opentext™

OpenText™ Fortify License and Infrastructure Manager

Software Version: 26.4.0
Windows® and Linux® operating systems

Installation and Usage Guide

Document Release Date: November 2026
Software Release Date: November 2026

Legal notices

Open Text Corporation

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

Copyright notice

Copyright 2009-2026 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 for OpenText™ Fortify License and Infrastructure Manager 26.4 on November 06, 2026.

Contents

Preface 7
Contacting Customer Support 7
For more information 7
Product feature videos 7

Change Log 8

Chapter 1: About the Fortify 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
Important information for configuring Fortify products 12
Options for LIM deployment 12
Product name changes 13
Related documents 13
All products 14
OpenText ScanCentral DAST 14
OpenText SAST 15
Fortify DAST 16

Chapter 2: System requirements 18
Software requirements 18
Hardware requirements 18
LIM on Docker requirements 19

Chapter 3: Preparing Windows Server and installing the LIM 20
Locating the installation file 20
Preparing to install the LIM 20
Web management tools 21

World Wide Web services 21
Common HTTP features 21
Security 21
HTTPS binding for SSL communications 21
Installing the LIM 22
Initializing the LIM 22
Accessing the LIM 25
Logging out 25
Reseting your password 26
Troubleshooting the LIM installation 26

Chapter 4: Manually configuring the LIM Docker image 28
What is Docker? 28
Benefits of Docker 28
Supported Docker version 28
Audience 28
Requesting access 29
Setting Up Docker 29
About the Docker image 29
Process for getting the image and starting the container 29
Editing the Docker compose file 30
Important information about mapped volumes 30
Mapping volumes for log files 31
Environment variable format 31
Unused optional environment variables 31
Understanding the Kestrel variables 31
Understanding the database variable 32
Understanding the signing certificate variables 32
Understanding the JSON Web Token variables 33
Understanding the default administrator variables 33
Understanding the proxy variables 34
Understanding the miscellaneous variables 35
Understanding the licensing URL variable 35
Running the container 35
Accessing the container UI 36
Logging out 37

Upgrading LIM on Docker 37

Chapter 5: Using the LIM 39
Getting started 39
Activating or updating the LIM 39
Activating a new installation 39
Updating the application 40
Activating offline 40
Offline activation 40
Creating the request file 40
Sending the request to OpenText 41
Submitting the response file to the LIM 41
Offline deactivation 41
Creating the request file 41
Sending the request to OpenText 42
Submitting the response file to the LIM 42
Configuring a proxy server 42
Configuring email notifications 43
Working with administrative users 44
Adding an administrator 44
Editing an administrator's account 44
Removing an administrator 44
Working with product licenses 45
Server-type licenses 45
Adding a license 45
Creating a license pool 45
Renewing a license 46
Deleting a license 46
Working with license pools 47
Creating a license pool 47
Adding a license to a pool 48
Editing a license pool 48
Deleting a license pool 48
Viewing current product usage 49
Accessing the Current Product Usage page 49
Understanding the current product usage information 49
Refreshing the page 49

Viewing current activity 49
Accessing the Current Activity Detail page 50
Understanding the current activity detail information 50
Releasing a seat 50
Revoking a seat 51
Releasing all seats 51
Viewing lease history 51
Accessing the Lease History page 51
Understanding the lease history information 52
Refreshing the page 53
Backing up and restoring the LIM 53
Task 1: Copy the LIM database 53
Task 2: Restore the LIM onto another server 53
Task 3: Activate the restored application 53
Task 4: Refresh product licenses 54
Task 5: Verify license pools and tokens 54
Task 6: Configure clients to use new server 54
Alternative back-up strategy 54
LIM troubleshooting 55

Send documentation feedback 60

Preface

Contacting Customer Support

Visit the Customer Support website to:

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

For more information

For more information about OpenText Application Security Testing products, visit OpenText Application Security.

Product feature videos

You can find videos that highlight OpenText Application Security Software products and features on the Fortify Unplugged YouTube™ channel.

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
26.4.0	Updated: • Added support for "Offline deactivation" on page 41. • Improved error reporting for licensing and activation operations • Added configurable password policies, including password strength, minimum password length, failed login attempts, inactivity logout time, password reset interval, and absolute session timeout • Added automatic redirection to the Reset Password page when a user's password expires • Documented how to select SQLite or PostgreSQL as the Fortify License and Infrastructure Manager database during initialization • Simplified JWT configuration by automaticallygenerating the JWT secret • Removed support for V1 APIs. All integrations nowuse the supported V2 API endpoints • Enhanced product security through dependencyupdates and removal of SHA-1 usage • Updated LIM to .NET 10
26.2.0	Updated: • Version number and release date.
25.4.0	Updated: • Version number and release date.
25.2.0 / July 2025	Updated: • Content related to permissions for mapped volumes in the

