opentext™

OpenText™ Dynamic Application Security Testing (Fortify WebInspect)

Software Version: 25.4.0
Windows® operating systems

Installation Guide

Document Release Date: October 2025
Software Release Date: October 2025

Legal notices

Open Text Corporation

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

Copyright notice

Trademark notices

Documentation updates

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

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

This document was produced for OpenText™ Dynamic Application Security Testing CE 25.4 on October 03, 2025.

Contents

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 between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
25.4.0	Removed: • Windows 10 from the list of supported software. See "Software requirements" on page 18.
25.2.0	Added: • System requirements for OpenText DAST and WebInspect SDK. See "Software requirements" on page 18. Removed: • References to using a classic OpenText DAST installation with the OpenText™ ScanCentral DAST sensor service.
24.4.0	Updated: • Licensing information to clarify LIM URL. See "Licensing with the License Wizard" on page 40 and "Configuring OpenText DAST to use the LIM" on page 46.
24.2.0	Updated: • Licensing information with new LIM URL format. See "Licensing with the License Wizard" on page 40 and "Connect to LIM" on page 43. Removed: • Images from Setup Wizard content.

Chapter 1: Welcome to OpenText DAST

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

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

Product name changes

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

Previous name	New name
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
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.

The main features of OpenText DAST

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

Crawling and auditing

OpenText DAST uses two basic modes for determining your security weaknesses:

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

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

Reporting

Use OpenText DAST reports to gain valuable, organized application information. You can customize report details, deciding what level of information to include in each report, and gear the report for a specific audience. You can save reports in a variety of formats, and you can also include graphic summaries of vulnerability data.

Manual hacking control

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

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

Summary and fixes

OpenText DAST provides summary and remediation information for all vulnerabilities detected during a scan. This includes reference material, links to patches, instructions for prevention of future problems, and vulnerability solutions. As new attacks and exploits are formulated, we update our

remediation database. Use Smart Update on the OpenText DAST toolbar to update your database with the latest vulnerability solution information.

Scanning policies

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

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

Sortable and customizable views

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

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

Enterprise-wide usage capabilities

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

API and web services scans

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

API discovery

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

Integration capabilities

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

- Burp
- Postman
- Selenium WebDriver

Export wizard

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

Hacker-level insights

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

If the detected library is open source, the hacker-level insights check includes information from the National Vulnerability Database (NVD). If OpenText™ Core Software Composition Analysis (Debricked or Core SCA) access is configured, then OpenText Core SCA health metrics for open source libraries is also included. For more information on configuring access to the OpenText Core SCA database, see "Using the WIConfig program" on page 30

Testing tools

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

- Audit Inputs Editor
- Compliance Manager
- Encoders/Decoders
- HTTP Editor
- Log Viewer
- Policy Manager
- Regular Expression Editor

- Server Analyzer
- SQL Injector
- Traffic Tool
- Web Discovery
- Web Form Editor
- Web Fuzzer
- Event-based Web Macro Recorder
- Session-based Web Macro Recorder
- Web Proxy
- Web Services Test Designer

Related documents

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

Note: Most guides are available in both PDF and HTML formats. Product help is available within the OpenText 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 Softwareproducts.
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 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 and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText 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 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	This document provides an overview of OpenText DAST and instructions for installing and activating the product

Document / file name	Description
dast-igd-<*version*>.pdf	license.
OpenText™ Dynamic Application Security Testing User Guide dast-ugd-<*version*>.pdf	This document describes how to configure and use OpenText DAST to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the OpenText 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 OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText 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™ 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 OpenText DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and Fortify WebInspect Enterprise.

Document / file name	Description
OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide dast-agent-igd-<*version*>.pdf	This document describes how to install the OpenText DAST Agent and describes the detection capabilities of the OpenText DAST Agent Rulepack Kit. OpenText DAST Agent Rulepack Kit runs atop the OpenText DAST Agent, allowing it to monitor your code for software security vulnerabilities as it runs. OpenText DAST Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect Enterprise

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

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

Document / file name	Description
	linked content may not be present in this PDF version.
OpenText™ Dynamic Application Security Testing Tools Guide dast-tgd-<*version*>.pdf	This document describes how to use the OpenText DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and Fortify WebInspect Enterprise.

Chapter 2: System requirements

Before you install OpenText DAST, make sure that your system meets the requirements described in this section. OpenText does not support beta or pre-release versions of operating systems, service packs, or required third-party components.

