23.1.0	Added: <ul style="list-style-type: none">• Environment variable for logs directory in Docker container. See "Configuring the Environment File" on page 29.• Procedure for accessing the log files on Docker. See "Accessing LIM Log Files on Docker" on page 41.

Software Release / Document Version	Changes
	<ul style="list-style-type: none"> • Process for upgrading a LIM Docker container. See "Upgrading LIM on Docker" on page 41.
22.2.0 / December	<p>Updated:</p> <ul style="list-style-type: none"> • Important information about updating the LIM on the Fortify License Server when running the LIM in a container. See "Accessing the Windows Container UI" on page 33.
22.2.0	<p>Updated:</p> <ul style="list-style-type: none"> • Procedure for configuring IIS with .NET Framework 4.8 and ASP.NET 4.8. See "Installing IIS, ASP.NET, and .NET Framework in Server Manager" on page 18. • Docker set up information regarding Docker engine. See "Setting Up Docker" on page 28. • Docker content with details about requesting access to the LIM image. See "Using the Windows Version" on page 28.
22.1.0 / July 11, 2022	<p>Updated:</p> <ul style="list-style-type: none"> • Corrected the URL for accessing the LIM Admin page user interface for the Docker container. See "Accessing the Windows Container UI" on page 33.
22.1.0 / June 21, 2022	<p>Updated:</p> <ul style="list-style-type: none"> • Replaced <code>-ti</code> with <code>-d</code> in the sample Docker run commands. See "Running the Windows Container" on page 32.
22.1.0	<p>Updated:</p> <ul style="list-style-type: none"> • Initializer content to support the LIM API for Fortify ScanCentral DAST and Fortify Webinspect. See "Initializing the LIM" on page 19. • Troubleshooting with "403 access denied" error for LIM Service. See "Troubleshooting the LIM Installation" on page 22.

Chapter 1: About the License and Infrastructure Manager

The OpenText™ Fortify License and Infrastructure Manager (LIM) enables you to centrally manage the concurrent licenses for your OpenText Fortify products. The LIM is required when using concurrent licenses.

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

Understanding Concurrent Licenses

A concurrent license offers flexibility in how the license is used. Multiple instances of a Fortify product or products can share a single, concurrent license. For example, if you have five concurrent licenses, then five users can be licensed through the LIM simultaneously, even though you may have more than five instances of the licensed Fortify product or products installed.

Understanding License Seats and Leases

Each product license has a defined number of seats (or concurrent users). When a Fortify product is configured to use the LIM, it leases a license seat from the LIM upon start up and returns the lease to the LIM when the product is shut down.

Understanding Detached Leases

A detached lease allows a computer to run the Fortify software anywhere, even when disconnected from your corporate intranet (on which the LIM is normally located), but only for the number of days that you specify. This feature allows users to take a laptop to a remote site and run the Fortify software. The lease will remain detached until the detached lease duration limit expires or the user returns the lease.

Note: Detachable leases are an option at time of purchase and may not be available for all licenses. Detachable leases are not supported on the Linux version.

Understanding License Pools

License pools allow you to allocate the license seats in a manner that best meets your organization's needs. For instance, if you have a concurrent license with 10 seats to be shared among two teams, then you can create two license pools and allocate the number of seats to each pool according to the size of the teams or some other attribute of the teams.

Sensor Licenses May Be Shared Between Products

When an OpenText™ Fortify ScanCentral DAST sensor license is activated in the LIM, it can then be used by any of the Fortify products that get licenses from that LIM. For example, if a standard desktop installation of OpenText™ Fortify WebInspect contacts the LIM for a license, and the associated license pool includes a ScanCentral DAST sensor license with an available seat, then that instance of Fortify WebInspect can lease the available seat.

Related Documents

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

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

All Products

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

Document / File Name	Description
<i>About Fortify Software Documentation</i> About_Fortify_Docs_<version>.pdf	This paper provides information about how to access Fortify product documentation. Note: This document is included only with the product download.
<i>Fortify Software System Requirements</i>	This document provides the details about the environments and products supported for this version of

Document / File Name	Description
Fortify_Sys_Reqs_<version>.pdf	Fortify Software.
<i>Fortify Software Release Notes</i> 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.
<i>What's New in Fortify Software</i> <version> Fortify_Whats_New_<version>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral DAST

The following document provides information about Fortify ScanCentral DAST. Unless otherwise noted, this document is available on the Product Documentation website at <https://www.microfocus.com/documentation/fortify-ScanCentral-DAST>.

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

Document / File Name	Description
	OAST vulnerabilities.

Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Product Documentation website at <https://www.microfocus.com/documentation/fortify-static-code>.