Software Release / Document Version	Changes
	Docker compose file. See "Editing the Docker compose file" on page 30.
25.2.0	Updated: • Version number and release date.
24.4.0 / November 2024	Updated: • Introduction with deployment options. See"About the Fortify License and Infrastructure Manager" on page 11. Removed: • Guideline for not deploying a LIM Docker image in an air-gapped environment.
24.4.0	Updated: • Introductory content to clarify LIM URL for licensing Fortify products. See "About the Fortify License and Infrastructure Manager" on page 11. • Preparation content with information about ASP.NET Core Runtime Hosting Bundle. See "Preparing to install the LIM" on page 20. • Initialization content with new information for upgrading with an existing LIM Administrator. See "Initializing the LIM" on page 22. • Docker universal base image (UBI) from UBI 8 to UBI 9. See "Manually configuring the LIM Docker image" on page 28. • Tip for finding the IP address of the container with a Docker CLI command. See "Running the container" on page 35.
24.2.0	Updated: • Content related to configuring Internet Information Services (IIS), ASP.NET, and the Microsoft .NET Framework. See "Preparing to install the LIM" on page 20. • Installation and initialization content with changes for streamlined configuration process. See "Installing the LIM" on page 22 and "Initializing the LIM" on page 22. • LIM Docker image content with important guidelines for using

Software Release / Document Version	Changes

	Docker versions of the LIM. See "Manually configuring the LIM Docker image" on page 28.
	• Information about privileges for mapped folders on the host system. See "Editing the Docker compose file" on page 30.
	• All procedures to reflect updated user interface.
	• Troubleshooting and backup and restore information to encompass latest revisions. See the following topics:
	  • "Troubleshooting the LIM installation" on page 26
	  • "Backing up and restoring the LIM" on page 53
	  • "LIM troubleshooting" on page 55
	Removed:
	• Content related to using the Windows version of the Docker image.
	• Out-dated data migration content.

Chapter 1: About the Fortify 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.

The following rules apply to detached leases:

- You cannot delete a license pool that includes detached leases.
- You cannot assign fewer seats to a license pool than the number of detached leases.
- You cannot deactivate a license that has detached leases.

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™ 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 DAST contacts the LIM for a license, and the associated license pool includes a OpenText ScanCentral DAST sensor license with an available seat, then that instance of Fortify DAST can lease the available seat.

Important information for configuring Fortify products

When configuing a Fortify product to use the LIM for licensing, you must specify the LIM URL in the format `https://<location>:<port>`, where *location* is IP address, hostname, or domain name.

Note: This format example uses the https protocol. If SSL certificates are not used for the LIM, the protocol is http.

Options for LIM deployment

You can use the following options to deploy the LIM:

- Install the LIM on a local Windows server as described in "Preparing Windows Server and installing the LIM" on page 20.

- Manually configure a LIM Docker image using the processes and procedures described in "Manually configuring the LIM Docker image" on page 28.
- Configure and use the `helm-lim` Helm chart for complete LIM container orchestration in Kubernetes. You can find the LIM Helm chart at https://hub.docker.com/r/fortifydocker/helm-lim/.

  Note: Helm charts might not be available immediately upon product release. When Helm charts for the current release are available, Helm chart documentation will be available on the Product Documentation website.

- For information on creating a Docker® pull secret, see Pull an Image from a Private Registry on the Kubernetes website.

Product name changes

OpenText is in the process of changing the following product names:

Previous name	New name
OpenText™ Static Application Security Testing (OpenText SAST)	OpenText™ Fortify SAST
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Fortify DAST (Fortify DAST)
OpenText™ Core Application Security	OpenText™ Fortify on Demand
OpenText Core Software Composition Analysis (OpenText Core SCA)	OpenText™ Fortify Core Software Composition Analysis (OpenText™ Fortify Core SCA)
OpenText Application Security Aviator	OpenText™ Fortify Remediation Aviator
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

Related documents

This topic describes documents that provide information about OpenText Application Security Software products.

Note: Most guides are available in both PDF and HTML formats. Product help is available within the Fortify DAST product.

All products

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

Document / file name	Description
About OpenText Application Security Software Documentation appsec-docs-n-*<version>*.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. **Note:** This document is included only with the product download.
What's New in OpenText Application Security Software <version> appsec-wn-*<version>*.pdf	This document describes the new features in OpenText Application Security Software products.
OpenText Application Security Software Release Notes appsec-rn-*<version>*.pdf	This document provides an overview of the changes made to OpenText Application Security Software for this release and important information not included elsewhere in the product documentation.

OpenText ScanCentral DAST

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

Document / file name	Description
OpenText™ ScanCentral DAST Configuration and Usage Guide sc-dast-ugd-*<version>*.pdf	This document provides information about how to configure and use OpenText ScanCentral DAST to conduct dynamic scans of Web applications.
OpenText™ Fortify License and	This document describes how to install, configure,

Document / file name	Description
Infrastructure Manager Installation and Usage Guide lim-ugd-*<version>*.pdf	and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-*<version>*.pdf	This document describes how to download, configure, and use Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The Fortify DAST 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 an OpenText ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.