Hardware requirements

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

Component	Requirement	Notes
Processor	2.5 GHz quad-core or faster	Complex applications might benefit from additional cores.
RAM	16 GB	Complex applications might benefit from additional memory. OpenText recommends 32 GB of memory to scan with single-page application (SPA) support.
Hard disk	40 GB	Using SQL Express and storing scans locally requires additional disk space per scan.
Display	1280 x 1024	

Virtual Machine support

You can run OpenText Application Security Software products on an approved operating system in virtual machine environments. You must provide dedicated CPU and memory resources that meet the minimum hardware requirements. If you find issues that cannot be reproduced on the native environments with the recommended processing, memory, and disk resources, you must work with the provider of the virtual environment to resolve them.

Note: If you run OpenText Application Security Software products in a VM environment, OpenText strongly recommends that you have CPU and memory resources fully committed to the VM to avoid performance degradation.

Software requirements

OpenText DAST runs on and works with the software packages listed in the following table.

Package	Versions	Notes
Windows	Windows 11	Recommended This version is required for conducting scans of gRPC APIs.
	Windows Server 2019	
	Windows Server 2022	
.NET Platform	.NET Framework 4.8	
SQL Server (English-language versions only)	SQL Server 2019	Recommended No scan database limit
	SQL Server 2022	No scan database limit
	Azure SQL Server	Using Azure SQL Server outside the Azure infrastructure might cause poor performance for OpenText DAST. OpenText recommends using Azure SQL Server with OpenText DAST inside the Azure infrastructure only.
SQL Server Express (English-language versions only)	SQL Server 2019 Express	Recommended 10 GB scan database limit
	SQL Server 2022 Express	10 GB scan database limit
Portable Document Format	Adobe Acrobat Reader 11	Recommended
	Adobe Acrobat Reader 8.1.2	Minimum

Support for Postman

A Postman collection version 2.0 or 2.1 is required to conduct scans in OpenText DAST.

Additionally, you must install the following third-party software on the machine where OpenText DAST is installed:

- Newman command-line collection runner 4.5.1 or later

  Important! You must install Newman globally rather than locally. You can do this by adding a `-g` option to the installation command, as follows:

  ```
  npm install -g newman
  ```

  When you install Newman, a path variable for Newman is automatically added to the user variables. The path variable is similar to the following:

  <directory_path>`\AppData\Roaming\npm`

  You must manually add the same Newman path variable to the system environment variables. Ensure that the variable is in both the user variables and system environment variables before proceeding.

  System variables are read only when the machine boots, so after manually adding the path variable, you must restart your machine. See your Windows documentation for specific instructions on how to add a system environment variable.

- Node.js and the included Node Package Manager (NPM)

  Note: Install the Node.js version that is required for the version of Newman that you install. For more information, see https://www.npmjs.com/package/newman.

Notes on SQL Server editions

When using the Express edition of SQL Server:

- Scan data must not exceed the database size limit. If you require a larger database or need to share your scan data, use the full version of SQL Server.
- During the installation you might want to enable “Hide advanced installation options.” Accept all default settings. OpenText DAST requires that the default instance is named SQLEXPRESS.

When using the full edition of SQL Server:

- You can install the full version of SQL Server on the local host or nearby (co-located). You can configure this option in OpenText DAST Application Settings (**Edit > Application Settings > Database**).
- The account specified for the database connection must also be a database owner (DBO) for the named database. However, the account does not require sysadmin (SA) privileges for the database server. If the database administrator (DBA) did not generate the database for the specified user, then the account must also have the permission to create a database and to manipulate the security permissions. The DBA can rescind these permissions after OpenText DAST sets up the database, but the account must remain a DBO for that database.

OpenText DAST ports and protocols

This section describes the ports and protocols OpenText DAST uses to make required and optional connections.

Required connections

The following table lists the ports and protocols OpenText DAST uses to make required connections.

Direction	Endpoint	URL or details	Port	Protocol	Notes
OpenText DAST to target host	Target host	Scan target host	Any	HTTP	OpenText DAST must connect to the web application or web service to be scanned.
OpenText DAST to SQL database	SQL Server Express, SQL Server Standard/Enterprise, or Azure SQL Server	SQLEXPRESS service on localhost or SQL TCP service locally installed or remote host	1433	SQL TCP	Used to maintain the scan data and to generate reports within the OpenText DAST application.