Document / File Name	Description
<p><i>OpenText™ Fortify Static Code Analyzer User Guide</i></p> <p>SCA_Guide_<version>.pdf</p>	<p>This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.</p>
<p><i>OpenText™ Fortify Static Code Analyzer Applications and Tools Guide</i></p> <p>SCA_Apps_Tools_<version>.pdf</p>	<p>This document describes how to install Fortify Static Code Analyzer applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with Fortify Static Code Analyzer, review analysis results, work with analysis results files, and more.</p>
<p><i>OpenText™ Fortify Static Code Analyzer Custom Rules Guide</i></p> <p>SCA_Cust_Rules_Guide_<version>.zip</p>	<p>This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: This document is included only with the product download.</p> </div>
<p><i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i></p> <p>LIM_Guide_<version>.pdf</p>	<p>This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.</p>

Fortify WebInspect

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

<https://www.microfocus.com/documentation/fortify-webinspect>.

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

Document / File Name	Description
<i>Usage Guide</i> LIM_Guide_<version>.pdf	(LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
<i>OpenText™ Fortify WebInspect Tools Guide</i> 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.
<i>OpenText™ Fortify WebInspect Agent Installation and Rulepack Guide</i> WI_Agent_Install_<version>.pdf	This document describes how to install the OpenText™ Fortify WebInspect Agent and describes the detection capabilities of the Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Chapter 2: Preparing Windows Server and Installing the LIM

This chapter provides procedures for preparing your Windows server for installation of the License and Infrastructure Manager (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.

Locating the Installation File

The LIM installation file is named `LocalLicenseServer64.msi`.

The following table describes where to find the installation file based on the Fortify product you have purchased.

Product	File Location
Fortify WebInspect	The LIM software is part of the Fortify WebInspect electronic download. The LIM installation file is copied to the directory where you installed Fortify WebInspect.
OpenText™ Fortify Static Code Analyzer	The LIM software is a part of the Fortify Static Code Analyzer electronic download.

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 in Server Manager

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 4.8 Features**, select **.NET Framework 4.8** and **ASP.NET 4.8**.
6. Click **Next**.
7. On the **Role Services** window under **Application Development**, select **ASP.NET 4.8**.
8. Click **Install** to install IIS with the features, roles, and role services you selected.

Installing IIS, ASP.NET, and .NET Framework in PowerShell

Optionally, you can install IIS and configure the required server roles and features in PowerShell.

1. In PowerShell, enter the following command:

```
Install-WindowsFeature Web-server ; Install-WindowsFeature NET-  
Framework-45-ASPNET ; Install-WindowsFeature Web-Asp-Net45  
; Install-WindowsFeature Web-Mgmt-Compat ;
```

2. Download and install .NET Framework 4.8.

After installing .NET Framework 4.8, the appropriate prerequisites are installed.

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

To install the LIM:

1. Locate and copy the LocalLicenseServer64.msi file to the Windows Server where you want to run the LIM. For more information, see ["Locating the Installation File" on page 17](#).
2. Double-click the LocalLicenseServer64.msi file.
3. On the **Welcome** window, click **Next**.
4. Review the license agreement. If you agree with the terms, select the check box and click **Next**; otherwise, click **Cancel**.
5. Specify the destination folder or accept the default location.
6. Click **Next**.
7. Click **Install** and follow the prompts to complete the installation.
8. Click **Finish** to launch the initialization program. Proceed with ["Initializing the LIM" below](#).

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 **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 Web Site. You must use this URL when configuring your Fortify product 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. Accept the default names of the virtual directories (and make note of the defaults) or specify names as follows:
 - In the **Admin Virtual Directory Name** box, type a name to use for the LIM Web site. This is the Web site for the LIM Admin Console application. The default setting is LIM.Admin.
 - In the **Service Virtual Directory Name** box, type a name to use for the LIM Web service. This virtual directory provides support for Fortify ScanCentral DAST and Fortify WebInspect versions earlier than 22.1.0 to connect to the LIM using the SOAP service. The default setting

is LIM.Service.

Note: For product versions 22.1.0 or later, we recommend using the LIM REST API instead of the SOAP service.

Tip: Write down the virtual directory name that you specify for the Web service. You must enter this service virtual directory when configuring Fortify ScanCentral DAST and Fortify WebInspect to use the LIM.

Using the default setting, the URL resembles the following:

```
http://<IP_Address>/LIM.Service
```

```
https://<IP_Address>/LIM.Service
```

- In the **API Virtual Directory Name** box, type a name to use for the LIM REST API. This virtual directory provides support for Fortify ScanCentral DAST, Fortify Static Code Analyzer, and Fortify WebInspect to connect to the LIM using the REST API. The default setting is LIM.API.

Tip: Write down the virtual directory name that you specify for the LIM REST API. You must use this API virtual directory as part of the URL when configuring Fortify ScanCentral DAST, Fortify Static Code Analyzer, and Fortify WebInspect to use the LIM.

Using the default setting, the URL resembles the following:

```
http://<IP_Address>/LIM.API
```

```
https://<IP_Address>/LIM.API
```

4. Click **Next**.
5. (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).
6. Click **Next**.
The Setup LIM Administrator window appears.
7. Continue as follows to create the first LIM Administrator account:
 - a. In the **User Name** box, type a user name. This is the name that will appear as the Login Name in the list of LIM Administrators.
 - b. In the **Full Name** box, type the user's first and last names.
 - c. In the **Password** and **Retype Password** boxes, type a password for the account.