OpenText SAST

The following documents provide information about OpenText SAST (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
OpenText™ Static Application Security Testing User Guide sast-ugd-*<version>*.pdf	This document describes how to install and use OpenText SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
OpenText™ Static Application Security Testing Custom Rules Guide sast-cr-ugd-*<version>*.zip	This document provides the information that you need to create custom rules for OpenText SAST. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.

Document / file name	Description
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-*<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.

Fortify DAST

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

Document / file name	Description
OpenText™ Dynamic Application Security Testing Installation Guide dast-igd-*<version>*.pdf	This document provides an overview of Fortify DAST and instructions for installing and activating the product license.
OpenText™ Dynamic Application Security Testing User Guide dast-ugd-*<version>*.pdf	This document describes how to configure and use Fortify DAST to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify DAST help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-*<version>*.pdf	This document describes how to download, configure, and use Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The Fortify DAST 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

Document / file name	Description
	programming interface (API). It can also be run as an OpenText ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-*<version>*.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing Tools Guide dast-tgd-*<version>*.pdf	This document describes how to use the Fortify DAST diagnostic and penetration testing tools and configuration utilities packaged with Fortify DAST and Fortify WebInspect Enterprise.
OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide dast-agent-igd-*<version>*.pdf	This document describes how to install the OpenText Fortify DAST Agent and describes the detection capabilities of the OpenText Fortify DAST Agent Rulepack Kit. OpenText Fortify DAST Agent Rulepack Kit runs atop the OpenText Fortify DAST Agent, allowing it to monitor your code for software security vulnerabilities as it runs. OpenText Fortify DAST Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Chapter 2: System requirements

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

Software requirements

LIM runs on and works with the software packages listed in the following table. Beta or pre-release versions of operating systems, service packs, and required third-party components are not supported.

Package	Versions	Notes
Microsoft Windows Server®	Windows Server 2019	
	Windows Server 2022	
Web Server	IIS 8.5	Recommended
	IIS 7.5, 8.0, 10	
.NET Platform	ASP.NET Core Runtime 10.0.10 Hosting Bundle or later	
	.NET SDK Core Runtime 10.0.10 or later	
Browser	All modern browsers and versions	

Hardware requirements

OpenText recommends that you install the LIM on a system that conforms to the supported components listed in following table.

Component	Requirement	Notes
Processor	2.5 GHz single-core or faster	Recommended
	1.5 GHz single-core	Minimum

Component	Requirement	Notes
RAM	2+ GB	Recommended
	1 GB	Minimum
Hard disk	50+ GB	Recommended
	20 GB	Minimum
Display	1280 x 1024	Recommended
	1024 x 768	Minimum

LIM on Docker requirements

LIM on Docker has the requirements listed in the following table.

Software	Version
Red Hat Universal Base Image (UBI)	10.x x86_64

Chapter 3: Preparing Windows Server and installing the LIM

This chapter provides important information about preparing your Microsoft Windows Server® for installation of the Fortify License and Infrastructure Manager (LIM), and procedures for installing and initializing the LIM and accessing the LIM for administrative tasks. If you experience issues related to installation and configuration, troubleshooting information is also included.

Locating the installation file

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

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

Product	File Location
OpenText™ Fortify DAST (DAST)	The LIM software is part of the Fortify DAST electronic download. The LIM installation file is copied to the directory where you installed Fortify DAST.
OpenText™ Static Application Security Testing (SAST)	The LIM software is a part of the OpenText SAST 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, ASP.NET Hosting Bundle, and the Microsoft .NET Framework, if applicable. This topic lists the required components. Refer to your Windows server documentation for specific instructions pertaining to your software version.

Important! You must install IIS before installing the ASP.NET Core Runtime 8.0.2 Hosting Bundle. For more information about ASP.NET Core Runtime, refer to https://dotnet.microsoft.com/en-us/download/dotnet/8.0.

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.

Web management tools

You must install the following Web management tools in Server Manager:

- IIS Management Console
- IIS Management Scripts and Tools
- IIS Management Service

World Wide Web services

You must install the following Web services in Server Manager:

- Application Development Features
  - .NET Extensibility 4.5
  - ASP.NET 4.5
  - ISAPI Extensions
  - ISAPI Filters
  - WebSocket Protocol

Common HTTP features

You must install the following common HTTP features in Server Manager:

- Default Document
- Static Content

Security

You must install the following security in Server Manager:

- Basic Authentication
- Request Filtering

HTTPS binding for SSL communications

Optionally, if you are using SSL for your LIM, 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 `LimSetup.msi` file to the Microsoft Windows Server® where you want to run the LIM. For more information, see "Locating the installation file" on page 20.
2. Double-click the `LimSetup.msi` file.
3. On the **Welcome to the Fortify License and Infrastructure Manager Setup Wizard** window, click **Next**.