Direction	Endpoint	URL or details	Port	Protocol	Notes
OpenText DAST to Certificate Revocation List (CRL)	DigiCert CRL	http://crl3.digicert.com/DigiCertTrustedG4RSA4096SHA256TimeStampingCA.crl	80	HTTP	Offline installations of OpenText DAST or Fortify WebInspect Enterprise require you to manually download and apply the CRL from DigiCert. OpenText DAST products prompt for these lists from Windows and their absence can cause problems with the application. A one-time download is sufficient, however OpenText recommends that you download the CRL as part of regular maintenance.

Optional connections

The following table lists the ports and protocols OpenText DAST uses to make optional connections.

Direction	Endpoint	URL or details	Port	Protocol	Notes
OpenText DAST to Fortify License activation server	Remote Fortify Licensing Service	https://licenseservice.fortify.microfocus.com	443	HTTPS over SSL	For one-time activation of an OpenText DAST Named User license. You may optionally

Direction	Endpoint	URL or details	Port	Protocol	Notes
					use the following: • An offline activation process instead of using this direct connection • Upstream proxy with authentication instead of a direct connection
OpenText DAST to SmartUpdate server	Remote SmartUpdate service	https://smartupdate.fortify.microfocus.com	443	HTTPS over SSL	Used to automatically update the OpenText DAST product. SmartUpdate is automatic when opening the product UI, but can be disabled and run manually. Can optionally use upstream proxy with authentication instead of a direct connection.
OpenText DAST to Fortify Support Channel server	Remote Fortify Support Channel service	https://supportchannel.fortify.microfocus.com	443	HTTPS over SSL	Used to retrieve product marketing messages and to upload OpenText DAST data or product suggestions to Customer Support. Message check is automatic when opening the product UI, but can be disabled and run manually. Can optionally use upstream proxy with authentication instead of a direct connection.
OpenText	OpenText DAST LIM	Lease Concurrent User license	443	Web services	Required for

Direction	Endpoint	URL or details	Port	Protocol	Notes
DAST to Fortify License and Infrastructure Manager (LIM)	(Local Licensing Service)			over SSL	OpenText DAST client to lease and use a Concurrent User license maintained in a LIM license pool. You can detach the client license from LIM after activation to avoid a constant connection.
OpenText DAST API listener	Local machine API, or network IP address	http://localhost:8083/webinspect/api	8083 or user-specified	HTTP	Use to activate an OpenText DAST API Windows Service. This opens a listening port on your machine, which you can use locally or remotely to generate scans and retrieve the results programmatically. This API can be SSL enabled, and supports Basic or Windows authentication.
OpenText DAST to Fortify WebInspect Enterprise	Fortify WebInspect Enterprise server	User-specified OpenText DAST server	443 or user-specified	HTTP or HTTPS over SSL	The Enterprise Server menu connects OpenText DAST as a client to the enterprise security solution to transfer findings and user role and permissions management.
OpenText DAST sensor service to Fortify WebInspect Enterprise	Fortify WebInspect Enterprise server	User-specified OpenText DAST server	443 or user-specified	HTTP or HTTPS over SSL	Separate from the OpenText DAST UI, you can configure the local installation as a remote scan engine for use by the enterprise security solution community. This is done through

Direction	Endpoint	URL or details	Port	Protocol	Notes
					a Windows Service. This constitutes a different product from OpenText DAST desktop and is recommended to be run on its own, non-user-focused machine.
Browser to OpenText DAST	localhost	Manual Step-Mode Scan	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	OpenText DAST serves as a web proxy to the browser, enabling manual testing of the target web server through OpenText DAST.
OpenText DAST to OpenText Application Quality Management	OpenText Application Quality Management server	User-specified OpenText Application Quality Management server	Server-specified	HTTP or HTTPS over SSL	Permits submission of findings as defects to the OpenText Application Quality Management bug tracker.
OpenText DAST to OpenText™ Core Software Composition Analysis API	OpenText Core (Debricked) service	https://www.debricked.com/api/ https://www.debricked.com/select/	443	HTTPS over SSL	If enabled, provides OpenText Core SCA Health Metrics and extends the local NVD to include the newest CVEs.

Connections for tools

The following table lists the ports and protocols that the OpenText DAST tools use to make connections.

