Micro Focus
Fortify ScanCentral DAST

Software Version: 23.1.0
Windows® and Linux

Configuration and Usage Guide

Document Release Date: June 2023
Software Release Date: May 2023

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 on June 05, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/application-security

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	Changes

23.1.0 / June 2023	Updated:
	• Settings file content to indicate which settings are required and which are optional and to provide an explanation of placeholder text used in setting samples. See "Creating and Using a Settings File" on page 55.
	• LIM settings samples to use `LIM.API` as `LimUrl`. See the following topics:
	  • "LIM Settings" on page 65
	  • "JSON Sample File" on page 79
	  • "YAML Sample File" on page 81
	• DAST API SSL and Utility Service SSL settings to indicate the type of certificate required. See "DAST API SSL Settings" on page 68 and "Utility Service SSL Settings" on page 71.
	• Proxy settings to indicate the comma separated list may contain wildcards and to add important requirement for the `ProxyBypassList` setting. See "Environment Settings" on page 73.
	• .NET SDK and ASP.NET Core Runtime version for sensor service. See "Using Fortify WebInspect with the Sensor Service" on page 103.

23.1.0	Added: • Setting for accessing the Debricked database. See "Client-side Library Analysis and Debricked Settings" on page 77. • Content for creating and using key stores. See "Understanding Key Stores" on page 327 and "Using Key Stores in Settings" on page 141. • Content for creating and using artifacts repositories. See "Understanding Artifacts Repositories" on page 334 and "Using Artifacts from a Repository in Settings" on page 143. • Content creating private data settings. See "Working with Private Data

Software Release / Document Version	Changes

	Settings" on page 324.
	
	Updated:
	
	• Settings files samples with Debricked settings. See "JSON Sample File" on page 79 and "YAML Sample File" on page 81.
	• Miscellaneous content with details about key stores. See the following topics:
	  • "Accessing Settings Configuration from Software Security Center" on page 140
	  • "Rescanning an Application" on page 210
	  • "Downloading DAST Scans, Settings, and Logs" on page 211
	  • "Accessing Base Settings in Software Security Center" on page 258
	• Architecture drawings and descriptions to include artifacts repository. See "What is ScanCentral DAST?" on page 36 and "ScanCentral DAST with Two-factor Authentication" on page 39.
	• Proxy Settings Bypass field to indicate semicolons separate list items rather than commas. See "Configuring Scan Priority" on page 173 and "Configuring Proxy Settings in Base Settings" on page 271.
	• Site tree description for API scan visualization. See "Working with the Site Tree" on page 214.
	• Content for configuring Postman scans with changes to validation and a new edit button; content for configuring Open API scans with important requirement for Open API definition file. See "Configuring an API Scan" on page 151 and "Configuring Base Settings for an API Scan" on page 265.
	• Application settings with private data settings. See "Understanding the Application Settings View" on page 296 and "Managing Application Settings" on page 297.
	• List of policies with description of the PCI DSS 4.0 policy. See "Policies" on page 363.

22.2.0 / January 2023	Added: • Description of intended audience and scope of document. See

Software Release / Document Version	Changes
	"Introduction" on page 36. • Procedures for using the Windows and Linux Configuration Tool CLI TAR files. See "Using the Windows TAR File" on page 85 and "Using the Linux TAR File" on page 87. Updated: • Configuration Tool version content in the checklist. See "Configuration Checklist" on page 42. • Information about using special characters in setting values. See "Creating and Using a Settings File" on page 55 and "Generating a Connection String" on page 95. • LIM settings with information regarding Linux sensors requiring the LIM REST API. See "LIM Settings" on page 65. • ScanCentral DAST Configuration Tool CLI overview with additional information about available versions. See "Using the Configuration Tool CLI" on page 83. • Logs troubleshooting content with details for Windows and Linux Configuration Tool CLI TAR files. See "DAST Configuration Tool CLI Logs" on page 342. Removed: • Procedure for Using the Configuration Tool CLI Docker Image.
22.2.0 / December 2022	Added: • Checklist to aid in installation preparation. See "Configuration Checklist" on page 42. • Information about applying updated settings to containers after using the Configuration Tool CLI with manage mode. See "Applying Updated Settings to Containers" on page 92. Updated: • Merged former requirements list into the recommendations list along with new content and renamed the list "Best Practices." See "Configuring the ScanCentral DAST Environment" on page 48. • RetainCompletedScans parameter description with important content

Software Release / Document Version	Changes
	related to scan database limit on Docker images. See "Miscellaneous DAST Settings" on page 59. • SSCRootUrl parameter description to advise not to include a trailing slash. See "SSC Settings" on page 61. • WebInspect on Docker information with direct link to the *Micro Focus Fortify WebInspect and OAST on Docker User Guide* on the Micro Focus Documentation web site. See "Using Fortify WebInspect on Docker" on page 103. Removed: • Procedure for installing the sensor into the Kubernetes cluster with wi-22.2.0.tgz. This file is no longer included in the download package. Helm charts are available on GitHub at https://github.com/fortify/helm3-charts.

22.2.0	Added:
	• Content related to API content and filters. See the following topics:
	  • "Configuring Scan Details" on page 166
	  • "Configuring API Content and Filters" on page 167
	  • "Understanding Parameter Type Matches" on page 171
	  • "Configuring Base Settings Details" on page 280
	  • "Configuring API Content and Filters in Base Settings" on page 281
	• Content related to Auto Scale Job Templates. See "Working with Auto Scale Job Templates" on page 233
	
	Updated:
	• ScanCentral DAST architecture with recommendation for LIM installation and information about Linux Docker images. See "What is ScanCentral DAST?" on page 36
	• Content related to Helm deployment with important statement about enabling the TTL-after-finished feature. See "Optional Helm Deployment Available" on page 48.
	• Supported Docker versions. See "Setting Up Docker" on page 54.

Software Release / Document Version	Changes

	• DAST API and Utility Service settings in the Configuration Tool CLI to include options for setting the containers' internal IP addresses and ports. See "DAST API Settings" on page 63 and "Utility Service Settings" on page 67.
	• Launch artifacts with descriptions of the bash scripts for Linux. See "Understanding the Launch Artifacts" on page 96.
	• Docker compose file content with procedure for Linux. See "Using the Compose File" on page 99.
	• Prerequisite software for installing the sensor service and example of installation where FIPS is enabled. See "Using Fortify WebInspect with the Sensor Service" on page 103.
	• API scan configuration content with GraphQL, gRPC, and SOAP API types. See the following topics:
	  • "Important Consideration About API Definition Files" on page 137
	  • "Configuring an API Scan" on page 151
	  • "Configuring Authentication for API Scans" on page 161
	  • "Configuring Base Settings for an API Scan" on page 265
	  • "Configuring Authentication in Base Settings for API Scans" on page 275
	• Sensor pool content with information about sensor auto scaling. See "Working with Sensor Pools" on page 227 and "Configuring Sensor Auto Scaling and Scan Scaling" on page 230.
	• Content related to tables with information about how to access new columns in a customized a table view. See "Managing Columns in Tables" on page 125.
	• Added Red Hat version of Two-factor Authentication server. See "ScanCentral DAST with Two-factor Authentication" on page 39 and "Running the 2FA Server" on page 304.
	• Content related to downloading DAST files with information about exporting settings files. See "Downloading DAST Scans, Settings, and Logs" on page 211.

22.1.0 /	Updated:

Software Release / Document Version	Changes
November 11, 2022	• Settings file samples to correct discrepancies and clarify setting descriptions. See the following topics: • "Database Settings" on page 56 • "DAST API Settings" on page 63 • "LIM Settings" on page 65 • "DAST API SSL Settings" on page 68 • "Utility Service SSL Settings" on page 71 • "SecureBase Settings" on page 76 • "JSON Sample File" on page 79 • "YAML Sample File" on page 81
22.1.0 / June 21, 2022	Updated: • Content related to the Configuration Tool CLI Docker image to provide more information about the TAR file and clarify information regarding the settings files. • Information related to log files when using the Configuration Tool CLI Docker image. See "Locating Log Files" on page 341.
22.1.0	Added: • Content related to container startup order and other prerequisites. See "Order of Orchestration" on page 53. • Content related to the Configuration Tool CLI. See "Creating and Using a Settings File" on page 55 and "Troubleshooting the Configuration Tool CLI" on page 343. • Content related to advanced settings. See "Using Advanced Settings in Scan Settings" on page 187 and "Using Advanced Settings in Base Settings" on page 292. • Content related to importing scans. See the following topics: • "Understanding the Scans View" on page 198 • "Managing the DAST Scans View" on page 207 • "Importing a Scan" on page 209

Software Release / Document Version	Changes

	• Content related to rescanning an application. See "Rescanning an Application" on page 210.
	• Content related to two-factor authentication. See the following topics:
	  • "ScanCentral DAST with Two-factor Authentication" on page 39
	  • "Understanding the Launch Artifacts" on page 96 (updated)
	  • "Working with Two-factor Authentication" on page 302
	• Content related to global restrictions. See "Working with Global Restrictions" on page 321.
	
	Updated:
	• Permissions content with new permission for managing global restrictions and restricted scan settings. See "Permissions in Fortify Software Security Center" on page 40.
	• Configuring scan settings and scan schedules with new application and application version search feature. See "Getting Started" on page 145 and "Managing Schedules" on page 244.
	• Scan status content with new Status Reason and Publish Status Reason. See "Understanding the Scans View" on page 198 and "Downloading DAST Scans, Settings, and Logs" on page 211.
	• Application settings content with global domain restrictions. See "Understanding the Application Settings View" on page 296 and "Managing Application Settings" on page 297.
	• Scan settings and base settings content with restricted editing of settings. See "Accessing Settings Configuration from Software Security Center" on page 140 and "Accessing Base Settings in Software Security Center" on page 258.
	• Workflow-driven scan content to include support for .har files. See "Configuring a Workflow-driven Scan" on page 148 and "Configuring Base Settings for a Workflow-driven Scan" on page 263.
	• FAST content with Linux Docker image version. See "Conducting an Automated Scan with FAST" on page 189 and "Using the FAST Linux Version" on page 193.
	• Request and response session details content with attack and vulnerability highlighting. See "Working with Findings" on page 218.

Software Release / Document Version	Changes
	• Sensors list table with new details for sensor Name and new Description column. See "Understanding the Sensors View" on page 224. • Scans list with description of application version link. See "Understanding the Scans View" on page 198. • List of policies with description of the Aggressive Log4Shell and OAST policies. See "Policies" on page 363. Removed: • Content related to the DAST Configuration Tool. (Links to removed content have been removed from the Change Log.)

21.2.0	Added:
	
	• Content describing tables and table preferences. See "Working with Tables" on page 124.
	• Content describing advanced filtering. See "Understanding Advanced Filters in Tables" on page 130 and "Using Advanced Filters in Tables" on page 131.
	• Content for redundant page detection in scan settings. See "Configuring Redundant Page Detection" on page 182 and "Configuring Redundant Page Detection in Base Settings" on page 290.
	• Content for SAST correlation in scan settings. See "Enabling SAST Correlation" on page 183 and "Enabling SAST Correlation in Base Settings" on page 291.
	• Content related to scan visualization. See the following topics:
	  • "Scan Visualization" on page 121
	  • "Viewing Scan Results" on page 214
	  • "Working with the Site Tree" on page 214
	  • "Understanding the Findings Table" on page 216
	  • "Working with Findings" on page 218
	  • "Understanding the Traffic Table" on page 219
	  • "Working with Traffic" on page 221

Software Release / Document Version	Changes

	• "Understanding SPA Coverage" on page 222
	• Content describing advanced scan prioritization. See "Understanding Advanced Scan Prioritization" on page 174.
	• Procedure for using a client certificate in a scan. See "Configuring Authentication for Standard and Workflow-driven Scans" on page 158.
	• HTTP status codes for reference. See "HTTP Status Codes" on page 368.
	
	Updated:
	• Configuration tool content with new upgrade and manage options. See the following topics:
	  • "Configuring the ScanCentral DAST Environment" on page 48
	  • "Upgrading ScanCentral DAST" on page 51
	  • Configuring the Database and Core Containers
	  • Configuring the Database Connection
	  • Initializing the Database
	  • Configuring DAST SSL
	  • Configuring Utility Service SSL
	  • Configuring Environment Settings
	  • Configuring ScanCentral DAST Settings
	  • Applying the Settings
	  • "Understanding the Launch Artifacts" on page 96
	• Database connection configuration with important information about when to specify the server port. See Configuring the Database Connection.
	• Miscellaneous content with procedures for using the table preferences panel. See the following:
	  • "Understanding Basic Filters in Tables" on page 127
	  • "Using Basic Filters in Tables" on page 127

Software Release / Document Version	Changes
	• "Sorting Data in Columns" on page 133 • "Viewing Content on Multiple Pages" on page 135 • Postman scanning information with known limitations for Postman variables. See "Scanning with a Postman Collection" on page 356. • FAST proxy content with important statement regarding where *not* to install the proxy. See "Conducting an Automated Scan with FAST" on page 189. • Scans list table description with Scan Id and new statuses related to scan priority. See "Understanding the Scans View" on page 198. • Scan detail panel description with Scan Id. See "Understanding the Scan Detail Panel" on page 203. • Application settings with SAST correlation. See "Managing Application Settings" on page 297. • Content related to managing the scans list with the force delete option. See "Managing the DAST Scans View" on page 207. • File types that can be downloaded with new scan statuses. See "Downloading DAST Scans, Settings, and Logs" on page 211. • Proxy settings content with note regarding Utility Service being automatically added to the proxy bypass list, and a known issue with using host name, machine name, and container name for proxy bypass. See Configuring Environment Settings. • Configuration tool content with important information about not retaining traffic files on sensor containers and option to disable advanced scan prioritization. See Configuring ScanCentral DAST Settings. • Procedures for generating certificates to indicate that certificate passwords are required. See Configuring DAST SSL and Configuring Utility Service SSL. • Target list and Type list with new options for exclusions. See "Creating and Managing Exclusions" on page 177. • Troubleshooting for proxy issue during configuration. See Troubleshooting the Configuration Tool. • Troubleshooting for redundant content alert. See "Troubleshooting Alerts" on page 351.

Software Release / Document Version	Changes
	• Troubleshooting for client certificates. See "Troubleshooting DAST Scans" on page 349. • DAST sensor service content with information regarding encrypted communication for the DAST API service. See "Using Fortify WebInspect with the Sensor Service" on page 103 and "Troubleshooting the Sensor Service" on page 354. • Summary page content to include the error messages dialog box in the Configuration Tool. See Applying the Settings.

Chapter 1: Introduction

Fortify ScanCentral DAST allows you to download and run a set of Docker containers, configure a connection with your instance of Fortify Software Security Center, and then configure and conduct dynamic scans of your web applications from Fortify Software Security Center.

Audience

This document is intended for users who have experience installing, configuring, and using Docker. Experience with Helm charts and Kubernetes is also recommended if those technologies will be used.

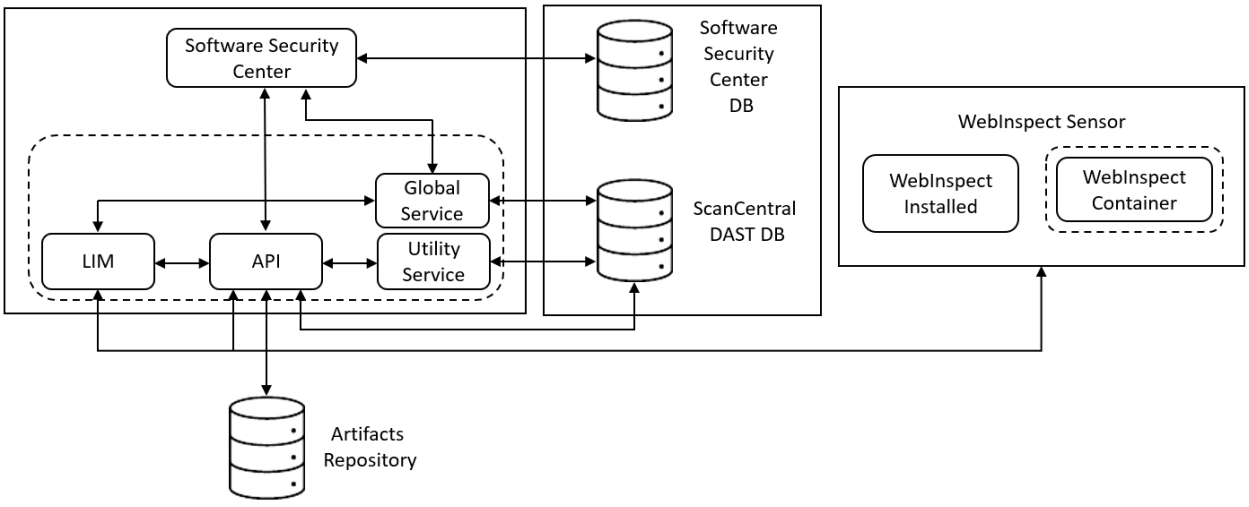
Documentation Scope

This document includes Fortify recommended best practices. Other options may be available, but the details for those options are not included in this document.

What is ScanCentral DAST?

Fortify ScanCentral DAST is a dynamic application security testing tool that is comprised of the Fortify WebInspect sensor service and other supporting technologies that you can use in conjunction with Fortify Software Security Center.

The following diagram illustrates the Fortify ScanCentral DAST architecture.



The following paragraphs describe these components in more detail.

Note: The version numbers included in the image names in this document are accurate at the time of publication. However, Docker images may be updated between releases. Refer to the Read Me file accompanying the image for information about the specific version.

Software Security Center

The Fortify Software Security Center user interface (UI) provides a way to view the DAST scans list, sensors list, sensor pools, settings, scan schedules, and scan results. You can also access the DAST Settings Configuration wizard from the UI.

ScanCentral DAST communicates with Fortify Software Security Center by way of the Software Security Center Rest API.

ScanCentral DAST retrieves Application and Version information and user permissions from the Fortify Software Security Center database. ScanCentral DAST uploads scans for triage to the database as FPR files.

LIM

The License and Infrastructure Manager (LIM) Docker image provides the licensing service for the ScanCentral DAST components. For more information about the LIM, see the *Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide*.

Note: The architecture diagram shows a LIM Docker container. However, you may use a LIM that is installed on an IIS server.

ScanCentral DAST API

The ScanCentral DAST REST API Docker image provides communication between the sensor and the ScanCentral DAST database. It also communicates with the LIM for licensing, and Fortify Software Security Center. It communicates with the Utility Service for Postman validation.

Optionally, it communicates with a configured artifacts repository to retrieve referenced artifacts to use in a scan.

The Windows image name is `scancentral-dast-api:23.1`. The Linux image name is `scancentral-dast-api:23.1.ubi.8`.

ScanCentral DAST Utility Service

The ScanCentral DAST Utility Service is the Fortify WebInspect image. However, it runs in a restricted mode and handles lightweight executable utilities without regard to whether a sensor is running and available. It provides support for Postman scans, creates scan settings, and imports scans to the DAST database.

The Windows image name is `webinspect:23.1` and the container name is `scancentral-dast-utilityservice`. The Linux image name is `dast-scanner:23.1.ubi.8`.

Important! Before you can run the Windows version of the DAST Utility Service container, you must install Microsoft update KB4561608 on the host machine. For more information, see https://support.microsoft.com/en-us/topic/june-9-2020-kb4561608-os-build-17763-1282-437af506-e3ef-a8a1-09e7-26cc94e509c7.

ScanCentral DAST Global Service

The ScanCentral DAST Global Service Docker image does the following:

- Communicates with the LIM to acquire a license
- Starts scans (including scheduled scans), manages scan prioritization, and builds the site tree for completed scans
- Communicates with the DAST database to insert, update, and select messages for the system, including scan statistics from the sensor
- Imports scan results to the Fortify Software Security Center database
- Performs additional background tasks, such as message queuing and processing deny intervals

Note: The ScanCentral DAST Global Service uses SmartUpdate to obtain the most recent SecureBase updates.

The Windows image name is `scancentral-dast-globalservice:23.1`. The Linux image name is `scancentral-dast-globalservice:23.1.ubi.8`.

ScanCentral DAST Database

The database stores configuration settings for ScanCentral DAST, as well as dynamic scan settings and dynamic scans. The DAST REST API and Global Service connect to the database on start up to retrieve configuration settings. The Utility Service imports scans to the DAST database.

WebInspect Sensor

The Fortify WebInspect sensor is a Docker image, Windows or Linux, or a Windows computer with both Fortify WebInspect and the ScanCentral DAST sensor service installed.

The Windows Docker image includes the full version of Fortify WebInspect 23.1.0 software. The Linux Docker image is available for the Red Hat Linux distribution and is comprised of the following components:

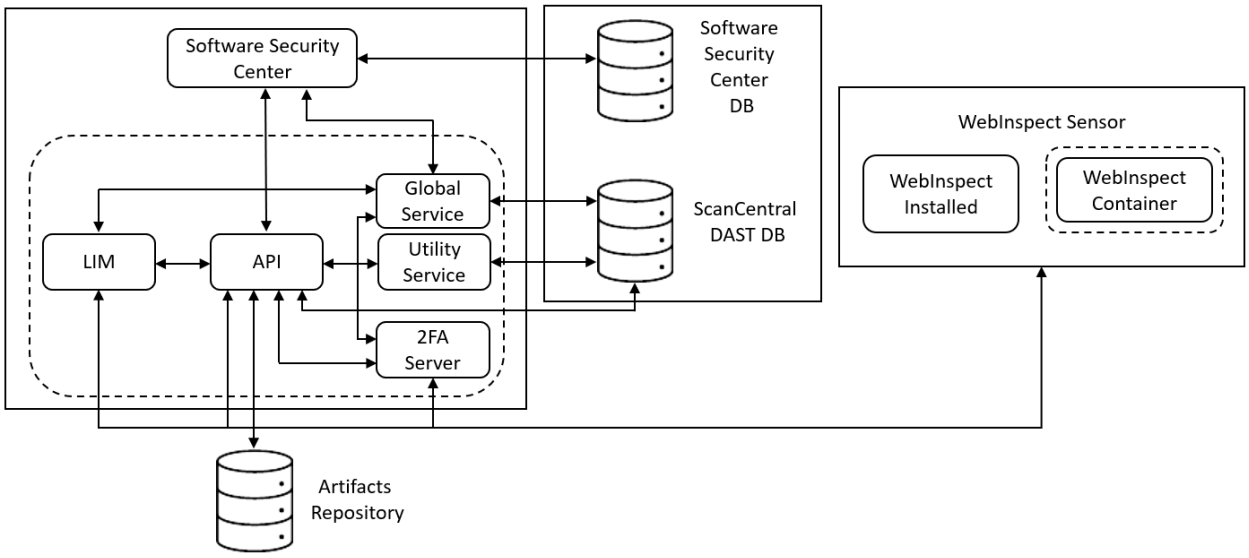
- wi application for scan logic (also called a scanner)
- Database for scan data
- WebInspect script engine (WISE) for JavaScript execution and Web Macro Recorder macro playbacks
- 2FA server to synchronize two-factor authentication requests (used only if the scan is configured to playback a two-factor authentication login macro)

The sensor does the following:

- Starts and runs scans
- Reports scan statistics to the DAST database by way of the API; the Global Service retrieves and processes statistics from the database
- Uploads the scan to the API

ScanCentral DAST with Two-factor Authentication

The following diagram illustrates the Fortify ScanCentral DAST architecture when the optional two-factor authentication server is deployed.



DAST 2FA Server

The ScanCentral DAST 2FA Server Docker image provides support for scans that require two-factor authentication. The 2FA Server container communicates with the following components:

- DAST API to generate the QR code used to register a mobile phone for two-factor authentication
- Global Service to indicate that the 2FA Server is up and running
- Fortify WebInspect sensor to process two-factor authentication requests and responses

Installation Recommendation

Fortify recommends that you run the 2FA Server on a host or VM that is separate from any other ScanCentral DAST component—DAST API, DAST Global Service, DAST Utility Service, or DAST sensor.

2FA Server Versions

The image is available for both Windows and Linux operating systems. The image names are as follows:

- Windows – `fortify-2fa:23.1.nanoserver.1809`
- Red Hat Linux – `fortify-2fa:23.1.ubi.8`

Permissions in Fortify Software Security Center

The permissions designated by your user role in Fortify Software Security Center determine the types of tasks that you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and global features such as deny windows and base settings. The following table describes the predefined roles in Fortify Software Security Center that allow dynamic-related tasks.

ScanCentral DAST Tasks	Application Security Tester	Developer	Manager	Security Lead	View-only
Manage pools and sensors			x	x	
View data	x	x	x	x	x
Create, run, change, and delete scans, schedules, and settings	x			x	
Run scans from existing templates and base settings	x	x		x	
Download artifacts (settings, scans, and logs)	x	x		x	
Manage deny intervals, application priority level, and retention policy				x	
Manage global restrictions, restricted scan settings, and private data settings				x	
Manage key stores and artifacts repositories				x	

For information about creating custom user roles, see the *Micro Focus Fortify Software Security Center User Guide*.

Tasks Requiring Admin Permissions

The following ScanCentral DAST tasks require Fortify Software Security Center administrator-level privileges (with the **Universal access** option):

- Creating and maintaining custom policies
- Creating and maintaining base settings
- Force deleting scans from the ScanCentral DAST database

Configuration Checklist

The Fortify ScanCentral DAST environment includes multiple components that you must configure in a settings file as part of the installation process. The following checklist is provided to aid you in configuring these settings.

Component	Selection
What is the installation environment?	☐ Amazon Web Services (AWS) ☐ Azure ☐ Google Cloud Platform ☐ Local
Which deployment method will you use?	☐ Docker Compose ☐ Kubernetes / Helm Chart ☐ Standalone Containers ☐ Other (Not Recommended): _____
Which operating system will the containers use?	☐ Linux (Red Hat) ☐ Windows
Does your environment use SSL certificates? If yes, the certificate is located at: _____ If yes, is the certificate self-signed? ☐ Yes ☐ No	☐ Yes ☐ No
Which Configuration Tool version will you use? The .tar file is recommended for initial installations and upgrades. The CLI executable is recommended for managing an existing environment.	☐ .tar File ☐ CLI Executable ☐ Docker Hub Image
Which type of configuration file will you use?	☐ json ☐ yaml
Which type of SQL database will you use? Database server name or IP address: _____	☐ AmazonRdsPostgreSQL ☐ AmazonRdsSQLServer ☐ AzurePostgreSQL ☐ AzureSQLServer ☐ PostgreSQL ☐ SQLServer

Component	Selection
Do you want to allow the Global Service to move a scan to a different sensor? For more information, see "Miscellaneous DAST Settings" on page 59.	☐ Yes / DisableAdvancedScanPrioritization = false ☐ No / DisableAdvancedScanPrioritization = true
Do you want to save scans in the sensor container after uploading to the DAST database? For more information, see "Miscellaneous DAST Settings" on page 59.	☐ Yes / RetainCompletedScans = true ☐ No / RetainCompletedScans = false
Do you want to enable global restrictions? For more information, see "Miscellaneous DAST Settings" on page 59.	☐ Yes / EnableRestrictedScanSettings = true ☐ No / EnableRestrictedScanSettings = false
Do you want to disable all origins for Cross-Origin Resource Sharing (CORS) policy? For more information, see "DAST API Settings" on page 63.	☐ Yes / DisableCorsOrigins = true ☐ No / DisableCorsOrigins = false
Do you want to allow ScanCentral DAST components to accept self-signed (untrusted) certificates when communicating with other Fortify products? For more information, see "Environment Settings" on page 73.	☐ Yes / AllowNontrustedServerCertificates = true ☐ No / AllowNontrustedServerCertificates = false
Is a proxy required for communications in your ScanCentral DAST environment? For more information, see "Environment Settings" on page 73.	☐ Yes / UseProxy = true ☐ No / UseProxy = false
Do you want to update SecureBase after installation? For more information, see "SecureBase Settings" on page 76.	☐ Yes / ApplySecureBase = true ☐ No / ApplySecureBase = false

Related Documents

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

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

All Products

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

Document / File Name	Description
About Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral DAST

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

Document / File Name	Description
Fortify ScanCentral DAST Configuration and Usage Guide SC_DAST_Guide_<*version*>.pdf	This document provides information about how to configure and use Fortify ScanCentral DAST to conduct dynamic scans of Web applications.

Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, this document is available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Fortify Software Security Center User Guide SSC_Guide_<*version*>.pdf	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use Software Security Center. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project.

Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
Fortify WebInspect Installation Guide	This document provides an overview of Fortify

Document / File Name	Description
WI_Install_<*version*>.pdf	WebInspect and instructions for installing Fortify WebInspect and activating the product license.
Fortify WebInspect User Guide WI_Guide_<*version*>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
Fortify WebInspect and OAST on Docker User Guide WI_Docker_Guide_<*version*>.pdf	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.
Fortify WebInspect Agent Installation Guide WI_Agent_Install_<*version*>.pdf	This document describes how to install the Fortify WebInspect Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a

Document / File Name	Description
	supported version of IIS.
Fortify WebInspect Agent Rulepack Kit Guide WI_Agent_Rulepack_Guide_<*version*>.pdf	This document describes the detection capabilities of Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Chapter 2: Configuring the ScanCentral DAST Environment

This chapter provides the information you need to install and subsequently manage a ScanCentral DAST environment.

Optional Helm Deployment Available

This document contains processes and procedures for manually configuring the ScanCentral DAST components without using Helm or with minimal integration with Kubernetes for scan scaling. To use Kubernetes for complete ScanCentral DAST container orchestration, Helm deployment is available on GitHub at https://github.com/fortify/helm3-charts.

Important! When using Helm deployment, ensure that the TTL-after-finished feature is enabled (`TTLAfterFinished=true`) in your Kubernetes cluster. This feature provides automatic clean-up of finished jobs. If this feature is not enabled, Kubernetes cluster jobs and pods lists can quickly become cluttered.

Installation Best Practices

Docker container configuration is complex and each environment is unique. Fortify makes the following recommendations as a best practice:

- Install and manage the DAST API, DAST Global Service, and DAST Utility Service containers on a VM, and each Fortify WebInspect sensor service on its own, separate VM.
- Do not mix operating systems for the DAST API, DAST Global Service, and DAST Utility Service containers. Select either Windows or Linux.
- Run the LIM on a host or VM that is separate from any other ScanCentral DAST component—DAST API, DAST Global Service, DAST Utility Service, or DAST sensor.
- Run the 2FA Server on a host or VM that is separate from any other ScanCentral DAST component—DAST API, DAST Global Service, DAST Utility Service, or DAST sensor.

Important Information about SSL

You can deploy both Fortify Software Security Center and ScanCentral DAST without SSL. However, Fortify recommends that you deploy both Fortify Software Security Center and ScanCentral DAST with SSL.

You cannot deploy Fortify Software Security Center with a certificate authority (CA) certificate and ScanCentral DAST without a certificate and vice versa. Mixing secure and non-secure content is not supported.

You cannot use a CA certificate for Fortify Software Security Center and a self-signed certificate for ScanCentral DAST. Mixing self-signed and trusted CA certificates is not supported.

Requesting Access to Fortify Docker Repository

Access to the Fortify Docker repository requires credentials and is granted through your Docker ID. To access the Fortify Docker repository, email your Docker ID to fortifydocker@microfocus.com.

Before You Begin

Ensure that you have met the following prerequisites before you begin configuring your Fortify ScanCentral DAST components:

- You must have a Fortify License and Infrastructure Manager (LIM) container downloaded, configured, and running in your environment or have a LIM installed on an IIS server.
  - The LIM must be accessible to the network where your VMs will be running Fortify ScanCentral DAST components.
  - You must know the LIM URL and LIM user credentials to configure licensing for Fortify ScanCentral DAST.
- You must know the Fortify Software Security Center URL and user credentials to connect Fortify ScanCentral DAST to Fortify Software Security Center.
- You must have a database installed and accessible to the VMs on which you install your Fortify ScanCentral DAST environment and to your instance of Fortify Software Security Center.

Understanding the Installation Process

The following table describes the process you must use to install and configure the Fortify ScanCentral DAST environment.

Stage	Description
1.	Receive the following licenses from Micro Focus: • Fortify ScanCentral DAST Server License (server-type license) • Fortify WebInspect Concurrent License
2.	Do the following:

Stage	Description
	1. Install a License and Infrastructure Manager (LIM) from the Docker Hub or by using the MSI. 2. Add the licenses received in Stage 1 to the LIM. For information about how to install the LIM and add licenses, see the *Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide*.
3.	Do the following: 1. Download and deploy Fortify Software Security Center 23.1.0 from the Micro Focus Software License and Downloads (SLD) portal. 2. Create user accounts for users who will access Fortify ScanCentral DAST. For information about how to install and configure Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.
4.	Set up Docker on the host that will run the core ScanCentral DAST containers (DAST API, DAST Global Service, and DAST Utility Service). For more information, see "Setting Up Docker" on page 54.
5.	Download the ScanCentral DAST 23.1.0 package from the Micro Focus SLD portal.
6.	Create a JSON or YAML DAST configuration settings file. **Tip:** You can edit one of the two sample settings files that are included in the Configuration Tool CLI download package. For more information, see "Creating and Using a Settings File" on page 55.
7.	Use the ScanCentral DAST Configuration Tool CLI to do the following: • Configure and initialize the ScanCentral DAST database. • Configure the settings that are used by the ScanCentral DAST API, DAST Global Service, and DAST Utility Service, and then generate compose files, PowerShell scripts for Windows, and shell scripts for Linux. For more information, see "Using the Configuration Tool CLI" on page 83.
8.	Use a compose file, PowerShell script, or shell script to pull and launch the core ScanCentral DAST 23.1.0 containers (DAST API, DAST Global Service, and DAST Utility Service). For more information, see "Understanding the Launch Artifacts" on page 96.

Stage	Description

9.	Log in to Fortify Software Security Center and enable ScanCentral DAST in the ADMINISTRATION view.
	
	Important! You must provide the ScanCentral DAST server URL to the Fortify Software Security Center administrator. The URL should be similar to the following:
	
	`https://<DAST_API_Hostname>:<Port>/api/`
	
	`https://<DAST_API_IP_Address>:<Port>/api/`
	
	Make sure that you include the trailing `/api/` in the URL.
	
	The URL can use the `http` protocol instead.
	
	For more information, see the *Micro Focus Fortify Software Security Center User Guide*.

10.	Deploy the Fortify WebInspect on Docker container or deploy classic Fortify WebInspect with the sensor service. For more information, see "Using Fortify WebInspect on Docker" on page 103 or "Using Fortify WebInspect with the Sensor Service" on page 103.

Tip: If you plan to conduct scans using two-factor authentication, see "Working with Two-factor Authentication" on page 302 for information about getting and configuring the 2FA Server Docker image.

Upgrading ScanCentral DAST

After initial installation and configuration of the Fortify ScanCentral DAST environment, you may need to upgrade the environment. The upgrade process is similar to the installation process. As part of the installation process, however, you will already have received licenses and setup LIM, Fortify Software Security Center, and Docker.

The following table describes the upgrade process.

Stage	Description
1.	Download the ScanCentral DAST 23.1.0 package from the Micro Focus Software License and Downloads (SLD) portal.
2.	Edit your JSON or YAML DAST configuration settings file with necessary changes. For more information, see "Creating and Using a Settings File" on page 55.

Stage	Description
3.	Use the ScanCentral DAST Configuration Tool CLI 23.1.0 to do the following: • Configure the ScanCentral DAST database with the latest database schema, if applicable. • Configure the settings that are used by the ScanCentral DAST API, DAST Global Service, and DAST Utility Service, and then generate compose files, PowerShell scripts for Windows, and shell scripts for Linux.
4.	Use a compose file, PowerShell script, or shell script to pull and launch the core ScanCentral DAST 23.1.0 containers (DAST API, DAST Global Service, and DAST Utility Service). For more information, see "Understanding the Launch Artifacts" on page 96.

Requirements for Upgrading

When upgrading your ScanCentral DAST environment, follow these requirements:

- Use the ScanCentral DAST Configuration Tool CLI that is packaged with the version of ScanCentral DAST software that you downloaded. Do *not* use a previous version of the tool.
- Upgrade your Fortify Software Security Center to the current compatible version. For version compatibility, see "Software Integrations for Fortify ScanCentral DAST" in the *Micro Focus Fortify Software System Requirements*.
- Upgrade all ScanCentral DAST components, including the DAST database, DAST API container, DAST Global Service container, DAST Utility Service container, and the Fortify WebInspect on Docker image or the classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service.