   The End-User License Agreement window appears.
4. Review the license agreement. If you agree with the terms, select the check box and click **Next**; otherwise, click **Cancel**.

   The Destination Folder window appears.
5. Accept the default location where the LIM will be installed or click **Change...** to specify a different destination folder.
6. Click **Next**.
7. Click **Install**.

   The LIM is installed and the Opentext License and Infrastructure Manager Initialization window opens. Proceed with "Initializing the LIM" below.

Initializing the LIM

After installing the software, the LIM installation program opens the initialization program which adds and configures required services to the Web Application.

To initialize the LIM:

1. On the **Welcome to the Fortify License and Infrastructure Manager Initialization** window, click **Next**.

   The Setup Web Service window appears.
2. Continue according to the following table.

To...	Then...
Create a new website	a. Select **Create New Website**. b. In the **Name** box, enter the website name. c. In the **Host** box, enter the host name.

To...	Then...
	d. In the **Port** box, enter the port number.
Use an existing website	a. Select **Select Existing Website**. b. From the **Website** list, select the site on which the LIM services will be installed. **Important!** The website you select must be running, must have anonymous access enabled during initialization, and must not require SSL during initialization. Also, be aware that the existing website will be overwritten with the LIM application.

Tip: Write down the URL you select as the website. You must use this URL when configuring your Fortify products to use the LIM. 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. Click **Next**.
   The Setup SSL window appears.
4. (Optional) To associate an SSL certificate with the site, continue as follows:
   a. Select the **Require Secure Channel (SSL)** checkbox.
   b. In the **SSL Port** box, enter the port on which the SSL service will establish an encrypted connection.
   c. Select an available certificate.

   Important! For SSL communications, you must add a valid certificate to the site in IIS that is hosting the LIM application. Self-signed certificates are not supported.
5. Click **Next**.
   The **Database Configuration** dialog box opens.
6. In the **Database Configuration** dialog box, select the database that you want to use from the following options:
   - **SQLite (Embedded Database)**
   - **PostgreSQL Server**: If you select this option, specify the following details:
     - **Host**: Specify the hostname or IP address of the PostgreSQL server.
     - **Port**: Specify the port number used by the PostgreSQL server to accept connections. Database Name: Specify the name of the database.

- **Username**: Enter the username for connecting to the database. Password: Enter the password for the specified username.

7. Click **Next**.

   The **Setup Password Policy** dialog box opens.
8. In the **Setup Password Policy** dialog box, configure the following password policy rules:
   - **Required Password Strength**: Select the required password characteristics, such as special characters, uppercase, lowercase, and digits.
   - **Minimum Password Length**: Specify the minimum number of characters required for a password.
   - **Login Attempts**: Specify the maximum number of failed login attempts allowed.
   - **Logout Time (minutes)**: Specify the period of inactivity after which the user is logged out.
   - **Days Before Password Reset**: Specify the number of days after which users must reset their passwords.
   - **Absolute Session Timeout (minutes)**: Specify the maximum duration of a user session, regardless of activity.
9. Continue as follows to create a LIM Administrator account:

   Note: If you are upgrading, an Administrator account has already been created and the input boxes on the Setup LIM Administrator window are disabled. If you want to create another Administrator account, however, select **Create User**, and then provide the information requested in the input boxes as follows.

   a. In the **Login** 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 **Email** box, type the email address for the user.
   d. In the **Password** and **Retype Password** boxes, type a password for the account.

      Tip: The password should contain at least six characters and include at least one of each of the following character groups:

      - Uppercase character (A through Z)
      - Lowercase character (a through z)
      - Numerals (0 through 9)

   e. Click **Next**.

   The Setup JWT window appears. You can accept the default JSON web token (JWT) settings or input values that are specific for your system.

10. Optionally, continue as follows in the Setup JWT window:
    a. In the **Audience** box, type the audience that identifies the recipient for which the token is intended. The default setting is `FortifyLimAuthAudience`.
    b. In the **Issuer** box, type the issuer that identifies the principal that issued the token. The default setting is `FortifyLimAuthIssuer`.
    c. In the **Security key** box, type the key to be used for signing access tokens.
    d. In the **Expiration** box, type the lifespan of the access token in minutes. The default setting is `5`.
    e. In the **Refresh token expiration** box, type the lifespan of the refresh token in minutes. The refresh token is used for obtaining a new access token without having to enter a user name and password. The default setting is `60`.
11. Click **Finish** to complete initialization and terminate the program.

Accessing the LIM

After installation, you can access the LIM in a browser.

To access the LIM:

- In a browser, navigate to:

  `https://<LIM_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 LIM initialization program. For instructions on using the LIM, see "Using the LIM" on page 39.

Important! The first time you access the LIM 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 39.

Logging out

To log out from the LIM:

- Click the user icon (), and then select **LOG OUT**.