Tool	Direction	Endpoint	Port	Protocol	Notes
Web Proxy	To target host	localhost	8080 or user-specified	HTTP or HTTPS over SSL	Intercepts and displays web traffic
Web Form Editor	To target host	localhost	Dynamic, 8100, or user-specified	HTTP or HTTPS over SSL	Intercepts web traffic and captures submitted forms

Tool	Direction	Endpoint	Port	Protocol	Notes
Login or Workflow Macro Recorders	To target host	localhost	Dynamic, 8081, or user-specified	HTTP or HTTPS over SSL	Records browser sessions for replay during scan
Web Discovery	OpenText DAST machine to targeted IP range	Target host network range	User-specified range	HTTP and HTTPS over SSL	Scanner for identifying rogue web applications hosted among the targeted scanned IP and port ranges Use to provide targets to OpenText DAST (manually)

WebInspect Software Development Kit (SDK)

The WebInspect SDK requires the following software:

- Visual Studio 2019 (version 16.9.0)
- Visual Studio 2022
- .NET Framework 4.8

Important! Visual Studio Express versions do not support third-party extensions. Therefore, these versions do not meet the software requirements to use the WebInspect SDK.

Acquiring OpenText DAST software

The OpenText DAST 64-bit package is available as an electronic download. For instructions on how to download the software from the Software Licenses and Downloads (SLD) portal, click **Contact Us / Self Help**to review the videos and the *Quick Start Guide*.

The OpenText DAST_64_<*version*>.zip includes the following:

- Installer
- About OpenText Application Security Software Documentation

Verifying software downloads

This topic describes how to verify the digital signature of the signed file that you downloaded from the Customer Support website. Verification ensures that the downloaded package has not been altered since it was signed and posted to the site. Before proceeding with verification, download the OpenText Application Security Software product files and their associated signature (`*.sig`) files. You are not required to verify the package to use the software, but your organization might require it for security reasons.

Preparing your system for digital signature verification

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.

To prepare your system for electronic media verification:

1. Go to the GnuPG website.
2. Download and install GnuPG Privacy Guard.
3. Generate a private key, as follows:
   a. Run the following command (on a Windows system, run the command without the $ prompt):
      ```
      $ gpg --gen-key
      ```
   b. When prompted for key type, select `DSA and Elgamal`.
   c. When prompted for a key size, select `2048`.
   d. When prompted for the length of time the key should be valid, select `key does not expire`.
   e. Answer the user identification questions and provide a passphrase to protect your private key.
4. Download the OpenText GPG public keys (compressed tar file) from https://mysupport.microfocus.com/documents/10180/0/MF_public_keys.tar.gz.
5. Extract the public keys.

   Tip: For environments lacking an Internet connection, you can find a copy of CodeSEAL's public key (`OT-package-sign-gpg-pub.key`) within the `Program Files` directory.
6. Import each downloaded key with GnuPG with the following command:

   ```
   gpg --import <path_to_key>/<key_file>
   ```

Chapter 3: Installing OpenText DAST

This chapter contains instructions on installing OpenText DAST.

Installation recommendation

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

Prerequisites

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

- .NET Framework
- SQL Server or SQL Server Express

For information about the supported versions of these software products and other system requirements, see the "System requirements" on page 17.

SQL Server database privileges

The account specified for the database connection must also be a database owner (DBO) for the named database. However, the account does not require sysadmin (SA) privileges for the database server. If the database administrator (DBA) did not generate the database for the specified user, then the account must also have the permission to create a database and to manipulate the security permissions. The DBA can rescind these permissions after OpenText DAST sets up the database, but the account must remain a DBO for that database.

About the installer files

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

- Dast64.exe – An executable file that launches an embedded Windows installer file
- Dast64.msi – A Windows installer file

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

Installation options

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

Using the Setup Wizard

Use the following procedure to install OpenText DAST using the Setup Wizard.

Note: After installing OpenText DAST, the program will auto launch and require that you license the product before continuing. For information on licensing OpenText DAST, see "Licensing with the License Wizard" on page 40.

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

   The Welcome to the OpenText DAST Setup Wizard window appears.
2. Click **Next.**

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

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

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

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

     The Sensor Configuration window appears.
5. Optionally, to install OpenText DAST as a sensor:
   a. In the **Configure DAST as a Sensor for this installation (optional)** area, select **Configure DAST as a WebInspect Enterprise Sensor**.
   b. Enter the **Enterprise Manager URL**, that is, the URL of Fortify WebInspect Enterprise manager.
   c. In the Sensor Authentication group, enter the following Windows account credentials for this sensor:
      - In the **User Name** box, type the sensor user name.
      - In the **Password** and **Confirm Password** boxes, type the password for the sensor user.

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

6. Click **Next**.

   The Ready to install OpenText DAST window appears.

7. Click **Install**.

   When the installation process is complete, the Completed the OpenText DAST Setup Wizard window appears.