Recommendation for Upgrading

Fortify recommends that you stop all ScanCentral DAST containers and services before upgrading your environment. Many settings that you configure in the ScanCentral DAST Configuration Tool CLI are applied immediately to the database when the `configureEnvironment` command is run. These changes, however, are not recognized by containers that have not been upgraded. If stopping containers and services is not possible because scans are running, then you must upgrade those containers later for any database changes to be recognized.

Effect of Upgrades on Scheduled Scans

When upgrading your DAST environment, you cannot upgrade existing containers. You can only create new containers based on updated images.

When you create a new Fortify WebInspect sensor container with an updated Fortify WebInspect on Docker image, any scheduled scans that were assigned to the sensor and configured with the **Use this sensor only** option will not start on the new container. You must edit the scheduled scan settings to use the new sensor container.

Order of Orchestration

For proper operation of the ScanCentral DAST environment, some of the components must be started in a specific order or with specific prerequisites. Limited functionality can result when prerequisite components are not running and accessible. The following paragraphs describe these prerequisites.

ScanCentral DAST Database

The ScanCentral DAST database must be up and running, and the ScanCentral DAST Configuration Tool CLI must have been run prior to any other containers being started.

Tip: You may use an init container—a specialized container that runs before application containers in Kubernetes—to ensure that the database is up and running. Init containers contain utilities or setup scripts that are not included in an application image.

ScanCentral DAST API

The ScanCentral DAST database must be available to start the ScanCentral DAST API container. If no database is available, then the API service will stop.

If Fortify Software Security Center is not running, then you cannot use the DAST API even though the container is running. ScanCentral DAST must get an authentication token, validate permissions, validate application access, and so forth from Fortify Software Security Center.

If the ScanCentral DAST Utility Service is not running, then the following features will not work in the DAST API:

- Validating Postman collections
- Importing scans
- Converting `.burp` and `.har` files to `.webmacro` files

ScanCentral DAST Utility Service

The ScanCentral DAST database must be available to start the ScanCentral DAST Utility Service container. If no database is available, then the Utility Service will stop.

Postman validation is initiated by the DAST API. If the DAST API is not running, then the DAST Utility Service will not receive a request for validation.

Scan import is initiated by way of the DAST user interface or DAST API, and the DAST API is required to complete the import process. If the DAST API is not available after a scan import begins, then the scan import will fail.

Converting a `.burp` or `.har` file to a `.webmacro` file is initiated in the DAST user interface (which calls the DAST API) or in the DAST API directly. After the file is converted, it is returned to the DAST API. If the DAST API is not running, this process cannot be started.

ScanCentral DAST Global Service

The ScanCentral DAST database must be available to start the ScanCentral DAST Global Service container. If no database is available, then the Global Service will stop.

If Fortify Software Security Center is not running, then certain backend process will fail and prevent syncing data with Fortify Software Security Center.

ScanCentral DAST Sensor Service

The ScanCentral DAST API must be running and available to start the Sensor Service. If the DAST API is not available during start up, then the Sensor Service will try to connect every 10 seconds until it is able to connect.

Setting Up Docker

Before you can run Docker containers, you must set up Docker on the host that will run the containers. Set up Docker according to the process described in the following table.

Stage	Description
1.	Download and install the appropriate Docker version on the host machine. **Note:** Follow Docker recommendations for the Docker engine version to use for Windows and Red Hat Enterprise Linux (RHEL) 8.x x86_64 host operating systems.
2.	Optionally, if you plan to use a compose file to pull and run the core ScanCentral DAST containers (DAST API, DAST Global Service, and DAST Utility Service), download and install Docker Compose (for Windows) or Compose on Linux.
3.	Configure your machine for Docker containers.
4.	Register and start the Docker service.

For Docker documentation, see https://docs.docker.com/.

Creating and Using a Settings File

You can use the Configuration Tool CLI to generate a settings file from an existing ScanCentral DAST environment. For more information, see "Exporting an Existing Settings File" on page 89. You can also create a settings file or edit an existing settings file by hand, and then use the file with the Configuration Tool CLI to create or maintain an environment.

For the `new`, `upgrade`, and `autodeploy` modes, you must provide all of the settings in the settings file. For the `manage` mode, you must provide only the setting or settings that you are managing. For example, if you want to change your Fortify Software Security Center URL, then you need to provide only the SSC settings. For more information about these modes, see "Configuring the Environment" on page 91.

Note: The settings contents in this section appear in the order in which the settings appear by default in the sample settings file.

Using Special Characters in YAML Files

When using a YAML settings file, enclose in double quotation marks (") any value that includes one or more of the following special characters:

:, {, }, [,], ,, &, *, #, ?, |, -, <, >, =, !, %, @, \, `

Placeholder Text in Setting Samples

The sample settings in this document use placeholder text to help illustrate the types of information needed in the settings. Placeholder text is encapsulated with angle brackets (<>), such as "*<directory_path>*", *<ip_address>*, and '*<string>*'. Your settings file should not include any placeholder text. You must replace the placeholder text with values that are specific for your environment. If the setting is not applicable to your environment, then provide empty quotes rather than the placeholder text.

For example, if your proxy settings do not require a username and password, then change the placeholder text in the settings from this:

```
proxyUserName: '<string>'
proxyPassword: '<string>'
```

To this:

```
proxyUserName: ''
proxyPassword: ''
```

Database Settings

Use the database settings to configure connections to an existing database or create a new database with the information you provide.

Important! To avoid automatically upgrading the database schema when you are managing an existing DAST environment, the Configuration Tool CLI checks to see if the database schema is up to date. If the schema is not up to date, the Configuration Tool CLI stops executing and writes a warning to the log file.

Configuring a DBO-level Account

You must configure a connection to the database using an existing database owner (DBO) server-level account that has full access to the database. DBO access is required to create the schema on the database server. Ensure that the following permissions requirements are met:

- If you are creating a new database, the DBO account must have the `CREATE ANY DATABASE` server-level permission.
- If you are managing or updating an existing database, the DBO account must be a member of the `db_owner` database-level role.
- If available, the DBO account may use the `dbcreator` server-level role in lieu of the previously mentioned permission and role.

  Note: The `dbcreator` role is not available in the Amazon Relational Database Service (Amazon RDS).

- If you are creating a login, the DBO account must have the `ALTER ANY LOGIN` permission, which is part of the `securityadmin` server-level role. To give the new login access to a database, the account must have the `ALTER ANY USER` permission.

Configuring a Standard Account

You must configure a standard user account for everyday use, preferably with non-DBO credentials. This account must have one of the following sets of permissions:

- Both the `db_datareader` and `db_datawriter` database-level roles
- All of the `SELECT`, `INSERT`, `UPDATE`, and `DELETE` privileges on the database

JSON Example

The following example shows the database settings in a JSON file.

```
"DatabaseSettings":{
       "DatabaseProvider": "<database_type>",
       "Server": "<ip_address>,<port>",
       "Database": "<database_name>",
```

```
        "DboLevelDatabaseAccount":{
              "Username": "<string>",
              "Password": "<string>",
              "UseWindowsAuthentication": false
              "AdditionalConnectionProperties": null
        },
        "StandardDatabaseAccount":{
              "Username": "<string>",
              "Password": "<string>",
              "CreateLogin": false,
              "AdditionalConnectionProperties": null
        }
      }
```

YAML Example

The following example shows the database settings in a YAML file.

```
databaseSettings:
  databaseProvider: <database_type>
  server: <ip_address>,<port>
  database: <database_name>
  dboLevelDatabaseAccount:
    username: <string>
    password: <string>
    useWindowsAuthentication: false
    additionalConnectionProperties: null
  standardDatabaseAccount:
    username: <string>
    password: <string>
    createLogin: false
    additionalConnectionProperties: null
```

Parameter Descriptions

The following table describes the parameters for the database settings.

Parameter	Description
`DatabaseProvider`	Required setting that identifies the type of SQL database being used. Valid providers are: • `SQLServer`

Parameter	Description
	• `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`Server`	Required setting that specifies the database server name or the server IP address. **Important!** If SQL Server Browser is not running and you are using a port other than 1433, then you must also specify the port. Use the following format: *<server_name>,<port>* *<ip_address>,<port>* Note that a comma separates the values.
`Database`	Optional setting that specifies the name of the database. If you are upgrading or managing an existing DAST environment, then you must use an existing database. **Caution!** An existing database might be upgraded during this process. Be sure to create a backup of the existing database before proceeding.
`DboLevelDatabaseAccount`	Optional setting that specifies the database owner (DBO) server-level account that has full access to the database. You must provide the following parameters: • `Username` – Indicates the DBO account user name • `Password` – Indicates the DBO account password • `UseWindowsAuthentication` – Uses the credentials of the user who is currently logged into Windows Options are `true` or `false`. If set to `true`, then

Parameter	Description
	`Username` and `Password` are not required.
`StandardDatabaseAccount`	Required setting that specifies the standard user account for everyday use, preferably with non-DBO credentials. This account should have select, insert, update, and delete functions, but should not be able to create tables and so forth. **Tip:** You may use the same credentials as the DBO-level account. However, it is generally considered a safer option to provide limited access for general use after the schema has been created. You must provide the following parameters: • `Username` – Indicates the database account user name • `Password` – Indicates the database account password • `CreateLogin` – Creates a login for the standard user to connect to the database Options are `true` or `false`. If set to `false`, no changes will be made to the login or user account.
`AdditionalConnectionProperties`	Optional setting that specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information on additional connection properties, refer to your SQL database documentation.

Miscellaneous DAST Settings

You can specify ScanCentral DAST settings for licensing and SmartUpdate, as well as other miscellaneous settings.

JSON Example

The following example shows these settings in a JSON file.

```
{
     "RetainCompletedScans": false,
     "DisableAdvancedScanPrioritization": false,
     "EnableRestrictedScanSettings": false,
     "ServiceToken": "<string>",
     "SmartUpdateSettings": {
       "SmartUpdateUrl": "https://smartupdate.fortify.microfocus.com/",
       "LicensingUrl": "https://licenseservice.fortify.microfocus.com/"
     },
```

YAML Example

The following example shows these settings in a YAML file.

```
retainCompletedScans: false
disableAdvancedScanPrioritization: false
enableRestrictedScanSettings: false
serviceToken: <string>
smartUpdateSettings:
  smartUpdateUrl: https://smartupdate.fortify.microfocus.com/
  licensingUrl: https://licenseservice.fortify.microfocus.com/
```

Parameter Descriptions

The following table describes the parameters for the miscellaneous settings.

Parameter	Description
`DisableAdvancedScan Prioritization`	Optional setting prevents or allows the Global Service to move a scan to a different sensor, depending on the scan priority and other settings. By default, advanced scan prioritization is allowed. Options are `true` or `false`. For more information, see "Understanding Advanced Scan Prioritization" on page 174.
`RetainCompletedScans`	Optional setting specifies whether to save scans in the sensor container. By default, scans are not saved in the sensor container after the sensor completes the scan and uploads the data to the DAST database. Options are `true` or `false`.

Parameter	Description
	Important! SQL Server Express is the default database for the Fortify WebInspect Docker images. There is a 10 GB scan database limit.
`EnableRestrictedScanSettings`	Optional setting enables or disables global restrictions. Options are `true` or `false`. For more information, see "Working with Global Restrictions" on page 321.
`ServiceToken`	Required setting specifies a shared secret for all of your sensors to use to authenticate with the ScanCentral DAST API. The setting is a string with a minimum of 10 characters. The value is encrypted.
`SmartUpdateUrl`	Required setting indicates the URL for the SmartUpdate service. This setting is an element of `SmartUpdateSettings`. The default URL is `https://smartupdate.fortify.microfocus.com/`.
`LicensingUrl`	Required setting indicates the URL for the licensing service. This setting is an element of `SmartUpdateSettings`. The default URL is `https://licenseservice.fortify.microfocus.com/`.

SSC Settings

You can use the SSC settings to configure the connection between Fortify ScanCentral DAST and Fortify Software Security Center.

JSON Example

The following example shows the SSC settings in a JSON file.

```
  "SSCSettings": {
       "SSCRootUrl": "http://<ip_address>:<port>/ssc",
       "ServiceAccountUserName": "<username>",
```

```
      "ServiceAccountPassword": "<password>"
    },
```

YAML Example

The following example shows the SSC settings in a YAML file.

```
sSCSettings:
  sSCRootUrl: http://<hostname>:<port>/ssc
  serviceAccountUserName: <username>
  serviceAccountPassword: <password>
```

Parameter Descriptions

The following table describes the parameters for the SSC settings.

Parameter	Description
`SSCRootUrl`	Required setting that specifies the URL for your Fortify Software Security Center application. **Important!** You cannot use localhost for the Software Security Center URL. You must use a routable IP address or hostname. Additionally, do not use a trailing slash (`/`) at the end of the URL.
`ServiceAccountUserName`	Required setting that identifies the user name under which Fortify ScanCentral DAST will communicate with Fortify Software Security Center. **Important!** This account must be an Admin account that can perform service-level functions. Individual users who log into Fortify Software Security Center in a browser to use Fortify ScanCentral DAST are restricted based on the permissions designated by their user role in Fortify Software Security Center. For more information, see "Permissions in Fortify Software Security Center" on page 40.
`ServiceAccountPassword`	Required setting that identifies the password for the service account.

Parameter	Description
	Tip: Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93.

DAST API Settings

You can use the DAST API settings to configure the URL for the DAST API and configure cross-origin resource sharing (CORS) settings.

JSON Example

The following example shows the DAST API settings in a JSON file.

```
  "DASTApiSettings": {
       "RootUrl": "http://<hostname>:<port>",
       "DisableCorsOrigins": true,
       "CorsOrigins": [
         "http://<hostname>:<port>",
         "http://<hostname>:<port>",
         "http://<ip_address>:<port>"
       ]
       "ContainerListenIPAddress": "<ip_address>",
       "ContainerListenPort": <port>
     },
```

YAML Example

The following example shows the DAST API settings in a YAML file.

```
dASTApiSettings:
  rootUrl: http://<ip_address>:<port>
  disableCorsOrigins: true
  corsOrigins:
  - http://<hostname>:<port>
  - http://<hostname>:<port>
  - http://<ip_address>:<port>
  containerListenIPAddress: <ip_address>
  containerListenPort: <port>
```

Parameter Descriptions

The following table describes the parameters for the DAST API settings.

Parameter	Description

`RootUrl`	Required setting that specifies the URL and port where the DAST API service will run.
	
	Important! You cannot use localhost in the URL. You must use a routable IP address or hostname as shown in the following examples:
	
	`https://<DAST_API_hostname>:<port>`
	
	`https://<DAST_API_ip_address>:<port>`
	
	The URL can use the http protocol instead.
	
	Make note of this URL. It is required to enable Fortify ScanCentral DAST in Fortify Software Security Center.

`DisableCorsOrigins`	Optional cross-origin resource sharing (CORS) setting to restrict traffic to specific URLs or allow traffic from all URLs. By default, disable all origins for CORS policy is set to `true`. The Fortify Software Security Center URL is the only one that is automatically allowed. Options are: • `true` – Restricts traffic to the specified `corsOrigins` list • `false` – Allows traffic from all URLs
`CorsOrigins`	Specifies the allowed CORS origins list of URLs . Required when `disableCorsOrigins` is set to `true`, then you must add the allowed URLs.
`ContainerListenIPAddress`	Optional setting that specifies the container's internal IP address on which the DAST service will listen. The default value is "`0.0.0.0`".
`ContainerListenPort`	Optional setting that specifies the container's internal port on which the DAST service will listen. For `RootUrls` starting with `https`, the default value is `443`. Otherwise, it is `80`.

LIM Settings

You can use the LIM settings to configure a LIM and LIM pool to associate with the default sensor pool for licensing.

JSON Example

The following example shows the LIM settings in a JSON file.

```
  "LIMSettings": {
       "LimUrl": "https://<ip_address>/LIM.API",
       "ServiceAccountUserName": "<string>",
       "ServiceAccountPassword": "<string>",
       "DefaultLimPoolName": "<string>",
       "DefaultLimPoolPassword": "<string>",
       "UseLimRestApi": true
      },
```

YAML Example

The following example shows the LIM settings in a YAML file.

```
lIMSettings:
     limUrl: https://<ip_address>/LIM.API
     serviceAccountUserName: <string>
     serviceAccountPassword: <string>
     defaultLimPoolName: <string>
     defaultLimPoolPassword: <string>
     useLimRestApi: true
```

Parameter Descriptions

The following table describes the parameters for the LIM settings.

Parameter	Description
`LimUrl`	Required setting that identifies the LIM service URL. If you are using a LIM version 21.2.0 or later, then type the LIM REST API URL, which uses the following format: `https://<server_url>/<rest-directory>` where *server_url* is the root web site and *rest-directory* is the API

Parameter	Description
	virtual directory name. The default virtual directory name is `LIM.API`. **Important!** If using the LIM REST API, you must set `useLimRestApi` to `true`. The Linux WebInspect sensor must use the LIM REST API. If you are using a LIM version 21.1.0 or earlier, then type the SOAP service URL, which uses the following format: `https://<server_url>/<service-directory>` where *server_url* is the root web site and *service-directory* is the service virtual directory name. The default virtual directory name is `LIM.Service`. **Important!** If using the SOAP service URL, you must set `useLimRestApi` to `false`. The Linux WebInspect sensor does not support the LIM SOAP service URL.
`ServiceAccountUserName`	Required setting that specifies the LIM account username to be used for licensing.
`ServiceAccountPassword`	Required setting that specifies the password for the account. **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93.
`DefaultLimPoolName`	Required setting that specifies the LIM pool name to associate with the default sensor pool for licensing.
`DefaultLimPoolPassword`	Required setting that specifies the password for the LIM pool. **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93.
`UseLimRestApi`	Required setting that indicates whether to use the LIM REST API for the licensing service. Follow these guidelines for setting the value:

Parameter	Description
	• If you are using a LIM version 21.2.0 or later with the LIM REST API URL as `LimUrl`, then set the value to `true`. • If you are using a LIM version 21.1.0 or earlier with the SOAP service URL as `LimUrl`, then set the value to `false`.

Utility Service Settings

Use the Utility Service settings to configure the URL and port where the DAST Utility Service will run.

Important! You cannot use `localhost` in the URL. You must use a routable IP address or hostname as shown in the following examples:

`https://<DAST_Utility_hostname>:<port>`

`https://<DAST_Utility_ip_address>:<port>`

The URL can use the `http` protocol instead.

JSON Example

The following example shows the Utility Service settings in a JSON file.

```
  "UtilityWorkerServiceSettings": {
       "RootUrl": "https://<ip_address>:<port>/"
       "ContainerListenIPAddress": "<ip_address>",
       "ContainerListenPort": <port>
     },
```

YAML Example

The following example shows the Utility Service settings in a YAML file.

```
utilityWorkerServiceSettings:
     rootUrl: https://<hostname>:<port>/
     containerListenIPAddress: <ip_address>
     containerListenPort: <port>
```

Parameter Descriptions

The following table describes the parameters for the Utility Service settings.

Parameter	Description
`RootUrl`	Required setting that specifies the URL for the DAST Utility Service.
`ContainerListenIPAddress`	Optional setting that specifies the container's internal IP address on which the Utility Service will listen. The default value is "`0.0.0.0`".
`ContainerListenPort`	Optional setting that specifies the container's internal port on which the Utility Service will listen. For `RootUrls` starting with `https`, the default value is `5001`. Otherwise, it is `5000`.

DAST API SSL Settings

You can use the DAST API SSL settings to configure whether to use encrypted communication for the DAST API service. If you use encrypted communication, you can generate a certificate or use an existing certificate for this service.

Important! The certificate must have a PFX file extension.

About the Certificate Path

Generating a certificate or using an existing certificate requires you to specify a certificate path. It is not necessary to install the certificate on your local machine, but the certificate path must be accessible from the computer where you run the Docker compose file or PowerShell scripts to pull and start the ScanCentral DAST containers. The certificate is passed to the Docker container when you run the compose file or the PowerShell scripts.

JSON Example

The following example shows DAST API SSL settings that generate a self-signed certificate in a JSON file.

```
  "DastApiSSLSettings": {
       "SSLPreferenceType": "GenerateCertificate",
       "GenerateCertificateModel": {
         "CertificateDirectory": "<directory_path>",
         "Host": "<ip_address | hostname>",
         "Password": "<string>",
         "Validity": 1000,
         "Location": "",
```

```
        "Email": ""
      },
      "ExistingCertificateModel": {
        "CertificateFullPath": "",
        "Password": ""
      }
    },
```

YAML Example

The following example shows the DAST API SSL settings that use an existing certificate in a YAML file.

```
dastApiSSLSettings:
     sSLPreferenceType: UseExistingCertificate
     generateCertificateModel:
       certificateDirectory:
       host:
       password:
       validity:
       location:
       email:
     existingCertificateModel:
       certificateFullPath: '<directory_path>'
       password: '<string>'
```

Parameter Descriptions

The following table describes the parameters for the DAST API SSL settings.

Parameter	Description
`SSLPreferenceType`	Required setting that indicates whether to use encrypted communication for the DAST API service. Options are: • 1 or `GenerateCertificate` • 2 or `UseExistingCertificate` • 3 or `NoSSL` **Important!** Encrypted communication for the DAST API service is not required, but Fortify highly recommends it.

Parameter	Description
`GenerateCertificateModel`	Generates a self-signed certificate. If `SSLPreferenceType` is set to `1` or `GenerateCertificate`, then you must also provide the following parameters: • `CertificateDirectory` – Specifies the directory path where you will place the certificate on the host computer that will run the API container • `Host` – Specifies the IP address of the machine running the DAST API service container • `Password` – Specifies the password for the private key **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93. • `Validity` – Optionally, indicates the number of days the certificate will be valid **Note:** The default is `1000`. • `Location` – Optionally, indicates your city • `Email` – Optionally, indicates your email address
`ExistingCertificateModel`	Uses an existing certificate. If `SSLPreferenceType` is set to `2` or `UseExistingCertificate`, then you must also provide the following parameters: • `CertificateFullPath` – Specifies the directory path to the existing certificate • `Password` – Specifies the password for the private key **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93. **Important!** Ensure that you enter the correct password for

Parameter	Description
	the certificate. The Configuration Tool CLI does not validate certificate passwords.

Utility Service SSL Settings

You can use the Utility Service SSL settings to configure whether to use encrypted communication for the DAST Utility Service. If you use encrypted communication, you can generate a certificate or use an existing certificate for this service.

Important! The certificate must have a PFX file extension.

About the Certificate Path

Generating a certificate or using an existing certificate requires you to specify a certificate path. It is not necessary to install the certificate on your local machine, but the certificate path must be accessible from the computer where you run the Docker compose file or PowerShell scripts to pull and start the ScanCentral DAST containers. The certificate is passed to the Docker container when you run the compose file or the PowerShell scripts.

JSON Example

The following example shows the Utility Service SSL settings that generate a self-signed certificate in a JSON file.

```
"UtilityWorkerServiceSSLSettings": {
  "SSLPreferenceType": "GenerateCertificate",
  "GenerateCertificateModel": {
    "CertificateDirectory": "<directory_path>",
    "Host": "<ip_address>",
    "Password": "<string>",
    "Validity": 1000,
    "Location": "",
    "Email": ""
  },
  "ExistingCertificateModel": {
    "CertificateFullPath": "",
    "Password": ""
  }
},
```

YAML Example

The following example shows the Utility Service SSL settings that use an existing certificate in a YAML file.

```
utilityWorkerServiceSSLSettings:
  sSLPreferenceType: UseExistingCertificate
  generateCertificateModel:
    certificateDirectory:
    host:
    password:
    validity: 1000
    location:
    email:
  existingCertificateModel:
    certificateFullPath: '<directory_path>'
    password: '<string>'
```

Parameter Descriptions

The following table describes the parameters for the Utility Service SSL settings.

Parameter	Description
`SSLPreferenceType`	Required setting that indicates whether to use encrypted communication for the Utility Service. Options are: • `1` or `GenerateCertificate` • `2` or `UseExistingCertificate` • `3` or `NoSSL` **Important!** Encrypted communication for the DAST Utility Service is not required, but Fortify highly recommends it.
`GenerateCertificateModel`	Generates a self-signed certificate. If `SSLPreferenceType` is set to `1` or `GenerateCertificate`, then you must also provide the following parameters: • `CertificateDirectory` – Specifies the directory path where you will place the certificate on the host computer that will run the Utility Service container • `Host` – Specifies the IP address of the machine running the

Parameter	Description
	Utility Service container • `Password` – Specifies the password for the private key **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93. • `Validity` – Optionally, indicates the number of days the certificate will be valid **Note:** The default is 1000. • `Location` – Optionally, indicates your city • `Email` – Optionally, indicates your email address
`ExistingCertificateModel`	Uses an existing certificate. If `SSLPreferenceType` is set to `2` or `UseExistingCertificate`, then you must also provide the following parameters: • `CertificateFullPath` – Specifies the directory path to the existing certificate • `Password` – Specifies the password for the private key **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93. **Important!** Ensure that you enter the correct password for the certificate. The Configuration Tool CLI does not validate certificate passwords.

Environment Settings

You can use the environment settings to configure proxy settings and allow untrusted certificates.

Using a Proxy

The proxy settings configured here, including the exclusions, are used for internal communications between ScanCentral DAST components. The settings also apply when communicating with Fortify Software Security Center, LIM, SmartUpdate, DAST API, DAST Utility Service, and OpenAPI and OData definition URLs.

JSON Example

The following example shows the environment settings in a JSON file.

```
  "EnvironmentSettings": {
    "AllowNonTrustedServerCertificate": true,
    "ProxySettings": {
      "UseProxy": false,
      "ProxyAddress": "<ip_address>",
      "ProxyPassword": "<string>",
      "ProxyUserName": "<string>",
      "ProxyBypassList": "<hostname>,<ip_address>"
    }
  },
```

YAML Example

The following example shows the environment settings in a YAML file.

```
environmentSettings:
  allowNonTrustedServerCertificate: true
  proxySettings:
    useProxy: false
    proxyAddress: '<ip_address>'
    proxyPassword: '<string>'
    proxyUserName: '<string>'
    proxyBypassList: <hostname>,<ip_address>
```

Parameter Descriptions

The following table describes the parameters for the environment settings.

`AllowNontrustedServerCertificates`	Optional setting that specifies whether Fortify ScanCentral DAST components can accept self-

	signed (untrusted) certificates when communicating with other Fortify products. Options are `true` or `false`.
`UseProxy`	Optional setting that specifies whether to use a proxy for communications in your ScanCentral DAST environment. Options are `true` or `false`. If set to `true`, then you must also provide the following parameters: • `ProxyAddress` – Identifies the URL or IP address and port number of your proxy server • `ProxyPassword` – If your proxy server requires authentication, specifies the qualifying password **Tip:** Fortify recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting Values" on page 93. • `ProxyUserName` – If your proxy server requires authentication, specifies the qualifying user name • `ProxyBypassList` – Lists hostnames or IP addresses that do not need to use a proxy server for access, such as internal testing sites **Tip:** Your comma separated list may contain wildcards and regular expressions. For example: `localhost,198.51.*.*,[a-z]+\.myestore\.net$` **Important!** If you use Fully Qualified Domain Names (FQDN) to define the host/location in URLs in your YAML or JSON

	file, then you must use the same in the `ProxyBypassList`. If you use IP addresses, then you must use those in the `ProxyBypassList`.

Known Issue with Host Name, Machine Name, and Container Name

Configuring a proxy in the environment settings and then bypassing the proxy for communications with Fortify Software Security Center and the LIM may cause issues when using the host name, machine name, or container name for these products.

If you want to use the host name, machine name, or container name for Fortify Software Security Center and the LIM without a proxy, then set `UseProxy` to `false` and configure `HTTP_PROXY` and `NO_PROXY` environment variables instead. Additionally, add the host names, machine names, or container names for Fortify Software Security Center and the LIM to the `NO_PROXY` variable as a comma-separated list.

Refer to your OS documentation and change these environment variables.

You must also add these variables to the Docker containers' run commands as shown in the following example:

```
-e "HTTP_PROXY=http://<proxy_address>" -e "NO_PROXY=localhost,<ssc_
machine>,<lim_machine>"
```

SecureBase Settings

When initializing the database, you can use the default SecureBase ZIP file that is packaged with ScanCentral DAST or you can use a local version of SecureBase content to seed the database.

Updating SecureBase

If you use the `upgrade` or `autodeploy` mode for an existing DAST environment, then you must update your SecureBase. If you use the `manage` mode for an existing DAST environment, then updating SecureBase is optional. For more information about these modes, see "Understanding the configureEnvironment Command" on page 91.

JSON Example

The following JSON example shows SecureBase settings that use the default ZIP file to seed the database.

```
  "ApplySecureBase": true,
  "SecureBasePath": "<drive>:\\<directory_path>\\DefaultData.zip",
```

YAML Example

The following YAML example shows SecureBase settings that do not update the database.

```
applySecureBase: false
secureBasePath: <drive>:\<path_to_securebase_data>\DefaultData.zip
```

Parameter Descriptions

The following table describes the parameters for the SecureBase settings.

Parameter	Description
`ApplySecureBase`	Optional setting that specifies whether to update SecureBase. Options are: • `true` – Update SecureBase • `false` – Do not update SecureBase
`SecureBasePath`	If `applySecureBase` is set to `true` or `configureEnvironment --mode` (from the command line arguments) is `AutoDeploy` or `New`, this setting specifies the location of the SecureBase ZIP file to use for seeding the database. For more information about the command line arguments, see "Understanding the configureEnvironment Command" on page 91.

Client-side Library Analysis and Debricked Settings

The hacker-level insights check has been enhanced to include information from the National Vulnerability Database (NVD) as well as Debricked health metrics.

NVD Information

If you select a policy in your scan settings that has the **Hacker Level Insights (HLI) Detected Libraries** check enabled, and a vulnerable library is detected on the client side, information from a local copy of the NVD about common vulnerabilities and exposures (CVE) will be included in the vulnerability description.

Note: The NVD is shipped with the Fortify WebInspect installer or with the Docker image. It is updated once per release, and is not updated between releases.

You can learn more about the National Vulnerability Database (NVD) at https://nvd.nist.gov/.

Debricked Health Metrics

If the detected library is open source, and you have a subscription to Debricked and have configured ScanCentral DAST with your Debricked access token, then information about the library contributors, popularity, and security will be retrieved from the Debricked database and included in the vulnerability description.

A Debricked configuration also extends the local NVD and includes the newest CVEs. If there are no records for a CVE inside the local NVD, then data about the CVE and its description will be obtained from the Debricked database.

The Debricked information may also include correlated GitHub Security Advisory (GHSA) information for open source projects.

You can learn more about the Debricked health metrics at https://portal.debricked.com/project-health-45. You can learn more about GitHub Security Advisories at https://docs.github.com/.

Debricked Content Contingent Upon Access

If the Debricked service is down or unreachable for any reason at the start of a scan, the scan will continue. However, if access to the Debricked service has not been established upon scan completion, then Debricked information will not be included in the scan results.

Configuring Access to Debricked

To include the Debricked health metrics, you must provide your Debricked access token in the settings file when you install or manage your ScanCentral DAST environment.

Tip: To disable Debricked integration, run the Config Tool CLI with empty double quotation marks ("") in the JSON file or an empty string in the YAML file to remove the access token and return the configuration to the default state.

JSON Example

The following JSON example shows the Debricked setting.

```
  "DebrickedSettings": {
     "AccessToken": "<access_token>"
   }
```

YAML Example

The following YAML example shows the Debricked setting.

```
debrickedSettings:
   accessToken: <access_token>
```

JSON Sample File

After you have configured the various settings in your JSON file, they should resemble the following sample.

```
{
  "DatabaseSettings":{
    "DatabaseProvider": "<database_type>",
    "Server": "<ip_address>,<port>",
    "Database": "<database_name>",
    "DboLevelDatabaseAccount": {
      "Username": "<string>",
      "Password": "<string>",
      "UseWindowsAuthentication": false
      "AdditionalConnectionProperties": null
  },
  "StandardDatabaseAccount": {
    "Username": "<string>",
    "Password": "<string>",
    "CreateLogin": false,
    "AdditionalConnectionProperties": null
   }
  },
  "RetainCompletedScans": false,
  "DisableAdvancedScanPrioritization": false,
  "EnableRestrictedScanSettings": false,
  "ServiceToken": "<string>",
  "SmartUpdateSettings": {
    "SmartUpdateUrl": "https://smartupdate.fortify.microfocus.com/",
    "LicensingUrl": "https://licenseservice.fortify.microfocus.com/"
  },
  "SSCSettings": {
    "SSCRootUrl": "http://<ip_address>:<port>/ssc",
    "ServiceAccountUserName": "<username>",
    "ServiceAccountPassword": "<password>"
  },
  "DASTApiSettings": {
    "RootUrl": "http://<hostname>:<port>",
    "DisableCorsOrigins": true,
    "CorsOrigins": [
      "http://<hostname>:<port>",
```

```
      "http://<hostname>:<port>",
      "http://<ip_address>:<port>"
    ]
    "ContainerListenIPAddress": "<ip_address>",
    "ContainerListenPort": <port>
  },
  "LIMSettings": {
    "LimUrl": "https://<ip_address>/LIM.API",
    "ServiceAccountUserName": "<string>",
    "ServiceAccountPassword": "<string>",
    "DefaultLimPoolName": "<string>",
    "DefaultLimPoolPassword": "<string>",
    "UseLimRestApi": true
  },
  "UtilityWorkerServiceSettings": {
    "RootUrl": "https://<ip_address>:<port>/"
    "ContainerListenIPAddress": "<ip_address>",
    "ContainerListenPort": <port>
  },
  "DastApiSSLSettings": {
    "SSLPreferenceType": "GenerateCertificate",
    "generateCertificateModel": {
      "certificateDirectory": "<directory_path>",
      "host": "<ip_address>",
      "password": "<string>",
      "validity": 1000,
      "location": "",
      "email": ""
    },
    "existingCertificateModel": {
      "certificateFullPath": "",
      "password": ""
    }
  },
  "UtilityWorkerServiceSSLSettings": {
    "SSLPreferenceType": "GenerateCertificate",
    "GenerateCertificateModel": {
      "CertificateDirectory": "<directory_path>",
      "Host": "<ip_address>",
      "Password": "<string>",
      "Validity": 1000,
      "Location": "",
```

```
      "Email": ""
    },
    "ExistingCertificateModel": {
      "CertificateFullPath": "",
      "Password": ""
    }
  },
  "EnvironmentSettings": {
    "AllowNonTrustedServerCertificate": true,
    "ProxySettings": {
      "UseProxy": false,
      "ProxyAddress": "<ip_address>",
      "ProxyPassword": "<string>",
      "ProxyUserName": "<string>",
      "ProxyBypassList": "<hostname>,<ip_address>"
    }
  },
  "ApplySecureBase": true,
  "SecureBasePath": "<drive>:\\<path_to_securebase_data>\\DefaultData.zip",
  "DebrickedSettings": {
    "AccessToken": "<access_token>"
    }
}
```

YAML Sample File

After you have configured the various settings in your YAML file, they should resemble the following sample.

```
databaseSettings:
  databaseProvider: <database_type>
  server: <ip_address>,<port>
  database: <database_name>
  dboLevelDatabaseAccount:
    username: <string>
    password: <string>
    useWindowsAuthentication: false
    additionalConnectionProperties: null
  standardDatabaseAccount:
    username: <string>
    password: <string>
```

```
    createLogin: false
    additionalConnectionProperties: null
retainCompletedScans: false
disableAdvancedScanPrioritization: false
enableRestrictedScanSettings: false
serviceToken: <string>
smartUpdateSettings:
  smartUpdateUrl: https://smartupdate.fortify.microfocus.com/
  licensingUrl: https://licenseservice.fortify.microfocus.com/
sSCSettings:
  sSCRootUrl: http://<hostname>:<port>/ssc
  serviceAccountUserName: <username>
  serviceAccountPassword: <password>
dASTApiSettings:
  rootUrl: http://<ip_address>:<port>
  disableCorsOrigins: true
  corsOrigins:
  - http://<hostname>:<port>
  - http://<hostname>:<port>
  - http://<ip_address>:<port>
  containerListenIPAddress: <ip_address>
  containerListenPort: <port>
lIMSettings:
  limUrl: https://<ip_address>/LIM.API
  serviceAccountUserName: <string>
  serviceAccountPassword: <string>
  defaultLimPoolName: <string>
  defaultLimPoolPassword: <string>
  useLimRestApi: true
utilityWorkerServiceSettings:
  rootUrl: https://<hostname>:<port>/
  containerListenIPAddress: <ip_address>
  containerListenPort: <port>
dastApiSSLSettings:
  sSLPreferenceType: UseExistingCertificate
  generateCertificateModel:
    certificateDirectory:
    host:
    password:
    validity: 1000
    location:
    email:
```

```
  existingCertificateModel:
    certificateFullPath: '<directory_path>'
    password: '<string>'
utilityWorkerServiceSSLSettings:
  sSLPreferenceType: UseExistingCertificate
  generateCertificateModel:
    certificateDirectory:
    host:
    password:
    validity: 1000
    location:
    email:
  existingCertificateModel:
    certificateFullPath: '<directory_path>'
    password: '<string>'
environmentSettings:
  allowNonTrustedServerCertificate: true
  proxySettings:
    useProxy: false
    proxyAddress: '<ip_address>'
    proxyPassword: '<string>'
    proxyUserName: '<string>'
    proxyBypassList: <hostname>,<ip_address>
applySecureBase: true
secureBasePath: <drive>:\<path_to_securebase_data>\DefaultData.zip
debrickedSettings:
    accessToken: <access_token>
```

Using the Configuration Tool CLI

To assist you in setting up and maintaining the Fortify ScanCentral DAST components, Fortify engineers have created the ScanCentral DAST Configuration Tool CLI. The tool uses command line parameters and a configuration file to configure the ScanCentral DAST environment. The tool allows you to perform the following tasks:

- Create and configure a new ScanCentral DAST environment
- Upgrade all ScanCentral DAST components from one version to another
- Change ScanCentral DAST settings, such as a proxy or database account information, without upgrading the version

Upgrade Limitations for Linux

If you are upgrading from ScanCentral DAST version 22.1.0 or earlier, then you must run the Configuration Tool CLI on a Windows OS. If you are creating a new environment, then you may run the Configuration Tool CLI on a Windows OS or a Linux distribution.