Reseting your password

If your password expires, you will be directed to the Reset Password page at your next log in attempt. Enter your **username**, a new **password**. and confirm the password. After you change your password, you will be redirected to the login page. Use your **username** and updated **password** to log in.

Troubleshooting the LIM installation

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

Symptom or Error Message	Possible Cause	Possible Solution
The LIM Installer completes but the LIM Initialize Wizard does not appear.	You are not running the executable files with Administrator rights.	Do the following: 1. Navigate to the `Initialize` subfolder in the LIM installation directory. 2. Right-click the `LimInitialize.exe` file and select **Run as Administrator**.
The 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.	Do the following: 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 the error.
When logging into the LIM your login fails with the following error:	The LIM application pool does not have access to the	Do one of the following: • Give the built-in IIS_

Symptom or Error Message	Possible Cause	Possible Solution
“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.”	Machine Keys folder on the machine located at `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys`.	IUSRS group Read permission to the Machine Keys folder. • Change the identity of the Fortify License and Infrastructure Manager application pool to a user with permission to the Machine Keys folder (for example, LocalSystem).
When logging into the LIM your login fails with the following error: “Your login attempt has failed. Please try again.”	If you previously had access, you forgot your LIM credentials. Otherwise, you do not have LIM credentials.	Re-run the LIM Initialize Wizard from the Initialize subfolder in the LIM installation directory to create a new admin user.
After logging into the LIM, the Admin, License Management, Activity Management, and My Account tabs are not clickable.	Scripting may be disabled in your browser.	Enable scripting in your browser's settings. See your browser documentation for specific instructions.

Chapter 4: Manually configuring the LIM Docker image

OpenText engineers have created a version of the Fortify License and Infrastructure Manager (LIM) image for Linux that is available for download on the Docker® container platform. The image includes the full version of LIM 26.4.0 software. This chapter provides information about setting up Docker®, 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 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 version

Follow Docker® recommendations for the Docker® engine version to use for the Red Hat® Universal Base Image (UBI) 10.x x86_64 host operating systems.

Audience

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

Requesting access

Access to LIM on Docker® images requires credentials and is granted through your Docker® ID. To access 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 the Red Hat® Universal Base Image (UBI) 10.x x86_64 host operating systems.
2.	Configure your machine for Docker® containers.
3.	Register and start the Docker® service.

About the Docker image

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

`fortifydocker/lim:<version.linux_os_version>`

Process for getting the image and starting the container

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 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/26.4/docker-compose.yml The file is downloaded to the default download directory on your machine. The file name is `docker-compose.yml`. Download the environment file from the following URL: https://smartupdate.fortify.microfocus.com/documents/lim/26.4/environment-lim.env
2.	Configure the environment variables in the Docker® compose file. For more information, see "Editing the Docker compose file" 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 container" on page 35.

Editing the Docker compose file

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

Important information about mapped volumes

This topic primarily describes editing only the environment variables in the Docker® compose file. However, the compose file also includes commands for mapping volumes (or directories) from the container to directories on the host system as follows:

```
volumes :
    - ~/lim/logs:/app/logs
    - ~/lim/database:/app/database
    - ~/lim/certificates:/app/certificates
```

When you map these directories from the container to directories on the host system, make sure the filesystem mounted to these volumes grants read and write privileges to the default UID (limuser) and GID (limgroup) for the LIM image you are using.

Tip: You can use the following command to determine the UID and GID:

```
docker run --rm --entrypoint id fortifydocker/lim:26.4.ubi.9
uid=1001(limuser) gid=1001(limgroup) groups=1001(limgroup)
```

Mapping volumes for log files

To access LIM log files in the container, use the following volume configuration when setting up the docker-compose.yml file:

```
volumes:
    - ~/lim/logs:/app/logs
```

This configuration allows direct access to the logs at `/app/logs`, eliminating the need to extract them from the container.

Environment variable format

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.

Variable	Description
`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 identifies the recipient for which the token is intended. A sample setting is: `"JWT__ValidAudience=FortifyLimAuthAudience"`
`JWT__ValidIssuer`	Required setting that identifies the principal that issued the token. A sample setting is: `"JWT__ValidIssuer=FortifyLimAuthIssuer"`
`JWT__SecurityKey`	Required setting that specifies the secret key to be used for signing access tokens. A sample setting is: `"JWT__SecurityKey=aS1l6IUxmbf9X6PCVpmkG8vraqlpPFU9"`
`JWT__ExpirationMinutes`	Optional setting that specifies the lifespan of the access token in minutes. If not included, the setting defaults to `5` minutes. A sample setting is: `"JWT__ExpirationMinutes=10"`
`JWT__RefreshTokenExpirationMinutes`	Optional setting that specifies the lifespan of the refresh token in minutes. The refresh token is used for obtaining a new access token without having to enter a user name and password. 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

Variable	Description
	user name that will appear as the Login Name in the list of LIM Administrators. This variable creates the default administrator's account 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`	If `DefaultAdministrator__Login` is configured, this required setting specifies the password for the default administrator's account. **Tip:** The password should contain at least six characters and include at least one of each of the following character groups: • Uppercase character (A through Z) • Lowercase character (a through z) • Numerals (0 through 9)
`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`	Optional setting for configuring a proxy. Possible values are: • None = `0` • AutoDetect = `1` • Manual = `2` The default setting is `0`.