8. Select **Launch OpenText DAST *<version>*** and click **Finish**.

   The Setup Wizard closes and OpenText DAST launches.

Using the msiexec program

You can install OpenText DASTusing the `msiexec` program from the command line interface (CLI) or with a script. After installing the product, you can license it from the CLI with the License Utility. For more information, see "Licensing with the License Utility" on page 45.

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

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

The following paragraphs provide details about these installation methods.

Normal installation

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

```
msiexec /I "<directory>:\Dast64.msi"
```

Replace *<directory>* with the location where the `Dast64.msi` file resides on your machine.

Reboot message suppression

If some files that need to be updated are in use during the installation, the installer prompts you that a reboot is required to complete the installation. Using the `msiexec` program, you can suppress these messages during the installation. To suppress reboot messages, type the following at the command line prompt or in a script:

```
msiexec /I "<directory>:\Dast64.msi" REBOOT=Suppress
```

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

Silent mode

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

```
msiexec /I "<directory>:\Dast64.msi" REBOOT=Suppress /qn
```

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

Synchronous installation

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

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

```
Start /wait msiexec /I "<directory>:\Dast64.msi" REBOOT=Suppress /qn
```

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

```
Start-Process -FilePath 'msiexec.exe' -ArgumentList @('/I', '<directory>:
   \Dast64.msi', 'REBOOT=Suppress', '/qn') -Wait
```

Using the WIConfig program

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

Important facts about WIConfig

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

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

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

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

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

Syntax

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

Parameters

The following table describes the optional parameters.

Parameter	Description

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

`/?`	Displays the help information.
`/AcceptUntrustedCerts`	Accepts untrusted SSL certificates and suppresses warnings. **Caution!** This option can be insecure. Use this option only with self-signed certificates from parties you trust.
`/CreateDatabase`	Creates the database specified by `SqlConnString` if the database does not exist. If the database exists and the schema is correct, this option will have no effect. If the database exists, but the schema is the wrong version, this command will fail.
`-DbSizeCheckInterval <number>`	Specifies the time interval in seconds at which the scan database file size should be checked.
`DbSizeLimitMB <number>`	Configures the file size limit in megabytes for the scan database.
`/DbSizeStopScan`	Stops a scan when the scan database file size has reached the configured limit.

Parameter	Description
`-DebrickedAccessToken`	Specifies the OpenText Core SCA access token to use for retrieving open source client-side library health metrics and correlated GitHub Security Advisory (GHSA) information from the OpenText Core SCA database. To disable OpenText Core SCA integration, run this parameter with empty double quotation marks ("") to remove the access token and return the configuration to the default state. For example: `WIConfig -DebrickedAccessToken ""`
`/DisableSmartUpdateOnStartup`	Prevents SmartUpdate from running automatically when OpenText DAST starts.
`/EnableAzureDatabaseSupport`	Enables support for Azure SQL database. For more information, see "Guidelines when using Azure SQL database" on page 36. **Tip:** After configuring support for Azure SQL database, you can add the connection to your OpenText DAST database configuration in the same way as a remote SQL Server. For more information, see the *OpenText™ Dynamic Application Security Testing User Guide*.
`/EnableJsonScanSettings`	Enables the composite scan settings feature. For experimental use only. For more information, see the *OpenText™ Dynamic Application Security Testing User Guide*.
`-FipsCompliance`	Enables/disables FIPS compliance. The value can be one of the following: `{enable|disable}`
`-LicenseFile`	Specifies the path to the OpenText license file.
`/LIMDeactivate`	Deactivates the LIM license.
`-LIMPassword`	Specifies the LIM pool password.

Parameter	Description
`-LIMPool`	Specifies the LIM pool name.
`-LIMUrl`	Specifies the LIM URL.
`-RCServerAuthType`	Specifies the OpenText DAST API Server authentication type. The value can be one of the following: `{None|Basic|NTLM|ClientCert}`
`-RCServerHost`	Specifies the hostname the OpenText DAST API Server should listen on. Use + for all.
`-RCServerPort`	Specifies the OpenText DAST API Server port to listen on.
`/RCServerUseHTTPS`	Runs the OpenText DAST API Server over HTTPS.
`-SqlConnString`	Specifies the SQL Server database connection string.
`/TryDBUpgrade`	Performs a remote SQL schema upgrade for the scan database.
`-TwoFAListenerAddress`	Internal use only.
`-TwoFAListenerPort`	Internal use only.
`-WIOASTServerAddress`	Specifies the OpenText DAST out-of-band application security testing (OAST) server address to configure local DNS service (for use in networks that lack an Internet connection).
`-WISECluster`	Internal use only.
`-WISEClusterAuthToken`	Internal use only.
`-WISEClusterMaxPoolSize`	Internal use only.