Tip: The password must 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 !, \$, #, %)

- d. In the **Email** box, type the email address for the user.
- e. Click **Next**.

The Setup Authentication window appears.

8. Does your IIS require authentication?
 - If *yes*, select the **Configure user account for windows service access to the web services** option. In the **User Name** box, provide a valid user name. In the **Password** and **Retype Password** boxes, type the corresponding password.
 - If *no*, select **Use anonymous access**.

Note: If you turn off anonymous authentication in the future, you will need to re-run the LIM Initializer to configure a user account for Windows service access to the web services.

9. Click **Next**.
10. If the settings displayed on the Summary window are correct, click **Next**; otherwise, click **Back** and correct the settings.
11. 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 43](#).

Getting Help

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: <ol style="list-style-type: none"> 1. Navigate to the Bin subfolder in the LIM installation directory. 2. Right-click the <code>LimInitialize.exe</code> 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 in Server Manager" on page 18.
The LIM Initialize Wizard displays the following error: “Failed to start agent service”	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 .
<p>Note: You can find details of the specific error in the <code>HP.AppSec.Lim.Agent</code> log file in the Logs subfolder in the LIM installation directory. However, the quickest</p>		

Symptom or Error Message	Possible Cause	Possible Solution
resolution might be to return to the installation directions ("Preparing to Install the LIM" on page 17) and ensure that you followed all the requisite steps.		

Symptom or Error Message	Possible Cause	Possible Solution
	<p>The Fortify License and Infrastructure Manager application pool is not configured properly.</p>	<p>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.</p>
	<p>The default timeout of 30 seconds set by the operating system is insufficient.</p>	<p>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.</p>
	<p>The Agent Task Service URL is invalid.</p>	<p>Do the following:</p> <ol style="list-style-type: none"> 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. <p>A page listing the AgentTaskService web service endpoints should appear.</p> <p>If browsing to that URL does 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</p>

Symptom or Error Message	Possible Cause	Possible Solution
		then manually start the service named Fortify License and Infrastructure Manager Agent Service in the Windows Service Manager.
<p>When logging into the LIM Admin Console your login fails with the following error:</p> <p>“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.”</p>	<p>The LIM application pool does not have access to the Machine Keys folder on the machine located at</p> <p>C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys-</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> • 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).
<p>When logging into the LIM Admin Console your login fails with the following error:</p> <p>“Your login attempt has failed. Please try again.”</p>	<p>If you previously had access, you forgot your LIM Admin Console credentials.</p> <p>Otherwise, you do not have LIM Admin Console credentials.</p>	<p>Re-run the LIM Initialize Wizard to create a new admin user.</p>
<p>After logging into the LIM, the Admin, License Management, Activity Management, and My Account tabs are not clickable.</p>	<p>Scripting may be disabled in your browser.</p>	<p>Enable scripting in your browser's settings. See your browser documentation for specific instructions.</p>
	<p>Internet Explorer Enhanced Security Configuration may be preventing access to the LIM.</p>	<p>Add the LIM host to the list of trusted sites in Internet Explorer. See your browser documentation for specific instructions.</p>
<p>The Windows Service fails to start, reporting a</p>	<p>HTTPS bindings may not be configured in IIS.</p>	<p>Enable and configure HTTPS bindings in IIS Site Bindings for the</p>

Symptom or Error Message	Possible Cause	Possible Solution
<p>service timeout in the LIM logs.</p>		<p>default web site. For more information, refer to your IIS documentation.</p>
<p>After completing the LIM setup, you successfully access the LIM Admin Console in a browser at <code>https://<IP_Address>/LIM.Admin</code> (default URL). You then try to access the LIM Service URL at <code>https://<IP_Address>/LIM.Service</code> (default URL) in the same browser, but receive a "403 - Forbidden: Access is denied" error.</p>	<p>The URL <code>https://<IP_Address>/LIM.Service</code> is not the correct URL for testing whether the LIM Service is properly configured.</p>	<p>To verify correct configuration of the LIM Service, do one of the following:</p> <ul style="list-style-type: none"> • Try to access <code>https://<IP_Address>/LIM.Service/LeaseService.asmx</code> in the browser. • Attempt to connect to the service from a Fortify product, such as Fortify WebInspect, ScanCentral DAST, or Fortify Static Code Analyzer.

Chapter 3: Using the LIM Docker Images

OpenText engineers have created Fortify License and Infrastructure Manager (LIM) images that are available for download on the Docker container platform. Windows and Red Hat image versions are available. The images include the full version of Fortify LIM 23.2.0 software. This chapter provides information about setting up Docker, pulling a Fortify LIM Docker image, configuring environment variables, 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 Docker Versions

Follow Docker recommendations for the Docker engine version to use for Windows and Red Hat Universal Base Image (UBI) 8.x x86_64 host operating systems.