Variable	Description
`Proxy__Address`	If `Proxy__Mode=2`, specifies the URL or IP address of your proxy server.
`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 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 container UI

You can perform administration tasks using the 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 Docker® inspect command:

```
docker inspect -f='{{range .NetworkSettings.Networks}}{{.IPAddress}}
   {{end}}' lim
```

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 LIM, see "Using the LIM" on page 39.

Important! The first time you access the LIM 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 39.

Logging out

To log out from the LIM:

- Click the user icon (), and then select **LOG OUT**.

Upgrading LIM on Docker

When upgrading a LIM Docker® container to version 26.4, 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.

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

Stage	Description
1.	1. Download the LIM Docker® compose file from the SmartUpdate server at the following URL: https://smartupdate.fortify.microfocus.com/documents/lim/26.4/docker-compose.yml 2. Configure the environment variables in the file. For more information, see "Editing the Docker compose file" on page 30. Download the environment file from the following URL: https://smartupdate.fortify.microfocus.com/documents/lim/26.4/environment-lim.env

2.	At the terminal prompt on the Linux® host machine, enter the following commands to delete the existing container:
	`docker compose down`
	`docker rm lim`
	Important! Do not simply stop the existing container. You must delete the existing container before starting the new container.

3.	Use the `docker compose up` command to pull the image and start the container. For more information, see "Running the container" on page 35.
4.	After starting the new container, update the LIM as follows: 1. Access the container UI and log in using LIM administrator credentials. For more information, see "Accessing the container UI" on the previous

Stage	Description
	page. 2. Select **ADMIN** > **SERVER CONFIGURATION** > **Activation**. 3. Click **Update**. The LIM does not provide confirmation of the update. However, the Server Configuration page refreshes. **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.

Chapter 5: 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 for 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. Add administrators as described in "Working with administrative users" on page 44.
3. Add a product license to the database as described in "Working with product licenses" on page 45.
4. Create a license pool, add a license to the pool, and add/delete license pool seats as described in "Working with license pools" on page 47.

Activating or updating the LIM

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

Activating a new installation

To activate a new installation:

1. Select **ADMIN** > **ACTIVATION**.
2. Click **ACTIVATE**.

Updating the application

To update the application:

1. Select **ADMIN** > **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 page will repopulate and display instructions for offline activation. For more information, see "Offline activation" below.

Offline activation

Use the following procedure to activate your license if you have installed the 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 an 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** > **ACTIVATION**.
2. Clear the **Server has Internet connection** check box.
   The screen will repopulate and display instructions for offline activation.
3. Enter the License Server Activation Token string.
4. (Optional) You can activate other products in addition to the LIM:
   a. Click **Add LicenseToken**.
   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.
5. 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**.

Offline deactivation

While in offline mode, you can deactivate your license from a computer that is not connected to the internet.

Use the following procedure to deactivate your license if you have installed the LIM on a computer that is not connected to the Internet.

Creating the request file

1. Browse to **LICENSES** > **PRODUCT LICENSES** and click **DELETE**.

   Note: This step does not fully deactivate the license when working offline.

2. Click **ADMIN** > **ACTIVATION**.
   Clear the **Server has Internet connection** check box.
   The screen will repopulate and display instructions for offline deactivation.

3. 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, click **Browse** to select the request 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 **Process Offline Response**.

Configuring a proxy server

To configure a proxy server:

1. Click **ADMIN** > **PROXY**.
2. Select **Use Proxy Server**.

3. In the **Proxy settings type** list, select a type as described in the following table.

Option	Description
Direct Connect	Select this option if you are not using a proxy server. Proxy is disabled.
Explicitly configure proxy settings	Select this option to configure a proxy. Provide the following information: a. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080). b. If authentication is required, select an authentication type from the **Authentication** list. c. Type the required credentials in the **User Name** and **Password** boxes.

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** > **EMAIL**.
2. Select **Use SMTP**.
3. In the **SMTP Server Address** box, enter the IP address of your email server.
4. In the **SMTP Port** box, enter the port number of your email server.
5. In the **SMTP Authentication Type** list, select either **Basic**, **None**, or **Windows**.
6. In the **SMTP Server User ID** box, enter your email address.
7. In the **SMTP Server Password** box, enter your email address password.
8. If the SMTP server requires a secure link, select **Server Requires SSL**.
9. Enter an **Email Address to be used as From**. This email address will appear as the originator of the message in the "From" field.
10. Click **OK**.

Working with administrative users

The LIM administrators are authorized to add product licenses, create and maintain license pools, and manage license-related activities. You can manage administrative users on the USERS page.