Required parameters to configure a sensor

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

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

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

Optional parameters to configure a sensor

The following table describes the optional parameters for configuring OpenText DAST as a sensor.

Parameter	Description
`-SensorServiceUsername`	Specifies the user account for the OpenText DAST Sensor Windows service. If no user name is provided, `LOCAL SYSTEM` will be used.
`-SensorServicePassword`	Specifies the password for the user account to be used for the OpenText DAST Sensor Windows service.
`-SensorID`	A GUID that indicates the sensor ID.
`-SensorProxyAddress`	Specifies the proxy address if required to access the Fortify WebInspect Enterprise server.
`-SensorProxyPort`	Specifies the proxy port if required to access the Fortify WebInspect Enterprise server.
`-SensorProxyUsername`	Specifies the proxy user name if required to access the Fortify WebInspect Enterprise server.
`-SensorProxyPassword`	Specifies the proxy password if required to access the Fortify WebInspect Enterprise server.

Parameter	Description
`-SensorSqlConnType`	Specifies the SQL connection type. The value can be one of the following: `{SQLServer|SQLExpress}` If this parameter is not provided, the connection type defined for OpenText DAST will be used. If this parameter is defined, validation will occur to ensure the connection.
`-SensorSqlConnString`	Specifies the SQL Server database connection string for the sensor. If none is provided, SQL Express will be used. The connection string must be in the standard format. Example: `Data Source=<server>;Initial Catalog=<database>;Integrated Security=False;User ID=<DB user>;Password=<password>;User Instance=False`

Guidelines when using Azure SQL database

Follow these guidelines when using Azure SQL database:

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

Recommended Process for Configuring Azure SQL Database

OpenText recommends using the following process to configure an Azure SQL database.

Stage	Description
1.	Run the following command only: `wiconfig /EnableAzureDatabaseSupport`
2.	Open OpenText DAST.

Stage	Description
3.	In OpenText DAST, configure the database connection and create a new database. For more information, see the *OpenText™ Dynamic Application Security Testing User Guide*.

Updating OpenText DAST

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

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

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

Directory structure

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

Purpose	Path	Comments
Installation Directory	`C:\Program Files\Fortify\Fortify WebInspect` **Note:** If you are updating from an earlier version, the default installation directory is `C:\Program Files\HP\HP WebInspect`	Can be set by the user during installation. SmartUpdate of full OpenText DAST version will override everything that exists in this directory. **Important!** When OpenText DAST is installed as a sensor for Fortify WebInspect Enterprise, you must use the default Destination Folder. Otherwise, SmartUpdates to the

Purpose	Path	Comments
		sensor will not work.
	<Installation Directory>\ ComplianceTemplates	Compliance template directory; can be modified by SmartUpdate.
	<Installation Directory>\Samples	Contains subdirectories for sample scans, and a login macro and a WSDL file for zero.webappsecurity.com.
	C:\ProgramData\HP\HP WebInspect	Subdirectories include Policies, Schedule, SecureBase database, Server Analyzer, Settings, and SupportChannel.
	C:\ProgramData\HP\Licenses\WebInspect	Licenses activated on the local machine.
	C:\ProgramData\HP\SmartUpdate	SmartUpdate directory where new patches are downloaded. Security checks are copied and inserted into the database; other artifacts are copied into installation directory (for example, Compliance Template).
Application Data Directory	**%localappdata%\HP** [1]	All data required for OpenText DAST that is not user-specific.
User Data Directory	**%localappdata%\HP\HP WebInspect** [1]	All data created by the user and not global for the application. Subdirectories include ComplianceTemplates, Exports, Logs, Plugins, Reporting, ScanData, and Tools.

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

Disclaimer

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

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

Chapter 4: Licensing OpenText DAST

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

Licensing with the License Wizard

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

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

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

Activating your software

You can activate OpenText DAST in one of the following ways:

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

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

To activate OpenText DAST:

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

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

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

3. Click **Next**.

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

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

If you chose **Connect to Fortify License and Infrastructure Manager**, the License Wizard displays the Concurrent License Activation window. Go to "Connect to LIM" on page 43.

Connect to OpenText

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

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

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

The Congratulations window appears and OpenText DAST is activated.