Audience

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

Requesting Access

Access to Fortify LIM on Docker images requires credentials and is granted through your Docker ID. To access Fortify LIM on Docker, email your Docker ID to mfi-fortifydocker@opentext.com.

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 the appropriate Docker version on the host machine. Note: Follow Docker recommendations for the Docker engine version to use for Windows and Red Hat Universal Base Image (UBI) 8.x x86_64 host operating systems.
2.	Configure your machine for Docker containers.
3.	Register and start the Docker service.

About the Docker Images

The Fortify Docker repository uses the following naming convention for the Fortify LIM Windows version image:

```
fortifydocker/lim:<version>
```

The Fortify Docker repository uses the following naming convention for the Fortify LIM Linux version image:

```
fortifydocker/lim:<version.linux_os_version>
```

Using the Windows Version

After starting the Docker service and requesting access to the private Fortify LIM repository on Docker Hub, you can pull a Windows image of Fortify LIM from the Fortify Docker repository.

Process for Getting and Starting a Windows Image

After setting up Docker, you can pull 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: <ul style="list-style-type: none">• "About the Docker Images" on the previous page• "Using the Windows Version" on the previous 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" below .
5.	Run the Docker container. For more information, see "Running the Windows Container" on page 32 .

Pulling a Windows Image

To pull the current Windows version of the Fortify LIM image:

- In PowerShell, type the following command:

```
docker pull fortifydocker/lim:23.2
```

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/environment-variables/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	<p>Specifies whether the LIM will use an SSL certification. The options are:</p> <ul style="list-style-type: none">• true – Use an SSL certificate. <p>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 Windows Image" on the previous page.</p> <ul style="list-style-type: none">• false – Do not an SSL certificate.
LimAdminWebSiteName	<p>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-related activities.</p> <p>An example setting is LIM.Admin.</p>
LimServiceSiteName	<p>Specifies the site on which the LIM services will run. This is the same as the Service Virtual Directory Name. This site provides support for Fortify ScanCentral DAST and Fortify WebInspect versions earlier than 22.1.0 to connect to the LIM using the SOAP service.</p> <p>An example setting is LIM.Service.</p> <p>Note: For product versions 22.1.0 or later, we recommend using the LIM REST API instead of the SOAP service.</p>
LimApiSiteName	<p>Specifies the site on which the LIM REST API will run. This is the same as the API Virtual Directory Name. This site provides support for Fortify ScanCentral DAST, Fortify Static Code Analyzer, and Fortify WebInspect to connect to the LIM using the REST API.</p> <p>An example setting is LIM.API.</p>

Variable	Description
LimDirectory	<p>Identifies the client directory in the container. When you run the Docker container, the <code>-v</code> option binds the local host directory to this client directory. For more information, see "Running the Windows Container" on the next page.</p> <p>An example setting is <code>c:\lim</code>.</p>
certpath	<p>Specifies the directory path to the certificate used for SSL.</p>
certpassword	<p>Specifies the password for the SSL certificate.</p>
LimAdminUsername	<p>Specifies the LIM administrator user name.</p>
LimAdminPassword	<p>Specifies the LIM administrator user password.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Tip: The password must contain at least eight characters and include at least three of the following four character groups:</p> <ul style="list-style-type: none"> Uppercase characters (A through Z) Lowercase characters (a through z) Numerals (0 through 9) Non-alphabetic characters (such as !, \$, #, %) </div>
LimAdminEmail	<p>Identifies the email address to which notifications regarding the LIM administration will be sent.</p>
LimAdminFriendlyName	<p>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.</p>
LimLogsDirectory	<p>Identifies the directory in the container where all logs are written. With this directory mapped to a folder on the host system, you can access the logs locally without stopping the container and extracting the log files. For more information, see "Running the Windows Container" on the next page.</p> <p>An example setting is <code>c:\lim\logs\</code>.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: If this setting is not provided, then logs will be written to the default location in the container, which is:</p> <p><code>c:\Program Files\Fortify\Fortify License and</code></p> </div>

Variable	Description
	<p>Infrastructure Manager\Logs</p> <p>When the default is used, you must use the Docker cp command to copy (or extract) log files from the container. For more information, see "Accessing LIM Log Files on Docker" on page 41.</p>

Sample LIM Environment File

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

```
#!/-- LIM Docker env file. --!  
LimUseSSL=true  
LimAdminWebSiteName=LIM.Admin  
LimServiceSiteName=LIM.Service  
LimApiSiteName=LIM.API  
LimDirectory=c:\lim  
certpath=c:\lim\limcert.pfx  
certpassword=limcert  
LimAdminUsername=limuser  
LimAdminPassword=limuser!1  
LimAdminEmail=limadmin@limadmin.com  
LimAdminFriendlyName=LimAdmin!  
LimLogsDirectory=c:\lim\logs\  

```

What's next?