Adding an administrator

To add an administrative user:

1. Click **ADMIN** > **USERS**.
2. Click **+ NEW USER**.
   The CREATE NEW USER dialog box opens.
3. In the **Full Name** box, type a user name.

   Note: This is the name that will appear in the Full Name column of the USERS view.

4. In the **Login Name** box, type a login name.

   Note: This is the name the user will enter on the LIM login page.

5. In the **Email Address** box, type an email address where the user will receive emails.
6. In the **Password** and **Confirm Password** boxes, type a password for the account.
7. To enable the LIM to send email notification of certain events to the administrator, select **Receives Email**.

Editing an administrator's account

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

1. Click **ADMIN** > **USERS**.
2. Select the checkbox for the user to edit, and then click **EDIT**.
   The EDIT USER dialog box opens.
3. Make changes as needed, and then click **OK**.

Removing an administrator

To remove a user:

1. Click **ADMIN** > **USERS**.
2. Select the checkbox for the user to be deleted, and then click **DELETE**.

A DELETE USERS confirmation message appears.

3. Click **OK** to confirm the deletion.

Working with product licenses

You can view all OpenText product licenses currently associated with the LIM on the Product Licenses page. On this page, you can view product license details, add or delete a product license, create a license pool, and renew a license.

Server-type licenses

Server-type licenses are used to activate certain products, such as components that are used in OpenText 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 **+ LICENSE**.
   The ADD PRODUCT LICENSE dialog box opens.
2. In the **Activation Token** box, 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. Optionally, in the **Description** box, enter a description of the license.
4. Click **OK**.

Creating a license pool

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.

d. Optionally, to allow detached leases:
   i. Select **Allow Detached Lease**.
   ii. In the **Detached Lease Duration Limit** box, enter the number in days a lease can be detached.
   iii. In the **Detached Lease Limit** box, enter the number of detached seats allowed for the licenses in the pool.

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**.

Renewing a license

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

To renew a license:

- On the **PRODUCT LICENSES** page, click **LICENSE RENEW** to initiate communication with the OpenText global license server.

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

Deleting 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 delete it from the original LIM database. Otherwise, the license will remain attached to the original LIM and cannot be used in another LIM.

To delete a license from the LIM database:

1. On the **PRODUCT LICENSES** page, select the checkbox for the license that you want to delete.
2. Click **DELETE**.

   A confirmation message appears.
3. Click **OK**.

The license is removed from the LIM database. You can now add the license to a different LIM.

Working with license pools

The License Pools page lists all license pools currently defined within the LIM. On this page, you can view the license pool details and add, edit, and delete a license pool.

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

Creating a license pool

To create a license pool:

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.
   d. Optionally, to allow detached leases:
      i. Select **Allow Detached Lease**.
      ii. In the **Detached Lease Duration Limit** box, enter the number in days a lease can be detached.
      iii. In the **Detached Lease Limit** box, enter the number of detached seats allowed for the licenses in the pool.
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. On the **LICENSE POOLS** page, select the checkbox for the pool to which you want to add a license, and then click **EDIT**.

   The License Pool Configuration wizard opens to the LICENSE POOL DETAILS page.
2. Click **NEXT**.

   The Product License Select page opens.
3. 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.
4. Click **SAVE**.

Editing a license pool

To edit a pool:

1. On the **LICENSE POOLS** page, select the checkbox for the pool you want to edit, and then click **EDIT**.

   The License Pool Configuration wizard opens to the LICENSE POOL DETAILS page.
2. Proceed with Steps 2 through 5 of "Creating a license pool" on the previous page.

Deleting a license pool

To delete a license pool:

1. On the **LICENSE POOLS** page, select the checkbox for the pool you want to delete.
2. Click **DELETE**.

   A confirmation message appears.
3. Click **OK**.

Viewing current product usage

You can view the product seats currently in use on the Current Product Usage page.

Accessing the Current Product Usage page

To access the page:

- Click **ACTIVITY** > **CURRENT PRODUCT USAGE**.

Understanding the current product usage information

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: • 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)
License Count	The number of licenses associated with the product
License Seats	The total number of seats available
Leased Seats	The number of seats in use

Refreshing the page

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

- Click **REFRESH**.

Viewing current activity

You can view the current activity involving licenses on the Current Activity Detail page. On this page, you can release a set, revoke a seat, and release all seats.

Accessing the Current Activity Detail page

To access the page:

- Select **ACTIVITY** > **CURRENT ACTIVITY DETAIL**.

Understanding the current activity detail information

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

Field	Description
User Name	The Microsoft 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: • 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 in relation to the LIM. Possible statuses are **Detached**, **Connected**, or **Check for approval**.
Detached Expiration Date	If detached, the date by which the machine is scheduled to be reconnected to the LIM.

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 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:

1. Select the checkbox for the instance to release.
2. Click **RELEASE**.

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, Customer Support must be involved. The inclusion of support is a control measure designed to discourage concurrent license theft.