License file activation

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

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

Fortify activation

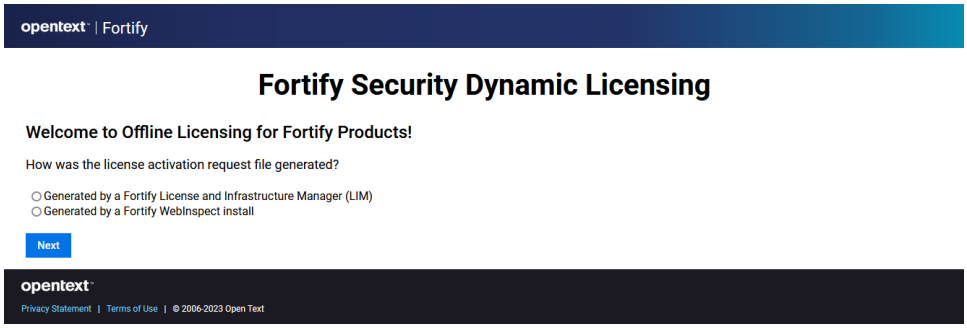
For this option, you must create a license request file containing information about the computer where OpenText DAST is installed. Then, using a separate Internet-connected computer, access a web site (https://licenseservice.fortify.microfocus.com/OfflineLicensing.aspx) to transmit the file to a server,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

To activate a license generated by the Fortify license server:

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

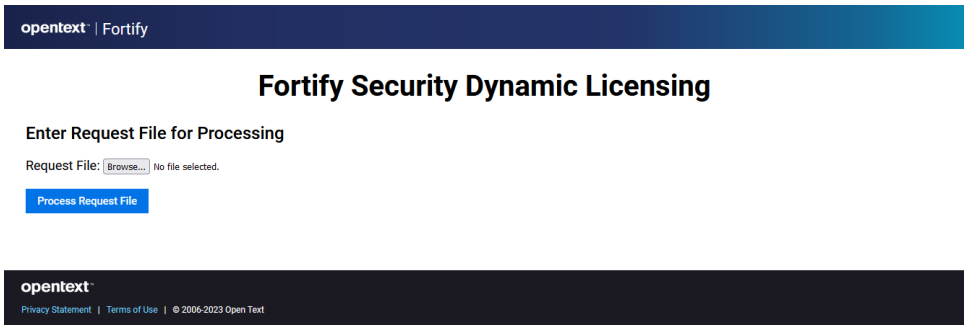
   Tip: Be sure to save this file to a portable device or in a location that is accessible by a machine that has access to the Internet.

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



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

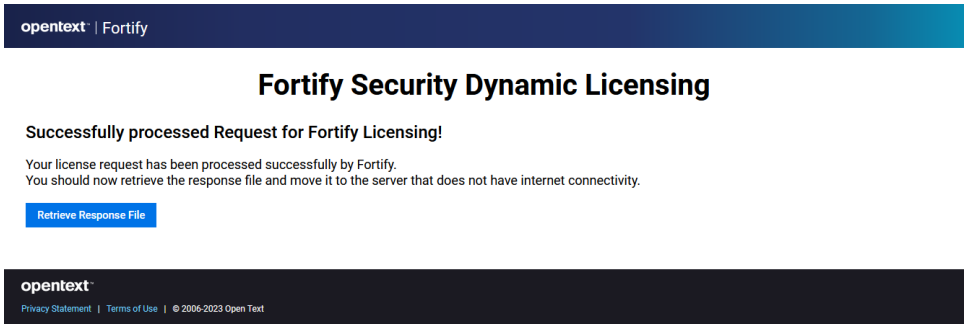
   The Enter Request File for Processing page appears.



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

9. Click **Process Request File**.

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



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

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

    This completes the licensing procedure.

Connect to LIM

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

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

To configure OpenText DAST to use the LIM:

1. In the **URL** field, type the URL of the LIM server in the format `https://<location>:<port>`, where *location* is IP address, hostname, or domain name.

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

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

These format examples use the https protocol. If SSL certificates are not used for the LIM, the protocol is http.

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

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

   This completes the licensing procedure.

License revocation

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

To regain a license if you use the LIM:

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

If necessary, contact Customer Support or your LIM administrator.

Licensing with the License Utility

If you installed OpenText DAST from the command line interface (CLI) or with a script using the `msiexec` program, you can use the `LicenseUtility.exe` application to license your product. The License Utility application is installed in the OpenText DAST installation directory. For more information, see "Directory structure" on page 37.