After you have configured and saved your environment file, you can run the image in a container. Go to ["Running the Windows Container"](#) below.

Running the Windows 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 Commands

The following example uses Docker CLI options to run the container without SSL:

```
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:23.2
```

If the `LimDocker.env` file includes the setting `LimUseSSL=true` and IIS is installed on the host where the Docker container will be running, then the following example runs the container with SSL:

```
docker run -v d:/lim:c:/lim -d -p 8443:443 --restart always --env-file  
d:\lim\LimDocker.env --memory=8g --cpus=2 --name lim fortifydocker/lim:23.2
```

If IIS is *not* installed on the host where the Docker container will be running, then the following example runs the container with SSL:

```
docker run -v d:/lim:c:/lim -d -p 443:443 --restart always --env-file  
d:\lim\LimDocker.env --memory=8g --cpus=2 --name lim fortifydocker/lim:23.2
```

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 Windows 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>:<Port>/LIM.Admin
```

The `<IP_Address>` is the IP address that appeared in the PowerShell console after the Docker run command executed. The LIM Admin page used in the URL must match the

`LimAdminWebSiteName` definition in the environment file for the LIM Docker container. For more information, see ["Configuring the Environment File" on page 29](#).

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 43](#).

Important! The first time you access the LIM Admin Console after installation, you must activate or update the LIM on the Fortify License Server. Additionally, any time a LIM container is shut down and a new one started, you must update the LIM on the Fortify License Server. For more information, see ["Activating or Updating the LIM" on page 43](#).

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. We recommend 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 29 .
--memory	Specifies the amount of memory to allocate to the container. We recommend 16 GB.
--name	Specifies the container name to be run.
-p	Maps a port inside the container to a port on the host system. Tip: Use the following syntax: <code>-p <HostPort>:<ContainerPort></code>
--restart	Configures the restart policy for the container. Options are: <ul style="list-style-type: none">• 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! We recommend that you use <code>always</code> as the restart policy for your LIM container.
-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>.

Using the Linux Version

The Linux image of LIM uses a Docker compose file that contains settings and environment variables that you must edit before running the container. After starting the Docker service and requesting

access to the private Fortify LIM repository on Docker Hub, you can download and edit the Docker compose file for running a Linux image of Fortify LIM.

Process for Getting and Starting a Linux Image

After setting up Docker, you can configure the settings and environment variables in the Docker compose file and run the Docker container. The following table describes this process.

Stage	Description
1.	Download the LIM Docker compose file from the SmartUpdate server at the following URL: https://smartupdate.fortify.microfocus.com/documents/lim/23.2/docker-compose.yml The file is downloaded to the default download directory on your machine. The file name is <code>docker-compose.yml</code> .
2.	Configure the environment variables in the Docker compose file. For more information, see "Editing the Docker Compose File for Linux" below .
3.	Create a LIM directory on the host machine and copy the Docker compose file to the directory.
4.	Optionally, if you are using SSL, create a certificates directory in the LIM directory and place the SSL certificates in the directory.
5.	Run the Docker container. For more information, see "Running the Linux Container" on page 39 .

Editing the Docker Compose File for Linux

You must edit the environment variables in the Docker compose file with settings that are specific for your environment.

The environment variables are enclosed in double quotation marks and expressed as follows:

```
"<Env_Variable>=<Setting>"
```

Unused Optional Environment Variables

If you do not need to specify an optional variable for your environment, comment out the variable line by placing a number sign (#) at the start of the line or delete the line altogether.

Understanding the Kestrel Variables

The following table describes the ASP.NET Core Kestrel web server environment variables.

Variable	Description
ASPNETCORE_Kestrel__Certificates__Default__Path	Optional setting that specifies the path to the Kestrel certificate on the Docker host machine when using SSL in the container. The path must match the mapped volume.
ASPNETCORE_Kestrel__Certificates__Default__Password	If the Kestrel certificate requires a password, specifies the certificate password to use SSL in the container.
ASPNETCORE_URLS	Required setting that assigns ports for the HTTP and HTTPS protocols. Configure the ports as a semicolon-separated list using the following format: "ASPNETCORE_URLS=https://+:443;http://+:80"

Understanding the Database Variable

The following table describes the LIM database environment variable.

Variable	Description
ConnectionStrings__LimDb	Optional setting that specifies the connection string for connecting to your LIM database. If not specified in the Docker compose file, the container defaults to: Data Source=.\database\Lim.db.

Understanding the Signing Certificate Variables

The following table describes the signing certificate environment variables.

Variable	Description
Signing__CertificatePath	Optional setting that specifies a customer-supplied signing certificate, preferably a PFX file. Important! The signing certificate must contain a public/private key pair. If a certificate is not supplied, the LIM will create a self-signed certificate.
Signing__CertificatePassword	Optional setting that specifies the password for the customer-supplied signing certificate or for the LIM-created self-signed certificate.

Understanding the JSON Web Token Variables

The following table describes the JSON Web Token (JWT) environment variables.

Variable	Description
JWT__ValidAudience	Required setting that is used to validate the audience specified inside the access token. A sample setting is: "JWT__ValidAudience=FortifyLimAuthAudience"
JWT__ValidIssuer	Required setting that is used to validate the issuer of the token. A sample setting is: "JWT__ValidIssuer=FortifyLimAuthIssuer"
JWT__SecurityKey	Required setting that specifies the secret key for JWT authentication. A sample setting is: "JWT__SecurityKey=aS116IUxmbf9X6PCVpmkG8vraq1pPFU9"
JWT__ExpirationMinutes	Optional setting that specifies the expiration time in minutes for the token. If not included, the setting defaults to 5 minutes. A sample setting is: "JWT__ExpirationMinutes=10"
JWT__RefreshTokenExpirationMinutes	Optional setting that specifies the expiration time in minutes for the refresh token. If not included, the setting defaults to 60 minutes. A sample setting is: "JWT__RefreshTokenExpirationMinutes=120"

Understanding the Default Administrator Variables

The following table describes the default administrator environment variables.

Variable	Description
DefaultAdministrator__Login	Required setting for a new LIM environment, but optional when updating an existing LIM. This is the user name that will appear as the Login Name in the list of LIM Administrators. This variable creates the default administrator's account

Variable	Description
	for a new LIM environment. If the account already exists, and you provide credentials, the account will be updated with the new credentials.
DefaultAdministrator__FullName	If DefaultAdministrator__Login is configured, this required setting specifies the display name for the user.
DefaultAdministrator__Password	<p>If DefaultAdministrator__Login is configured, this required setting specifies the password for the default administrator's account.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p>Tip: The password must contain at least eight characters and include at least three of the following four character groups:</p> <ul style="list-style-type: none"> • Uppercase characters (A through Z) • Lowercase characters (a through z) • Numerals (0 through 9) • Non-alphabetic characters (such as !, \$, #, %) </div>
DefaultAdministrator__Email	If DefaultAdministrator__Login is configured, this required setting specifies the email address for the default administrator's account.

Understanding the Proxy Variables

The following table describes the proxy environment variables.

Variable	Description
Proxy__Mode	<p>Optional setting for configuring a proxy. Possible values are:</p> <ul style="list-style-type: none"> • None = 0 • AutoDetect = 1 • Manual = 2 <p>The default setting is 0.</p>
Proxy__Address	If Proxy__Mode=2, specifies the URL or IP address of your proxy server.

Variable	Description
Proxy__Port	If Proxy__Mode=2, specifies the port number.
Proxy__UserName	If Proxy__Mode=2 and your proxy server requires authentication, specifies the qualifying user name.
Proxy__Password	If Proxy__Mode=2 and your proxy server requires authentication, specifies the qualifying password.

Understanding the Miscellaneous Variables

The following table describes the miscellaneous environment variables.

Variable	Description
AllowNonTrustedServerCertificate	Optional setting that specifies whether the LIM can accept self-signed (untrusted) certificates when communicating with other Fortify products. Options are true or false.
AllowedHosts	Optional setting that identifies the hosts that are allowed to access the LIM Admin console.

Understanding the Licensing URL Variable

The following table describes the licensing URL environment variable.

Variable	Description
FortifyLicensingUrl	Indicates the URL for the licensing service. The default URL is: https://licenseservice.fortify.microfocus.com/

Running the Linux Container

After you have edited the environment variables in the Docker compose file, you can use the file to pull the Linux image from Docker Hub and start the container.

To pull the image and start the container:

- At the terminal prompt on the Linux Docker host machine, enter the following commands:

```
cd LIM
docker compose up -d
```

Important! If you are using SSL and the LIM cannot access the SSL certificates, then the application will stop and you will find the following error in the log file:

```
Stopped program because of exception System.IO.FileNotFoundException:  
  Could not find file '/app/certificates/cert.pfx'.
```

To correct this error, stop the LIM with the `docker compose down` command, copy the certificates into the directory specified in the error, and restart the LIM.

Accessing the Linux Container UI

You can perform administration tasks using the Fortify LIM container.

Tip: You may use the Docker Host hostname, Docker Host IP address, or the Linux container IP address and port number to access the container UI. To find the IP address of the container, use the following interface configuration command:

```
ifconfig -a
```

The command displays all the interfaces that are available on the machine.

To access the user interface:

- In a browser, navigate to:

```
https://<Docker_Hostname>:<Port>/login
```

OR

```
https://<IP_Address>:<Port>/login
```

Note: The previous samples use the https protocol. If SSL certificates are not used, the protocol is http.

You must log in using the LIM administrator user name and password you configured in the Docker compose file. For instructions on using the Fortify LIM, see ["Using the LIM" on page 43](#).

Important! The first time you access the LIM Admin Console after installation, you must activate or update the LIM on the Fortify License Server. Additionally, any time a LIM container is shut down and a new one started, you must update the LIM on the Fortify License Server. For more information, see ["Activating or Updating the LIM" on page 43](#).

Important Information for Configuring Fortify Products

When configuring a Fortify product to use the Linux version of LIM for licensing, the product must connect to the LIM using the Docker Host hostname, Docker Host IP address, or the Linux container IP address and port number:

```
https://<Docker_Hostname>:<Port>
```

```
https://<IP_Address>:<Port>
```


Note: The previous samples use the https protocol. If SSL certificates are not used, the protocol is http.

Accessing LIM Log Files on Docker

If you used the `LimLogsDirectory` setting in the LIM environment file, then you can access the logs in the directory you specified without stopping the container and extracting the log files. For more information, see ["Configuring the Environment File" on page 29](#).

Otherwise, you must use the Docker `cp` command to copy (or extract) log files from the default location in the container.

To copy the log files from the default location:

1. In PowerShell on the Docker host, enter the following command:

```
docker stop lim  
The LIM container stops.
```

2. Enter the following command to copy the log files:

```
docker cp lim:'C:\Program Files\Fortify\Fortify License and Infrastructure  
Manager\Logs' <Drive>:\<Directory>  
The LIM logs are copied to the directory you specify in the command.
```

Upgrading LIM on Docker

When upgrading a LIM Docker container to version 23.2, you must delete the existing LIM container before starting a new one. Otherwise, a naming conflict may occur, resulting in the inability to authenticate the upgraded container. This topic describes the process for properly upgrading a LIM Docker container.

Important! If the previous version of the LIM container used different values in the environment file, such as `LimServiceSiteName` rather than `LimApiSiteName`, you must update the values in the environment file.

Upgrade a LIM Docker container according to the process described in the following table.

Stage	Description
1.	Do one of the following: <ul style="list-style-type: none">• For Windows, download the new Docker image. For more information, see "Using the Windows Version" on page 28.• For Linux:<ol style="list-style-type: none">a. Download the LIM Docker compose file from the SmartUpdate server at the

Stage	Description
	<p>following URL:</p> <p>https://smartupdate.fortify.microfocus.com/documents/lim/23.2/docker-compose.yml</p> <p>b. Configure the environment variables in the file. For more information, see "Editing the Docker Compose File for Linux" on page 35.</p>
2.	<p>Delete the existing container:</p> <ul style="list-style-type: none">• In a PowerShell console on the Windows host, enter the following command: <pre>docker stop lim docker container rm -f lim</pre>• At the terminal prompt on the Linux host machine, enter the following commands: <pre>docker compose down docker rm lim</pre> <p>Important! Do not simply stop the existing container. You must delete the existing container before starting the new container.</p>
3.	<p>Start the new container:</p> <ul style="list-style-type: none">• For Windows, use the Docker run command with the 23.2 tag to start the new LIM container. For more information, see "Running the Windows Container" on page 32.• For Linux, use the <code>docker compose up</code> command to pull the image and start the container. For more information, see "Running the Linux Container" on page 39.
4.	<p>After starting the new container, update the LIM as follows:</p> <ol style="list-style-type: none">a. Access the container UI and log in using LIM administrator credentials. For more information, see "Accessing the Windows Container UI" on page 33 or "Accessing the Linux Container UI" on page 40.b. Select ADMIN > SERVER CONFIGURATION > Activation.c. Click Update. <p>The LIM does not provide confirmation of the update. However, the Server Configuration page refreshes.</p> <p>Important! Updating the LIM is required if you are upgrading to a new version or creating a new container with the same version. Anytime you delete a container and create a new one, you must click the Update button.</p>

Chapter 4: Using the LIM

This chapter provides instructions for getting started, such as activating or updating the Fortify License and Infrastructure Manager (LIM) installation, configuring the server, adding administrators, adding product licenses, and creating and managing license pools.

It also includes procedures for routine tasks such as viewing product license details, current product usage and activity details, and lease histories.

Information regarding data migration, backing up and restoring the LIM, and troubleshooting the LIM is also included.

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 47](#).
4. Add a product license to the database as described in ["Product Licenses" on page 49](#).
5. Create a license pool, add a license to the pool, and add/delete license pool seats as described in ["License Pools" on page 51](#).

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 45](#))

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

Activating or Updating the LIM

When you install the License and Infrastructure Manager (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 46.

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: <ol style="list-style-type: none">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).From the Type list, select a protocol type for handling TCP traffic through a proxy server: Socks4, Socks5, or Standard.If authentication is required, select an authentication type from the Authentication list.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 OpenText 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 OpenText

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 OpenText 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.

Logging Out

To log out from the LIM Admin Console:

- Click the user icon () and then select **Logout**.

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.
The EDIT MY ACCOUNT page opens.

Tip: You can click the user icon () and then select **Edit My Account** to access this page.

2. Make changes as needed.
3. When finished, click **OK**.

Product Licenses

You can view all OpenText 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 and perform the following tasks:

- Add a product license (see ["Adding a License" below](#))
- Add a license pool (see ["Adding a License Pool" below](#))
- Force a license refresh (see ["Forcing a License Refresh" on the next page](#))