Versions Available

The Configuration Tool CLI is available as executable files and as Docker images.

Docker Image Versions Available

Two versions of the Configuration Tool CLI Docker image are available: TAR files *with* SecureBase and DockerHub images *without* SecureBase.

About the TAR Files

Windows and Linux versions of the Configuration Tool CLI Docker image *with* SecureBase are available as TAR files in the ScanCentral DAST software download package. The TAR files are as follows:

- `scancentral-dast-config.tar` – for Windows
- `scancentral-dast-config-ubi.tar` – for RedHat Linux distribution

About the Images on DockerHub

The Configuration Tool CLI Docker images *without* SecureBase are available in the Fortify Docker repository on DockerHub.

The Fortify Docker repository uses the following naming convention for the Fortify Configuration Tool CLI images:

`fortifydocker/scancentral-dast-config:<version>`

The latest image versions that are available as of this writing are:

- `fortifydocker/scancentral-dast-config:23.1` – for Windows
- `fortifydocker/scancentral-dast-config:23.1.ubi.8` – for RedHat Linux distribution

Deciding Which Configuration Tool CLI to Use

Fortify recommends that you use one of the TAR files for the following tasks which will seed the database with the embedded `DefaultData.zip` file:

- Installing a new ScanCentral DAST environment
- Upgrading an existing ScanCentral DAST environment

For more information, see "Using the Windows TAR File" below or "Using the Linux TAR File" on page 87.

Fortify recommends that you use the executable file or the DockerHub image for the following tasks which do not involve the `DefaultData.zip` file:

- Creating a settings file or migration script
- Encrypting a password or token
- Managing an existing ScanCentral DAST environment

For more information, see "Using the Executable File" on page 88.

Using the Windows TAR File

The Configuration Tool CLI Docker image is available in a TAR file for Windows. This topic describes how to load the image from the TAR file, locate the sample settings files for editing, and run the container.

Note: In certain circumstances, such as when Windows authentication is used for SQL Server, you may not be able to use the TAR file for Windows. In such cases, you must use the `DAST.ConfigurationToolCLI.exe` file for Windows.

Loading the Image from the TAR File in Windows

To load the Fortify Configuration Tool CLI image from the TAR file in Windows:

- In PowerShell, enter the following command to load the image:

  ```
  docker load --input scancentral-dast-config.tar
  ```

  The image is extracted with the name `dast-config-sb`.

Continue with "Editing the Settings File" below.

Editing the Settings File

The Configuration Tool CLI download package includes two sample settings files: `SampleSettingsFile.json` and `SampleSettingsFile.yaml`. For convenience, you can edit one of these files with settings that are specific for your environment, and then reference the file in the Docker run command.

To edit the settings file:

- Edit the `SampleSettingsFile.json` or `SampleSettingsFile.yaml` file as needed. For more information, see "Creating and Using a Settings File" on page 55.

Note: By default, the "`secureBasePath:`" entry for Windows is set to "`C:\app\DefaultData.zip`".

After you have edited the settings file, continue with "Running the Container" below.

Running the Container

To run the container:

1. In PowerShell, enter the following command:

```
docker run --rm -v <Config_Dir_Full_Path>:C:\app\logs dast-config-sb
   <CLI_Commands>
```

Note: *<Config_Dir_Full_Path>* is the location of the configuration file. Mapping the volume to the `C:\app\logs` directory on the host system in the Docker run command exposes the log file to your workstation.

When using the Docker image, you must add CLI commands to the *end* of the Docker run command. The following example shows the `configureEnvironment` command with the `--mode` and `--settingsFile` parameters and a working directory of `C:\app\logs`:

```
docker run --rm -v <Config_Dir_Full_Path>:C:\app\logs dast-config-sb
   configureEnvironment --mode autodeploy
   --settingsFile C:\app\logs\SampleSettingsFile.yaml
```

You must pass in command parameters by way of environment variables *before* the image name reference, as shown in the following example:

```
docker run --rm -v <Config_Dir_Full_Path>:C:\app\logs -e
   "<environmentVariableName>=<value>" dast-config-sb <CLI_Commands>
```

For more information on the CLI commands, see the following:

- "Exporting an Existing Settings File" on page 89
- "Configuring the Environment" on page 91
- "Using Environment Variables" on page 92
- "Encrypting Values" on page 93
- "Generating a Migration Script" on page 93
- "Generating a Connection String" on page 95

Understanding the Docker CLI Options

The following table describes the Docker CLI options used in "Running the Container" above.

Option	Description
--rm	Automatically removes the container when it exits.
-v	Maps the volume (or folder) from the container to a folder on the host system. Separate multiple folder names with a colon.

Using the Linux TAR File

The Configuration Tool CLI Docker image is available in a TAR file for Linux. This topic describes how to load the image from the TAR file, locate the sample settings files for editing, and run the container.

Loading the Image from the TAR File in Linux

Note: This procedure describes how to load the RedHat Universal Base Image (UBI) version.

To load the Fortify Configuration Tool CLI image from the TAR file in Linux:

- At the console, enter the following command to load the image:

  ```
  docker load --input scancentral-dast-config-ubi.tar
  ```

  The image is extracted with the name `dast_configsb_redhat_linux`.

Continue with "Editing the Settings File" below.

Editing the Settings File

The Configuration Tool CLI download package includes two sample settings files: `SampleSettingsFile.json` and `SampleSettingsFile.yaml`. For convenience, you can edit one of these files with settings that are specific for your environment, and then reference the file in the Docker run command.

To edit the settings file:

- Edit the `SampleSettingsFile.json` or `SampleSettingsFile.yaml` file as needed. For more information, see "Creating and Using a Settings File" on page 55.

  Note: By default, the "`secureBasePath:`" entry for Linux is set to "`/app/DefaultData.zip`".

After you have edited the settings file, continue with "Running the Container" below.

Running the Container

To run the container:

- At the command prompt, enter the following command:

```
docker run –rm -v <Config_Dir_Full_Path>:/
   <Working_Directory> dast_configsb_redhat_linux <CLI_Commands>
```

Note: *<Config_Dir_Full_Path>* is the location of the configuration file.

When using the Docker image, you must add CLI commands to the *end* of the Docker run command. The following example shows the `configureEnvironment` command with the `--mode` and `--settingsFile` parameters and a working directory of `:/app/logs`:

```
docker run --rm -v <Config_Dir_Full_Path>:/app/logs dast_configsb_redhat_
   linux configureenvironment --mode autodeploy --settingsFile
   /app/logs/SampleSettingsFile.yaml --outputDirectory /app/logs
```

You must pass in command parameters by way of environment variables *before* the image name reference, as shown in the following example:

```
docker run --rm -v <Config_Dir_Full_Path>:/app/logs -e
   "<environmentVariableName>=<value>" dast_configsb_redhat_linux <CLI_
   Commands>
```

For more information on the CLI commands, see the following:

- "Exporting an Existing Settings File" on the next page
- "Configuring the Environment" on page 91
- "Using Environment Variables" on page 92
- "Encrypting Values" on page 93
- "Generating a Migration Script" on page 93
- "Generating a Connection String" on page 95

Understanding the Docker CLI Options

The following table describes the Docker CLI options used in "Running the Container" on the previous page.

Option	Description
--rm	Automatically removes the container when it exits.
-v	Maps the volume (or folder) from the container to a folder on the host system. Separate multiple folder names with a colon.

Using the Executable File

The following paragraphs describe where to find the EXE file and how to use the program.

Locating the EXE File

The `DAST.ConfigurationToolCLI.exe` file is included in the Fortify ScanCentral DAST software download package (a ZIP file).

Launching the CLI

To launch the command-line interface (CLI):

- Right-click the Windows **Command Prompt** (cmd.exe) application, and select **Run as administrator**.

  The Administrator: Command Prompt window appears.

Important! At the command prompt, use the `cd` command to change the current working directory to the directory where the Configuration Tool CLI application resides.

Using the Configuration Tool CLI

To use the Configuration Tool CLI:

- At the command prompt, use the following syntax:

  `DAST.ConfigurationToolCLI.exe <CLI_Command>`

For more information on the CLI commands, see the following:

- "Exporting an Existing Settings File" below
- "Configuring the Environment" on page 91
- "Using Environment Variables" on page 92
- "Encrypting Values" on page 93
- "Generating a Migration Script" on page 93
- "Generating a Connection String" on page 95

Accessing the Help

To view the Configuration Tool CLI help:

- At the command prompt, type `DAST.ConfigurationToolCLI.exe -h`.

Exporting an Existing Settings File

If you have an existing ScanCentral DAST environment, you can use the `createSettingsFile` command to export a settings file that contains the current settings for the existing environment.

Understanding the createSettingsFile Command

The `createSettingsFile` command includes the parameters shown in the following syntax sample.

```
DAST.ConfigurationToolCLI.exe createSettingsFile
   --dbProvider <SQLServer | PostgreSQL | AzureSQLServer |
   AzurePostgreSQL | AmazonRdsSQLServer | AmazonRdsPostgreSQL>
   --server <string> --database <string> --username <string>
   --password <string> --useWindowsAuthentication
   --additionalConnectionProperties <string>
   --settingsFileType <yaml | json> --outputDirectory <string>
```

The following table describes the `createSettingsFile` parameters.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or the server IP address. **Important!** If SQL Server Browser is not running and you are using a port other than 1433, then you must also specify the port. Use the following format: *<server_name>,<port>* *<ip_address>,<port>* Note that a comma separates the values.
`--database`	Specifies the name of the database.
`--username`	Indicates the database account user name. **Note:** With an existing database, you can use the non-DBO credentials.
`--password`	Indicates the database account password.
`--settingsFileType`	Specifies the file type for the settings file. Options are `json` or `yaml`.

Parameter	Description
`--outputDirectory`	Specifies the directory path where the settings file will be written.

Configuring the Environment

After you configure your settings file, you can use the Configuration Tool CLI to generate the Docker compose file or PowerShell script to pull and launch the core ScanCentral DAST 23.1.0 containers (DAST API, DAST Global Service, and DAST Utility Service).

Before You Begin

All ScanCentral DAST components must be offline (not running) when using the CLI tool.

Understanding the configureEnvironment Command

The `configureEnvironment` command includes the parameters shown in the following syntax sample.

```
DAST.ConfigurationToolCLI.exe configureEnvironment
   --mode <new | upgrade | manage | autodeploy>
   --settingsFile <string> --outputDirectory <string>
```

The following table describes the `configureEnvironment` parameters.

Parameter	Description
`--mode`	Indicates the intended function of the settings file. Options are: • `new` – Creates and configures a new ScanCentral DAST environment • `upgrade` – Upgrades all ScanCentral DAST components from one version to another • `manage` – Changes ScanCentral DAST settings, such as a proxy or database account information, or uploads new SecureBase content, without upgrading the version • `autodeploy` – Detects whether the database exists. If no, then the `new` function is performed. Otherwise, the database is updated or managed.
`--settingsFile`	Specifies the directory path and name of the settings file to use for creating, managing, or upgrading a ScanCentral DAST environment. The file can be either JSON or YML file type.
`--outputDirectory`	Optionally, indicates the directory path where the artifacts file is written.

Parameter	Description
	The artifacts are saved to a ZIP file. If you do not provide an `--outputDirectory` setting, then the ZIP file is written to the directory where the `DAST.ConfigurationToolCLI.exe` file is located.

Applying Updated Settings to Containers

When you use the Configuration Tool CLI with the `--mode manage` parameter, you may need to apply the updated settings to one or more of your containers.

The following list describes how to apply settings based on the settings that changed:

- Changing any database setting requires new DAST API, Utility Service, and Global Service containers.
- Changing service ports requires a new container for the service whose port was changed.
- Changing DAST API SSL settings requires a new container for the DAST API.
- Changing Utility Service SSL settings requires a new container for the Utility Service.
- All other changes are picked up automatically by each service within two minutes of making the change or upon restarting the containers.

Using Environment Variables

The Configuration Tool CLI allows you to replace placeholders in a settings file with environment variables. This feature protects your sensitive data and supports the use of Kubernetes secrets. For more information on Kubernetes secrets, refer to your Kubernetes configuration documentation.

How Replacement Works

Each environment variable placeholder in the settings file is replaced with an environment variable value. If no environment variable value is available, then the value will not be replaced.

The replacement values are not written to the source settings file. Instead, the Configuration Tool CLI creates a temporary copy of the settings file that contains the values to be used.

Format and Usage

The format of the placeholder in the settings file is as follows:

```
${environment variable name}
```

The following sample shows an environment variable with the name `my_secret_password` in a YAML settings file.

```
databaseSettings:
  databaseProvider: SQLServer
  server: .
  database: DAST
  dboLevelDatabaseAccount:
    username: myusername
    password : ${my_secret_password}
    useWindowsAuthentication: false
    additionalConnectionProperties:
```

Encrypting Values

The Configuration Tool CLI provides the `encrypt` command that encrypts a value. This feature allows you to encrypt sensitive data, such as passwords, to use in a settings file.

If the value to be encrypted contains spaces, then the value must be enclosed in double quotation marks (").

The `encrypt` command is shown in the following sample.

```
DAST.ConfigurationToolCLI.exe encrypt "<string>"
```

The encrypted value is logged to the console as "`encrypt result: {encrypted value}`".

Generating a Migration Script

The Configuration Tool CLI provides the `generateMigrationScript` command that generates a migration script that you can run on the database server. This feature is useful in environments where policies do not allow applications to change database schema and require a manual script to run.

All non-optional parameters are required and are validated upon execution. If any parameter fails validation, a message is written to the log file and the application exits with a -1.

Migration Script Name

The generated migration script is named: `DAST-Migration-MMddyyyyHHmmss.sql`. The time stamp in the name is composed of the following:

- `MM` – Month, with a leading 0
- `dd` – Day, with a leading 0
- `yyyy` – 4-digit year
- `HH` – 24-hour clock hour, with a leading 0
- `mm` – Minutes, with a leading zero
- `ss` – Seconds, with a leading zero

Understanding the generateMigrationScript Command

The `generateMigrationScript` command includes the parameters shown in the following sample.

```
DAST.ConfigurationToolCLI.exe generateMigrationScript
   --dbProvider <SQLServer | PostgreSQL | AzureSQLServer |
   AzurePostgreSQL | AmazonRdsSQLServer | AmazonRdsPostgreSQL>
   --server <string> --database <string> --username <string>
   --password <string> --useWindowsAuthentication
   --additionalConnectionProperties <string> --outputDirectory <string>
```

The following table describes the parameters for the `generateMigrationScript` command.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or IP address.
`--database`	Specifies the database name.
`--username`	Indicates the database account user name to connect to the database. This parameter is not required if `-useWindowsAuthentication` is used.
`--password`	Indicates the database account password to connect to the database. This parameter is not required if `-useWindowsAuthentication` is used.
`--useWindowsAuthentication`	Indicates that the connection should use Windows authentication.

Parameter	Description
`--additionalConnectionProperties`	Optionally, specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information about additional connection properties, refer to your SQL database documentation.
`--outputDirectory`	Optionally, indicates the directory path where the migration script will be saved. If not specified, the script will be saved in the current working directory. **Note:** If the specified directory does not exist, it will be created.

Generating a Connection String

The Configuration Tool CLI can generate a connection string for connecting to your ScanCentral DAST database. All non-optional parameters are required and are validated upon execution. If a parameter fails validation, a message is written to the log file and the application exits with a -1.

Understanding the generateConnectionString Command

The `generateConnectionString` command includes the parameters shown in the following sample.

```
DAST.ConfigurationToolCLI.exe generateConnectionString --dbProvider
   <SQLServer | PostgreSQL | AzureSQLServer | AzurePostgreSQL |
   AmazonRdsSQLServer | AmazonRdsPostgreSQL> --server <string>
   --database <string> --username <string> --password <string>
   --useWindowsAuthentication --additionalConnectionProperties <string>
   --encrypt
```

The following table describes the parameters for the `generateConnectionString` command.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer`

Parameter	Description
	• `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or IP address.
`--database`	Specifies the database name.
`--username`	Indicates the database account user name to connect to the database. This parameter is not required if `--useWindowsAuthentication` is used.
`--password`	Indicates the database account password to connect to the database. This parameter is not required if `--useWindowsAuthentication` is used. **Important!** Use double quotation marks if your password includes any of the following special characters: :, {, }, [,], ,, &, *, #, ?, |, -, <, >, =, !, %, @, \, `
`--useWindowsAuthentication`	Indicates that the connection should use Windows authentication.
`--additionalConnectionProperties`	Optionally, specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information about additional connection properties, refer to your SQL database documentation.
`--encrypt`	Encrypts the results.

Understanding the Launch Artifacts

The Configuration Tool CLI creates scripts for Windows and Linux containers. The `dast-windows-start.zip` file contains scripts for starting Windows containers. The `dast-linux-start.tar.gz`

file contains scripts for starting Linux containers.

If you provide an `--outputDirectory` setting in the `configureEnvironment` command, then these files will be written to the directory you specify. If you do not provide an `--outputDirectory` setting, then these files will be written to the directory where the `DAST.ConfigurationToolCLI.exe` file is located.

For more information about the DAST components mentioned here, see "What is ScanCentral DAST?" on page 36 and "ScanCentral DAST with Two-factor Authentication" on page 39.

The following table provides details about these files.

File	Description
`appsettings.json`	Configures the sensor service. Use this file to run the Fortify ScanCentral DAST Sensor Service and a Fortify WebInspect sensor.
`DAST-api.pfx`	If you generated a certificate for the DAST API service using the Configuration Tool CLI, this certificate file must be on the host computer where the DAST API container will be running. **Note:** This file is not downloaded if you use a certificate provided by a certificate authority (CA) or use an existing certificate.
`DAST-utilityservice.pfx`	If you generated a certificate for the DAST Utility service using the Configuration Tool CLI, this certificate file must be on the host computer where the DAST Utility service container will be running. **Note:** This file is not downloaded if you use a certificate provided by a certificate authority (CA) or use an existing certificate.
`docker-compose.scancentral-dast-sensor.yaml` (Linux only)	Pulls the Fortify WebInspect Linux scanner, database, WebInspect script engine (WISE), and 2FA server images from Docker Hub, and then starts the containers as a DAST sensor.
`docker-compose.scancentral-dast-utilityservice.yaml` (Linux only)	Pulls the Fortify WebInspect Linux scanner image and database from Docker Hub, and then starts the containers as the DAST Utility Service.

File	Description
`docker-compose.yml`	Pulls images and starts containers for the DAST API, DAST Global Service, and DAST Utility Service.
`pull-and-start-containers.ps1` `pull-and-start-containers.sh`	Pulls the DAST API, DAST Global Service, and DAST Utility Service images from Docker Hub, and then starts the containers.
`pull-and-start-sensor-container.ps1` `pull-and-start-sensor-container.sh`	Pulls the Fortify WebInspect Windows image or the scanner Linux image from Docker Hub, and then starts the container.
`pull-and-start-twofactorauth-container.ps1` `pull-and-start-twofactorauth-container.sh`	Pulls the 2FA Server image from Docker Hub, and then starts the container. For instructions on using the PowerShell script, see "Using PowerShell Scripts for the 2FA Server" on page 306. For information about executing the bash script, refer to your Linux distribution documentation.
`pull-images.ps1` `pull-images.sh`	Pulls the DAST API, DAST Global Service, and DAST Utility Service images from Docker Hub, but does not start the containers.
`pull-sensor-image.ps1` `pull-sensor-image.sh`	Pulls the Fortify WebInspect Windows image or the scanner Linux image from Docker Hub, but does not start the container.
`pull-twofactorauth-image.ps1` `pull-twofactorauth-image.sh`	Pulls the 2FA Server image from Docker Hub, but does not start the container. For instructions on using the PowerShell script, see "Using PowerShell Scripts for the 2FA Server" on page 306. For information about executing the bash script, refer to your Linux distribution documentation.
`service-token.txt`	Contains the shared secret that all your DAST sensors must use to authenticate with the DAST API.
`start-containers.ps1` `start-containers.sh`	Starts the DAST API, DAST Global Service, and DAST Utility Service containers, but does not pull the images.

File	Description
`start-sensor-container.ps1` `start-sensor-container.sh`	Starts the Fortify WebInspect container, but does not pull the image.
`start-twofactorauth-container.ps1` `start-twofactorauth-container.sh`	Starts the 2FA Server container, but does not pull the image. For instructions on using the PowerShell script, see "Using PowerShell Scripts for the 2FA Server" on page 306. For information about executing the bash script, refer to your Linux distribution documentation.

What's Next?

You can use the launch artifacts to pull the DAST API, DAST Global Service, DAST Utility Service, and Fortify WebInspect images from Docker Hub and start the containers. You can accomplish this task in one of the following ways:

- "Using the Compose File" below
- "Using PowerShell Scripts" on the next page
- Using Bash Scripts (For more information, refer to your Red Hat documentation.)

Using the Compose File

The `docker-compose.yml` file contains the various service settings required to pull images of the DAST API, DAST Global Service, and DAST Utility Service, and then start the containers. You use the compose file on the host where you want to run these containers.

Using the Compose File on Windows

Important! To use the compose file, you must first download and install Docker Compose on the host machine. For more information, see "Setting Up Docker" on page 54.

Use the following process to use the compose file on Windows.

Stage	Description
1.	Copy the following files to the host where you want to run the DAST API, DAST Global Service, and DAST Utility Service containers: • `DAST-api.pfx` (Required only if generated by the Configuration Tool)

Stage	Description
	• `DAST-utilityservice.pfx` (Required only if generated by the Configuration Tool) • `docker-compose.yml`
2.	On this same host, start Windows PowerShell as Administrator. For more information about PowerShell, refer to your Windows documentation.
3.	At the prompt, type `docker-compose up`, and press **Enter**. The DAST API, DAST Global Service, and DAST Utility Service images are pulled and the containers are started.

Using the Compose File on Linux

Important! To use the compose file, you must first download and install Docker Compose on Linux on the host machine. For more information, see "Setting Up Docker" on page 54.

Use the following process to use the compose file on Linux.

Stage	Description
1.	Copy the following files to the Linux host where you want to run the DAST API, DAST Global Service, and DAST Utility Service containers: • `DAST-api.pfx` (Required only if generated by the Configuration Tool) • `DAST-utilityservice.pfx` (Required only if generated by the Configuration Tool) • `docker-compose.yml`
2.	At the terminal prompt, type `docker-compose up`, and press **Enter**. The DAST API, DAST Global Service, and DAST Utility Service images are pulled and the containers are started.

Using PowerShell Scripts

The Configuration Tool CLI creates and downloads PowerShell scripts for the core ScanCentral DAST containers. These scripts offer the following options:

- Use one script to pull images of the DAST API, DAST Global Service, and DAST Utility Service, and then start the containers.
- Use two scripts: one to pull the images, and then another to start the containers.

You use the script or scripts on the host where you want to run the DAST API, DAST Global Service, and DAST Utility Service containers.

For information on how to use the PowerShell scripts to pull a Windows version of the Fortify WebInspect on Docker image and start the container as a DAST sensor, see the *Micro Focus Fortify WebInspect and OAST on Docker User Guide*.

Using One Script

Use the following process to use a single PowerShell script to pull images and start the containers.

Stage	Description
1.	Copy the following files to the host where you want to run the DAST API, DAST Global Service, and DAST Utility Service containers: • `DAST-api.pfx` (Required only if generated by the Configuration Tool CLI) • `DAST-utilityservice.pfx` (Required only if generated by the Configuration Tool CLI) • `pull-and-start-containers.ps1`
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information about using PowerShell, refer to your Windows PowerShell documentation.
3.	To avoid errors regarding non-digitally signed scripts, run the contents of the `pull-and-start-containers.ps1` script as follows: 1. Copy the contents from the `pull-and-start-containers.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-and-start-containers.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The DAST API, DAST Global Service, and DAST Utility Service images are pulled and the containers are started.

Using Two Scripts

Use the following process to use separate pull and start PowerShell scripts.

Stage	Description
1.	Copy the following files to the host where you want to run the DAST API, DAST Global Service, and DAST Utility Service containers: • `DAST-api.pfx` (Required only if generated by the Configuration Tool CLI) • `DAST-utilityservice.pfx` (Required only if generated by the Configuration Tool CLI) • `pull-images.ps1` • `start-containers.ps1`
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information about using PowerShell, refer to your Windows PowerShell documentation.
3.	Pull the images. To avoid errors regarding non-digitally signed scripts, run the contents of the `pull-images.ps1` script as follows: 1. Copy the contents from the `pull-images.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-images.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The DAST API, DAST Global Service, and DAST Utility Service images are pulled.
4.	Start the containers. To avoid errors regarding non-digitally signed scripts, run the contents of the `start-containers.ps1` script as follows: 1. Copy the contents from the `start-containers.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, if you set the execution policy to allow all scripts as described in Stage 3, you can run the script as follows:

Stage	Description
	`& "<drive>:<path_to_script>\start-containers.ps1"` The DAST API, DAST Global Service, and DAST Utility Service containers are started.

Using Fortify WebInspect on Docker

Windows and Linux images of Fortify WebInspect on Docker are available for download on the Docker container platform. For more information about these images, see "WebInspect Sensor" on page 38.

For information on how to use the launch artifacts to pull one of these images and start the container as a DAST sensor, see the *Micro Focus Fortify WebInspect and OAST on Docker User Guide* at https://www.microfocus.com/documentation/fortify-webinspect/2310/WI_Docker_Guide_23.1.0.pdf.

Using Fortify WebInspect with the Sensor Service

You can use a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service. To do so, you must first configure and start the WebInspect REST API, and then install and configure the DAST sensor service.

Before You Begin

If you use encrypted communication for the DAST API service, then you must copy the API SSL certificate from the Configuration Tool artifacts and add it to the Trusted Store on the machine where the DAST sensor service will run.

Important Information About Licenses

When running a scan using ScanCentral DAST with the sensor service and a Fortify WebInspect installation, the license that is configured in the Fortify WebInspect user interface is overridden to use a LIM license. When the ScanCentral DAST scan is complete, the LIM license is released. The next time you open the Fortify WebInspect user interface, it will be unlicensed.

As a workaround, reactivate the installed version of Fortify WebInspect using the previous license in the Fortify WebInspect UI.

Important Prerequisite

Before installing the DAST sensor service, you must first install the full .NET SDK or ASP.NET Core Runtime 7.0.0 or later. Otherwise, the following error occurs:

```
A fatal error occurred. The required library hostfxr.dll could not be
found.
If this is a self-contained application, that library should exist in
[C:\ScannerService\].
If this is a framework-dependent application, install the runtime in
the global location [C:\Program Files\dotnet] or use the DOTNET_ROOT
environment variable to specify the runtime location or register the
runtime location in [HKLM\SOFTWARE\dotnet\Setup\InstalledVersions\
x64\InstallLocation].
```

Configuring the Fortify WebInspect REST API

On the machine where Fortify WebInspect is installed, configure the Fortify WebInspect REST API as follows:

1. From the Windows Start menu, click **All Programs** > **Fortify** > **Fortify WebInspect** > **Micro Focus Fortify Monitor**.

   The Micro Focus Fortify Monitor icon appears in the system tray.
2. Right-click the **Micro Focus Fortify Monitor** icon, and select **Configure WebInspect API**.

   The Configure WebInspect API dialog box appears.
3. Configure the API Server settings as described in the following table.

Setting	Value
Host	Both Fortify WebInspect and the Fortify WebInspect REST API must reside on the same machine. The default setting, +, is a wild card that tells the Fortify WebInspect REST API to intercept all request on the port identified in the Port field. If you have another service running on the same port and want to define a specific hostname just for the API service, this value can be changed.
Port	Use the provided value or change it using the up/down arrows to an available port number.
Authentication	Choose **None**, **Windows**, **Basic**, or **Client Certificate** from the Authentication drop-down list.

Setting	Value

	If you choose **Basic** for authentication, you must provide user name(s) and password(s). To do this:
	a. Click the **Edit passwords** button and select a text editor.
	The `wircserver.keys` file opens in the text editor. The file includes sample user name and password entries:
	`username1:password1`
	`username2:password2`
	b. Replace the samples with user credentials for access to your server. If additional credentials are needed, add a user name and password, separated by a colon, for each user to be authenticated. There should be only one user name and password per line.
	c. Save the file.
	If you choose **Client Certificate** for authentication, you must first generate a client certificate based on your root SSL certificate issued by a trusted certificate authority (CA), and then install it on the client machine.
	Tip: You can use a tool, such as the MakeCert utility in the Windows Software Development Kit (SDK), to create your client certificate.

Use HTTPS	Select this check box to access the server over an HTTPS connection.
	To run the server over HTTPS, you must create a server certificate and bind it to the API service. To quickly create a self-signed certificate to test the API over HTTPS, run the following script in an Administrator PowerShell console:
	`$rootcertID = (New-SelfSignedCertificate -DnsName "DO NOT TRUST - WIRC Test Root CA","localhost", "$($env:computername)" -CertStoreLocation "cert:\LocalMachine\My").Thumbprint`
	`$rootcert = (Get-Item -Path "cert:\LocalMachine\My\$($rootcertID)")`
	`$trustedRootStore = (Get-Item -Path "cert:\LocalMachine\Root")`
	`$trustedRootStore.open("ReadWrite")`
	`$trustedRootStore.add($rootcert)`
	`$trustedRootStore.close()`
	`netsh http add sslcert ipport=0.0.0.0:8443`

Setting	Value
	`certhash=$($rootcertID) appid="{160e1003-0b46-47c2-a2bc-01ea1e49b9dc}"` The preceding script creates a certificate for the local host and the computer name, puts the certificate in the Personal Store and Trusted Root, and binds the certificate to port 8443. If you use a different port, specify the port you use in the script. **Important!** Use the self-signed certificate created by the preceding script for testing only. The certificate works only on your local machine and does not provide the security of a certificate from a certificate authority. For production, use a certificate that is generated by a certificate authority.
Log Level	Choose the level of log information you want to collect.

4. Do one of the following:
   - To start the Fortify WebInspect REST API service and test the API configuration, click **Test API**.

     The service starts, and a browser opens and navigates to the Fortify WebInspect REST API Swagger UI page.
   - To start the Fortify WebInspect REST API service without testing the API configuration, click **Start**.

Installing and Configuring the DAST Sensor Service

Important! To install and run the DAST sensor service, you must run the service with the `appsettings.json` file that the ScanCentral DAST Configuration Tool created. Make sure you have access to this file. For more information, see "Understanding the Launch Artifacts" on page 96.

On the machine where Fortify WebInspect is installed, install and run the DAST sensor service as follows:

1. Download the `ScannerService<version>.zip` file from the Fortify ScanCentral DAST software download package.

   Tip: The software download package is the file that you downloaded after your purchase .

2. Extract the `ScannerService<version>.zip` file to any directory, such as the following:

   `c:\ScannerService`

3. Place the `appsettings.json` file that the ScanCentral DAST Configuration Tool created in the same directory, replacing the existing file.

   Important! If Fortify WebInspect is not installed in the default location or the datapath has changed, you must update entries in the `appsettings.json` file accordingly.

   For example, when the ScanCentral DAST Sensor service is installed on a Fortify WebInspect instance where FIPS is enabled, DAST is not able to locate the Logs, Policies, or Settings files. In this installation, these files are located under `C:\ProgramData\HP\HP WebInspect\FIPS\`. Therefore, you must edit the following lines in the `appsettings.json` file:

   ```
   "WebInspectLogsDirectory": "C:\\ProgramData\\hp\\HP
   WebInspect\\Schedule\\logs”,
   "WebInspectSettingsPath": "C:\\ProgramData\\hp\\HP
   WebInspect\\Settings",
   "WebInspectPoliciesDirectory": "C:\\ProgramData\\HP\\HP
   WebInspect\\Policies",
   ```

   With the following changes:

   ```
   "WebInspectLogsDirectory": "C:\\ProgramData\\hp\\HP
   WebInspect\\FIPS\\Schedule\\logs",
   "WebInspectSettingsPath": "C:\\ProgramData\\hp\\HP
   WebInspect\\FIPS\\Settings",
   "WebInspectPoliciesDirectory": "C:\\PrograrmData\\HP\\HP
   WebInspect\\FIPS\\Policies",
   ```

4. Run the Command Prompt as Administrator, and then enter the following command:

   ```
   sc create ScannerWorkerService binpath= "<PathToScannerService>
      \DAST.ScannerWorkerService.exe" start= auto depend= "WebInspect API"
      displayname= "WebInspect DAST Scanner Worker Service"
   ```

   The following sample uses the `c:\ScannerService` directory in the path:

   ```
   sc create ScannerWorkerService binpath= "C:\ScannerService
      \DAST.ScannerWorkerService.exe" start= auto depend= "WebInspect API"
      displayname= "WebInspect DAST Scanner Worker Service"
   ```

   The ScannerWorkerService is created and automatically starts each time the computer is restarted. Additional options provide the following benefits:

   - `depend= "WebInspect API"` – Starts the Fortify WebInspect API service if it has stopped. It also stops the ScannerWorkerService if the Fortify WebInspect API service is stopped for any reason.
   - `displayname= "WebInspect DAST Scanner Worker Service"` - Groups the services together in Windows Service Manager, which may help with troubleshooting.

5. Open Windows Services Manager (`services.msc`). For more information, refer to your Windows documentation.
6. In Windows Services Manager, configure the scanner worker service as follows:
   a. Right-click the newly created **ScannerWorkerService**.
   b. Configure the user account and password under which the service should run.

      Note: You can use credentials for any user account that has access to log in to the Windows OS.

   c. Apply the changes.

      Note: You might need to manually start the service the first time.

   The service starts and polls the Fortify WebInspect API for instructions.