To revoke a seat:

1. Select the checkbox for the lease to revoke.
2. Click **REVOKE**.
   The RELEASING A DETACHED LEASE dialog box opens.
3. Continue as follows:
   a. In the **Reason** box, type the reason for revocation.
   b. In the **Email** box, type the email address that will receive an approval notice when the revocation is complete.
   c. Click **OK**.
      The Connection Mode is changed to **Check for approval**.
4. Contact Customer Support and identify the lease that needs to be revoked.
5. Support logs into the license portal and processes the revoke request.

Releasing all seats

To release all seats:

- Click **RELEASE ALL EXPIRED LICENSES**.

Viewing lease history

A lease is defined as the period of time during which a product licensed through the LIM is active. You can view lease history on the Lease History page.

Accessing the Lease History page

To access the page:

- Select **ACTIVITY** > **LEASE HISTORY**.

Understanding the lease history information

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: • 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 DD.HH:MM:SS, where • DD = days • HH = hours • MM = minutes • SS = seconds
Release Status	The condition under which the product became inactive. Possible values are: • **Released**: A product using a connected concurrent license shut down normally. The seat was returned to the pool; the client is no longer licensed. • **Revoked**: A LIM administrator initiated a revoke on the lease, Customer Support processed the revoke, and the LIM connected

Field	Description
	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**.

Backing up and restoring the LIM

Read all of the tasks in this topic before backing up and restoring your LIM.

Task 1: Copy the LIM database

Make a back-up copy of the LIM database. The database files are in the root directory at:

```
x:\Program Data\Fortify\Fortify License and Infrastructure Manager\*.*
```

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 to the new server.
4. Run the initialization. The file name is `LimInitialize.exe`.

Task 3: Activate the restored application

1. Log in to the admin console.
2. Click **ADMIN** > **ACTIVATION**.

3. 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 Customer Support for assistance.

Task 4: Refresh product licenses

1. Click **LICENSES** > **PRODUCT LICENSES**.
2. Select the checkbox for the license you wish to refresh, and then click **LICENSE RENEW**

Task 5: Verify license pools and tokens

1. View product tokens and execute a license renew.
2. View license pools and token associations.

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 one of the following options to ensure that the products can use the replacement LIM:

- Option 1: 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 2: 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 (for example, 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 Microsoft Windows Server® environments.

LIM troubleshooting

This section addresses some of the problems or malfunctions that may occur when using the LIM.

Symptom or Error Message	Possible Cause	Possible Solution
The LIM installer indicates that a required component is not installed and terminates.	A required component is not installed or is not configured.	Provide the missing components and restart the installation. Consult your Microsoft Windows Server® documentation for assistance with the following: • Adding IIS • Enabling ASP.Net on a web site • Enabling/restoring the network services account See the "Preparing to install the LIM" on page 20 for a list of required modules.
You receive an HTTP response status code **405 Method Not Allowed** when attempting to release a seat lease.	WebDAV Publishing is enabled.	Disable WebDAV Publishing in IIS. Consult your Windows server documentation for assistance with disabling (or removing) WebDAV Publishing.
You receive **HTTP Error 500.30 - ASP.NET Core app failed to start** after stopping and restarting the LIM website in IIS on the Windows server.	The **Load User Profile** setting for LimPool might be configured incorrectly.	In IIS Manager, ensure that the **Application Pools** > **LimPool** > **Advanced Settings** > **Process Model** > **LoadUserProfile** setting is set to **True**.
The LIM cannot activate its license.	The LIM cannot to connect to the OpenText license service.	Do the following: 1. Check your proxy settings. You may need to enter

Symptom or Error Message	Possible Cause	Possible Solution
		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 "Offline activation" on page 40.
Error message during activation indicates 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.	Do one of the following: • If the LIM has been reinstalled, contact Customer Support and ask to have the previous instance deactivated for that specific activation token. • If the LIM was not reinstalled, contact 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 token is not valid product.	You may have mistyped the activation token string.	Re-enter or paste the LIM token from the original OpenText email and resubmit. Make sure there are no trailing spaces.

Symptom or Error Message	Possible Cause	Possible Solution
	The activation token is a unique string of characters and is unique for a specific product.	Use the command line interface to resolve the IP address of the license service URL and verify that the address is correct. Contact 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.
The 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.	Do the following 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 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.
The LIM does not release expired leases automatically.	The LIM Windows service is unable to communicate with the	Do the following to verify that the Windows service is running:

Symptom or Error Message	Possible Cause	Possible Solution
	LIM web services.	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.
The 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.	Do the following 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 "The LIM does not refresh licenses manually." on the next page If unsuccessful, contact Customer Support and verify that the license token exists in the license database and is intended for the

Symptom or Error Message	Possible Cause	Possible Solution
		product being activated. Also verify that the token is configured to be a concurrent license.
The 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.opentext.com/products/fortify-webinspect`. 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 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.

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 26.4.0)

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!