Syntax for named users

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

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

Syntax for concurrent users

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

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

Options

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

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

Option	Description	License Type
	domain\username to support a domain account.	
`-limPacFile`	Configures the proxy using a PAC file URL.	Concurrent User
`-limPool`	Specifies the LIM pool name. If used with the `-p`, `-limURL`, and `-limPswd` options, configures the product to use a LIM for licensing.	Concurrent User
`-limProxy`	Sets an explicit proxy using the format `user:password@host:port` or `user:password@ip:port`. **Tip:** The user can be passed in as `domain\username` to support a domain account.	Concurrent User
`-limPswd`	Specifies the LIM Pool password.	Concurrent User
`-limURL`	Specifies the LIM service URL.	Concurrent User
`-p`	Indicates the Fortify product you are licensing. If used alone, skips the product selection step.	Named User
`-serviceURL`	Specifies the OpenText Fortify License Service URL.	Named User
`-silent`	Suppresses all popups and answers 'no' to interactive prompts. See `-y` option for more information.	Both
`-token`	Specifies the Fortify Product Activation Token GUID. If used with the `-p` option, licenses the product and exits using the command line arguments.	Named User
`-topMost`	Places the application as the top window on the desktop.	Both
`-y`	When running in silent mode, answers 'yes' to interactive prompts.	Both

Configuring OpenText DAST to use the LIM

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

For existing (licensed) OpenText DAST installations

To configure OpenText DAST installations that are already licensed:

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

   The License Wizard appears.
5. In the **Licensing Method** group, click **Connect to Fortify License and Infrastructure Manager** and click **Next**.
6. In the **URL** field, type the URL of the LIM server in the format `https://<location>:<port>`, where *location* is IP address, hostname, or domain name.

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

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

   These format examples use the https protocol. If SSL certificates are not used for the LIM, the protocol is http.
7. In the **Pool Name** field, type the pool name from which to extract a license for this instance of OpenText DAST.
8. In the **Password** field, type the password that will allow access to the specified license pool.
9. If network authentication is required, select the **Network Authentication** check box, and in the **User Name** and **Password** fields, enter a valid user name and password.
10. Click **Next**.
11. Do one of the following:
    - To allow others to use this license when OpenText DAST closes, select **Concurrent License**.
    - To allow OpenText DAST to disconnect from the LIM for an extended period of time, select **Detached Lease** and enter an **Expiration Date**.
12. Click **Next**.
13. Click **Finish** and **OK**.

For new (unlicensed) OpenText DAST installations

To configure new OpenText DAST installations:

1. Start OpenText DAST.

   The License Wizard appears.
2. Select **Activate Now**.
3. In the **Licensing Method** group, click **Connect to Fortify License and Infrastructure Manager** and click **Next**.
4. In the **URL** field, type the URL of the LIM server in the format `https://<location>:<port>`, where *location* is IP address, hostname, or domain name.

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

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

   These format examples use the https protocol. If SSL certificates are not used for the LIM, the protocol is http.
5. In the **Pool Name** field, type the pool name from which to extract a license for this instance of OpenText DAST.
6. In the **Password** field, type the password that will allow access to the specified license pool.
7. If network authentication is required, select the **Network Authentication** check box, and in the **User Name** and **Password** fields, enter a valid user name and password.
8. Click **Next**.
9. Do one of the following:
   - To allow others to use this license when OpenText DAST closes, select **Concurrent License**.
   - To allow OpenText DAST to disconnect from the LIM for an extended period of time, select **Detached Lease** and enter an **Expiration Date**.
10. Click **Next**.
11. Click **Finish** and **OK**.

Chapter 5: The WebInspect SDK

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

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

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

Installation recommendation

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

For minimum requirements for installing and using the WebInspect SDK, see the "WebInspect Software Development Kit (SDK)" on page 25.

Installing the WebInspect SDK

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

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

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

To install the SDK where OpenText DAST is installed on the developer's machine:

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

To install the SDK where OpenText DAST is *not* installed on the developer's machine:

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

Verifying the installation

To verify that the extension was successfully installed:

1. In Visual Studio, select **Extensions > Manage Extensions**.

   Note: The Manage Extensions dialog (2019) and the Extension Manager tab (2022) do not initially open to the Installed section. You might need to browse to that section to view the installed extensions.

2. Scroll down the list of extensions.
   If you see WebInspect SDK in the list, the extension was installed successfully.

Send Documentation Feedback

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

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

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

Feedback on Installation Guide (Dynamic Application Security Testing 25.4.0)

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!