- Remove a license (see ["Removing a License" 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 OpenText.

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:

1. Click **ADD LICENSE POOL**.
2. Enter the **POOL NAME**.
3. Enter a **POOL DESCRIPTION**.
4. Enter and confirm the **POOL PASSWORD**.
There are no restrictions on the password.
5. (Optional) To allow detached licenses, select the **ALLOW DETACHED LEASES** check box and continue as follows:

- a. In the **DETACHED LEASE DURATION LIMIT** box, enter the number of days that the lease may be detached. The maximum number of days allowed is 30.
 - b. In the **DETACHED LEASE LIMIT** box, enter 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 OpenText global license server.

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

Removing a License

A concurrent license can be associated with only one LIM at a time. To use a concurrent license with a different LIM, you must first remove it from the original LIM database. Otherwise, the license will remain attached to the original LIM and cannot be used in another LIM.

To remove a license from the LIM database:

1. On the **PRODUCT LICENSES** page, click **REMOVE** for the license that you want to remove.
A confirmation message appears.
2. Click **OK**.
The license is removed from the LIM database. You can now add the license to a different LIM.
3. Repeat Steps 1 and 2 for each license to remove.

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 (Windows Version)

To create a license pool:

1. Click **ADD LICENSE POOL**.
2. Enter the **POOL NAME**.
3. Enter a **POOL DESCRIPTION**.
4. Enter and confirm the **POOL PASSWORD**.
There are no restrictions on the password.
5. (Optional) To allow detached licenses, select the **ALLOW DETACHED LEASES** check box and continue as follows:
 - a. In the **DETACHED LEASE DURATION LIMIT** box, enter the number of days that the lease may be detached. The maximum number of days allowed is 30.
 - b. In the **DETACHED LEASE LIMIT** box, enter the number of seats that may be assigned a detached lease.
6. Click **OK**.

Creating a License Pool (Linux Version)

To create a license pool:

1. Click **+ LICENSE POOL**.

The License Pool Configuration wizard opens to the LICENSE POOL DETAILS page.

2. Configure the license pool details as follows:

- a. Enter the **Pool Name**.
- b. Enter a **Pool Description**.
- c. Enter and confirm the **Pool Password**.

There are no restrictions on the password.

3. Click **NEXT**.

The Product License Select page opens.

4. Configure the product licenses as follows:

- a. In the **PRODUCT LICENSES** list, select one or more product licenses to add to the pool.

Tip: To add licenses for all products, select the **Product** check box in the list heading.

- b. In the **SELECTED PRODUCT LICENSES** list, select from the **Assigned Seats** drop-down list the number of seats for each product to assign to the pool.

5. Click **SAVE**.

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, 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 product license, which may be any of the following: <ul style="list-style-type: none">• Fortify ScanCentral DAST (a server-type license)• Fortify WebInspect• Fortify Scanning Machine (which licenses Fortify WebInspect and Fortify Static Code Analyzer)• Fortify SCA (Static Code Analyzer)
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 product license, which may be any of the following: <ul style="list-style-type: none">• Fortify ScanCentral DAST (a server-type license)• Fortify WebInspect• Fortify Scanning Machine (which licenses Fortify WebInspect and Fortify Static Code Analyzer)• Fortify SCA (Static Code Analyzer)
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" below](#))
- Releasing All Seats (see ["Releasing All Seats" below](#))

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 Fortify 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
PRODUCT	The product license, which may be any of the following: <ul style="list-style-type: none">• Fortify ScanCentral DAST (a server-type license)• Fortify WebInspect• Fortify Scanning Machine (which licenses Fortify WebInspect and Fortify Static Code Analyzer)• Fortify SCA (Static Code Analyzer)
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 <ul style="list-style-type: none">• HH = hours• MM = minutes• SS = seconds
RELEASE STATUS	The condition under which the product became inactive. Possible values are: <ul style="list-style-type: none">• Released: A product using a connected concurrent license shut down normally. The seat was returned to the pool; the client is no longer licensed.

Field	Description
	<ul style="list-style-type: none">• 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:\<lim_install_dir>\DB*.*`
- `x:\<lim_install_dir>\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 options 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 *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:\<lim_install_dir>\Logs`, where `X` is the drive and `<lim_install_dir>` 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}:\<lim_install_dir>\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}:\<lim_install_dir>\ 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 OpenText license service.

1. Check your proxy settings. You may need to enter network credentials for the web service to use when connecting to OpenText 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 OpenText 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 OpenText 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 OpenText 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 OpenText 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://www.microfocus.com/solutions/application-security>.

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 does not 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}:\<lim_install_dir>\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 LIM Admin 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.

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

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

Feedback on Installation and Usage Guide (Fortify License and Infrastructure Manager 23.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!