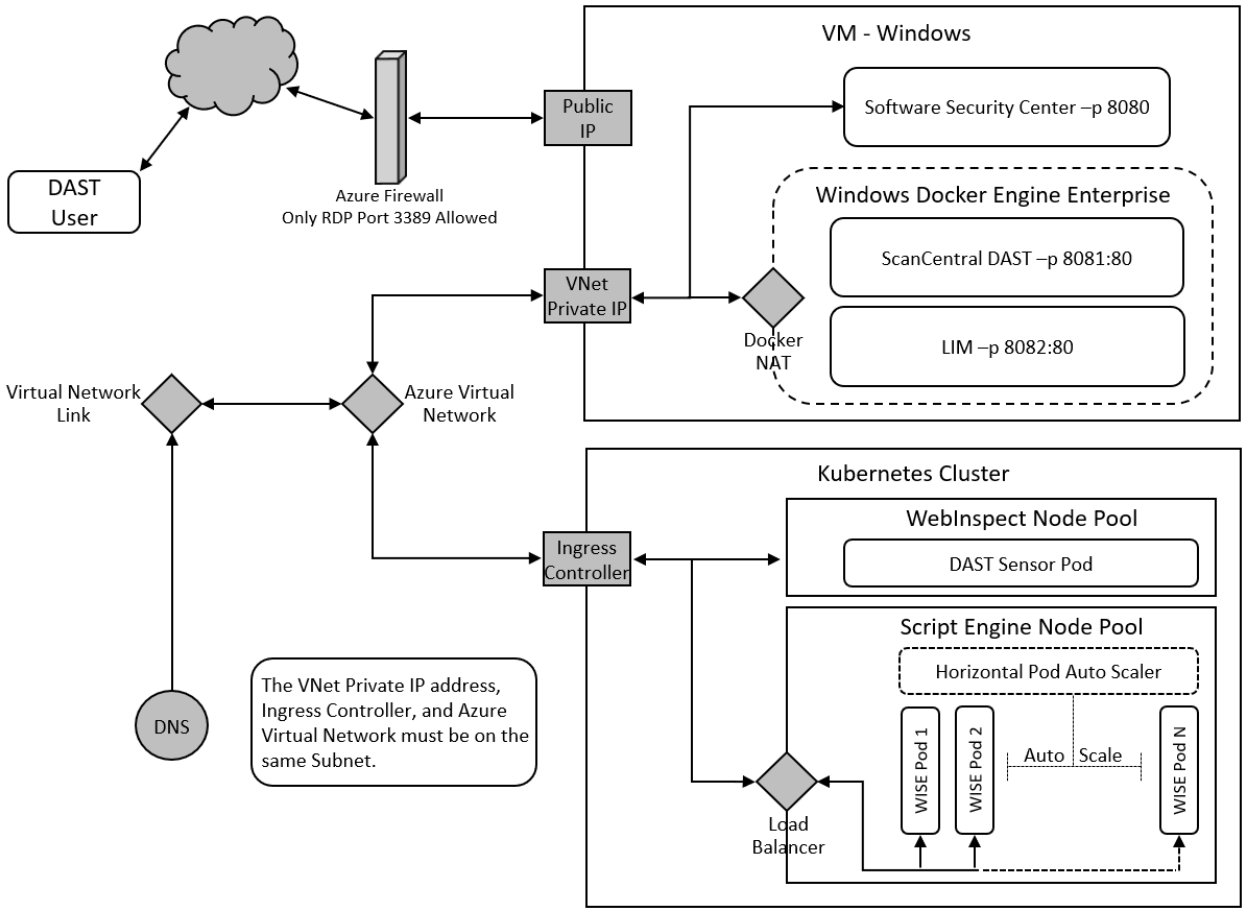
Integrating with Kubernetes for Scan Scaling

You can integrate Fortify ScanCentral DAST with Kubernetes to create a scalable cloud architecture that provides scan scaling functionality, resulting in faster scans of your applications.

During a scan, script engines replay TruClient macros and run scripts to reveal the Document Object Model (DOM) of the application and events on the page. Scan scaling involves automatically creating multiple pools of these script engines in Kubernetes. In essence, it distributes the work of performing the scan across multiple script engines, thereby reducing the amount of time it takes to conduct the scan.

Scan scaling might be beneficial for applications that generally have long-running scans.

The following diagram illustrates the integration of ScanCentral DAST with Kubernetes.



DNS Requirement

Your Domain Name System (DNS) can use Azure Private DNS zones. However, you must add a record into the DNS for the WebInspect script engine (WISE) ingress host name and the Kubernetes ingress controller IP address.

Sensor Installation Requirement

You must use one of the following options to install the Fortify WebInspect sensor for integration with Kubernetes:

- Install the Fortify WebInspect sensor on a machine that is located in the same subnet that is used by the Kubernetes cluster.
- If the Kubernetes cluster supports both Windows and Linux nodes on the same subnet, then you can install the Fortify WebInspect sensor into the Kubernetes cluster using the WebInspect Helm Charts.

Tip: Make note of the sensors that you install for integration with Kubernetes. You will need to add one or more of these sensors to the sensor pool(s) that you create for scan scaling.

Implementing Scan Scaling with Kubernetes

You must configure the machine(s) where the remote script engines will run and the Kubernetes node that will manage them. You must also configure at least one sensor pool for scan scaling and then enable scaling in your scan. The following table describes this process.

Stage	Description
1.	Download and configure kubectl and Helm software. For more information, see "Downloading kubectl and Helm" below.
2.	Deploy the HAProxy ingress Kubernetes controller. For more information, see "Deploying HAProxy in Kubernetes" on page 112.
3.	Deploy the Kubernetes Metrics Server to handle horizontal auto scaling for the Kubernetes WISE pods. For more information, "Deploying the Kubernetes Metrics Server" on page 113.
4.	Deploy the WebInspect Script Engine (WISE) cluster in Kubernetes. For more information, see "Deploying WISE in Kubernetes" on page 114.
5.	Optionally, install the Fortify WebInspect sensor into the Kubernetes cluster using the WebInspect Helm Charts available on GitHub at https://github.com/fortify/helm3-charts.
6.	Configure one or more sensor pools for scan scaling. For more information, see "Creating a DAST Sensor Pool" on page 229. **Note:** Not all pools need to use scan scaling. You may only need one or two pools configured for scan scaling. You can then add your applications with long-running scans to the sensor pools that are configured for scan scaling.
7.	Configure scan scaling in scan settings. For more information, see "Enabling Scan Scaling" on page 183.

Downloading kubectl and Helm

Integrating ScanCentral DAST with Kubernetes requires use of the following software:

- kubectl - the command line tool used to control Kubernetes clusters. For more information about kubectl, refer to your Kubernetes documentation.

- Helm - the package manager for Kubernetes. For more information about Helm, refer to the Helm documentation at https://helm.sh/docs/.

The Helm CLI tool uses kubectl for all its interactions with Kubernetes clusters, so download and install these two software packages on the same machine.

Downloading in Windows PowerShell

To download kubectl and Helm in Windows:

1. In PowerShell, enter the following to download kubectl for Windows and add it to $PATH:

```
mkdir C:\docker\tools
cd C:\docker\tools Invoke-WebRequest `
 -Uri https://dl.k8s.io/release/v1.20.0/bin/windows/amd64/kubectl.exe `
 -OutFile .\kubectl.exe;
$env:Path += ";C:\docker\tools"
[Environment]::SetEnvironmentVariable("Path", $env:Path,
[EnvironmentVariableTarget]::Machine)
[Environment]::SetEnvironmentVariable("Path", $env:Path,
[EnvironmentVariableTarget]::User)
```

2. Enter the following to download and install Helm for windows:

```
Invoke-WebRequest `
 -Uri https://get.helm.sh/helm-v3.5.1-windows-amd64.zip `
 -OutFile .\helm-v3.5.1-windows-amd64.zip;
Unzip and copy helm.exe into: C:\docker\tools
rm .\helm-v3.5.1-windows-amd64.zip;
```

3. Enter the following to determine if the kubeconfig file points to the correct cluster:

```
kubectl cluster-info
```

Tip: You can change the default cluster by way of the `kubectl config set-context` command.

If you are using the Azure command-line interface (CLI), then you can use the following command:

```
az aks get-credentials --resource-group <resource-group-name>
       --name <Kubernetes-cluster-name>
```

Downloading in Linux

To download kubectl and Helm in Linux:

1. Enter the following to download and install kubectl in Linux:

```
curl -LO "https://dl.k8s.io/release/$(curl -L -s
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
sudo install -o root -g root -m 0755 kubectl /usr/local/bin/kubectl
```

2. Enter the following to download and install Helm in Linux:

```
wget https://get.helm.sh/helm-v3.5.0-linux-amd64.tar.gz
tar -xzf helm-v3.5.0-linux-amd64.tar.gz
cd ./<helm-tar-dir>
sudo install -o root -g root -m 0755 helm /usr/local/bin/helm
```

Deploying HAProxy in Kubernetes

The HAProxy Kubernetes ingress controller provides a way to route traffic into your Kubernetes cluster while providing load balancing and other features.

Important! Fortify recommends that the HAProxy ingress controller be deployed only by users who have experience configuring and managing Kubernetes clusters.

For more information, refer to your Kubernetes documentation.

Before You Begin

Ensure that you have downloaded and configured the prerequisite software. For more information, see "Downloading kubectl and Helm" on page 110.

Guideline for Configuring HAProxy in Azure

ScanCentral DAST integration with Kubernetes does not require an external or public IP address. Use caution with your ingress controller configuration to ensure that you do not expose the ingress controller into the Internet. This exposure will not happen in local Kubernetes clusters. However, an Azure ingress controller could be exposed to the Internet using a public IP address.

To prevent using a public IP address in Azure, use the following command for HAProxy Helm install:

```
--set-string
controller.service.annotations.'service\.beta\.kubernetes\.io/azure-load-
balancer-internal'=true"
```

For details about using an ingress controller with restricted public access in Azure, refer to Microsoft documentation.

Deploying HAProxy Ingress Controller

To deploy the HAProxy ingress controller:

- On the machine where the kubectl client and Helm are installed, enter the following in PowerShell:

```
kubectl label node <node-name> role=ingress-controller
helm repo add haproxy-ingress https://haproxy-ingress.github.io/charts
helm install haproxy-ingress haproxy-ingress/haproxy-ingress `
    --create-namespace --namespace=ingress-controller `
    --set controller.hostNetwork=true `
    --set controller.nodeSelector.role=ingress-controller `
    --set controller.service.type=LoadBalancer `
    --set-string controller.service.annotations.'service\.beta\.
      kubernetes\.io/azure-load-balancer-internal'=true
```

To confirm that the HAProxy ingress has started:

- Enter the following in PowerShell:

```
kubectl --namespace ingress-controller get services haproxy-ingress -o
wide
```

You should see a response similar to the following:

```
NAME              TYPE           CLUSTER-IP       EXTERNAL-IP
      PORT(S)                       AGE
haproxy-ingress   LoadBalancer   <ip_address>  <Pending>
     80:31255/TCP,443:30766/TCP   34s
```

Deploying the Kubernetes Metrics Server

Before you can deploy the WebInspect script engine (WISE) Docker container, you must deploy the Kubernetes Metrics Server to handle horizontal auto scaling for the Kubernetes WISE pods. The Metrics Server measures resource allocations, such as CPU and RAM, for nodes and pods. It provides information for Kubernetes Wise pods horizontal auto scaling to increase the number of pods during loading or decrease the number to the `wise.replicas.min` setting when there is no loading. For more information, see "Understanding the Parameters for WISE Deployment" on page 117.

Before You Begin

Ensure that you have downloaded and configured the prerequisite software. For more information, see "Downloading kubectl and Helm" on page 110.

Deploying the Metrics Server

For Azure Kubernetes, the Metrics Server is installed by default. For local Kubernetes cluster installation, however, this component may need to be installed manually.

To deploy the Metrics Server to Kubernetes:

- On the machine where the kubectl client and Helm are installed, enter the following in PowerShell:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/
          releases/latest/download/components.yaml
```

Confirming the Metrics Server Installation

To confirm that the Metrics Server exists and is working:

1. Enter the following in PowerShell:

   ```
   kubectl top nodes
   ```

   You should see a response similar to the following:

   ```
   NAME        CPU(cores)   CPU%   MEMORY(bytes)   MEMORY%
   rbp-main    141m         3%     1550Mi          19%
   rbp-node1   45m          0%     1476Mi          9%
   rbp-node2   47m          0%     1519Mi          9%
   ```

2. Enter the following:

   ```
   kubectl top po
   ```

   You should see a response similar to the following:

   ```
   NAME                                       CPU(cores)   MEMORY(bytes)
   wise-cluster-deployment-7747bb68b5-7q8m7   2m           96Mi
   wise-cluster-deployment-7747bb68b5-wl79m   2m           99Mi
   ```

Note: You can use the `kubectl top po` command to return the CPU and memory metrics for the WISE pods after WISE has been installed as described in "Deploying WISE in Kubernetes" below.

Deploying WISE in Kubernetes

The WebInspect script engine (WISE) is a Docker container that provides a remote script server client for the Fortify WebInspect sensor.

Important! Fortify recommends that the WISE cluster be deployed only by users who have experience configuring and managing Kubernetes clusters.

Before You Begin

Ensure that you have downloaded and configured the prerequisite software. For more information, see "Downloading kubectl and Helm" on page 110.

The `wise-cluster-23.1.tgz` file that you use to install WISE is included in the Fortify Software Security Center download package. It is packaged in a ZIP file named `Dynamic_Addons.zip`. You can find this ZIP file in the directory where you downloaded the Fortify Software Security Center installation package.

Additionally, ensure that you have deployed the Kubernetes Metrics Server to handle horizontal auto scaling for the Kubernetes WISE pods. For more information, see "Deploying the Kubernetes Metrics Server" on page 113.

Using the Default Parameters

To deploy the WISE cluster in Kubernetes using the default parameters:

- On the machine where the kubectl client and Helm are installed, enter the following in PowerShell:

```
helm install wi-script-engine wise-cluster-23.1.tgz
```

Viewing the Default Parameters

To view the default parameters in the TGZ file:

- Enter the following in PowerShell:

```
helm show values wise-cluster-23.1.tgz
```

You should see a response similar to the following:

```
# Default values for wise-cluster.
# This is a YAML-formatted file.
# Declare variables to be passed into wise-cluster templates.

wise:
  authtoken: ""
  nodeSelector: ""
  replicas:
    min: 2
    max: 10
    autoscale: true
    cpu:
```

```
      cores: "4"

  ingress:
    host: "wise-cluster"

  image:
    repository: "fortifydocker/wise"
    tag: "23.1.ubuntu.2204"
    pull:
      policy: IfNotPresent
      secret: wise-regcred
      registry: "https://index.docker.io/v1/"
      username: ""
      password: ""
```

Overriding the Default Parameters

To override any of the default values, use the `--set` command with the parameter name and desired value for each parameter to override as shown in the following example:

```
helm install wi-script-engine wise-cluster-23.1.tgz `
       --set wise.image.pull.registry=<container_registry> `
       --set wise.image.repository=fortifydocker/wise `
       --set wise.image.pull.username=<username> `
       --set wise.image.pull.password=<password> `
       --set wise.image.tag=<tagname> `
       --set wise.replicas.min=2 `
       --set wise.ingress.host=<hostname> `
       --set wise.authtoken=<token>
```

Tip: For Helm in PowerShell, the backtick character (`) at the end of each line is the new line character. For Helm in Linux, the backslash character (\) is the new line character.

Installing WISE Into a Kubernetes Namespace

By default, the `helm install wi-script-engine...` command installs WISE into the Kubernetes default namespace. If your organization uses Kubernetes namespaces, you can create a new namespace and install WISE into it, or install WISE into an existing namespace.

Important! If you install WISE into a specific namespace, then all kubectl and Helm commands for managing the WISE installation must contain `--namespace=<wise_namespace>`. For example:

```
helm ls --namespace=<wise_namespace>
kubectl get po --namespace=<wise_namespace>
```

To create a namespace and install WISE:

- Add the following command to the `helm install...` command, either before or after the `--set` commands:

  ```
  --create-namespace --namespace=<wise_namespace> `
  ```

  The namespace is created and WISE is installed into it.

You can also view a list of your existing namespaces and choose a namespace for your WISE installation.

To view existing namespaces:

- Enter the following in PowerShell:

  ```
  kubectl get ns
  ```

  You should see a response similar to the following:

  ```
  NAME                 STATUS   AGE
  default              Active   54d
  ingress-controller   Active   54d
  kube-node-lease      Active   54d
  kube-public          Active   54d
  kube-system          Active   54d
  ```

To install WISE into an existing namespace:

- Add the following command to the `helm install...` command, either before or after the `--set` commands:

  ```
  --namespace=<wise_namespace> `
  ```

Understanding the Parameters for WISE Deployment

The following table describes the parameters that are used to deploy the WISE cluster.

Parameter	Description
`wise.image.pull.registry`	Optionally, specifies the Docker registry for a private repository. For example, if you use Azure and have created an Azure container registry to keep images that will be used in

Parameter	Description
	your Azure Kubernetes installation, you might specify something similar to `myreg.azurecr.io`.
`wise.image.pull.username`	Identifies the Docker repository username used to pull the WISE image.
`wise.image.pull.password`	Identifies the Docker repository password used to pull the WISE image.
`wise.image.repository`	Specifies the Fortify Docker repository from which to pull the WISE image. This is `fortifydocker/wise`. **Note:** If you use a private repository, you might specify something similar to `myreg.azurecr.io/wise`.
`wise.image.tag`	Specifies the WISE Docker image build and the operating system on which it was built.
`wise.replicas.min`	Indicates the minimal number of WISE Kubernetes pods that will be started. Consider the following facts when configuring this parameter: • If the `wise.replicas.min` setting is higher than Kubernetes cluster hardware resources can handle, then Kubernetes will not start all pods and their state will be set to "Pending." Kubernetes horizontal pods auto-scaler *will not* reduce the number of WISE pods lower than the configured `wise.replicas.min` setting. • If the `wise.replicas.min` setting is too low and Kubernetes cluster still has free resources during WISE cluster loading, then Kubernetes horizontal pods auto-scaler *will* increase the number of replicas.
`wise.ingress.host`	Specifies the ingress virtual wise cluster hostname. **Important!** You can use any hostname value, but you must configure your DNS server or the hostfile on your Fortify WebInspect sensor client box to associate it with the IP address of the Kubernetes node that runs the HAProxy ingress.

Parameter	Description
`wise.authtoken`	Optionally, specifies authentication for the WISE cluster. If the authtoken is configured, then Fortify WebInspect sensor clients will be required to provide an authtoken. **Tip:** Make note of this token. You must enter it when configuring your sensor pools for scan scaling.

Uninstalling WISE

To uninstall WISE:

- Enter the following in PowerShell:

```
helm uninstall wi-script-engine
```

Chapter 3: Understanding the User Interface

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with the following items directly in Fortify Software Security Center:

- DAST scans
- Sensors and sensor pools
- Scan settings
- Scan schedules

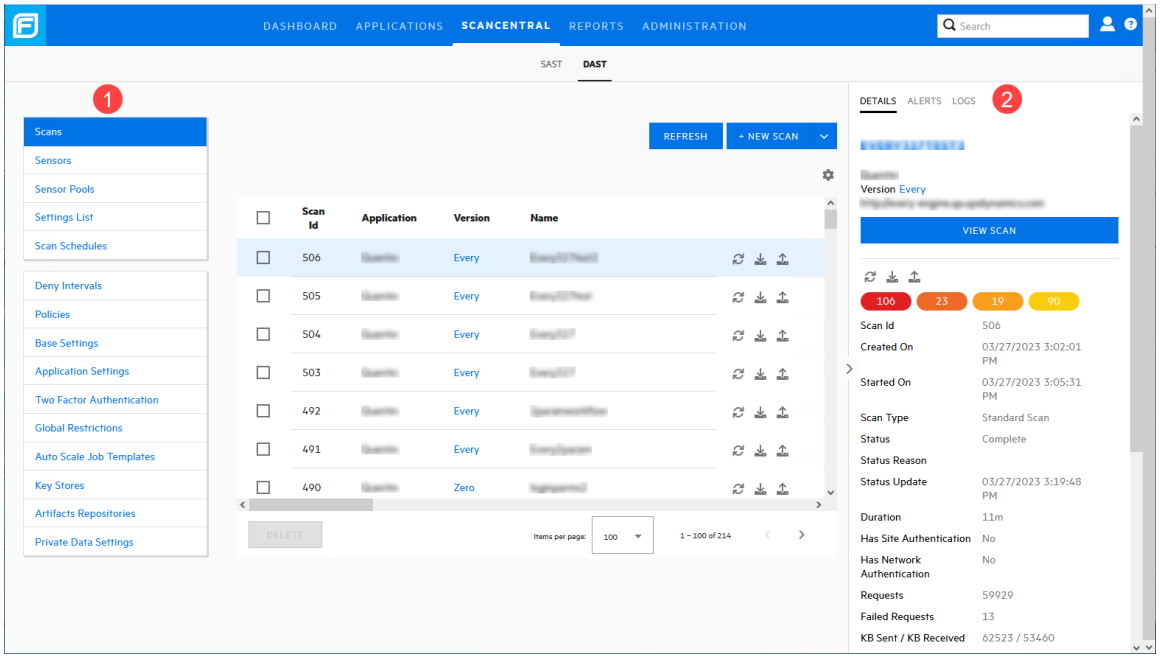
Depending on your permissions in Fortify Software Security Center, you may also be able to work with the following global settings:

- Deny intervals
- Custom policies
- Base settings
- Application settings
- Two-factor authentication
- Auto Scale Job Templates
- Global restrictions and private data settings
- Key Stores and artifacts repositories

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools.

ScanCentral DAST User Interface

The following image shows the Fortify ScanCentral DAST user interface in Fortify Software Security Center.

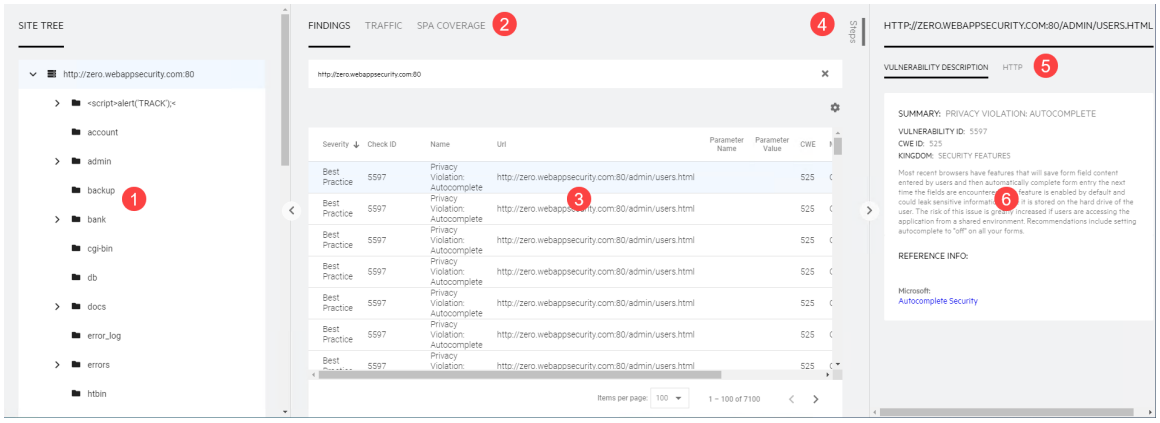


The following table describes the areas called out in the previous image.

Item	Description
1	The left panel allows you to navigate to the Fortify ScanCentral DAST pages that are available in Fortify Software Security Center.
2	The detail panel displays additional information about the item selected in the table.

Scan Visualization

When you open a scan, the scan appears on a new tab in your browser. The following image shows the default view for an open scan.



The following table describes the display areas of the default view for an open scan.

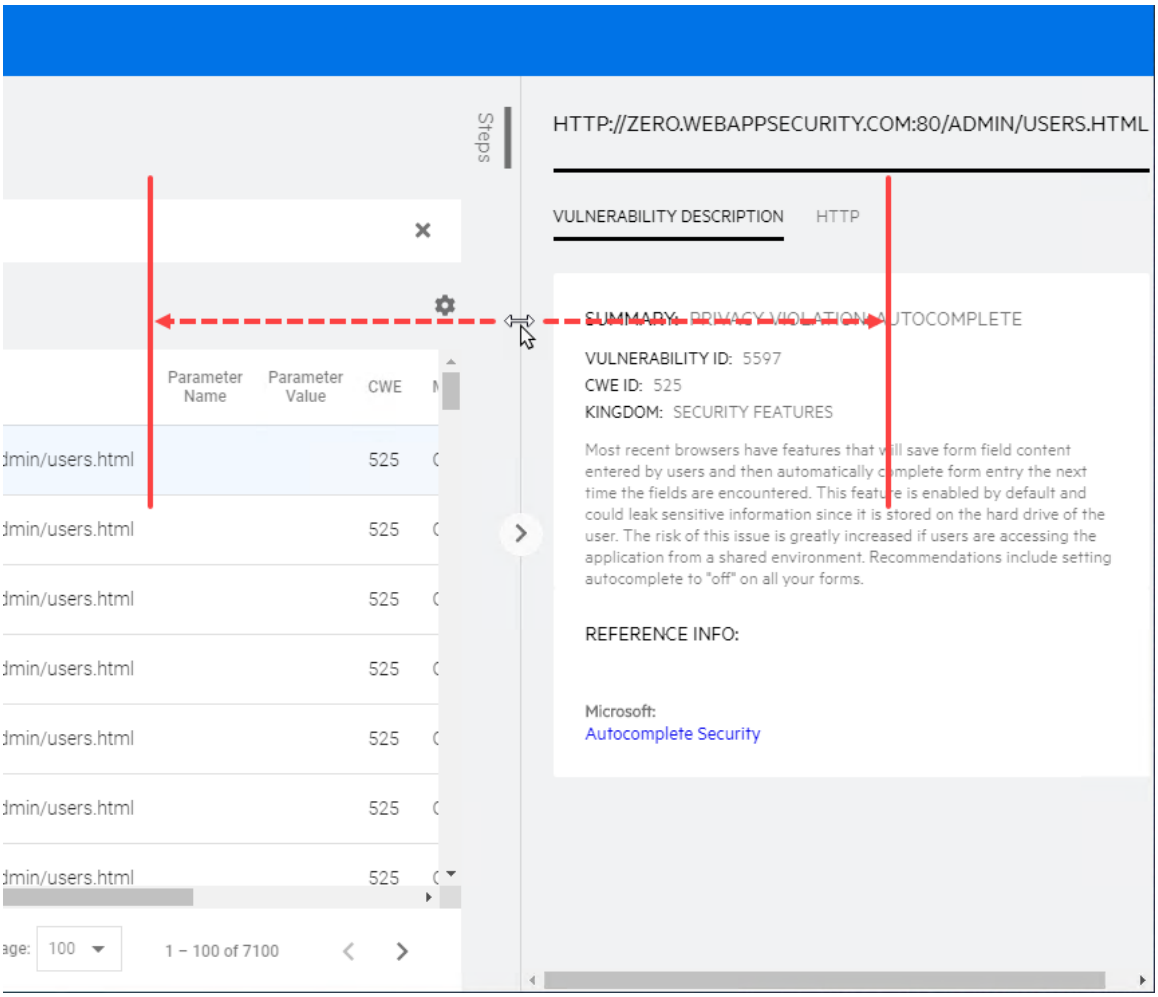
Item	Description
1	Site Tree (see "Working with the Site Tree" on page 214)
2	Findings, Traffic, and SPA Coverage tabs **Note:** The SPA Coverage tab is available only for scans that include SPA events.
3	Findings, Traffic, and SPA Coverage table views (See "Understanding the Findings Table" on page 216, "Understanding the Traffic Table" on page 219, and "Understanding SPA Coverage" on page 222)
4	Steps tab (See "Working with Findings" on page 218 and "Working with Traffic" on page 221)
5	Vulnerability Description, HTTP, and Parameter tabs
6	Vulnerability Description, HTTP, and Parameter detail views (See "Working with Findings" on page 218 and "Working with Traffic" on page 221)

Resizing the Display Areas

You can resize the Site Tree, the Findings, Traffic, and SPA Coverage view, and the Vulnerability Description, HTTP, and Parameter view.

To resize an area:

- Drag the display area border either right or left to the width you want.



Hiding and Showing a Display Area

By default, the Site Tree and the Vulnerability Description, HTTP, and Parameter view are visible when you open a scan. You can hide the Site Tree and the Vulnerability Description, HTTP, and Parameter view.

To hide an area:

- To hide the Site Tree, click the collapse icon (‹).
- To hide the Vulnerability Description, HTTP, and Parameter view, click the collapse icon (›).

To show an area:

- To show the Site Tree, click the expand icon (›).
- To show the Vulnerability Description, HTTP, and Parameter view, click the expand icon (‹).

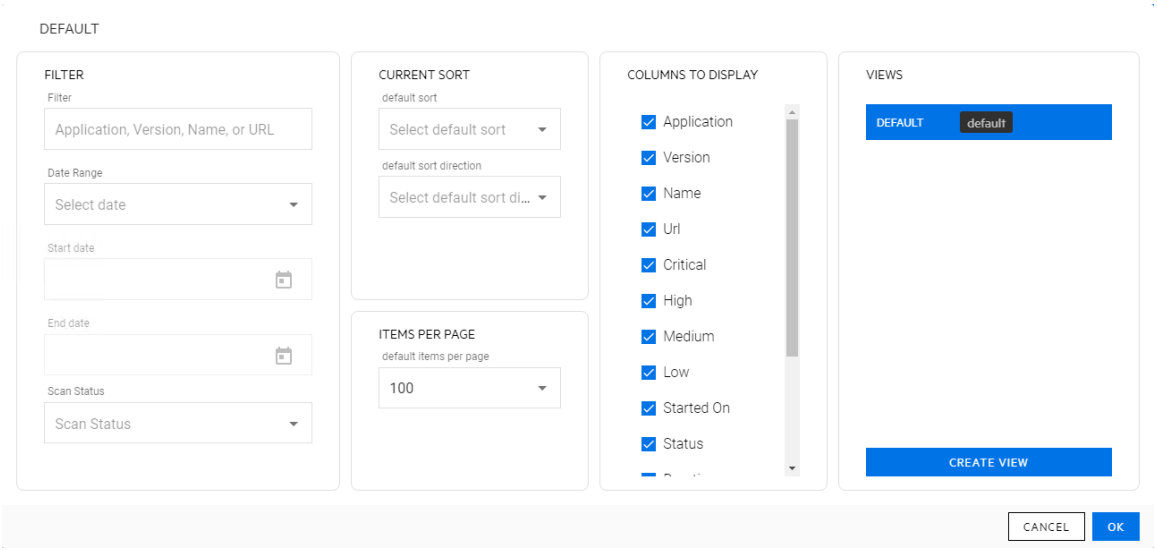
Working with Tables

Much of the data available in ScanCentral DAST is presented in tables. You can customize those tables and then save the customized views. Table preferences are saved per user.

The factory default view is named DEFAULT. You can edit the default view or use the default view to create custom views.

Customizing Table Views

You can edit existing views or create new views in the table preferences panel.



The table preferences panel allows you to customize the following:

- Filtering (see "Understanding Basic Filters in Tables" on page 127 and "Understanding Advanced Filters in Tables" on page 130)
- Sorting (see "Sorting Data in Columns" on page 133)
- Items Per Page (see "Viewing Content on Multiple Pages" on page 135)
- Columns to Display (see "Managing Columns in Tables" on the next page)

Note: Not all preference options are available for all tables. Some tables include only a subset of the preferences.

Updating or Creating a View

After making changes to an existing view, you can either update the existing view or create a new view.

To update the original view with the new settings:

- In the table preferences panel, click **UPDATE *<VIEW NAME>***.

To create a new view using the new settings:

1. In the table preferences panel, click **CREATE VIEW**.
   The CREATE VIEW dialog box opens.
2. In the **View name** box, type a name for the new view.
3. (Optional) To make the new view the default view, select **Make default**.
4. Click **OK**.

Selecting a Different View

To select an existing view:

1. Click the table preferences icon ( ).
   The table preferences panel opens.
2. In the **VIEWS** list, select a view.

   Note: If you have unsaved changes in the current view and attempt to switch views, you will be prompted that the changes will be lost.
3. Click **OK**.

Managing Columns in Tables

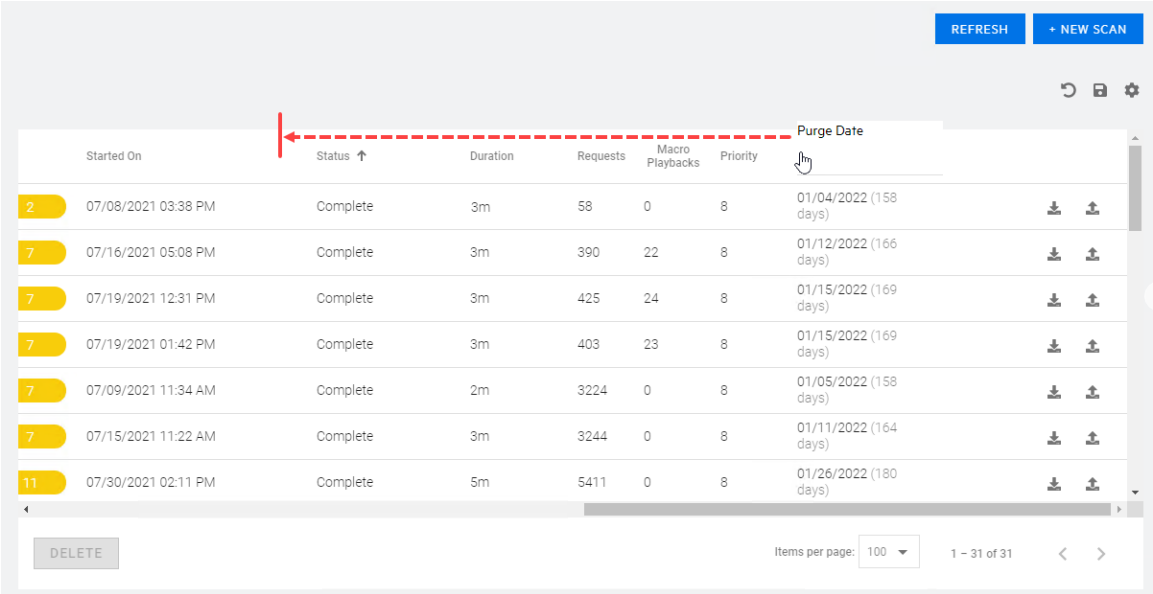
You can customize the order in which columns appear in tables, as well as change the columns to display in tables.

Rearranging the Columns

You can rearrange the order in which the columns appear in the table.

To move a column:

1. Click the column heading that you want to move.
2. Drag the column right or left and drop it into its new position.



Note: You cannot move the column of check boxes or columns containing icons, such as the download (⬇) and publish (⬆) icons.

Adding and Removing Columns

You can use the table preferences panel to select which columns of data you want visible in the table.

To add or remove displayed columns:

1. Click the table preferences icon (⚙).
   The table preferences panel opens.
2. In the **COLUMNS TO DISPLAY** area, do the following:
   - Select the column checkbox to display the column.
   - Clear the column checkbox to hide the column.
3. Click **OK**.

When New Columns Are Available

If you have customized a table view, such as added or removed columns, rearranged the order of columns, changed the sort order, and so forth, then when new columns of data are added to the table, you will not see them by default. Instead, the following message will appear near the top of the page:

New columns are available for the *<table_name>* table.

To view the new columns:

- Click the table preferences icon ( ).
  The table preferences panel opens.

To clear the message:

- Click **OK**.
  The message is cleared and will not appear again for the selected table unless new columns are added in a future update.

Understanding Basic Filters in Tables

Basic filtering allows you to filter on certain columns of data in the Scans and Settings List tables.

You can filter data in the Scans table by application, version, name, or URL. You can also filter by scan start date, end date, date range, scan status, or a combination thereof.

You can filter data in the Settings List table by name, application, or version. You can also filter by scan start date, end date, date range, scan type, or a combination thereof.

Additionally, you can combine filtering by Application, Version, Name, or URL with Date, Scan Status, or Scan Type.

Guidelines

The following guidelines apply to basic filtering:

- You can use partial words for filtering. For example, using the filter criteria "che" includes the application named "OnlineParcheesi" and scans named "Allchecks" in the filter results.
- You cannot use wildcard characters, such as the asterisk (*), as placeholders.
- You cannot use regular expressions.

Using Basic Filters in Tables

This topic describes how to access the basic filter user interface, specify filter criteria, and clear filters.

Accessing the Basic Filter Feature

You can access the basic filter feature in the table preferences panel for the Scans table and the Settings List table.

To access the basic filter feature:

- In the **Scans** or **Settings List** table view, click the table preferences icon ( ).
  The table preferences panel opens.

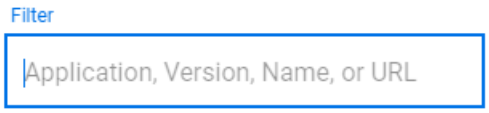
Specify the filter criteria in the **FILTER** area as described in "Filtering by Application, Version, Name, or URL" below and "Filtering by Date, Scan Status, or Scan Type" below.

Filtering by Application, Version, Name, or URL

You can use filter criteria to filter across the Application, Version, Name, and URL columns of data in the Scans table. For example, if you use the filter criteria "OurEstore," then all applications named "OurEstore" and all scans named "OurEstore" will be included in the filtered data. Similarly, you can filter across the Name, Application, and Version columns in the Settings List table. This procedure illustrates filtering in the Scans table, but it also works in the Settings List table.

To filter by application, version, name, or URL:

1. In the **FILTER** area, type the filter criteria into the **Filter** box.

   Note: Type only one application, one version, one name, or one URL. Do not combine filter criteria in the Filter box.

2. Click **OK**.

   The table displays the data matching the filter criteria in any of the four columns.

Tip: To combine filtering by Application, Version, Name, or URL with Date, Scan Status, or Scan Type, proceed to "Filtering by Date, Scan Status, or Scan Type" below before you click **OK**.

Filtering by Date, Scan Status, or Scan Type

You can filter by date range, specific date, scan status, or a combination of date and scan status in the Scans table. Similarly, you can filter by date range, specific date, scan type, or a combination of date and scan type in the Settings List table. However, when you filter on a date in the Settings List table, you are filtering on the Modified date column. This procedure describes filtering in either the Scans table or the Settings List table.

To filter by date or Scan Status or Scan Type:

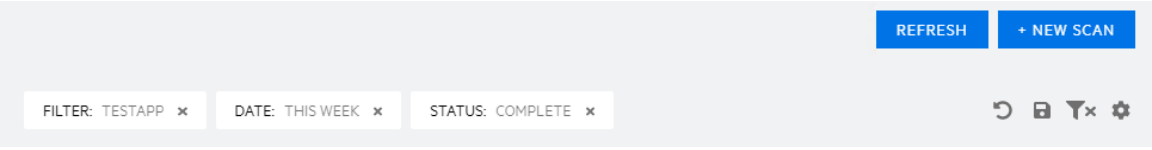
1. In the **FILTER** area, continue according to the following table.

To filter by...	Then...
A date range	Select a range from the **Date Range** list. Options are **This week**, **This month**, **Last year**, and **Custom Range**. If you select Custom Range, type dates for the range in the **Start date** and **End date** fields. **Tip:** Click the calendar icon ( ) to select dates from a calendar.
Scan status in the Scans list	Select a scan status from the **Scan Status** list.
A date range and scan status in the Scans list	Select a range from the **Date Range** list and a scan status from the **Scan Status** list.
Scan type in the Settings List	Select a scan type from the **Scan Type** list.
A date range and scan type in the Settings List	Select a range from the **Date Range** list and a scan status from the **Scan Status** list.

2. Click **OK**.

Clearing the Filter

Active filters appear as tiles at the top of the table. For basic filters, the filter value is listed in each filter tile.



To clear a filter:

- Click the remove filter icon (×) on the filter tile.

To clear all filters:

- Click the clear filters icon ( ).

Important! Making changes outside of the table preferences panel adds a save table preferences icon (💾) to the left of the table preferences icon. Clicking the save table preferences icon saves the changes to the current view.

Understanding Advanced Filters in Tables

Advanced filtering allows you to construct filters using fields, operators, and conditions. The Findings and Traffic tables of a completed scan offer advanced filtering.

Important! Bear in mind that selecting a resource in the Site Tree filters data to that resource in the Findings and Traffic tables. Advanced filters are then applied to the data that is already filtered.

Understanding the Operators

The following table describes the operators that are available for each type of data in advanced filtering.

Operator	Data Type			
	String	Numeric	Date/Time	Enum[1]
Equal	x	x	x	x
Not Equal	x	x	x	x
Less Than		x	x	
Less Than or Equal		x	x	
Greater Than		x	x	
Greater Than or Equal		x	x	
Between		x	x	
Contains	x	x		
Starts With	x	x		
Ends With	x	x		

[1]Enumerator data consists of a key-value pair and is always presented as a list for filtering.

Understanding Conditions and Field Filters

Field filters are treated as AND filters. For example, creating a field filter for a Severity of "High" and a field filter for a Method of "GET" filters in all records with a Severity of High AND a Method of GET.

For each field filter, you can add conditions. These conditions are treated as OR. For example, creating a field filter for a Severity of "High" and adding a condition for a Severity of "Medium" filters in all records with either a Severity of High or of Medium.

Using Advanced Filters in Tables

This topic describes how to access the advanced filter user interface, construct filters, and clear filters.

Accessing the Advance Filter Feature

You can access the advanced filter feature in the table preferences panel for the Findings table and the Traffic table.

To access the advance filter feature:

1. In the **Findings** or **Traffic** table of an open scan, click the table preferences (⚙) icon.
   The table preferences panel opens.
2. In the **FILTER** area, click **ADD FILTER**.
   The ADVANCED FILTER dialog box opens.

Creating an Advanced Filter

You can create an advanced filter by specifying a field, an operator, and one or more values.

To create an advanced filter in the ADVANCED FILTER dialog box:

1. In the **Field** list, select a field to filter.
2. In the **Operator** box, select an operator. For more information, see the "Understanding the Operators" on the previous page.
3. In the box to the right of the operator, select a value from the list or type a text string.
4. Do you want to add another condition to the current filter?
   - If *yes*, click **ADD CONDITION**, and repeat steps 2 and 3.

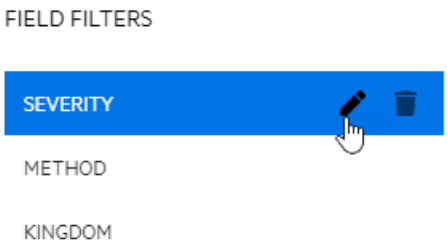
     Note: Each condition is treated as an "OR" condition. For more information, see "Understanding Conditions and Field Filters" above.
   - If *no*, go to step 5.
5. Click **OK**.

Editing an Advanced Filter Condition

You can edit the conditions for an advanced filter.

To edit a condition:

1. Click the table preferences icon ( ).
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click the edit filter icon for the condition you want to edit.



   The ADVANCED FILTER dialog box opens.
3. Make edits as needed.
4. Click **OK**.

Removing an Advanced Filter Condition

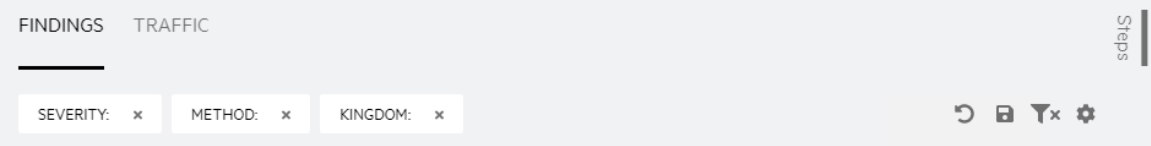
You can remove a condition for an advanced filter.

To remove a condition:

1. Click the table preferences icon ( ).
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click the edit filter icon.
   The ADVANCED FILTER dialog box opens.
3. In the **ADVANCED FILTER** dialog box, click the remove condition icon (×) next to condition to delete.
   The condition is removed.
4. Click **OK**.

Clearing Filters

Active filters appear as tiles at the top of the table. For advanced filters, the field name is listed in each filter tile.



To clear a filter:

- Click the remove filter icon (×) on the filter tile.

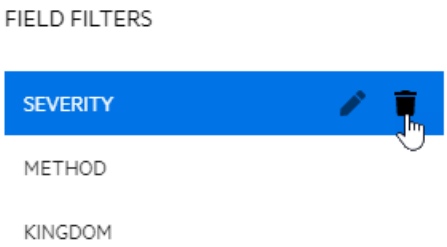
To clear all filters:

- Click the clear filters icon ( ).

Important! Making changes outside of the table preferences panel adds a save table preferences icon ( ) to the left of the table preferences icon. Clicking the save table preferences icon saves the changes to the current view.

To clear a filter from the table preferences:

1. Click the table preferences icon ( ).
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click the delete filter icon.



   The filter is deleted.
3. Click **OK**.

Sorting Data in Columns

By default, columns of text in tables are listed in alphabetical order, columns of dates are in chronological order, and columns of numerical data are in numerical order. You can change the sorting directly in the table or in the table preferences panel.

Important! Making changes outside of the table preferences panel adds a save table preferences icon ( ) to the left of the table preferences icon. Clicking the save table preferences icon saves the changes to the current view.

Known Issue with Sorting

In some columns, ascending and descending sorting sorts on a numeric value in the database, rather than on the alphabetical order of the text displayed. Therefore, sorting order may not appear as expected. For example, when sorting the sensor Status column in ascending order, one would expect to see the following alphabetical order:

- Offline
- Online

However, the sort order is based on the numeric values of 1 and 2 in the DAST database, rendering the following sort order:

- Online (represented by 1 in the database)
- Offline (represented by 2 in the database)

Sorting Directly in the Table

To change the sort order on any column of data:

- Click the column name.
  The arrow next to the column name indicates the new sort order.

To reverse the current sort order:

- Click the column name again.
  The arrow next to the column name indicates the reverse sort order.

To clear the sorting:

- Click the column name a third time.
  The arrow next to the column name disappears.

Sorting in the Table Preferences Panel

To sort table data in the table preferences panel:

1. Click the table preferences icon ( ).
   The table preferences panel opens.

2. In the **default sort** list of the **CURRENT SORT** area, select a column to sort.

   Note: If a column is hidden in the current view, you cannot select the column for sorting.

3. In the **default sort direction** list, do one of the following:
   - Select **asc** for ascending sort order.
   - Select **desc** for descending sort order.
4. Click **OK**.

Searching in Input Boxes

When search is available for an input box, a search tip appears in the box as shown below.

To search:

- Type the search criteria in the input box, and then click the search icon ( ).

Clearing Data from Input Boxes

For any input box in which you entered search criteria or for which you selected recently used data, such as recently used options from a drop-down list box, you can quickly clear the data without manually deleting it.

To clear data from an input box:

- Click the **Clear** ( ) icon.

Viewing Content on Multiple Pages

If you have multiple pages of content, you can use the page navigation options to change the number of items displayed per page and navigate through the pages.

Changing the Number of Items Displayed

The default number of items displayed per page is 100. You can change the number to 5, 10, 25, or 50.

To change the number of items displayed:

- Select a number from the **Items per page** drop-down list.

Important! Making changes outside of the table preferences panel adds a save table preferences icon ( ) to the left of the table preferences icon. Clicking the save table preferences icon saves the changes to the current view.

Navigating Multiple Pages

When the number of items you are viewing spans multiple pages, you can navigate through the pages using the page navigation icons.

To view the next page of items:

- Click the **Next page** ( ) icon.

To view the previous page of items:

- Click the **Previous page** ( ) icon.

Changing the Number of Items Displayed in the Table Preferences Panel

To change the number of items listed per page in the table preferences panel:

1. Click the table preferences icon ( ).
   The table preferences panel opens.
2. In the **default items per page** list in the **ITEMS PER PAGE** area, select the number of items to view.
3. Click **OK**.

Chapter 4: Configuring a Scan

Use the Settings Configuration wizard to configure a Fortify ScanCentral DAST scan of your Web application, API, and Web services to assess potential security flaws. A ScanCentral DAST scan is an automated scan of your Web application and Web services, rather than a scan of your code. It is designed to apply attack algorithms to locate vulnerabilities, determine their severity, and provide the information you need to fix them.

What is a Scan?

The ScanCentral DAST sensor, which is a Fortify WebInspect sensor, uses two basic modes for determining the security weaknesses of your Web application and Web services:

- Crawl - The process by which the sensor identifies the structure of the target Web site. In essence, a crawl runs until no more links on the URL can be followed.
- Audit - The actual vulnerability assessment.

A scan can combine the application crawl and audit phases into a single fluid process, or it can be a crawl-only or an audit-only scan. The scan is refined based on real-time audit findings, resulting in a comprehensive view of an entire Web application's attack surface.

Important Consideration About API Definition Files

The WebInspect sensor attempts to generate the definition from the URL provided in the settings. It assumes that the API endpoint is the same URL, but without the definition file name. If your service is at the same location as your definition file, which is generally the case for GraphQL, then providing a URL will work. However, the definition may be in a different location for SOAP and gRPC.

Important Information About gRPC Proto Files

All gRPC proto files must be self-contained. Any imports must be to internally recognized resources and not to user-generated files. The WebInspect sensor cannot identify file paths from imported proto files. If such files are used, the scan will fail to generate the client and will be interrupted. If additional imports are needed, they must be combined with the primary proto file into a "master" proto file.

Known Limitations of gRPC Scans

Be aware of the following known limitations associated with gRPC scans:

- A Fortify WebInspect sensor installed on Windows 11 or a Linux version of the sensor is required for conducting scans of gRPC APIs.
- You must use a Linux version of the Fortify WebInspect sensor to conduct a scan of a gRPC API running on a server with unencrypted HTTP/2 (H2C).

Preparing Your System for Audit

The Fortify WebInspect sensor is an aggressive web application analyzer that rigorously inspects your entire website for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which Fortify ScanCentral DAST policy you apply and the options you select, it can affect server and application throughput and efficiency. When using the most aggressive policies, Fortify recommends that you perform this analysis in a controlled environment while monitoring your servers.

Sensitive Data

The WebInspect sensor captures and displays all application data sent between the application and server. It might even discover sensitive data in your application that you are not aware of. Fortify recommends that you follow one of these best practices regarding sensitive data:

- Do not use potentially sensitive data, such as real user names and passwords, while testing with the WebInspect sensor.
- Do not allow ScanCentral DAST scans, related artifacts, and data stores to be accessed by anyone unauthorized to access potentially sensitive data.

Network authentication credentials are not displayed in ScanCentral DAST and are encrypted when stored in settings.

Firewalls, Anti-virus Software, and Intrusion Detection Systems

The WebInspect sensor sends attacks to servers, and then analyzes and stores the results. Web application firewalls (WAF), anti-virus software, firewalls, and intrusion detection/prevention systems (IDS/IPS) are in place to prevent these activities. Therefore, these tools can be problematic when conducting a scan for vulnerabilities.

First, these tools can interfere with the WebInspect sensor's scanning of a server. An attack that the WebInspect sensor sends to the server can be intercepted, resulting in a failed request to the server. If the server is vulnerable to that attack, then a false negative is possible.

Second, results or attacks that are in the ScanCentral DAST product, cached on disk locally, or in the database can be identified and quarantined by these tools. When working files used by the WebInspect sensor or data in the database are quarantined, the sensor can produce inconsistent results. Such quarantined files and data can also cause unexpected behavior.

These types of issues are environmentally specific, though McAfee IPS is known to cause both types of problems, and any WAF will cause the first problem. Fortify has seen other issues related to these tools as well.

If such issues arise while conducting a scan, Fortify recommends that you disable WAF, anti-virus software, firewall, and IDS/IPS tools for the duration of the scan. Doing so is the only way to be sure you are getting reliable scan results.

Effects to Consider

During an audit of any type, the WebInspect sensor submits a large number of HTTP requests, many of which have "invalid" parameters. On slower systems, the volume of requests may degrade or deny access to the system by other users. Additionally, if you are using an intrusion detection system, it will identify numerous illegal access attempts.

To conduct a thorough scan, the WebInspect sensor attempts to identify every page, form, file, and folder in your application. If the option to submit forms during a crawl of your site is selected, the sensor will complete and submit all forms it encounters. Although this enables the sensor to navigate seamlessly through your application, it may also produce the following consequences:

- If, when a user normally submits a form, the application creates and sends e-mails or bulletin board postings (to a product support or sales group, for example), the WebInspect sensor will also generate these messages as part of its probe.
- If normal form submission causes records to be added to a database, then the forms that the WebInspect sensor submits will create spurious records.

During the audit phase of a scan, the WebInspect sensor resubmits forms many times, manipulating every possible parameter to reveal problems in the applications. This greatly increases the number of messages and database records created.

Helpful Hints

- For systems that write records to a back-end server (database, LDAP, and so on) based on forms submitted by clients, some ScanCentral DAST users, before auditing their production system, backup their database, and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit to search for and delete records that contain one or more of the form values submitted by the WebInspect sensor. You can determine these values by opening the Web Form Editor.
- If your system generates e-mail messages in response to user-submitted forms, consider disabling your mail server. Alternatively, you could redirect all e-mails to a queue and then, following the audit, manually review and delete those e-mails that were generated in response to forms submitted by the WebInspect sensor.

- The WebInspect sensor can be configured to send up to 75 concurrent HTTP requests before it waits for an HTTP response to the first request. The default thread count setting is 5 for a crawl and 10 for an audit (if using separate requestors). In some environments, you may need to specify a lower number to avoid application or server failure. For more information, see Scan Settings: Requestor in the *Micro Focus Fortify WebInspect User Guide*.
- If, for any reason, you do not want the WebInspect sensor to crawl and attack certain directories, you must specify those directories in the Basic Exclusions list when configuring your scan. For more information, see "Creating and Managing Exclusions" on page 177 or "Creating and Managing Exclusions in Base Settings" on page 288.
- By default, the WebInspect sensor is configured to ignore many binary files (images, documents, and so on) that are commonly found in web applications. These documents cannot be crawled or attacked, so there is no value in auditing them. Bypassing these documents greatly increases the audit speed. If proprietary documents are in use, determine the file extensions of the documents and exclude them within the sensor's default settings. For more information, see Scan Settings: Session Exclusions and Crawl Settings: Session Exclusions in the *Micro Focus Fortify WebInspect User Guide*. If, during a crawl, the sensor becomes extremely slow or stops, it may be because it attempted to download a binary document.
- For form submission, the WebInspect sensor submits data extracted from a prepackaged file. If you require specific values (such as user names and passwords), you must create a file with Fortify's Web Form Editor and identify that file to the WebInspect sensor. For more information, see the *Micro Focus Fortify WebInspect Tools Guide*.
- The WebInspect sensor tests for certain vulnerabilities by attempting to upload files to your server. If your server allows this, the sensor will record this susceptibility in its scan report and attempt to delete the file. Sometimes, however, the server prevents file deletion. For this reason, search for and delete files with names that start with "CreatedByHP" as a routine part of your post-scan maintenance.

Accessing Settings Configuration from Software Security Center

You can access the Settings Configuration wizard and configure a ScanCentral DAST scan from Fortify Software Security Center.

Accessing from the DAST Scans List

To access the Settings Configuration wizard from the ScanCentral DAST Scans list:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. On the **Scans** list, click **+ NEW SCAN**.
   The Settings Configuration wizard opens.

Accessing from the Settings List

To access the Settings Configuration wizard from the ScanCentral DAST Settings List page:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Settings List**.
3. Click **+ NEW SETTINGS**.
   The Settings Configuration wizard opens.

Restricting or Allowing Edits

If you have permissions to manage restricted scan settings, then you can restrict the editing of settings. If a setting is already restricted, you can allow editing.

To restrict editing:

- Click the restrict *<setting name>* icon ( ).

To allow editing:

- Click the allow *<setting name>* icon ( ).

If you do not have permissions to manage restricted scan settings, then you cannot edit any settings with the restricted icon ( ).

For more information, see "Permissions in Fortify Software Security Center" on page 40.

What's Next?

To learn about using key store placeholders in scan settings, see "Using Key Stores in Settings" below.

To learn about using artifacts from repositories in scan settings, see "Using Artifacts from a Repository in Settings" on page 143.

Otherwise, proceed with "Getting Started" on page 145.

Using Key Stores in Settings

You can use a key store placeholder in scan settings, base settings, or macro parameters for any field that displays the **Open key store** icon ( ). When the settings are downloaded or used to start a scan, the placeholder in the settings is replaced with the corresponding value from the key store entry. Using placeholder text instead of hard-coded data in settings fields allows the ScanCentral DAST administrator to change the key store entry value in one place and the value is updated in all settings

where the placeholder is used. For more information about key stores, see "Understanding Key Stores" on page 327.

Guidelines for Key Store Usage

A scan setting field can use a single key store placeholder, a combination of text and placeholder, or multiple placeholders, as shown in the following examples:

- `${DAST_KS_KeystoreName_KeyStoreEntryName}`
- `www.${DAST_KS_KeystoreName_KeyStoreEntryName}.com`
- `${DAST_KS_KeystoreName_KeyStoreEntryName1}${DAST_KS_KeystoreName_KeyStoreEntryName2}`

Using a Key Store Placeholder

To use key store placeholder text in scan settings, base settings, or macro parameter:

1. Click the **Open key store** icon (🔑) in the setting field.
   The KEY STORE dialog box opens.
2. In the **KEY STORE** list, select the key store whose entry you want to use.
3. In the **KEY STORE ENTRY** list, select the entry whose placeholder and value you want to use.
   The KEY STORE ENTRY SELECTION displays your placeholder text with the value masked.

   Tip: To view the stored value for the placeholder text, click **REVEAL VALUE**.
4. Click **OK**.

The placeholder text is added to the settings field.

Viewing, Clearing, or Replacing the Key Store Entry Value

You may view the key store entry value after placeholder text is added to the settings field. You may also remove the placeholder from the field or replace it with a different placeholder.

To view, clear, or replace the key store entry value:

1. Click the **Open key store** icon (🔑) to the right of the placeholder text in the field.
   A summary dialog box opens with the value masked.
2. Continue according to the following table.

If you want to...	Then...
View the key store entry value	Click **REVEAL VALUE**.
Remove the key store placeholder from the	Click **CLEAR**.

If you want to...	Then...
field	
Replace the key store placeholder with a different placeholder	a. Click **REPLACE**. The KEY STORE dialog box opens. b. Follow Steps 2-4 of the "Using a Key Store Placeholder" on the previous page.

Manually Editing a Key Store Placeholder in Settings

You can type any text in the field before a placeholder or after a placeholder or before and after a placeholder. There are no restrictions on the text. The placeholder text will be replaced with the key store entry value.

For example, `http://www.myqa_testsite1.com`, could be expressed as `http://www.${DAST_KS_KeyStoreName_KeyStoreEntryName}.com` in the URL field.

Any entry in a field that includes the format `${DAST_KS_KeystoreName_KeyStoreEntryName}` is identified by ScanCentral DAST as a key store placeholder. If you manually edit this placeholder to include two sequential underscore characters, such as `${DAST_KS_KeystoreName__KeyStoreEntryName}`, or any other change that alters the format, it will no longer be identified by ScanCentral DAST as a key store placeholder.

If you manually type key store placeholder text, but the key store does not exist, the **Key store entry may not exist** icon (🔑) indicates that the key store placeholder text does not exist in the key store. This icon may also indicate that the key store placeholder text exists, but is not assigned to the selected application for which the settings apply.

What's Next?

To learn about using artifacts from repositories in scan settings, see "Using Artifacts from a Repository in Settings" below.

Otherwise, proceed with "Getting Started" on page 145.

Using Artifacts from a Repository in Settings

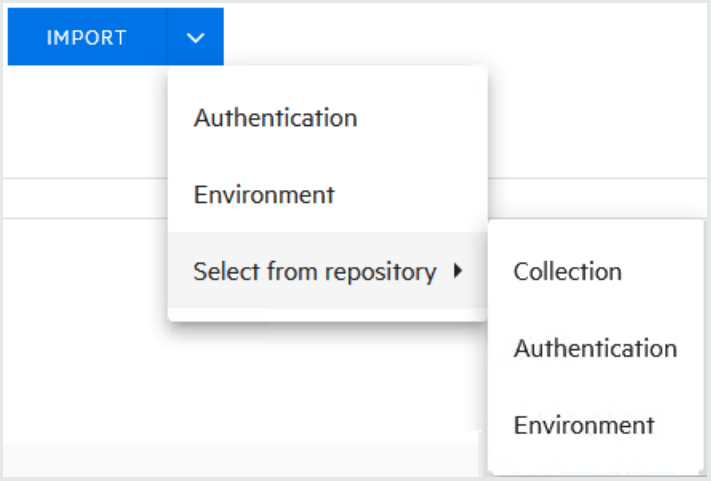
You can use an artifact from a repository for any setting in scan settings or base settings that allows you to import a file. For more information about key stores, see "Understanding Artifacts Repositories" on page 334.

To use an artifact from a repository:

1. Click the **IMPORT** drop-down arrow, and then click **Select From Repository**.

   The SELECT FILE FROM REPOSITORY dialog box opens.

   Note: The **Select from repository** option may also have sub-menu items as shown in the following image.



2. From the **Repository** list, select the repository where the artifact is stored.

   Tip: To see the complete URL for a repository, hover the cursor over the repository in the list.

   The dialog box displays a list of artifacts that are available in the repository.

3. Navigate to the artifact that you want to use.

   Note: For tips on navigating within the repository, see "Navigating in the Repository" on the next page.

4. Select the artifact to use, and then click **OK**.

   The file name is added to the settings field and the repository logo appears to the right of the file name.

Navigating in the Repository

When navigating down through multiple directories in the repository, you can use the breadcrumbs at the top of the list to navigate back up to any previous directory. Click the ellipses (...) at the start of the breadcrumbs to return to the root directory of the repository.

Click the two-dot ellipses (..) at the top of the artifacts list to return to the parent directory.

In the **Go to Path** box, type the directory path to the artifact inside the repository.

Tip: Do not include the root URL for the repository in the directory path.

To return to the SELECT FILE FROM REPOSITORY dialog box, click **SELECT REPOSITORY**.

What's Next?

Proceed with "Getting Started" below.

Getting Started

To configure a ScanCentral DAST scan:

1. In the **APPLICATIONS** area, select an application from the application **Name** list.

   Tip: To search for an application, type the application name in the **Application** box, and then click the search icon ( ).

   The APPLICATION VERSIONS area appears.
2. In the **APPLICATION VERSIONS** area, select a version from the application version **Name** list.

   Tip: To search for an application version, type the application version name in the **Application version** box, and then click the search icon ( ).

   The GETTING STARTED area appears with a START list that provides options for creating new settings or editing existing settings. A RECENT list also appears, displaying recently-opened scan settings for the specified application and version.

3. Continue according to the following table.

If you want to...	Then...
Configure scan settings for a new scan	Select **New settings** from the **START** list.
View and edit existing scan settings from a template in Fortify Software Security Center	a. Select **Open from SSC** from the **START** list. A Template list appears. b. Select the existing settings from the **Template** list.
View and edit existing scan settings from your local machine **Note:** If you import Fortify WebInspect settings, you will not be able to edit any settings that are not displayed in the Settings Configuration wizard. However, the settings will be used during the scan. Any settings that you change in the wizard override the values in the settings you upload.	a. Select **Open file** from the **START** list. An OPEN button appears. b. Click **OPEN** and use the standard Windows Open dialog box to locate and open the settings file.
View and edit scan settings from base settings For more information, see "Working with Base Settings" on page 258.	a. Select **Base Settings** from the **START** list. A Base Settings list appears. b. Select the existing settings from the **Base Settings** list.
View and edit recently-opened scan settings for the specified application and version	Select the settings from the **RECENT** list.

4. Click **NEXT**.

What's Next?

Do one of the following:

- To configure a standard scan, proceed with "Configuring a Standard Scan" on the next page.
- To configure a workflow-driven scan, proceed with "Configuring a Workflow-driven Scan" on page 148.
- To configure an API scan, proceed with "Configuring an API Scan" on page 151.

Configuring a Standard Scan

A standard scan performs an automated analysis, beginning from the start URL.

To configure a standard scan:

1. On the Target page, click **STANDARD SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.
3. Type the complete URL or IP address in the **Url** field.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, the sensor will not scan WWW.MYCOMPANY.COM or any other variation unless you specify alternatives in the **Allowed Hosts** setting. For more information, see "Adding and Managing Allowed Hosts" on page 172.

   An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

   Important! If the URL resolves to an IP address that is not in the valid range for scanning, then a warning appears. If you start the scan with an IP address that is not in the valid range, then the scan will stop and a reason will be provided.

   Scans by IP address will not follow links that use fully qualified URLs (as opposed to relative paths).

   Note: The sensor supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). You must enclose IPV6 addresses in brackets.
4. (Optional) To limit the scope of the scan to a specified area, select **Restrict to folder**, and from the list, select one of the following options:
   - **Directory only** – The sensor crawls and/or audits only the URL that you specify. For example, if you select this option and specify the URL www.mycompany/one/two/, the sensor will assess only the "two" directory.
   - **Directory and subdirectories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is higher in the directory tree.
   - **Directory and parent directories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is lower in the directory tree.

5. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

   Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.

   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (<system and browser information>) <platform> (<platform details>) <extensions>

What's Next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring Proxy Settings" on page 157.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring Authentication for Standard and Workflow-driven Scans" on page 158.

Configuring a Workflow-driven Scan

A workflow-driven scan audits only those URLs included in a macro that you previously recorded. It does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, all of them will be included in the same scan.

Types of Macros Supported

You can use `.webmacro` files, HTTP archive (`.har`) files, or Burp Proxy captures.

Important! If you use a login macro in conjunction with a workflow macro or startup macro or both, all macros must be of the same type: all `.webmacro` files, all `.har` files, or all Burp Proxy captures. You cannot use different types of macros in the same scan. Likewise, `.webmacro` login and workflow files must have been created using the same version of Web Macro Recorder. You cannot use a login file that was recorded in the Event-based Web Macro Recorder and a workflow file that was recorded in the Session-based Web Macro Recorder.

Configuring a Workflow-driven Scan

To configure a workflow-driven scan:

1. On the Target page, click **WORKFLOW-DRIVEN SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.
3. Continue according to the following table.

To...	Then...
Record a workflow macro	Click **Open Workflow Macro Recorder 23.1**. **Tip:** If you have not already downloaded and installed the Macro Recorder tool, the Open Workflow Macro Recorder 23.1 link will not open the tool. You must first download the tool and install it on your local machine.
Add a macro to the scan settings	a. Click **MANAGE**. b. Type a name for the macro in the **Name** field. c. Click **IMPORT** and browse to locate the workflow to add to the scan settings. d. Click **OK**. e. Repeat steps a through d to add another macro to

To...	Then...
	the scan settings.
Remove a macro from the list of macros	a. Select the macro in the macro list. b. Click **REMOVE**.

Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

You can use a key store placeholder for any field that displays the **Open key store** icon (). For more information, see "Using Key Stores in Settings" on page 141.

4. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

5. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

6. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.

   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (<system and browser information>) <platform> (<platform details>) <extensions>

What's Next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring Proxy Settings" on page 157.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring Authentication for Standard and Workflow-driven Scans" on page 158.

Configuring an API Scan

For Open API, OData, and Postman scans, the WebInspect sensor creates a macro from the REST API definition, and then performs an automated analysis. For GraphQL, gRPC, and SOAP scans, a more traditional scanning method is used.

Important! The DAST Utility Service container must be up and running to configure and run a Postman scan. Also, if the Postman scan requires a proxy, you must configure the proxy settings before you validate the Postman collection file(s). For more information, see "Configuring Proxy Settings" on page 157.

To configure an API scan:

1. On the **Target** page, click **API SCAN**.
2. In the **Type** list, select the API type to be scanned. The options are:
   - **GraphQL**
   - **GRPC**
   - **OData**
   - **Open API** (also known as Swagger)
   - **Postman**
   - **SOAP**

   Important! If you are configuring a Postman scan while using a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service, you must install prerequisite software on the sensor machine. For more information about this and other aspects of using Postman collection files, including configuring dynamic authentication using dynamic tokens,

see "Scanning with a Postman Collection" on page 356.

3. Continue according to the following table.

For this API type...	Do this...

GraphQL
GRPC
OData
Open API
	To use a file:
	a. In the **Definition** list, select **File**.
	b. Click **IMPORT** and import the definition file.
	Tip: Alternatively, you can paste in the full path to a definition file that is saved on your local machine.
	Important! Open API definition files must specify the host, scheme, and service path. Otherwise, undesirable results may occur.
	To use a URL:
	a. In the **Definition** list, select **URL**.
	b. Provide the URL to the API definition file, as shown in the following examples:
	`http://172.16.81.36/v1`
	`http://myapi/protos/client.proto`
	`http://myapi/graphql/`
	c. If HTTP authorization credentials are needed to access the API definition, enter them in the **Authentication Header** box, as shown in the following example:
	`Basic YWxhZGRpbjpvcGVuc2VzYW1l`
	Important! This authentication header is used only for accessing the API definition. It is not carried forward to the Authentication page of the Settings Configuration wizard. You must configure network authentication for the scan on the Authentication page.
	d. Click **VALIDATE** to verify that the DAST API can access the definition file and ensure that it is valid.

Postman	a. Do one of the following: ◦ To import a workflow collection, select **IMPORT** and then import the Postman collection file.

For this API type...	Do this...
	◦ To import an authentication collection, select **Authentication** from the **IMPORT** drop-down list, and then import the Postman collection file. ◦ To import an environment file, select **Environment** from the **IMPORT** drop-down list, and then import the Postman environment file. The file is added to the list of collection files. Repeat this Step to import additional files. **Important!** You can import only one authentication collection and one environment file. b. Click **VALIDATE** to validate the collection file(s). **Note:** At least one workflow collection must be imported before you can validate the files. The **VALIDATE** button is not available if only authentication and environment collections have been imported. Upon successful validation, the POSTMAN VALIDATION dialog box opens, displaying a list of sessions contained in the collection file(s). If authentication sessions are identified, they are preselected as **Auth** sessions. All other sessions are preselected as **Audit** sessions. Additionally, the Postman Authentication Results area displays the type of authentication detected as **None**, **Static**, or **Dynamic**. **Note:** **Auth** sessions will be used for authentication for the scan. **Audit** sessions will be audited in the scan. c. (Optional) Select the **Auth** or **Audit** check box for a session to change its type as needed. d. (Optional) Make changes to the **Postman Authentication Results** as follows: ◦ For **Static** authentication, enter a token in the **Custom Header Token** box. ◦ For **Dynamic** authentication, do the following: • Select the **Regex (Custom)** option to the right of the **Response**

For this API type...	Do this...
	Token Name box, and then enter a custom regular expression in the **Response Token Name** box. • Select the **Regex (Custom)** option to the right of the **Request Token Name** box, and then enter a custom regular expression in the **Request Token Name** box. • Clear the **Use Auto Detect** option to the right of the **Logout Condition** box, and then enter a new logout condition string in the **Logout Condition** box. e. Did you make changes to the Postman Authentication Results? ◦ If yes, click **VALIDATE** to validate the new authentication settings, and then click **OK**. **Note:** Clicking **VALIDATE** regenerates all sessions for the postman collection. It does not retain any previous changes to **Auth** or **Audit** sessions even if the collection and sessions are the same. ◦ If no, click **OK**. **Note:** After validation, an **EDIT** button is available. This button opens the POSTMAN VALIDATION dialog box for editing the sessions contained in the collection file(s) as described previously in this procedure.
SOAP	To use a file: a. In the **Definition** list, select **File**. b. Click **IMPORT** and import the definition file. **Tip:** Alternatively, you can paste in the full path to a definition file that is saved on your local machine. c. In the **Version** list, select a version to allow filtering of operations by the specific version. Options are as follows: ◦ **Legacy** – filters against the lowest supported version. ◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available.

For this API type...	Do this...

	◦ **Newest** – the default setting, filters against the latest version.
	To use a URL:
	a. In the **Definition** list, select **URL**.
	b. Provide the URL to the API definition file, as shown in the following example:
	`http://172.16.81.36/web-services/infoService?wsdl`
	c. In the **Version** list, select a version to allow filtering of operations by the specific version. Options are as follows:
	◦ **Legacy** – filters against the lowest supported version.
	◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available.
	◦ **Newest** – the default setting, filters against the latest version.
	d. If HTTP authorization credentials are needed to access the API definition, enter them in the **Authentication Header** box, as shown in the following example:
	`Basic YWxhZGRpbjpvcGVuc2VzYW1l`
	Important! This authentication header is used only for accessing the API definition. It is not carried forward to the Authentication page of the Settings Configuration wizard. You must configure network authentication for the scan on the Authentication page.
	e. Click **VALIDATE** to verify that the DAST API can access the definition file and ensure that it is valid.

4. If you imported a definition file, the **API location is different from API definition location** option is selected. Specify the following:
   a. In the **API Scheme Type** list, select a type. Options are **HTTP**, **HTTPS**, and **HTTP/HTTPS**.
   b. In the **API Host** box, type the URL or hostname.
   c. In the **API Service Path** box, type the directory path for the API service.

Note: The GraphQL service location is always the same as the definition location. For SOAP, if the query string "?wsdl" value is removed, then the SOAP service location may or may not be the same as the definition location. The gRPC service location is always different from the definition location.

Note: If the service path is not defined for an Open API scan, then the sensor will use the basePath that is defined in the Open API definition contents. For Open API scans, select **API location is different from API definition location** unless your service is explicitly run at the same location as the docs folder for Open API. Optionally, you may choose to define a service path if it differs from the basePath.

5. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

   Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

   Tip: The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. However, you can choose another policy if needed.

7. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.

   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (<system and browser information>) <platform> (<platform details>) <extensions>

What's Next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring Proxy Settings" on the next page.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring Authentication for API Scans" on page 161.

Configuring Proxy Settings

To configure proxy settings:

1. On the Target page, click **PROXY SETTINGS**.
   The PROXY CONFIGURATION dialog box opens.
2. Select the **Use Proxy Server** option.
   The settings become available for you to configure.
3. Configure the settings according to the following table.

To...	Then...
Use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the web proxy settings	Select **Auto detect proxy settings**.
Import your proxy server information from Firefox	Select **Use Firefox proxy settings**. **Note:** Using browser proxy settings does not guarantee that you can access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.
Load proxy settings from a Proxy Automatic Configuration (PAC) file	a. Select **Configure proxy settings using a PAC file**. b. In the **URL** box, type the URL location for the PAC file.
Access the Internet through a proxy server	a. Select **Explicitly configure proxy** settings. b. In the **Server** box, enter the URL or IP address of your proxy server. c. In the **Port** box, enter the port number (for example, 8080). d. From the **Type** list, select the protocol type for handling TCP traffic through the proxy server. The options are: **Standard**,

To...	Then...
	SOCKS4, or **SOCKS5**. e. If authentication is required, select a type from the **Authentication** list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, or **Negotiate**. f. If your proxy server requires authentication, enter the qualifying user name in the **User Name** field and the qualifying password in the **Password** field. g. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass** field. Use semicolons to separate entries.

4. Click **OK**.
   The proxy settings are saved and the PROXY CONFIGURATION dialog box closes.

What's Next?

To configure authentication for the scan, click **NEXT** and proceed with "Configuring Authentication for Standard and Workflow-driven Scans" below or "Configuring Authentication for API Scans" on page 161.

Configuring Authentication for Standard and Workflow-driven Scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Configuring Site Authentication

You can use a recorded login macro containing one or more usernames and passwords that allow you to log in to the target site. The macro must also contain a "logout condition," which indicates when an

inadvertent logout has occurred so that the sensor can rerun the macro to log in again.

To configure site authentication:

1. Select **Site Authentication**.
2. Do one of the following:
   - To import an existing login macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays the **Open key store** icon ( ). For more information, see "Using Key Stores in Settings" on page 141.
   - To record a login macro, click **Open Macro Recorder 23.1**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 23.1 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder Tool" below.

Downloading the Macro Recorder Tool

You can download the Event-based Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Windows-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, click **Download Macro Recorder 23.1**.

  The `MacroRecorder64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

  Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.

Using a Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

To use a client certificate:

1. Select **Use Client Certificate**.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.
   The certificate file is added to the Client certificate box.
4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

   Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring Network Authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Network Authentication**.
2. Select an **Authentication Type**. Options are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
3. Type the authentication username in the **Username** box.
4. Type the authentication password in the **Password** box.

Caution! The sensor crawls all servers granted access by this password (if the sites/servers are included in the Allowed Hosts setting). To avoid potential damage to your administrative systems, do not use credentials that have administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional.

What's Next?

To configure details for the scan, click **NEXT** and proceed with "Configuring Scan Details" on page 166.

Configuring Authentication for API Scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Options for configuring authentication include the following:

- "Using a Client Certificate" below
- "Configuring Network Authentication" on the next page
- "Using Custom Headers" on page 164
- "Configuring SOAP Settings" on page 165

Using a Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

Note: Client certificates do not apply to OData or Open API definition types.

To use a client certificate:

1. Select **Use API Client Certificate**.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.
   The certificate file is added to the Client certificate box.
4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

   Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring Network Authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Use API Network Authentication**.
2. Select an **Authentication Type**. The API Type determines the available authentication types. The complete list of authentication types is:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Bearer**
   - **Custom**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
3. Continue according to the following table.

For this authentication type...	Do this...
ADFS CBT **Automatic** **Basic** **Digest** **Kerberos** **NTLM**	a. Type the authentication username in the **Username** box. b. Type the authentication password in the **Password** box.
Bearer	Optionally, type the JSON token, generally from a response to a login form, in the **Token Value** box. When using Bearer, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a Token Value" on the next page.
Custom	a. Type the token name in the **Scheme** box.

For this authentication type...	Do this...
	b. Optionally, type the token value in the **Parameter** box. When using Custom, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a Token Value" below.

Fetching a Token Value

You can use a custom regular expression to fetch the token value from a login or workflow macro. If a match to the regular expression occurs in the response, then the value is fetched and used as a bearer token. If the regular expression contains parentheses, then the value inside the parentheses will be extracted and used as a bearer token. Only the first value inside parentheses will be used.

Note: Fetching a token value does not apply to OData or Open API definition types.

To fetch a token value:

1. Select **Use Fetch Token**.
2. Do one of the following:
   - To import an existing macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays the **Open key store** icon ( ). For more information, see "Using Key Stores in Settings" on page 141.
   - To record a macro, click **Open Macro Recorder 23.1**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 23.1 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder Tool" on the next page.
3. Type a regular expression for pattern matching in the **Search Pattern** box.
4. Do one of the following:
   - To have each scan thread run its own fetch macro playback and apply the bearer token value to the thread, select the **Isolate state** check box.
   - To have only one fetch macro playback run for all scan threads and the single shared bearer token value apply to all threads, clear the **Isolate state** check box.

Downloading the Macro Recorder Tool

You can download the Event-based Web Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Windows-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, click **Download Macro Recorder 23.1**.

  The `MacroRecorder64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

  Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.

Using Custom Headers

You can configure multiple custom headers.

Important! Fortify recommends that you do not configure more than one custom header using the same HTTP header name.

To add a custom header:

1. Select **Use Custom Headers**.
2. Click the add icon (+).
3. In the **header name** box, type the custom HTTP header name. For example, `X-MyCustomAuth`.

   Important! The header must be unique and cannot be `Authorization`.
4. In the **header scheme** box, type the header value prefix name. For example, `CustomToken`.
5. In the **header value** box, type the custom header value.
6. Click the check icon (✔).

   The custom header is added to the list.

To edit a custom header:

- Click the edit icon (✎) for the custom header you want to edit.

To remove a custom header:

- Click the delete icon (✕) for the custom header you want to delete.

Configuring SOAP Settings

You can configure message-based authentication for SOAP scans.

To configure SOAP authentication settings:

1. Select **Use SOAP Configuration**.
2. Select that authentication method to use from the **SOAP Method** list. Options are **Username Token** and **Certificate Pair**.
3. Continue according to the following table.

For this authentication method...	Do this...
Username Token	a. In the **Username** box, type the user name whose credentials are used to access the SOAP service. b. In the **Password** box, type the password for the user name. c. In the **Username Token Type** list, select the type of token. Options are **Text** and **Hash**. d. In the **Timestamp** list, select an option for when the Username Token was created and when it expires. Options are **Created**, **Full**, and **None**. e. If nonce is enabled for the token, select **Includes nonce**. **Important!** Nonce is required for hash tokens because it helps the server to recalculate the hash and compare it to the data the client sent.
Certificate Pair	a. Click **IMPORT** to the right of the **Client Certificate** box. A standard Windows file selection dialog box opens. b. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Client Certificate box. c. In the **Client Certificate Password** box, type the password. d. Click **IMPORT** to the right of the **Server Certificate** box. A standard Windows file selection dialog box opens. e. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Server Certificate box. f. If the server certificate requires a password, select **Requires**

For this authentication method...	Do this...
	password and type the password in the **Server Certificate Password** box.

4. Optionally, to identify the Web Services Addressing (WS-Addressing) schema version used by the SOAP service, select **Use WS Addressing** and continue as follows:
   a. In the **Schema Version** list, select the version. Options are **NONE**, **WSA0408**, and **WSA0508**.
   b. In the **WSA: To** box, enter the URL override for the Web service host.

> **Note:** SOAP services may be exposed by way of a load balancer or reverse proxy. This configuration may prevent the sensor from getting the correct information for the internal Web service host name. The "WSA: To" URL override provides the correct address into WS Addressing.
>
> The URL override uses the following format:
>
> `https://<host_name><service_path>/<port_name>`

What's Next?

To configure details for the scan, click **NEXT** and proceed with "Configuring Scan Details" below.

Configuring Scan Details

You can configure the following settings on the Details page:

- API Content and filters (API scans only. For more information, see "Configuring API Content and Filters" on the next page.)
- Allowed hosts (For more information, see "Adding and Managing Allowed Hosts" on page 172.)
- Scan priority (For more information, see "Configuring Scan Priority" on page 173.)
- Data retention (For more information, see "Configuring Data Retention" on page 176.)
- Single-page application (SPA) support (Standard and Workflow-driven scans only. For more information, see "Scanning Single-page Applications" on page 176.)
- Traffic Monitor (For more information, see "Enabling Traffic Monitor" on page 177.)
- Exclusions (For more information, see "Creating and Managing Exclusions" on page 177.)
- Redundant page detection (Standard and Workflow-driven scans only. For more information, see "Configuring Redundant Page Detection" on page 182.)
- Scan scaling (For more information, see "Enabling Scan Scaling" on page 183.)

What's Next?

After you configure the scan details, click **NEXT** and proceed with "Reviewing Scan Settings" on page 183.

Configuring API Content and Filters

When configuring API scans, you can use the Content and Filters page to configure the preferred content type, as well as operations and parameter names and types to include or exclude during the scan.

Specifying the Preferred Content Type

The preferred content type setting specifies the preferred content type of the request payload. If the preferred content type is in the list of supported content types for an operation, then the generated request payload will be of that type. Otherwise, the first content type listed in an operation will be used. By default, the preferred content type is application/json.

To change the preferred type:

- Type the preferred content type in the **Preferred Content Type** box.

Defining Specific Operations to Include

The Include feature defines an allow list of operation IDs that should be included in the output.

To define a specific operation to include:

1. Select **Specific Operations**.
2. Select **Include**.
3. Click the add icon (+).
4. In the **Operation to add** box, type the operation ID.
5. Click the check icon (✔).
   The operation ID is added to the allow list.

Defining Specific Operations to Exclude

The Exclude feature defines a deny list of operation IDs that should be excluded from the output.

To define a specific operation to exclude:

1. Select **Specific Operations**.
2. Select **Exclude**.
3. Click the add icon (+).
4. In the **Operation to add** box, type the operation ID.

5. Click the check icon (✔).
   The operation ID is added to the deny list.

Editing Specific Operations

To edit a specific operation in the allow or deny list:

1. Do one of the following:
   - To edit an operation in the allow list, select **Include**.
   - To edit an operation in the deny list, select **Exclude**.
2. Click the edit icon (✎) for the operation ID you want to edit.

Removing Specific Operations

To remove a specific operation from the allow or deny list:

1. Do one of the following:
   - To remove an operation from the allow list, select **Include**.
   - To remove an operation from the deny list, select **Exclude**.
2. Click the delete icon (✕) for the operation ID you want to remove.

Defining Parameter Rules

Parameter rules define a default value to use for a parameter when the parameter name and type are encountered. You can also specify operations to determine whether a specific parameter rule should or should not apply to those operations.

Important! If you configure a parameter rule and then change the API definition type for which the parameter rule type becomes invalid, the invalid parameter rule type will be changed to **Any**. The invalid parameter rule will be highlighted in the Parameter Rules list, and a warning message will be displayed below the list.

To add a parameter rule:

1. Select **Parameter Rules**.
2. Click **Add**.
   The PARAMETER RULE dialog box appears.
3. In the **Parameter Rule Name** box, type a name for the rule.
4. In the **Parameter Rule Type** list, select a type. Available options depend on the API type and may include the following:

- **Any**
- **Boolean**
- **Date**
- **File**
- **Guid**
- **Number**
- **String**

For more information on the Parameter Rule Types and their equivalents based on API type, see "Understanding Parameter Type Matches" on page 171.

5. Continue according to the following table:

For this Rule Type...	Do this...
Any	In the **Value** box, type any value.
Boolean	In the **Boolean Value** list, select **true** or **false**.
Date	To enter any string value as the date: • Type the string in the **Date** box. **Note:** You may enter a duration, time span, formatted date, or formatted time in the **Date** box. To select a date/time format and use a calendar and clock to generate a formatted string: a. Click **GENERATE DATE**. The GENERATE DATE STRING dialog box opens. b. From the **Date Type** list, select a format. Options are **Date and time**, **Date**, and **Time**. c. In the **Date** box, enter a date using the preferred format defined in your Fortify Software Security Center. **Tip:** To select a date from the calendar, click the calendar icon ( ). d. In the **Time** box, enter a time using the preferred format defined in your Fortify Software Security Center. **Tip:** To select a date from the calendar, click the clock

For this Rule Type...	Do this...
	icon ( ). e. Click **OK**.
File	a. Click **IMPORT** and browse to locate the file to add to the scan settings. b. Click **Open**.
Guid	In the **Value** box, enter a GUID.
Number	In the **Number Value** box, enter a numerical value.
String	In the **Value** box, type any value.

6. For Open API scans, in the **Parameter Rule Location** list, select a location where the parameter is found in the request. Options are:
   - **Any**
   - **Body**
   - **Header**
   - **Path**
   - **Query**
7. Optionally, select **Inject Parameter** to include the defined parameter in the request.

   Important! The **Inject Parameter** option does not work with schema-based APIs, such as SOAP, gRPC, and Postman. Those API types do not accept forced parameters. For GraphQL, **Inject Parameter** only works with the query operation if the property is in the query schema.
8. Optionally, to specify operations to which this parameter rule should or should not apply, select **Specific Operations** and perform steps 2-5 of "Defining Specific Operations to Include" on page 167 or "Defining Specific Operations to Exclude" on page 167.
9. Click **OK**.

   The rule is added to the Parameter Rules list.

Editing a Parameter Rule

To edit a rule in the Parameter Rules list:

- Select the check box for the rule to edit, and then click **EDIT**.

  The PARAMETER RULE dialog box appears. For more information about using this dialog box, see "Defining Parameter Rules" on page 168.

Removing a Parameter Rule

To remove a rule from the Parameter Rules list:

- Select the check box for the rule to remove, and then click **REMOVE**.

Understanding Parameter Type Matches

The following table describes the parameter rule type equivalents by API type.

ScanCentral DAST Parameter Rule Type	Equivalent				
	Open API (Swagger)	**OData**	**GraphQL**	**gRPC**	**SOAP**
Any	All	All	All	All	All
Boolean	boolean	Edm.Boolean	boolean	bool	boolean
Date	date (OpenAPI 2.0) string (OpenAPI 3.0)[1]	Edm.Date Edm.DateTime Edm.DateTimeOffset Edm.Duration Edm.Time Edm.TimeOfDay	N/A	N/A	date
File	file (OpenAPI 2.0)[2]	Edm.Binary	N/A	bytes	N/A
GUID	N/A	Edm.Guid	N/A	N/A	N/A
Number	number integer	Edm.Byte Edm.Decimal Edm.Double Edm.Int16 Edm.Int32 Edm.Int64 Edm.SByte Edm.Single	int float	double enum fixed32 fixed64 float int32 int64 sfixed32 sfixed64 sint32 sint64 uint32 uint64	base64Binary byte decimal double float hexBinary hexint int integer long signedInt short unsignedByte unsignedInt unsignedLong unsignedShort

[1]OpenAPI 3.0 implementation is qualified by date string format.

[2]OpenAPI 3.0 implementation is qualified by binary or byte string formats.

ScanCentral DAST Parameter Rule Type	Equivalent				
	Open API (Swagger)	**OData**	**GraphQL**	**gRPC**	**SOAP**
String	string	Edm.GeographyCollection Edm.GeographyLineString Edm.GeographyMultiLineString Edm.GeographyMultiPoint Edm.GeographyMultiPolygon Edm.GeographyPoint Edm.GeographyPolygon Edm.GeometryCollection Edm.GeometryLineString Edm.GeometryMultiLineString Edm.GeometryMultiPoint Edm.GeometryMultiPolygon Edm.GeometryPoint Edm.GeometryPolygon Edm.String	id string	string	string

Adding and Managing Allowed Hosts

Use the **Allowed Hosts** setting to add and manage domains to crawl and audit. If your Web application uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the scan.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As the sensor scans the target site, if it encounters a link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, the sensor would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Adding Allowed Hosts

To add allowed hosts:

1. Click **MANAGE**.
2. In the SPECIFY ALLOWED HOST dialog box, type a URL in the **Name** box.

   Important! When you specify the URL, do not include the protocol designator (such as http:// or https://).
3. (Optional) To use a regular expression to represent a URL, select **Use Regular Expression**.
4. Do one of the following:
   - To save the allowed host to the list, click the check mark icon (✔).
     The URL is added to the allowed hosts list. To add another allowed host, return to Step 2.
   - To clear the fields and start over, click the retry icon (↻) and return to Step 2.
5. When the list of allowed hosts is complete, click **OK**.

Editing or Removing Hosts

To edit or remove an allowed host:

1. Select a host from the **Allowed Hosts** list.
2. Do one of the following:
   - To edit the host name or regular expression, click **MANAGE**.
     The SPECIFY ALLOWED HOST dialog box opens. For more information about using this dialog box, see "Adding Allowed Hosts" above.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Configuring Scan Priority

Scans are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Before starting a scan, the Global Service determines if there is a higher-priority scan that needs to be started. If there is, the lower-priority scan will remain in the queue. Additionally, a lower-priority scan that is running will be paused for a higher-priority scan if no other sensor is available.

If Advanced Scan Prioritization is enabled, the Global Service may move scans to other sensors, depending on scan priority and other settings. For more information about Advanced Scan Prioritization, see "Understanding Advanced Scan Prioritization" on the next page.

Note: Applications are configured with a default priority level in the application settings. For more information, see "Understanding the Application Settings View" on page 296.

Changing the Priority

To select a priority other than the default setting for the scan:

- Select a priority from 0 to 10 in the **Priority** list.

  Note: If you set a priority that differs from the Application Settings, the lower of the two settings will be used.

Tip: You cannot disable scan priority. However, you can set all applications and scans to the same priority to accomplish something similar.

Understanding Advanced Scan Prioritization

Advanced scan prioritization allows the Global Service to move a scan to a different sensor, depending on the scan priority and other settings as described in the following paragraphs.

Priority and Sensor Pools

For prioritization, scans are grouped by the sensor pool to which the scan belongs. Grouping scans by pool ensures that a higher-priority scan in sensor pool 1 will not pause a lower priority scan in sensor pool 2.

Priority and Scan Status

Scans with the following statuses are processed first from the highest to lowest scan priority and then from the oldest to newest:

- Queued
- Resume Scan Queued
- Resume Scan Queued Scan Priority
- License Unavailable
- Paused Scan Priority

The following table provides examples using five scans with various statuses, priorities, and creation times.

Scan Status	Priority	Created On Date/Time	When Started or Resumed
Paused Scan Priority	0	5/3/2023 08:00 AM	Fifth
Resume Scan Queued	5	5/3/2023 08:15 AM	Second
Resume Scan Queued Scan Priority	5	5/3/2023 09:00 AM	Third

Scan Status	Priority	Created On Date/Time	When Started or Resumed
Queued	5	5/3/2023 11:26 AM	Fourth
Queued	10	5/3/2023 12:01 PM	First

Priority and Sensors

When configuring a scan, you can select a specific sensor in the Run Scan or Schedule Scan dialog boxes. You can also select the **Use this sensor only** option. The following table describes how these options affect advanced scan prioritization.

Selected Sensor Options	What Happens
A specific sensor is selected with the **Use this sensor only** option	If the sensor is available, then the scan starts on the sensor. If the sensor is not available and there is a lower-priority scan that is running on that sensor, then the lower-priority scan is paused and the higher-priority scan is started on the sensor.
A specific sensor is selected *without* the **Use this sensor only** option	If the sensor is available, then the scan starts on the sensor. If the sensor is not available, the Global Service attempts to find any other available sensor in the sensor pool. If an available sensor is found, the scan starts on that sensor. If no sensor is available, the Global Service checks whether a lower-priority scan is running. If a lower-priority scan is running, then the lower-priority scan is paused and the higher-priority scan is started on that sensor.
Any Available sensor is selected	If a sensor is available in the sensor pool, then the scan is started on the sensor. If no sensor is available in the sensor pool, the Global Service checks whether a lower-priority scan is running. If a lower-priority scan is running, then the lower-priority scan is paused and the higher-priority scan is started on that sensor.

When Advanced Scan Prioritization is Disabled

If the **Disable Advanced Scan Prioritization** option was selected in the ScanCentral DAST Configuration Tool, then when a lower-priority scan is paused for a higher-priority scan to run, the lower-priority scan resumes only on the sensor on which it was originally running, regardless to whether another sensor is available in the sensor pool. Partial scan results are uploaded to the

ScanCentral DAST database, but the paused scan remains on the sensor. If the scan is resumed, but the scan no longer exists on the sensor for any reason, the Global Service downloads and imports the partial results prior to resuming the scan.

For more information, see "Configuring Scan Priority" on page 173.

Configuring Data Retention

If data retention is enabled for the application being scanned, then a default number of days for scan retention is configured in the application settings. In such cases, the default number of days for scan retention is displayed in the Details page. For more information, see "Working with Application Settings" on page 295.

To set a number of days other than the default setting for the scan:

- Enter the number of days in the **Data Retention** box.

Note: If you set a number of days that differs from the Application Settings, the lower of the two settings will be used.

Scanning Single-page Applications

This topic describes single-page application (SPA) support for crawling and auditing the Document Object Model (DOM) of an application.

The Challenge of Single-page Applications

Developers use JavaScript frameworks such as Angular, Ext JS, and Ember.js to build SPAs. These frameworks make it easier for developers to build applications, but more difficult for security testers to scan those applications for security vulnerabilities.

Traditional sites use simple back-end server rendering, which involves constructing the complete HTML web page on the server side. SPAs and other Web 2.0 sites use front-end DOM rendering, or a mix of front-end and back-end DOM rendering. With SPAs, if the user selects a menu item, the entire page can be erased and recreated with new content. However, the event of selecting the menu item does not generate a request for a new page from the server. The content update occurs without reloading the page from the server.

With traditional vulnerability testing, the event that triggered the new content might destroy other events that were previously collected on the SPA for audit. Through its SPA support, the dynamic sensor offers a solution to the challenge of vulnerability testing on SPAs.

Configuring SPA Support

When SPA support is enabled, the DOM script engine finds JavaScript includes, frame and iframe includes, CSS file includes, and AJAX calls during the crawl, and then audits all traffic generated by those events.

To configure SPA support:

- Under **Single-Page Applications** on the Details page, select one of the following options:
  - **Automatic** - If the sensor detects a SPA framework, it automatically switches to SPA-support mode.
  - **Disabled** - Indicates that SPA frameworks are not used in the target application.
  - **Enabled** - Indicates that SPA frameworks are used in the target application.

    Caution! Enable SPA support for single-page applications only. Enabling SPA support to scan a non-SPA website results in a slow scan.

Enabling Traffic Monitor

The site tree of a scan normally displays only the hierarchical structure of the website or web service, plus those sessions in which a vulnerability was discovered. If traffic monitor is enabled, then the Traffic Viewer tool and the Traffic table in the scan results allow you to view every HTTP request sent by the sensor and the associated HTTP response received from the web server.

Note: The Traffic Viewer tool is not included with ScanCentral DAST. However, if you have Fortify WebInspect installed locally, you can use the tool that is included with your local installation.

Option Must be Enabled

To see all traffic in the Traffic Viewer tool or in the Traffic table in the scan results, you must enable Traffic Monitor logging in the scan settings.

Note: The Traffic table is always available in the scan results in ScanCentral DAST. However, enabling Traffic Monitor logging includes all of the scan traffic.

Enabling Traffic Monitor Logging

To enable traffic monitor logging:

- Under **Traffic Analysis** on the Details page, select **Enable Traffic Monitor**.

Creating and Managing Exclusions

You can exclude URLs and sessions—based on criteria in their requests or responses—from being crawled and audited. Excluding URLs means that the sensor will not examine the specified URL or host for links to other resources. Excluding sessions means that sensor will not process the sessions that meet the exclusion criteria.

To exclude these items from your scan, you must create a list of Basic Exclusions. Each exclusion in the list identifies one or more targets in which the criteria for exclusion is found.

Note: You can add multiple targets to each entry in the Basic Exclusions list.

Creating Exclusions

To create one or more exclusions:

1. Under **Basic Exclusions** on the Details page, click **CREATE**.
   The MANAGE EXCLUSIONS dialog box opens.
2. Type a name for the exclusion in the **Name** box.
3. From the **Target** list, select one of the following target types to configure for exclusion:
   - **Extension** - Excludes file extensions that match the exclusion criteria
   - **Host** - Excludes hosts that match the exclusion criteria
   - **Post parameter** - Excludes sessions with a POST request parameter that matches the exclusion criteria
   - **Query parameter** - Excludes sessions with a query parameter in the URL that matches the exclusion criteria
   - **Request** – Excludes sessions with a request that matches the exclusion criteria
   - **Response** – Excludes sessions with a response that matches the exclusion criteria
   - **Response header** - Excludes sessions with a response header that matches the exclusion criteria
   - **Status code** - Excludes sessions with a response status code that match the exclusion criteria
   - **URL** – Excludes URLs that match the exclusion criteria
4. Type a name for the target in the **Name** box.
5. Select one of the following types of exclusion for the target from the **Type** list:
   - **Matches Regex** – Matches the regular expression you specify in the **String** box
   - **Matches Regex extension** – Matches the regular expression extension you specify in the **String** box
   - **Matches** - Matches the specified criteria in the **String** box
   - **Contains** – Contains the text string you specify in the **String** box
6. Type the string to match in the **String** box.
   For examples of Target, Type, and String settings, see "Exclusion Examples" on the next page.
7. Do one of the following:
   - To save the exclusion to the list, click the check mark icon (✔).
     The exclusion is added to the list. To create another exclusion, return to Step 2.
   - To clear the fields and start over, click the retry icon (↻) and return to Step 2.
8. When the list of exclusions is complete, click **OK**.

Exclusion Examples

The following table provides examples of exclusions.

To...	Create the following exclusion...
Ensure that you never send requests to any resource at Microsoft.com	URL contains `Microsoft.com`

Exclude the following directories:
 	
`http://www.test.com/W3SVC55/`
`http://www.test.com/W3SVC5/`
`http://www.test.com/W3SVC550/`
	URL matches regex `/W3SVC[0-9]*/`

Ensure that you never process session responses with 404 Not Found	Response contains `Not Found`

For more information about creating exclusions, see "Understanding and Creating Inclusive Exclusions" below.

Editing or Removing Exclusions

To edit or remove an entry in the **Basic Exclusions** list:

1. Select an entry from the **Basic Exclusions** list.
2. Do one of the following:
   - To edit the exclusion settings, click **MANAGE**.

     The MANAGE EXCLUSIONS dialog box opens. For more information about using this dialog box, see "Creating Exclusions" on the previous page.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Understanding and Creating Inclusive Exclusions

When a site contains many pages that are essentially redundant, it makes sense to scan only a selection of such pages and exclude the rest. To accomplish this, we need to specify what to include by excluding everything else. Such exclusions are called "inclusive exclusions."

You can create regular expressions that exclude everything including the sessions you want to scan, and then add the inclusion regular expression within the negative look ahead construct.

Understanding Inclusive Exclusion Regular Expressions

Suppose you have the following URLs:

```
http://site.tld/sub/sub1
http://site.tld/sub/sub2
http://site.tld/sub/sub3
http://site.tld/sub/sub4
http://site.tld/sub/sub5
...
http://site.tld/sub/sub9999
```

And you want to include `sub1` in the scan but not `sub2` through `sub9999`.

A regular expression to match and exclude everything is:

```
\/sub/sub[0-9]+
```

Adding the negative look ahead to include `sub1` results in this regular expression:

```
\/sub/sub(?!1)[0-9]+
```

This regular expression matches and excludes everything in the previous list of URLs that does not include `sub1`.

Important! If the regular expression includes the host name, then it must also include the port as shown here:

```
site\.tld:80/sub/sub[0-9]+
```

```
site\.tld:80/sub/sub(?!1)[0-9]+
```

The following paragraphs provide additional examples of various inclusive exclusions.

Example One

Suppose you want to scan only the contents of folders where the folder name starts with the combination "N13" and omit the others in the following list:

```
http://10.0.6.124:22000/cssbundle/1666793387/bundles/service.css
http://10.0.6.124:22000/cssbundle/N1375383199/bundles/service.css
http://10.0.6.124:22000/jsbundle/1337374041/bundles/catalogs.js
http://10.0.6.124:22000/jsbundle/1337374041/bundles/general.js
http://10.0.6.124:22000/jsbundle/335652056/bundles/search.js
http://10.0.6.124:22000/jsbundle/N1222120407/bundles/
http://10.0.6.124:22000/jsbundle/N1408948977/bundles/
http://10.0.6.124:22000/jsbundle/N1982198842/bundles/
http://10.0.6.124:22000/jsbundle/N273479010/bundles/
```

A regular expression to match and exclude all folder names that begin with letter "N" is:

```
 \/N[\d]+\/
```

Adding the negative look ahead to include `(?!13)` results in this regular expression:

```
\/N(?!13)[\d]+\/
```

Using this regular expression as a session exclusion causes Fortify WebInspect to omit all of the paths except for those where the folder name starts with the combination "N13":

```
http://10.0.6.124:22000/cssbundle/N1375383199/bundles/service.css
```

Note: The number "13" is arbitrary. You could easily replace the "13" character set in the regular expression with your desired character set.

Example Two

Suppose you want to omit most of My Awesome Store's catalog while still permitting URLs that include keywords "awesome" or "core" in the following list:

```
http://my.awesome.store.com/dotcom/14k-gold-plated-ring/cat.jump
http://my.awesome.store.com/dotcom/2-panel-jewelry-box/prod.jump
http://my.awesome.store.com/dotcom/core-short-sleeve-top/prod.jump
http://my.awesome.store.com/dotcom/core-graphic-tee/prod.jump
http://my.awesome.store.com/dotcom/core-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/core-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/low-mid-
heel/cat.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/wedge-
sandals/cat.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/flat-
sandals/cat.jump
http://my.awesome.store.com/dotcom/shows/all-mens-shoes/slippers/cat.jump
http://my.awesome.store.com/dotcom/men/shorts/bermuda-core-beige/prod.jump
http://my.awesome.store.com/dotcom/men/shorts/pleated-core-beige/prod.jump
http://my.awesome.store.com/dotcom/men/shorts/bermuda-awesome-brand-
beige/prod.jump
http://my.awesome.store.com/dotcom/core-proportioned-pants/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand-slender-jean---plus/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand/half-zip-jacket/prod.jump
http://my.awesome.store.com/dotcom/toys/categories/costumes-dress-
up/boys/cat.jump
http://my.awesome.store.com/dotcom/shoes/kids-shoes/boys-shoes/cat.jump
http://my.awesome.store.com/dotcom/toys/gender/boys/cat.jump
http://my.awesome.store.com/dotcom/shoes/boots/ankle-boots-booties/cat.jump
http://my.awesome.store.com/dotcom/shoes/all-womens-shoes/view-all/cat.jump
http://my.awesome.store.com/dotcom/women/awesome-brand/tops-sweaters/cat.jump
http://my.awesome.store.com/dotcom/men/wallets-accessories/backpacks-
```

```
bags/cat.jump
http://my.awesome.store.com/dotcom/women/wear-to-work/skirts/cat.jump
```

A regular expression to include "awesome" or "core" keywords is:

```
\/dotcom\/((?!awesome|core)[\w-%\/])+(?:cat|prod)\.jump
```

Configuring Redundant Page Detection

Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, the sensor would never be able to finish the scan. The **Perform redundant page detection** option compares page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources.

Important! Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.

To configure redundant page detection:

1. Select the **Perform redundant page detection** check box.
2. Configure settings as described in the following table.

Setting	Description
Page Similarity Threshold (%)	Indicates how similar two pages must be to be considered redundant. Enter a percentage from 1 to 100, where 100 is an exact match. The default setting is 95 percent.
Tag attributes to include	Identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes in this list adds those attributes and their values in the page structure. By default, `id` and `class` tag attributes are included. To add tag attributes: a. Type the attribute name in the **Tag item** box. Do not include tag brackets (< and >). b. Click **ADD**. The tag attribute is added to the **Tag attributes to include** list. **Tip:** Certain sites may be primarily composed of one type of tag, such as `<div>`. Including these attributes creates a more rigid page match. Excluding these attributes creates a less strict match.

Enabling SAST Correlation

SAST correlation correlates the static and dynamic findings for your web application in Fortify Software Security Center. Correlation allows you to see the static findings that were also found in a dynamic scan. It can help you to prioritize which issues to fix and help verify that those issues are not false positives.

To enable SAST correlation:

- Select **Enable SAST Correlation**.

Enabling Scan Scaling

If the application is configured in a sensor pool that has scan scaling enabled, then the Scan Scaling check box is available on the Details page.

During a scan, script engines replay TruClient macros and run scripts to reveal the Document Object Model (DOM) of the application and events on the page. Scan scaling involves automatically creating multiple pools of these script engines in Kubernetes. In essence, it distributes the work of performing the scan across multiple script engines, thereby reducing the amount of time it takes to conduct the scan.

Scan scaling might be beneficial for applications that generally have long-running scans.

For more information, see "Integrating with Kubernetes for Scan Scaling" on page 108.

If you enable scan scaling, then the scan inherits the scan scaling settings that are configured in the sensor pool. Scan scaling adjusts the number of script engine pools to equal the number of crawl and audit threads in the scan or to the maximum number specified in the sensor pool settings, whichever is lower. For more information, see "Creating a DAST Sensor Pool" on page 229.

To enable scan scaling:

- In the **Scan Scaling** area, select **Use scan scaling**.

Reviewing Scan Settings

You can review the settings you configured for the scan on the Review page.

After you review the settings, do one of the following:

- If the settings are correct, type a name for the settings in the **Name** box.
- If changes are needed, click the page name in the navigation pane, and then make corrections.

> **Tip:** The names of pages that contain missing information or errors are displayed in red text in the navigation pane.

When the settings are correct, do one of the following:

- Save the settings to Fortify Software Security Center (For instructions, see "Saving the Settings to Software Security Center" below.)
- Schedule a scan (For instructions, see "Scheduling a Scan" below.)
- Run a scan (For instructions, see "Running a Scan" on page 186.)
- Use the settings in the API (For instructions, see "Using the Scan Settings in the DAST API" on page 186.)

Saving the Settings to Software Security Center

You can save the settings as a template to Fortify Software Security Center. The settings are stored in XML format along with a JSON object with setting overrides.

To save as a template:

- Click **SAVE**.

  The file is saved to Fortify Software Security Center.

Scheduling a Scan

You can use the settings for a scheduled scan to be run later.

To schedule a scan:

1. Click **SCHEDULE**.

   The SCAN SCHEDULE dialog box opens.
2. Type a name for the scheduled scan in the **Name** box.
3. Enter a date for the scan to run in the **Start Date** box.

   Tip: To select a date from the calendar, click the calendar icon ( ).
4. Enter a time for the scan to start in the **Start Time** box.

   Note: The schedule uses the time zone from your browser.
5. To schedule a recurring scan, in the **Pattern** section specify how often to run the scan according to the following table.

To run...	Then...
Daily	a. Select **DAILY**. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. b. Select a recurrence in the **Occur every ___ week** box.

To run...	Then...
	c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

6. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

     Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.
7. Select a dynamic sensor from the **Sensor** list.

   The list of sensors comes from the Fortify Software Security Center sensor pools. **Any Available** is the default.
8. (Optional) If you select a sensor that is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
9. Click **OK**.

   The scan schedule is added to the ScanCentral DAST database.

Running a Scan

You can use the settings to run a scan immediately. To run a scan:

1. Click **RUN**.

   The RUN SCAN dialog box opens.

   Note: The name you gave to the settings appears in the **Name** field. You can type a different name in the field if needed.

2. Select a ScanCentral DAST sensor from the **Sensor** list.

   The list of sensors comes from the Fortify Software Security Center sensor pools. **Any Available** is the default.

3. (Optional) If you select a sensor, but it is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
4. Click **RUN**.

   The scan is queued to run.

Using the Scan Settings in the DAST API

You can use the scan settings to conduct a scan from the DAST API.

After saving the settings, the GUID in the **Settings Identifier** field provides a unique identifier for the settings. You can copy a cURL sample that includes this GUID to use in the API.

Note: This GUID is also known as the CICD Identifier.

If you copy the settings before saving, a placeholder is used for the settings ID. You must manually update the sample with the settings ID.

To copy the cURL sample:

- Click the copy to clipboard ( ) icon.

Accessing the DAST API Swagger UI

Complete documentation—including detailed schema, parameter information, sample code, and functionality for testing endpoints—is included in the DAST API Swagger UI.

To access this information:

- In your browser, navigate to the DAST API URL using the following format:

  `http://<ScanCentral_DAST_API_URL>:<Port>/swagger/index.html`

Using the Swagger UI

To use the Swagger UI:

1. On the Swagger UI page, click an endpoint category.
2. Click the endpoint method to use.

   Detailed schema, parameter information, sample code, and functionality for testing the endpoint appear.
3. (Optionally) To view a previous version of the DAST API, select the version from the **Select a definition** list.

   Important! The latest version of the DAST API includes newer functionality than older versions. For this reason, Fortify recommends that you use the most recent version of the DAST API.

Using Advanced Settings in Scan Settings

You can edit advanced settings in the Scan Settings Configuration wizard.

Accessing Advanced Settings

At any time while configuring scan settings, you can access the advanced settings.

To access the advanced settings:

- Click **Advanced Settings** in the bottom left navigation.

  The ADVANCED SETTINGS panel opens.

Editing Advanced Settings

The following settings are available for editing:

- "Advanced Settings: Crawl and Audit Mode" on the next page
- "Advanced Setting: Requestor Performance" on the next page

When you have finished editing the advanced settings, click the hide icon ( ) to close the ADVANCED SETTINGS panel.

Advanced Settings: Crawl and Audit Mode

The crawl and audit mode advanced setting is available only if the SCAN MODE is set to **Crawl and Audit**.

Tip: If you selected **Crawl Only** or **Audit Only** on the Target page in the Scan Settings wizard, you can change it in the advanced settings to enable the crawl and audit mode advanced setting.

To change the crawl and audit mode advanced setting:

- In the **CRAWL AND AUDIT MODE** area, select one of the options described in the following table.

Option	Description
Simultaneously	As the sensor maps the site's hierarchical data structure, it audits each resource (page) as it is discovered, rather than crawling the entire site and then conducting an audit. This option is most useful for extremely large sites where the content could change before the crawl can be completed. **Note:** This is the default setting.
Sequentially	The sensor crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.

Advanced Setting: Requestor Performance

The requestor performance advanced setting allows you to configure shared or separate requestors, as well as the maximum number of threads per requestor.

Using a Shared Requestor

With this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This option is suitable for use when maintaining state is not a significant consideration.

To use a shared requestor:

1. In the **REQUESTOR PERFORMANCE** area, select **Shared** from the **Requestor Performance Type** drop-down list.
2. In the **Requestor thread count** box, enter the maximum number of threads (up to 75).

Using Separate Requestors

With this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl Requestor Thread Count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5.

The **Audit Requestor Thread Count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

To use separate requestors:

1. In the **REQUESTOR PERFORMANCE** area, select **Separate** from the **Requestor Performance Type** drop-down list.
2. In the **Crawl Requestor Thread Count** box, enter the maximum number of threads (up to 25).
3. In the **Audit Requestor Thread Count** box, enter the maximum number of threads (up to 50).

Conducting an Automated Scan with FAST

Functional Application Security Testing (FAST) is a lightweight proxy that integrates with Fortify ScanCentral DAST. FAST provides a way to capture traffic from functional test scripts, such as those of Selenium, Cucumber, Curl, Postman, Unified Functional Test (UFT), and others. FAST turns the captured traffic into a workflow macro and sends it to ScanCentral DAST, which uses the macro and an existing scan settings identifier to conduct a scan.

Automation Overview

The automation scenario involves three stages:

1. Start the FAST proxy using a CLI command (or commands).
2. Run functional tests though the FAST proxy.
3. Stop the FAST proxy using a CLI command.

FAST Versions Available

FAST is available in two versions:

- Windows MSI installer (For more information, see "Using the FAST Windows Version" below.)
- Linux Docker image (For more information, see "Using the FAST Linux Version" on page 193.)

Using the FAST Windows Version

The following paragraphs describe how to install and use the Windows version of FAST.

Installation Recommendation

Important! Do not install the FAST proxy on the same machine as Fortify WebInspect, a Fortify WebInspect installation running the sensor service in a DAST environment, or a Fortify WebInspect sensor being used with Fortify WebInspect Enterprise.

Fortify recommends that you install the FAST proxy on the machine that runs your functional tests, and then control the FAST proxy using the command line interface (CLI). This installation method allows you to integrate FAST CLI scripts into your functional testing automation pipeline.

Before You Begin

You will need to following items to conduct an automated scan with FAST:

- The `WIRCServerSetup64-ProxyOnly.msi` installer
- An authentication token from Fortify Software Security Center
- A settings identifier, or GUID, for scan settings in ScanCentral DAST
- The ScanCentral DAST API URL

Process Overview

The following table describes the process for conducting an automated scan with FAST.

Stage	Description
1.	Download and install the `WIRCServerSetup64-ProxyOnly.msi`. For more information, see "Downloading the FAST Installer" on the next page.
2.	Obtain an authentication token of type **CIToken** from Fortify Software Security Center. For more information, see the *Micro Focus Fortify Software Security Center User Guide*. **Tip:** This token is passed as the value for the `CIToken` in the FAST command.
3.	Obtain a settings identifier from a scan settings file in ScanCentral DAST. For more information, see "Understanding the Scan Settings Detail Panel" on page 238. **Tip:** This token is passed as the value for the `CICDToken` in the FAST command.
4.	On the machine where you installed the FAST proxy, open the command prompt and start the FAST proxy. **Tip:** The default installation directory for the FAST proxy is `C:\Program Files\Micro Focus WIRC Server\Fast.exe`.

Stage	Description

	The following is an example of the command to start the proxy:
	`Fast.exe -p <ListeningPort> -u http://<host|ip>:<port>/api/ -CIToken <Base64_encoded_token> -CICDToken <Guid>`
	You should see a response similar to the following:
	`0.0.0.0:<ListeningPort>`
	`Listening`
	For descriptions of these and other FAST command options, see "Understanding the FAST Options for Windows" below.

5.	Run the traffic from your functional tests through the FAST proxy IP address and port specified in the start command. **Note:** If your functional tests run on the same machine where you installed the FAST proxy, then you can use `127.0.0.1` for proxy address.
6.	After traffic has been captured, stop the FAST proxy. The following is an example of the command to stop the proxy: `Fast.exe -p <ListeningPort> -s`
7.	The ScanCentral DAST instance specified in the `<DAST_API_HOST|IP>/api/` option automatically runs the scan with workflow overrides applied to the settings.

Downloading the FAST Installer

The FAST installer, named `WIRCServerSetup64-ProxyOnly.msi`, is included in the ScanCentral DAST download package. It is packaged in a ZIP file named `Dynamic_Addons.zip`.

Understanding the FAST Options for Windows

The following table describes the FAST options used in the Windows command.

Option	Description
`-h`	Displays the help.
`-p`	Specifies the listening port for the FAST proxy. Example:

Option	Description
	`-p <port>`
`-n`	Identifies the scan name that will appear in ScanCentral DAST. For example: `-n <FAST_scan_name>`
`-u`	Specifies the ScanCentral DAST URL. Example: `-u https://<DAST_API_HOST|IP>:<port>/api/`
`-c`	Optionally, exports the FAST proxy root CA certificate. If your `https` application performs certificate validation, you can use this option alone to install the certificate on your client application to avoid an untrusted certificate error. Example: `-c c:\fast_proxy_ca.crt`
`-f`	Optionally when starting the proxy, specifies a regular expression for the allowed hosts for proxy capture. Example: `-f ".*\.<hostname>\.com"`
`-ps`	Optionally when starting the proxy, configures an external proxy server when the target application does not have direct access from the machine where the FAST proxy is installed. Example: `-ps <host|ip>:<port>`
`-s`	Stops listening. Example: `-s -p <port>`

Option	Description
`-q`	Runs the FAST proxy in quiet mode. This mode does not display messages.
`-k`	Keeps local traffic files after capture.
`-CICDToken`	Specifies the Guid for the scan settings in ScanCentral DAST.
`-CIToken`	Specifies the Base64-encoded authentication token from Fortify Software Security Center.

Using the FAST Linux Version

The following paragraphs describe how to configure and use the Linux Docker image version of FAST.

Options for Accessing Your Functional Tests

To create a macro from your functional tests, the FAST proxy must have access to those tests. Consider the following options for accessing your functional tests with the Linux Docker image version of FAST:

1. Run Docker on the machine that runs your functional tests.
2. Run the FAST proxy on a remote Docker host by using a run command similar to the following:

   ```
   docker -H=your-remote-docker:2375 run
   ```

3. Use remote Docker by way of the Docker REST API.

For Docker documentation, see https://docs.docker.com/.

For options 2 and 3, the functional tests can be on any machine with network access to the Docker host where FAST is running.

Regardless of the option you choose, the Docker host where FAST is running must have network access to the DAST API to upload the macro.

Process Overview

The following table describes the process of configuring and using the Linux version of FAST.

Stage	Description
1.	Prepare a Linux VM machine with Red Hat Enterprise Linux 8 distribution for x86-64 or Ubuntu 22.04, 20.04, 18.04, LTS x64. This machine will be the host for the FAST image.
2.	Install the appropriate Docker Engine for your host machine.

Stage	Description
	Important! Follow Docker recommendations for the Docker engine version to use for Red Hat Universal Base Image (UBI) 8.x x86_64 or Ubuntu 22.04 LTS x86_64 host operating systems.
3.	Pull the FAST Docker image. For more information, see "Pulling the FAST Image" below.
4.	Obtain an authentication token of type **CIToken** from Fortify Software Security Center. For more information, see the *Micro Focus Fortify Software Security Center User Guide*. **Tip:** This token is passed as the value for the `CIToken` in the FAST command.
5.	Obtain a settings identifier from a scan settings file in ScanCentral DAST. For more information, see "Understanding the Scan Settings Detail Panel" on page 238. **Tip:** This token is passed as the value for the `CICDToken` in the FAST command.
6.	Run the FAST Docker container. For more information, see "Running the FAST Container" on the next page.
7.	Run the traffic from your functional tests through the FAST proxy IP address and port specified in the run command.
8.	After traffic has been captured, stop the FAST proxy. For more information, see "Stopping the Container" on page 196.
9.	The ScanCentral DAST instance specified in the `<DAST_API_HOST|IP>/api/` option automatically runs the scan with workflow overrides applied to the settings.

Pulling the FAST Image

After installing the Docker Engine on your host machine and starting the Docker service, you can pull an image of Fortify FAST from the Fortify Docker repository.

To pull the current version of the Fortify FAST UBI image:

- At the terminal prompt on the Red Hat host machine, enter the following command:

```
docker pull fortifydocker/fortify-fast:23.1.ubi.8
```

To pull the current version of the Fortify FAST Ubuntu image:

- At the terminal prompt on the Ubuntu host machine, enter the following command:

```
docker pull fortifydocker/fortify-fast:23.1.ubuntu.2204
```

Running the FAST Container

After you have pulled the image, you can run a container to capture traffic from your functional test scripts.

To run the Fortify FAST UBI container:

- At the terminal prompt, enter the following commands:

```
CONTAINER_NAME="fortify-fast"
IMAGE_NAME="fortifydocker/fortify-fast:23.1.ubi.8"
mkdir -p "$HOME/.fast/certs"
docker run --name $CONTAINER_NAME \
    -p <port>:<port> \
    -v "$HOME/.fast/certs:/etc/fast/certs" \
    --rm \
    $IMAGE_NAME \
    -p <port> \
    -u http://<host|ip>:<port>/api/ \
    -CIToken <Base64_encoded_token> \
    -CICDToken <Guid>
```

To run the Fortify FAST Ubuntu container:

- At the terminal prompt, enter the following commands:

```
CONTAINER_NAME="fortify-fast"
IMAGE_NAME="fortifydocker/fortify-fast:23.1.ubuntu.2204"
mkdir -p "$HOME/.fast/certs"
docker run --name $CONTAINER_NAME \
    -p <port>:<port> \
    -v "$HOME/.fast/certs:/etc/fast/certs" \
    --rm \
    $IMAGE_NAME \
    -p <port> \
    -u http://<host|ip>:<port>/api/ \
    -CIToken <Base64_encoded_token> \
    -CICDToken <Guid>
```

You should see a response similar to the following:

```
0.0.0.0:<ListeningPort>
Listening
```

For descriptions of these run command options, see "Understanding the Run Command Options" below.

Stopping the Container

After you have captured the traffic, you can stop the container and upload the results to ScanCentral DAST.

To stop the container:

- At the terminal prompt, enter the following command:

```
docker exec $CONTAINER_NAME fast -p <port> -s
```

Understanding the Run Command Options

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

Option	Description
`--name`	Specifies the name of your Fortify FAST container. Any string is valid. In the sample code, the name is taken from the `CONTAINER_NAME="fortify-fast"` command.
`-p <port>:<port>`	Publishes the container's main TCP ingress port to the host. For example: `-p 8087:8087`
`-v "$HOME/.fast/certs:/etc/fast/certs" \`	Adds a volume for a Fortify FAST auto-generated certificates directory. This directory safeguards the certificates in case the Fortify FAST container needs to be removed or upgraded.
`--rm`	Automatically removes the container when it exits.
`$IMAGE_NAME \` `-p <port>`	Specifies the listening port for the FAST proxy. For example: `-p 8087`

Option	Description
`-u http://<host|ip>:<port>/api/`	Specifies the ScanCentral DAST URL. For example: `-u https://dast-web-api:64814/api/`
`-CICDToken`	Specifies the Guid for the scan settings in ScanCentral DAST.
`-CIToken`	Specifies the Base64-encoded authentication token from Fortify Software Security Center.
`-s`	Stops listening.

Chapter 5: Working with Scans

You can view the scans that are available in the ScanCentral DAST database in the Scans view. You can also start a new scan, refresh the scan table, delete scans, and download scans, settings, and logs. You can pause, stop, and resume scans that are currently running, and re-import completed scans that failed to import. You can view details about each scan in the scan detail panel.

Accessing DAST Scans in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST scans directly in Fortify Software Security Center.

To access DAST scans in Fortify Software Security Center:

- Select **SCANCENTRAL** > **DAST**.

  The Scans view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Scans View

The Scans view displays in a table the scans that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information that are available for each scan.

Column	Description
Scan Id	Indicates the integer ID in the ScanCentral DAST database for the scan. **Note:** Each scan is assigned an integer ID when it is added to the ScanCentral DAST database.
Application	Indicates the application that was selected when the scan was configured.

Column	Description
Version	Indicates the version that was selected when the scan was configured. **Tip:** The versions listed in this column are links. You can click a link to open the Application Version Overview in a new tab in Fortify Software Security Center.
Name	Indicates the name of the scan. This is the name that was assigned in the scan settings.
Url	Identifies the target URL for the scan.
Critical **High** **Medium** **Low**	Indicates the number of findings for each severity category in the scan. For more information, see "Understanding Vulnerability Severity" on page 217.
Started On	Indicates the date and time that the scan started. The start time is stored in the dynamic scan database as UTC time and is converted to the local machine's system time when displayed in the user interface.
Status	Indicates the current status of the scan. Possible statuses are as follows: • **Queued** – The scan has been submitted and is waiting for an available sensor. • **Pending** – The scan has been accepted by a sensor but is waiting for the sensor to acknowledge that it has accepted and started the scan. • **License Unavailable** - No license is available for a sensor to start the scan. The scan remains in the queue until a license is available for use. **Note:** If the **Use this sensor only** option was not selected when the scan was submitted, the scan will use any available sensor in the assigned pool. • **Paused** – The sensor might have accepted the scan but not yet started it, or the user might have paused the scan so that it is not in a running state. • **Running** – The sensor is actively conducting the scan. • **Complete** – The sensor has finished the scan and results are available. If the **Submit for triage** option was selected during scan configuration, then the scan has been published to Fortify Software Security Center, where you can perform audit analysis of the findings.

Column	Description

	• **Interrupted** – Something went wrong with the sensor that was conducting the scan. For example, the sensor heartbeat has expired.
	• **Unknown** – The scan failed to complete for an unknown reason.
	• **Importing** – The scan is being imported from the ScanCentral DAST database and published to Fortify Software Security Center.
	• **Import Failed** – Something went wrong while importing a `.fpr` or `.scan` file from the sensor to the ScanCentral DAST database.
	• **Import Scan File Queued** – The `.scan` file has been uploaded to ScanCentral DAST and is being saved to the database so that it can be processed by the Utility Service.
	• **Pending Scan File Import** – The `.scan` file was successfully saved to the database and is waiting to be processed by the Utility Service.
	• **Importing Scan File** – The Utility Service is importing the `.scan` file.
	• **Failed to Import Scan File** – Something went wrong while uploading and saving the `.scan` file to the database or during processing of the file.
	• **Failed to Start** – A sensor accepted the scan, but the scan failed to start. Possible reasons include:
	  • The Fortify Software Security Center DAST API is not running.
	  • The connection to the ScanCentral DAST database has been lost.
	  • Communication with the sensor has been lost.
	  • The sensor failed to start.
	  • The scan settings contain errors or invalid settings.
	• **Pausing** – The user has paused the scan, which now displays this transitional state before changing to Not Running.
	• **Resuming** – The user has resumed the scan, which now displays this transitional state before changing to Running.
	• **Completing Scan** – The user has paused the scan and subsequently clicked **Complete**, which stops the scan at that point and processes it as an incomplete scan.
	Tip: You can perform the same analysis and operations on an incomplete scan as you can a completed scan.
	• **Resume Scan Queued** – The user resumed a paused scan and the scan is

Column	Description
	waiting for the sensor to become available. • **Forced Complete** – The user paused a scan and subsequently clicked **Complete**. The scan completed with partial results.
Status Reason	Indicates the reason for Paused, Pausing, Resuming, Resume Scan Queued, Running, and Forced Complete statuses. Possible reasons are **Deny Interval**, **Scan Priority**, and **Deny Interval User Paused**. For more information, see "Working with Deny Intervals" on page 247, "Understanding Advanced Scan Prioritization" on page 174, and "Configuring Scan Priority" on page 173. The following paragraphs describe the combined status and status reasons: • **Paused / Deny Interval** – The scan was running when a deny interval started. The scan is now paused until the deny interval ends. • **Paused / Deny Interval User Paused** – The scan was paused by a user, but has since entered a deny interval. • **Paused / Scan Priority** – The scan was running when a higher-priority scan started. The scan is now paused until the higher-priority scan completes or another sensor accepts the scan. • **Pausing / Deny Interval** – The scan was running when a deny interval started. The scan now displays this transitional state before changing to Paused Deny Interval. • **Pausing / Scan Priority** – The scan was running when a higher-priority scan started. The scan now displays this transitional state before changing to Paused Scan Priority. • **Resuming / Deny Interval** – The scan was paused for a deny interval, but the deny interval has ended. The scan now displays this transitional state before changing to Running. • **Resuming / Scan Priority** – The scan was paused for a higher-priority scan. The scan now displays this transitional state before changing to **Running Scan Priority**. • **Resume Scan Queued / Deny Interval** – The scan was paused due to a deny interval which has ended, so the scan is queued to be resumed. • **Resume Scan Queued / Scan Priority** - The scan was paused for a higher-priority scan which has completed, so the scan is queued to be resumed. • **Running / Deny Interval** – The scan was paused for a deny interval. The deny interval has ended and the sensor is actively conducting the scan.

Column	Description
	• **Running / Scan Priority** – The scan was paused for a higher-priority scan. The higher-priority scan has completed or another sensor has accepted the scan and is actively conducting it. • **Forced Complete / Deny Interval** – The scan was running when a deny interval started. The scan stopped and completed with partial results.
Duration	Indicates how long the scan ran before completion. For scans that are not completed, the column displays the last known duration that was received from the sensor.
Requests	Indicates the total number of requests sent during the scan.
Macro Playbacks	Indicates the number of times that macros have been played during the scan.
Priority	Indicates the scan priority from 0 through 10. For more information, see "Configuring Scan Priority" on page 173.
Purge date	If data retention is enabled, indicates the date when the scan will be purged from the database. The number in parentheses indicates the number of days until the purge date.
Publish Status	Indicates whether the scan has been published to Fortify Software Security Center. Possible statuses are as follows: • **Not Published** – The `.fpr` file has not been published. • **Published** – The `.fpr` file has been published. • **Failed to Publish** – ScanCentral DAST attempted to publish the `.fpr` file, but it failed. Fortify Software Security Center might be down or there might be a network issue.
Publish Status Reason	Indicates why the `.fpr` file was not published to Fortify Software Security Center. Only applicable when the Publish Status is **Not Published** or **Failed to Publish**. Possible reason is **Artifact is too large**. **Important!** The files you upload to Fortify Software Security Center must not exceed 2GB.

Understanding the Scan Detail Panel

When you click a scan in the Scans view, the scan detail panel appears to the right. The scan detail panel provides options to view, rescan, download, and publish completed scans. For more information, see the following:

- "Viewing Scan Results" on page 214
- "Rescanning an Application" on page 210
- "Downloading a File" on page 214
- "Publishing to Fortify Software Security Center" on page 208

In addition to these options, the scan detail panel provides information about the scan, as described in the following paragraphs.

Findings by Severity

The number of findings for each severity category in the scan appears at the top of the panel. From left to right, the severity categories are: Critical, High, Medium, and Low.

Additional Scan Details

The detail panel displays the same information that is displayed in the Scans view for the selected scan, as well as the information described in the following table.

Item	Description
Created On	Indicates the date and time that the scan was created in the dynamic scan database and queued to be run.
Scan Type	Indicates the type of scan selected during scan configuration: **Standard Scan**, **Workflow-Driven Scan**, or **API Scan**.
Status Update	Indicates the date and time that the sensor last reported its status.
Has Site Authentication	Indicates whether site authentication was used to conduct the scan. Possible values are **Yes** and **No**.
Has Network Authentication	Indicates whether network authentication was used to conduct the scan. Possible values are **Yes** and **No**.

Item	Description
Has API Auth Credentials	For API scans, indicates whether authentication was used to conduct the scan. Possible values are **Yes** and **No**.
Failed Requests	Shows the number of failed requests that occurred during the scan.
KB Sent / KB Received	Shows the total number of kilobytes sent and received during the scan.
Pool	Identifies the pool to which the sensor belongs in Fortify Software Security Center.
Use Scan Scaling	Indicates whether scan scaling was enabled. Possible values are **Yes** and **No**.
Policy	Identifies the dynamic policy that was used to conduct the scan.
Completed Date	Indicates the date and time that the scan finished. Available only for scans with a "Complete" status. For more information, see "Understanding the Scans View" on page 198.
Sensor	Indicates the name of the dynamic sensor that conducted the scan.
Publish Status Update	Indicates the date and time that the scan was published to Fortify Software Security Center.
Scan Schedule	If the scan is the result of a schedule, indicates the name of the schedule.
Purge date	If data retention is enabled, indicates the date when the scan will be purged from the database. The number in parentheses indicates the number of days until the purge date.

Understanding the Scan Logs Tab

ScanCentral DAST records event logs that are displayed in the **LOGS** tab of the detail panel. The event logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scans.

Working with Active Scans

You can pause, stop, resume, and re-import active scans in the Scans view. The actions that you can take depend on the current status of the scan. Active scans are those that do not show a status of Complete.

Pausing a Scan

You can pause a scan that has a status of Running.

To pause a scan, do one of the following:

- In the scans view, click the pause icon (❚❚) for the scan you want to pause.
- In the scan detail panel for a selected scan, click the pause icon (❚❚).

The scan is paused.

Stopping a Scan

You can stop a scan that has a status of Not Running, Interrupted, Unknown, or Queued.

To stop a scan, do one of the following:

- In the scans view, click the stop icon (■) for the scan you want to stop.
- In the scan detail panel for a selected scan, click the stop icon (■).

The scan is stopped.

Resuming a Scan

You can resume a scan that has a status of Not Running or Interrupted.

To resume a scan, do one of the following:

- In the scans view, click the start icon (▶) for the scan you want to resume.
- In the scan detail panel for a selected scan, click the start icon (▶).

The scan is resumed.

Re-importing a Scan

If the "Submit for triage" option was selected during scan configuration, the scan is imported to Fortify Software Security Center upon completion. Importing a scan could take some time, during which the status in the scans view is "Importing." The status changes to "Import Failed" if unsuccessful. You can attempt to re-import a scan with the "Import Failed" status.

To re-import a scan, do one of the following:

- In the scans view, click the retry icon (↻) for the scan you want to re-import.
- In the scan detail panel for a selected scan, click the retry icon (↻).

Another attempt is made to import the scan.

Working with Alerts

Alerts occur when situations arise that *could* adversely affect scan performance or results. Alerts dealing with scan settings may provide you with suggested settings changes to improve performance of future scans. Other alerts may provide actionable information to help with a scan that is currently running.

Tip: The alerts feature includes sample intervals and active intervals. Sample interval alerts may occur as often as once per minute on the ALERTS tab. Although these alerts may not indicate a functional issue with the scan, if the number of alerts received becomes problematic, contact Fortify Customer Support for assistance in disabling the alerts feature. For more information, see "Preface" on page 24.

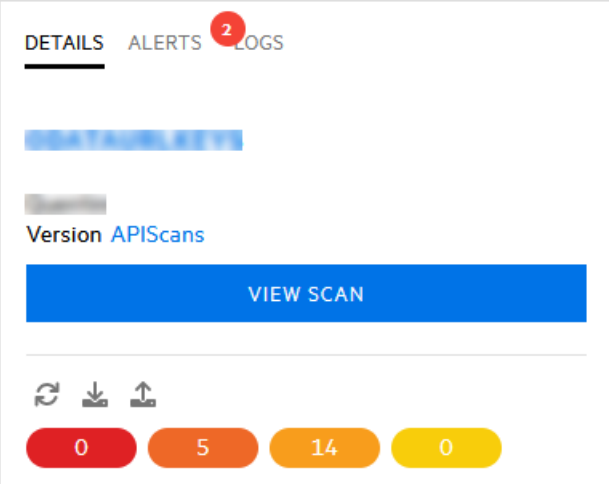
Accessing Alerts

If a scan has an active and unacknowledged alert, it will be highlighted in orange in the Scans view. When you click the scan, the detail panel appears to the right with an ALERTS tab. The number of unacknowledged alerts appears in a red circle next to the ALERTS tab.

Note: Alerts are written to the scan log in near real time. However, you must refresh the page to view updates to the ALERTS tab.

To access the alerts:

1. Click the highlighted scan in the Scans view.
   The scan detail panel, now with an ALERTS tab, appears to the right.



2. Click the **ALERTS** tab.
   The alerts that the scan triggered are listed.

Understanding the ALERTS Tab

The ALERTS tab displays the following categories of alerts:

- **NEW** – Lists the alerts that are active and have not yet been acknowledged. The number of alerts listed in this category should match the number displayed in the red circle.
- **ACTIVE** – Lists the alerts that are active and have been acknowledged. These alerts are still affecting the scan.
- **HISTORY** – Lists alerts that are no longer active, but that occurred during the scan. These alerts are no longer affecting the scan.

Note: After the scan has completed or been forced to complete, all alerts become historical alerts.

Acknowledging New Alerts

To acknowledge an alert in the NEW category:

1. On the **ALERTS** tab, click the alert.

   A check mark appears next to the alert, indicating that the alert is selected.
2. Click **MARK AS ACKNOWLEDGED**.

   The alert is moved to the ACTIVE category.

Important! Acknowledging an alert does not resolve the issue that caused the alert. You must perform troubleshooting to determine the cause and resolve it. For more information, see "Troubleshooting Alerts" on page 351.

Managing the DAST Scans View

You can configure and submit a new scan, refresh the scans view, publish scans to Fortify Software Security Center, and delete scans from the scans view on the Scans page. You can also import `.scan` files. For more information, see "Importing a Scan" on page 209.

Starting a New Scan

You can configure new settings or use existing settings, and then run a scan, which queues the scan in the scans view.

To configure settings or use existing settings for a new scan:

- Click **+ NEW SCAN**.

  The SETTINGS CONFIGURATION wizard opens.

Refreshing the Scans View

You must manually refresh the Scans view to see new scans that have been queued or scan statuses that have changed.

To refresh the Scans view:

- Click **REFRESH**.

Publishing to Fortify Software Security Center

You can publish FPR artifacts to Fortify Software Security Center.

Note: If a scan does not have FPR artifacts, the publish icon is not available.

To publish FPR artifacts for a scan:

- Do one of the following:
  - In the Scans view, click the publish icon (⬆) for the scan whose FPR artifacts you want to publish.
  - In the scan detail panel for a selected scan, click the publish icon (⬆).

  The FPR artifacts are published to the Fortify Software Security Center database.

Deleting a Scan

The scans displayed in the scans view come from the ScanCentral DAST database. You can delete scans from the database that you no longer need, depending on the scan status. Deleting scans from the database has no effect on scans that have already been published to Fortify Software Security Center.

You can delete scans that have a status of Complete, Queued, Pending, Failed to Start, Import Failed, Interrupted, Not Running, and Unknown.

To delete a scan, do one of the following:

- Select one or more check boxes for scans in the scans view, and then click **DELETE** at the bottom of the table.
- Select a scan to view the scan details, and then click **DELETE** at the bottom of the scan details panel.

Using the Force Delete Option

In some cases, scans may not be deleted from the ScanCentral DAST database after you click the delete button. When this occurs, a user with administrator-level privileges can force the deletion of the scan. For more information, see "Permissions in Fortify Software Security Center" on page 40.

To force delete a scan:

1. Select one or more check boxes for scans in the scans view, and then click **DELETE** at the bottom of the table.

   The Delete Scans dialog opens.
2. Select **Force delete**, and then click **OK**.

   Note: The Force delete option is available only for users with administrator-level privileges.

Importing a Scan

You can import a `.scan` file that was created by Fortify WebInspect or another ScanCentral DAST sensor. Afterward, the imported scan settings, scan results, scan logs, site tree, and FPR are available for download or for publishing to Fortify Software Security Center.

Important! The Utility Service starts the import process, and the Global Service completes the import process. Hence, both services must be running to import a scan.

To import a scan:

1. On the **Scans** view, click the **+ NEW SCAN** drop-down arrow and select **Import scan**.

   The SCAN IMPORT dialog box opens.
2. In the **APPLICATION** area, select an application to associate with the scan being imported.

   Tip: You can search for the application and application version. For more information about searching, see "Searching in Input Boxes" on page 135.
3. In the **APPLICATION VERSION** area, select a version to associate with the scan being imported.
4. In the **IMPORT SCAN** area, click **IMPORT**.

   A standard Windows Open dialog box appears.
5. Locate and select the `.scan` file to import, and then click **Open**.
6. If the scan already exists in the ScanCentral DAST database, you are prompted with the following options:
   - **CANCEL** – Stops the import
   - **CREATE** – Creates a new scan with a new Fortify WebInspect scan ID
   - **REPLACE** – Replaces the existing scan with the contents of the scan being imported
   - **OPEN** – Opens the existing scan
7. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**. Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

   A FILE UPLOAD dialog box shows the progress.

Important! It might take some time for large scans to complete the import process. After the initial phase, the dialog box shows the "parsing" phase. Fortify recommends that you do not cancel the import during the parsing phase. Doing so will cause the scan to be queued for import. However, the scan will not import, and you will need to delete the scan.

For information about scan statuses related to importing a scan, see "Understanding the Scans View" on page 198.

Tip: If the import fails, check the Global Service and Utility Service log files. For more information, see "Locating Log Files" on page 341.

Rescanning an Application

The rescan feature allows you to easily rescan an application from an existing scan. This feature is useful for conducting an identical scan of an updated site (using the same settings that were used for the original scan) to determine if previously discovered vulnerabilities have been fixed and if new ones have been introduced.

To rescan an application:

1. Do one of the following:
   - In the Scans view, click the rescan icon () for the scan whose application you want to rescan.
   - In the scan detail panel for a selected scan, click the rescan icon ().

   The RUN SCAN dialog box opens.
2. (Optional) in the **Name** box, enter a name for the scan.

   Tip: The original scan name is prepopulated in the **Name** box. Prepending the original name with "Rescan_" might help you to identify scan results for rescanned applications in your scans view.
3. Select a ScanCentral DAST sensor from the **Sensor** list.

   The list of sensors comes from the Fortify Software Security Center sensor pools. **Any Available** is the default.
4. (Optional) If you select a sensor, but it is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
5. Click **RUN**.

   The scan is queued to run.

Rescan and Key Store Placeholders

If the scan settings, base settings, or macro parameters of the original scan use key store placeholders, a rescan will use the latest values from the key store. The latest values may not be the values that were used in the original scan.

Downloading DAST Scans, Settings, and Logs

You can download a scan settings file (`.xml` format) from the ScanCentral DAST database to your local machine for any scan in the Scans view, except certain scans with the License Unavailable status. (For more information, see "License Unavailable Scan Status" on the next page.) Depending on the status of the associated scan, you can also download a log file, the site tree (`.csv` format), or the scan results (`.scan` or `.fpr` format).

Note: You must have Fortify WebInspect, Log Viewer, Site Explorer, Traffic Viewer, or another Fortify WebInspect tool on your local machine to work with the log file or scan results.

Important! While downloading a file, you must keep the browser open. Closing the browser will end the download prematurely.

Important Information about Settings

Settings that do not exist in Fortify WebInspect, such as Scan Priority, Submit for Triage, Enable SAST Correlation, and so forth, will not be exported when exporting ScanCentral DAST settings. If you have multiple ScanCentral DAST environments, and you export settings from one environment to another, settings that do not exist in Fortify WebInspect will be dropped. However, when performing an upgrade from the previous version of ScanCentral DAST to the current version, these settings are successfully migrated.

Settings that Include Key Store Placeholders

If an administrator changes the value for a key store placeholder, the scan settings that use the key store placeholder will consume the new value when the settings are downloaded or used to start a scan. When downloading scan settings that use key store placeholders, it may take time to replace the placeholders with the corresponding values from the key store entries. For more information about key stores, see "Understanding Key Stores" on page 327.

Paused Scans

Anytime a scan is paused—by a user, due to scan priority, or due to deny interval—the partial scan results are uploaded to the ScanCentral DAST database and are available for download. After the partial results have been uploaded, the scan is deleted from the sensor.

ScanCentral DAST does not send the results to Fortify Software Security Center until the scan is complete or forced complete.

License Unavailable Scan Status

If a scan has not started because a license is unavailable, then scan settings are not created. Therefore, no file types are available for download for these scans with the License Unavailable status.

However, if a scan is paused and then resumed, but no license is available, then scan settings, scan results, site tree, and scan log files are available for download for these scans with the License Unavailable status.

File Types Available

The following table describes the file types that are available for download for each scan status.

	File Types Available for Download		
Scan Status / Status Reason	**Scan Settings**	**Scan Result / Site Tree / FPR**	**Scan Logs**
Complete	x	x	x
Completing Scan	x		
Failed to Start	x		
Forced Complete Forced Complete / Deny Interval	x	x[1]	x
Import Scan File Queued Pending Scan File Import Importing Scan File Failed to Import Scan File		x[2]	
Importing Import Failed	x		
Interrupted	x		x

[1]Scans with a Forced Complete status might not have scan results or a site tree, depending on when the scan was stopped. For this reason, Scan Result and Site Tree might not be available file types to download.
[2]Only Scan Results are available for these import statuses.

Scan Status / Status Reason	File Types Available for Download		
	Scan Settings	Scan Result / Site Tree / FPR	Scan Logs
Not Running	x		
Paused Paused / Deny Interval Paused / Deny Interval User Paused Paused / Scan Priority	x	x[1]	
Pausing Pausing / Deny Interval Pausing / Scan Priority	x		
Pending	x		
Queued	x		
Resume Scan Queued Resume Scan Queued / Deny Interval Resume Scan Queued / Scan Priority	x		
Resuming Resuming / Deny Interval Resuming / Scan Priority	x		
Running Running / Deny Interval Running / Scan Priority	x		
Unknown	x		

For more information about the scan statuses, see "Understanding the Scans View" on page 198.

[1]Scans with a Paused status do not include an FPR and cannot be published to Fortify Software Security Center.

Downloading a File

To download a file for a scan:

1. Do one of the following:
   - In the Scans view, click the download icon (⬇) for the scan whose file you want to download.
   - In the scan detail panel for a selected scan, click the download icon (⬇).

   The DOWNLOAD dialog box opens.
2. Select the file type to download from the list.

   Tip: To view the scan results in Site Explorer, you must select **Scan Result**.

   Note: The available file types to download depend on the scan status. For details, see "File Types Available" on page 212.
3. Click **DOWNLOAD**.

   By default, the file is downloaded to the folder on your local machine that is specified in your browser settings for downloads.

Viewing Scan Results

You can examine the scan results for scans with a status of Complete or Forced Complete. For more information about scan statuses, see "Understanding the Scans View" on page 198.

To view scan results:

1. In the Scans view, click the scan that you want to view.

   The scan detail panel appears to the right.
2. Click **VIEW SCAN**.

   The scan opens in a new tab with the scan name displayed.

   Tip: If you run a scan in ScanCentral DAST, the findings are automatically imported. If the completed scan fails to import or if the completed scan was not conducted in ScanCentral DAST, the button will be labeled **IMPORT FINDINGS**. When this occurs, you must import the findings before you can view the scan.

Working with the Site Tree

By default, the Site Tree displays an unfiltered tree view of all traffic that was generated during the scan. The tree includes a list of hosts and all sub-directories within those hosts. In this view, you can select a top-level host and expand the sub-directories to examine the requests and responses that

occurred at each level. To display the requests that were made to a resource, select the resource in the Site Tree.

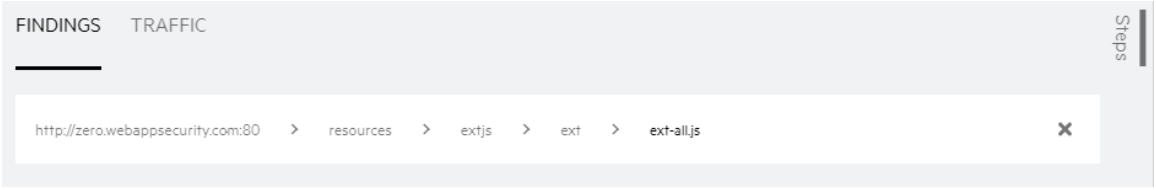
Site Tree Icons

The following table identifies the icons that appear in the Site Tree.

Icon	Name	Represents
	Server/host	The top level of your site's tree structure **Note:** You might have multiple server/host icons in your site tree representing different protocols and ports.
/	Folder	A directory
	Page	A file
	Operation	An API operation followed by the operation name in the following format: • `Operation: GetClients` • `Operation: UpdateClient`
	Parameter	An API parameter followed by the parameter name in the following format: • `Parameter: id` • `Parameter: first_name`

Using Breadcrumbs

When you select a resource in the Site Tree, breadcrumbs appear at the top of the Findings and Traffic tables, similar to the sample shown here.



Breadcrumbs provide a visual aid that indicates the location of the resource within the website's hierarchy. You can click a breadcrumb in the path to view findings or traffic for that resource.

To filter the findings or traffic for a specific resource listed in the breadcrumbs:

- Click the resource in the breadcrumbs.

  For example, if you want to view all findings or traffic for the extjs folder shown in the previous image, click **extjs**.

  The selected resource becomes the final breadcrumb and the Findings and Traffic tables are updated to show only data for the selected resource.

To remove the filter completely:

- Click the clear breadcrumbs icon (✖) at the end of the breadcrumbs.

  The breadcrumbs are removed and the findings and traffic data are no longer filtered.

Understanding the Findings Table

The Findings table displays information about each vulnerability discovered during an audit of your web presence. Each row (or session) in the Findings table represents a single finding.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

Available Columns

The following table describes the available columns.

Column	Description
Severity	A relative assessment of the vulnerability, ranging from low to critical. For more information, see "Understanding Vulnerability Severity" on the next page.
Check ID	The identification number of a Fortify WebInspect probe that checks for the existence of a specific vulnerability. For example, Check ID 742 tests for database server error messages.
Name	A Fortify WebInspect probe for a specific vulnerability, such as Cross-site Scripting, Unencrypted Log-in Form, and so on.
URL	The hierarchical path to the resource along with parameters.
Parameter Name	The name of the vulnerable parameter.
Parameter Value	The value assigned to the vulnerable parameter.
CWE	The Common Weakness Enumeration identifier(s) associated with the

Column	Description
	vulnerability.
Method	The HTTP request method used for the attack.
Kingdom	The vulnerability category from the Seven Pernicious Kingdoms taxonomy for ordering and organizing vulnerabilities. For more information, see https://vulncat.fortify.com/.
Session ID	The unique session ID for the request and response in the DAST database.

Known Limitation with Suppressed Findings

Currently, findings that are suppressed in Fortify Software Security Center are not suppressed in the ScanCentral DAST Findings table.

Understanding Vulnerability Severity

Every check in Fortify's SecureBase includes a severity. The severity is determined and assigned by Fortify Security Researchers.

Severity Descriptions

Severity descriptions are as follows:

- **Low** – Interesting issues, or issues that could potentially become more severe.
- **Medium** – Non-HTML errors or issues that could be sensitive.
- **High** – Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
- **Critical** – An attacker might have the ability to execute commands on the server or retrieve and modify private information.

How Severity is Determined

When assigning a severity, Fortify Security Researchers consider the real world impact of the vulnerability, including the following aspects:

- The maximum damage that could result if the vulnerability were exploited
- The conditions of the issue that the check can detect
- Any related Common Vulnerabilities and Exposures (CVEs)

The Research Team then debates to reach consensus and assigns a number as described in the following table.

Assigned Number	Severity
0 - 9	Normal [1]
10	Information [2]
11 - 25	Low
26 - 50	Medium
51 - 75	High
76 - 100	Critical

[1]This severity is not displayed in ScanCentral DAST findings.

[2]This severity is not displayed in ScanCentral DAST findings.

Working with Findings

You can view the vulnerabilities discovered during the scan on the Findings tab, which includes the Findings table and the Vulnerability Description, HTTP, and Steps tabs.

Tip: Remember that selecting a resource in the Site Tree filters the data to that resource in the Findings table. For more information, see "Working with the Site Tree" on page 214.

Viewing the Vulnerability Description

The Vulnerability Description tab displays content from SecureBase related to the selected vulnerability. In addition to a detailed description of the vulnerability, the SecureBase content might include information on how to verify the issue, possible implications if the issue is not fixed, remediation information, and links to additional references.

To view the Vulnerability Description:

- Select a finding in the **FINDINGS** table.
  The VULNERABILITY DESCRIPTION tab displays information about the vulnerability.

Viewing the Request and Response

The HTTP tab includes the request and response session details for the selected vulnerability.

To view the request and response:

1. Select a finding in the **FINDINGS** table.
2. Click the **HTTP** tab.

In the REQUEST area, the attack is highlighted. In the RESPONSE area, the vulnerability is highlighted.

Viewing Steps

The Steps tab displays the route taken by the sensor to arrive at the session selected in the Findings table. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

To view the steps:

1. Select a finding in the **FINDINGS** table.
2. Click the **Steps** tab.

   The STEPS table displays the route taken by the sensor to arrive at the session selected.

To close the Steps tab, do one of the following:

- Press the **ESC** key.
- Click the **Steps** tab again.

Understanding the Traffic Table

The Traffic table displays traffic generated during the scan, enabling you to explore the traffic for the scan. The Traffic table is always available in the scan results. If you enabled traffic monitor logging in the scan settings, then the Traffic table lists all of the scan traffic. For more information, see "Enabling Traffic Monitor" on page 177 and "Enabling Traffic Monitor in Base Settings" on page 288.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

Available Columns

The following table describes the available columns.

Column	Description
Request Start	The date and time the sensor started sending the request.
Request End	The date and time the sensor finished sending the request.
Host	The top-level URL of the target web site.
Port	The port number over which the requests were sent.
Path	The hierarchical path to the resource on the web server.
Method	The HTTP request method used, such as GET, POST, and PUT.

Column	Description
Status	The HTTP status code returned from the host. For more information, see "HTTP Status Codes" on page 368.
Category	Broadly defines the source of the request, such as audit, crawl, and so forth. This information might be useful for diagnostics.
Sequence	The order in which the request appeared in the traffic.
Scheme	The protocol used to make the request, such as `http://` or `https://`.
Error Code	An error code that indicates the request failed at the TCP/IP level, such as the connection closed or a time out occurred.
Request Length	The request length, expressed in bytes.
Response Length	The response length, expressed in bytes.
Scan.Sid	The unique session ID for the request and response in the DAST database.
Scan.Psid	The unique parent session ID for the request and response in the DAST database.
Scan.Sessiontype	Identifies why there is a session in the database, such as crawl, attack, triggered macro, and so on.
Scan.Attacktype	Identifies what the sensor did in the request, such as cookie injection, query injection, and so on.
Scan.Checkid	The identification number of a Fortify WebInspect probe that checks for the existence of a specific vulnerability.
Scan.Attacksequence	Shows the order of requests sent by the audit engine. This information might be useful for debugging a specific engine.
Scan.Engine	Name of the audit engine that sent the request.
Scan.Attackparamdesc	Name of the parameter being attacked in the request.
Scan.Attackparamindex	Identifies a parameter by index instead of by name. This might be useful because not all parameters have names and in some

Column	Description
	applications names are duplicated. Index of the parameter. The index count starts at 0, so if your site has 10 cookies and the audit engine attacked the third one, then the parameter index of the attacked cookie will be 2.
Scan.Attackparamsubindex	When we break up something smaller than Post and Query and cookie, such as a JSON document.
Scan.CrawlType	Identifies the type of crawl, such as from script execution, forms submission, dynamically generated URLs, HREF, and so forth.
Scan.Attributename	Used for diagnostics to help identify the request source.
Scan.Format	Used for diagnostics to help identify the request source.
Scan.Linkkind	Used for diagnostics to help identify the request source.
Scan.Locations	Used for diagnostics to help identify the request source.
Scan.Source	Used for diagnostics to help identify the request source.
Scan.Nodename	Used for diagnostics to help identify the request source.

Working with Traffic

You can view the traffic generated during the scan on the Traffic tab, which includes the Traffic table and the HTTP, Parameters, and Steps tabs.

Tip: Remember that selecting a resource in the Site Tree filters the data to that resource in the Traffic table. For more information, see "Working with the Site Tree" on page 214.

Viewing the Request and Response

The HTTP tab includes the request and response session details for the selected vulnerability.

To view the request and response:

1. Select a session in the **TRAFFIC** table.
2. Click the **HTTP** tab.

   In the REQUEST area, the attack is highlighted. In the RESPONSE area, the vulnerability is highlighted.

Viewing Parameters

You can view the Type, Name, and Value for parameters used in a traffic session. The Parameters detail view displays a table with one record for each cookie or query string used in the traffic session.

A parameter can be one of the following:

- Cookie data
- A query string submitted as part of the URL in the HTTP request (or contained in another header)
- Data submitted using the Post method (such as `set_<parametername>`)

To view the parameter details for a session:

1. Select a session in the **TRAFFIC** table.
2. Click the **PARAMETERS** tab.
   The PARAMETERS table displays the parameters used in the selected session.

Viewing Steps

The Steps tab displays the route taken by the sensor to arrive at the session selected in the Traffic table. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

To view the steps:

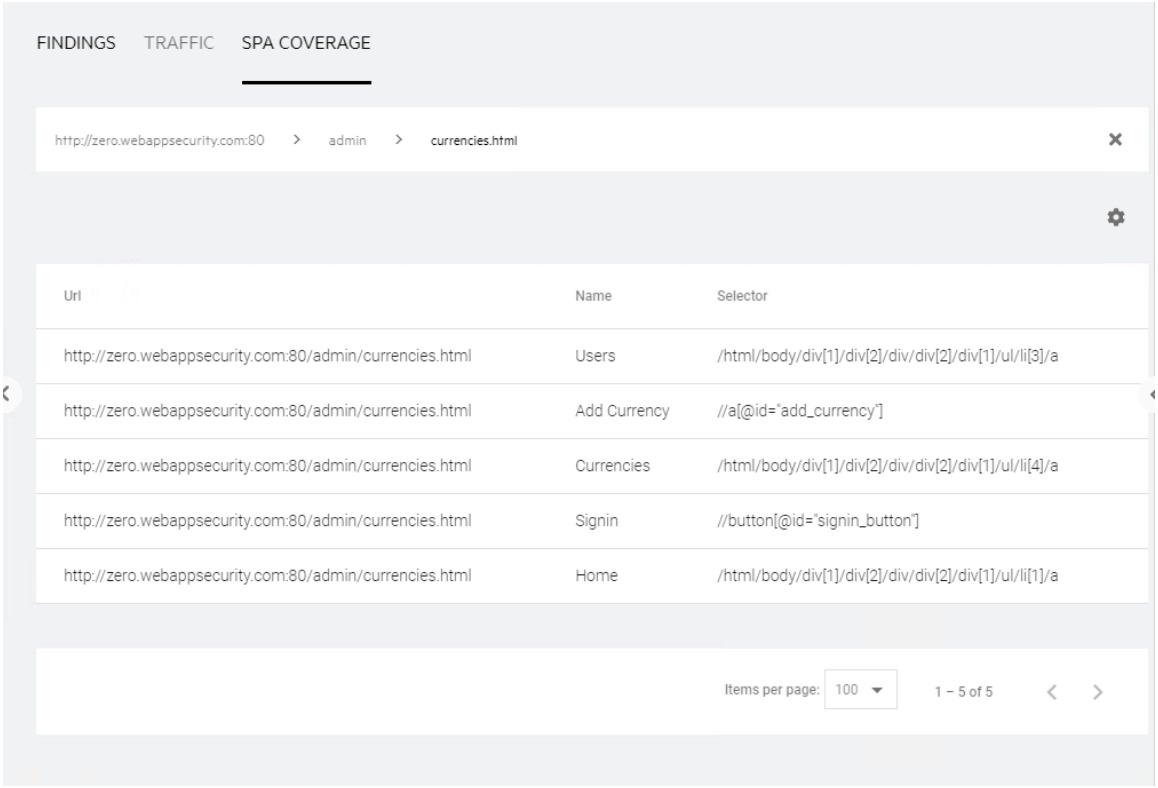
1. Select a session in the **TRAFFIC** table.
2. Click the **Steps** tab.
   The STEPS table displays the route taken by the sensor to arrive at the session selected.

To close the Steps tab, do one of the following:

- Press the **ESC** key.
- Click the **Steps** tab again.

Understanding SPA Coverage

The single-page application (SPA) Coverage view is available only if the scan includes SPA events. This view displays the elements in the page that the crawler interacted with during the crawl. The SPA events are filtered based on what you select in the Site Tree.



The SPA Coverage view lists the URLs where the elements were discovered, along with the following additional information:

- **Name** – The visible text, symbol, link, HTML tag name, or other UI information related to the element.
- **Selector** – The XPath location of the element in the page. This is used to find and perform operations on the element.

For more information, see "Scanning Single-page Applications" on page 176.

Chapter 6: Working with Sensors, Sensor Pools, and Auto Scale Job Templates

You can view and manage the ScanCentral DAST sensors in your environment as well as the sensor pools that handle sensor licensing and determine which applications each sensor can scan. Depending on your user role and permissions in Fortify Software Security Center, you can also work with auto scale job templates. The following pages describe managing sensors, sensor pools, and auto scale job templates.

Working with Sensors

You can view all of the sensors that are stored in the ScanCentral DAST database in the Sensors view. You can view a sensor's status and whether it is enabled, as well as other details, in the sensor detail panel. From the sensor detail panel, you can also enable or disable sensors.

Accessing DAST Sensors in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST sensors directly in Fortify Software Security Center.

To access DAST sensors in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Sensors**.
   The Sensors view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Sensors View

The Sensors view displays in a table all sensors that are stored in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each sensor.

Column	Description
Name	Displays the value specified as `--hostname` in the Docker run command. **Note:** If the host name is not set or returns an empty value for any reason, then ScanCentral DAST uses the internal Docker container ID. The value is automatically truncated to 15 characters and is displayed in upper case.
Description	Displays the value specified as the `ScannerDescription` environment variable in the Docker run command or in the `appsettings.json` file.
Pool	Identifies the pool to which the sensor belongs. **Note:** If the pool has been configured for sensor auto scaling but has been deleted, then "(deleted)" is appended to the pool name until all scaled sensors in the pool have completed their scans and been shut down. For more information, see "Understanding Sensor Auto Scaling" on page 231.
Current Scan ID	Indicates the integer ID in the ScanCentral DAST database for the scan that the sensor is actively conducting. **Note:** Each scan is assigned an integer ID when it is added to the ScanCentral DAST database.
Sensor Enabled	Indicates whether the sensor is enabled to perform scans. Possible values are **Enabled** and **Disabled**.
Status	Indicates the current status of the sensor. Possible values are **Online** and **Offline**.

Understanding the Sensor Detail Panel

When you select a sensor in the Sensors view, the sensor detail panel appears. The sensor details show the sensor's status and whether is it enabled.

The detail panel displays the same information that is displayed in the Sensors view for the selected sensor, as well as the information described in the following table.

Item	Description
IP Address	Identifies the IP address assigned to the sensor when the image was started.
Pool	Identifies the pool to which the sensor belongs.

Item	Description
Current Scan ID	Indicates the integer ID in the ScanCentral DAST database for the scan that the sensor is actively conducting. **Note:** Each scan is assigned an integer ID when it is added to the ScanCentral DAST database.
Last Connect	Indicates the last time the sensor sent an update on its status to the scanner service.
Operating System	Indicates the operating system of the VM or machine that is running the Docker container. Currently, Microsoft Windows is the only supported operating system.
Version	Indicates the operating system version of the VM or machine that is running the Docker container.
Application Version	Indicates the version of ScanCentral DAST Sensor Service, whether running as a container or as a service with a classic Fortify WebInspect installation.
WebInspect Version	Indicates the version of Fortify WebInspect being used to conduct scans.

Enabling or Disabling Sensors

The Sensors view shows all sensors that are stored in the ScanCentral DAST database. Depending on your permissions in Fortify Software Security Center, you can enable and disable the sensors in the view.

Facts About Disabled Sensors

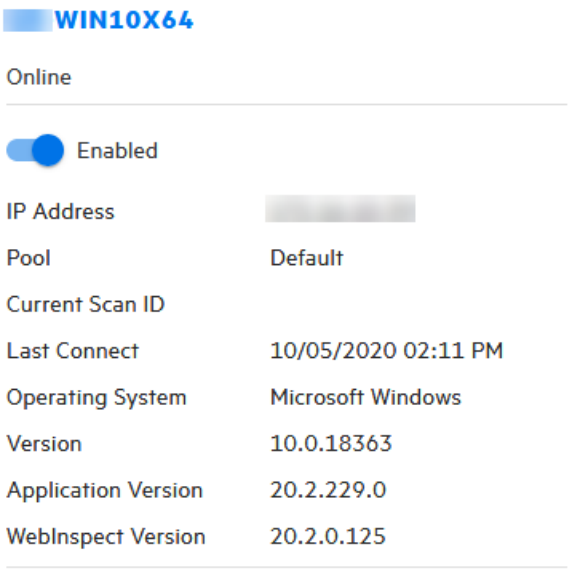
You should understand the following facts that apply to disabling a sensor:

- If a sensor is disabled, it is still online but cannot process any new scans.
- If a sensor is currently running a scan and you disable the sensor, the scan that is running will finish and then the sensor will not process any more scans until it is enabled again.

Enabling or Disabling a Sensor

To enable or disable a sensor:

1. Select the sensor in the view.
   The sensor details panel appears.



2. Do one of the following:
   - To enable the sensor, toggle the switch to **Enabled**.
   - To disable the sensor, toggle the switch to **Disabled**.

Working with Sensor Pools

A sensor pool provides a way for you to license your ScanCentral DAST sensors with a specific license pool in the License and Infrastructure Manager (LIM) and designate which applications each sensor can scan. You can also configure sensor auto scaling and scan scaling for a sensor pool.

Accessing DAST Sensor Pools in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST sensor pools directly in Fortify Software Security Center.

To access DAST sensor pools in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Sensor Pools**.
   The Sensors Pools view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Sensor Pools View

The Sensor Pools view displays in a table the ScanCentral DAST sensor pools that are configured in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information that are available for each pool.

Column	Description
Name	Identifies the name of the sensor pool.
Description	Provides a description of the pool.
LIM Pool	Identifies the license pool that is configured in the License and Infrastructure Manager (LIM).
Default	Indicates whether the pool is designated as the default pool. Possible values are **Yes** or **No**. If you spin up a new sensor and do not assign it to a pool, the sensor will be assigned to the default pool automatically.
2FA Server	Indicates the name of the two-factor authentication server that is configured for the pool. For more information, see "Working with Two-factor Authentication" on page 302.
Sensor Scaling	Indicates whether sensor auto scaling is enabled for the pool. Possible values are **Enabled** or **Disabled**.
Sensor Scaling Host	Identifies the host URL for the Kubernetes environment that was configured for sensor auto scaling.
Sensor Scaling Namespace	Identifies the Kubernetes namespace that was configured for sensor auto scaling.
Sensor Scaling Max Replicas	Specifies the maximum number of sensor replicas that can be run in the pool in the Kubernetes environment.

Column	Description
Sensor Scaling Template Name	Specifies the job template that manages Kubernetes pods for automatic sensor scaling. For more information, see "Working with Auto Scale Job Templates" on page 233.
Scan Scaling	Indicates whether scan scaling is enabled for the pool. Possible values are **Enabled** or **Disabled**.
Scan Scaling Host	Identifies the Kubernetes ingress host URL that was configured when the WISE cluster was deployed in Kubernetes.

Understanding the Pool Detail Panel

When you select a pool in the Sensor Pools view, the pool detail panel appears. If the pool you select is the default pool, it will be identified as DEFAULT at the top of the pool detail panel. Otherwise, an option is available to make the pool the default pool. For more information, see "Managing Sensor Pools" on page 232.

The detail panel displays the same information that is displayed in the Sensor Pools view for the selected pool, as well as the information described in the following table.

Item	Description
ASSIGNED APPLICATIONS	Lists the applications that sensors in the pool can scan.
ASSIGNED SENSORS	Lists the sensors that are assigned to the pool.
Maximum Per Scan Engines	If Scan Scaling is enabled, specifies the maximum number of sensor replicas that can be run in this pool.

Creating a DAST Sensor Pool

When you create a ScanCentral DAST sensor pool, you can assign a single sensor or group of sensors to specific applications. These assignments determine which sensors can scan each application in your environment.

To create a new sensor pool:

1. On the **Sensor Pools** page, click **+ NEW POOL**.
   The SENSOR POOL - CREATE dialog box opens with the Getting Started page in view.
2. In the **Name** box, type a name for the pool.

3. In the **Description** box, type a description for the pool.
4. In the **Pool** list, select the License and Infrastructure Manager (LIM) license pool for licensing the sensors in the pool.
5. In the **Password** box, type the password associated with the LIM license pool.
6. To verify that you can connect to the LIM with the license pool and password, click **VALIDATE**.
7. Click **Sensors** in the menu or click **NEXT**.

   The SENSORS list appears.
8. Select one or more sensors to add to the pool.

   Important! If you are creating a pool to allow sensor auto scaling or scan scaling, make sure that you select sensors that have been configured for integration with Kubernetes. For more information, see "Integrating with Kubernetes for Scan Scaling" on page 108.

   The sensors are added to the SENSORS SELECTED list.
9. Click **Applications** in the menu or click **NEXT**.

   The APPLICATIONS list appears.
10. Select one or more applications to add to the pool.

    The applications are added to the APPLICATIONS SELECTED list.

What's Next?

Do one of the following:

- To configure sensor auto scaling or scan scaling, click **Scan Scaling** in the menu or click **NEXT**, and proceed with "Configuring Sensor Auto Scaling and Scan Scaling" below.
- To review your settings:
  a. Click **Review** in the menu.

     Review your sensor pool settings.
  b. Click **SAVE**.

     The pool is added to the Sensor Pools list.

Configuring Sensor Auto Scaling and Scan Scaling

Optionally, you can configure sensor auto scaling and scan scaling for a sensor pool on the **Scan Scaling** page.

Important! When sensor auto scaling is configured, the DAST Global Service manages the scaling of sensors within your Kubernetes environment. However, to configure scan scaling, you must first configure a WebInspect Script Engine (WISE) cluster in Kubernetes. For more information about scan scaling, see "Integrating with Kubernetes for Scan Scaling" on page 108.

Understanding Sensor Auto Scaling

When creating or editing a sensor pool, you can configure sensor auto scaling for the pool. Sensor auto scaling applies only to sensors that are installed in your Kubernetes environment. These sensors are known as “scaled or scalable” sensors.

When sensor auto scaling is enabled for the sensor pool and a scan is queued, the DAST Global Service checks the number of running instances of a sensor. If the number of running instances is less than the maximum replica specified in the settings for sensor auto scaling, then the DAST Global Service will create a Kubernetes job that starts the container, runs the scan, and shuts down the container.

If a sensor is in the sensor pool but has been configured outside of Kubernetes, and the sensor is online and available, ScanCentral DAST will use this sensor rather than sensor auto scaling. Sensors that are configured outside of Kubernetes are known as “fixed” sensors.

Configuring Sensor Auto Scaling

Configure sensor auto scaling in the **SENSOR AUTO SCALING** area as follows:

1. Slide the Disabled-Enabled toggle to **Enabled**.
2. In the **Host** box, enter the host URL for the Kubernetes environment.
3. In the **Access Token** box, enter the access token for the Kubernetes environment.
4. Optionally, in the **Job Namespace** box, enter a namespace to provide Kubernetes.

   Note: If you do not provide a namespace, then Kubernetes will use the default namespace.
5. In the **Maximum Replicas** list, enter the maximum number of sensor replicas that can be run in this pool in the Kubernetes environment.

   Note: The minimum number of replicas allowed is 1.
6. In the **Job Template** list, select a template to use for sensor scaling. For more information, see "Working with Auto Scale Job Templates" on page 233.

Configuring Scan Scaling

Important! Fortify recommends that scan queues be empty before modifying scan scaling settings.

Configure scan scaling in the **SCAN SCALING** area as follows:

1. Slide the Disabled-Enabled toggle to **Enabled**.
2. In the **Host** box, enter the Kubernetes ingress host URL that was configured when the WISE cluster was deployed in Kubernetes. It uses the WebSocket protocol such as `ws://<wise-cluster-ingress-hostname>/`.

3. In the **Authorization Token** box, enter the token used to authenticate the sensor to use the WISE Kubernetes cluster.

   Tip: This user-specified token was generated by the `--set wise.authtoken` command during the WISE Helm installation.

4. Do one of the following:
   - To allow ScanCentral DAST to scale the number of script engine pools to equal the number of crawl and audit threads in the scan, select **Automatically set script engines per scan** check box.
   - To specify a maximum number of script engine pools per scan, clear the **Automatically set script engines per scan** check box, and then enter a number in the **Maximum script engines per scan** box.

     Tip: If your Kubernetes cluster has limited resources, setting the **Maximum script engines per scan** limits the amount of resources used in scan scaling and avoids having one or two scans consume all of your resources.

What's Next?

After you configure sensor auto scaling and scan scaling, do the following:

1. Click **Review** in the menu or click **NEXT**.

   Review your sensor pool settings.
2. Click **SAVE**.

   The pool is added to the Sensor Pools list.

Managing Sensor Pools

You can edit and delete pools, refresh the pools list, and change the default pool on the Sensor Pools page.

Important! Fortify recommends that scan queues be empty before modifying sensors pools.

Facts About Managing Sensor Pools

You should understand the following facts about managing sensor pools:

- You cannot delete the default sensor pool.
- If you delete a sensor pool, all sensors and applications assigned to that pool will be reassigned to the default pool.

Editing a Sensor Pool

To edit a sensor pool:

1. In the Sensor Pools list, select the pool to edit.
   The pool detail panel appears.
2. Click **EDIT**.
   The pool settings appear in a dialog box that is similar to the CREATE NEW POOL dialog box.
3. To make edits, follow the procedure listed in "Creating a DAST Sensor Pool" on page 229.

Refreshing the Pools View

Generally, the changes that you make to the sensor pools appear right away on the Sensor Pools view. However, if other users have access to the same sensor pools, any changes they make will not be updated in your view. To see such changes, you can manually refresh the pools view.

To refresh the Pools view:

- Click **REFRESH**.

Deleting a Sensor Pool

To delete a sensor pool, do one of the following:

- Select one or more check boxes for pools in the Sensor Pools view, and then click **DELETE** at the bottom of the table.
- Select a pool to view the pool details, and then click **DELETE** at the bottom of the pool details panel.

Tip: You cannot delete the default sensor pool.

Changing the Default Sensor Pool

The first pool you configure becomes the default pool. If you have only one pool configured, it will always be the default pool. If you have multiple pools configured, however, you can change the default pool at any time.

To change the default pool:

- Select a pool to view the pool details, and then select **Make default** in the pool details panel.

Working with Auto Scale Job Templates

Job templates are Kubernetes configuration YAML files that contain template information for Kubernetes jobs. ScanCentral DAST uses auto scale job templates to automatically start sensors to perform scans and then stop the sensors upon scan completion.

When a DAST environment is created, default auto scale job templates are created and stored in the DAST database. You can view and manage auto scale job templates on the Auto Scale Job Templates page.

Accessing Auto Scale Job Templates in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with auto scale job templates directly in Fortify Software Security Center.

To access auto scale job templates in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Auto Scale Job Templates**.
   The Auto Scale Job Templates view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to auto scale job templates may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Auto Scale Job Templates View

The Auto Scale Job Templates view table displays the auto scale job templates that are configured in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information that are available for each job template.

Column	Description
Name	Identifies the name of the job template.
Description	Provides a description of the job template.
Operating System	Identifies the operating system on which the job template runs. Options are **Windows** and **Linux**.

Managing Auto Scale Job Templates

You can import job templates, edit and delete job templates, and refresh the job templates table on the Auto Scale Job Templates view.

Importing a Job Template

You can import a new or edited auto scale job template to the DAST database.

To import a job template:

1. On the **Auto Scale Job Templates** page, click **+ JOB TEMPLATE**.
   The SCANNER AUTO SCALE JOB TEMPLATE dialog box opens.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the `YML` or `YAML` file, and then click **Open**.
4. In the **Name** box, enter a job template name. This is the name that will appear in the Sensor Pools list when the job template is assigned to the pool.
5. In the **Operating System Type** list, select the operating system on which the job template will run. Options are **Windows** and **Linux**.
6. Optionally, in the **Description** box, type a meaningful description of the job template.
7. Click **OK**.

Editing a Job Template

You can download and edit a default template in your editor of choice, and then import the edited version back to the DAST database.

Caution! Do not edit file content that is marked "`# DO NOT EDIT. Required for SC DAST.`" Doing so will invalidate the file.

Use the following process to edit a job template.

Stage	Description
1.	In the **Auto Scale Job Template** view, click the download icon (⬇) for the job template to edit.
2.	Edit the downloaded file and save the changes in your editor of choice.
3.	Do the following: 1. In the **Auto Scale Job Templates** view, select the check box for the job template to edit.

Stage	Description
	2. Click **EDIT**. The SCANNER AUTO SCALE JOB TEMPLATE dialog box opens. 3. Follow steps 2 through 7 of the procedure in "Importing a Job Template" on the previous page.

Deleting a Job Template

You can delete only one job template at a time, and you must select a replacement job template for the affected sensor pools to use. Also, you must have at least one job template.

To delete a job template:

1. In the **Auto Scale Job Templates** view, select the job template to delete.
2. Click **DELETE**.
   The DELETE SENSOR AUTO SCALE JOB TEMPLATE dialog box opens requesting a confirmation.
3. Select the **I'm sure. Select replacement template.** check box.
4. In the **Replacement Job Template** list, select a job template for the affected sensor pools to use.
5. Click **DELETE**.

Refreshing the Job Templates View

Generally, the changes that you make to the job templates appear right away on the Auto Scale Job Templates view. However, if other users have access to the same job templates, any changes they make will not be updated in your view. To see such changes, you can manually refresh the job templates view.

To see an updated job templates view:

- Click **REFRESH**.

Chapter 7: Working with Scan Settings

You can view the scan settings that are available in the ScanCentral DAST database in the Settings List view. You can view the application, version, and URL that are configured for each settings file, as well as other details, in the settings detail panel. From the Settings List view, you can also configure new scan settings, edit existing settings, download settings, and delete settings.

Accessing DAST Scan Settings in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST scan settings directly in Fortify Software Security Center.

To access DAST scan settings in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Settings List**.
   The Settings List view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Settings List View

The Settings List view displays in a table the scan settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each settings file.

Column	Description
Name	Indicates the name of the settings file. This is the name that was assigned at

Column	Description
	the time the settings were configured and saved.
Application	Indicates the application for which the settings apply.
Version	Indicates the version for which the settings apply.
Scan Type	Indicates the type of scan to be conducted using the settings. Types are: • **Standard Scan** • **Workflow-driven Scan** • **API Scan**
Modified	Indicates the date and time that the settings were created, or if edited, the last date and time that the settings were changed.
CICD identifier	Identifies the settings identifier GUID that was assigned to the settings.

Understanding the Scan Settings Detail Panel

When you click a settings file in the Settings List view, the settings detail panel appears to the right. The application, version, and URL that are configured in the scan settings are listed at the top of the panel.

The detail panel displays the same information that is displayed in the Settings List view for the selected settings, as well as the information described in the following table.

Item	Description
Created	Indicates the date and time that the settings were saved.
Policy	Identifies the dynamic policy to be used to conduct the scan.
User Agent	Indicates the user agent one or more of the following: • **Chrome** • **Chrome (Mobile Android)** • **Custom** • **Default** • **Edge** • **Safari**

Item	Description
	• **Safari (Mobile IOS)** **Note:** Default uses the user agent that is defined in Fortify WebInspect.
Login Macro	If applicable, indicates the file name of the login macro specified in the settings.
Has Network Auth	Indicates whether network authentication is specified in the settings. Possible values are **Yes** and **No**.
Allowed Hosts	If applicable, lists the first (or only) allowed host from the settings file. If the settings include more than one allowed host, a plus sign and number indicate the number of additional allowed hosts. **Tip:** To view the additional allowed hosts, click **EDIT**.
SPA Option	Indicates how SPA support is configured in the settings.
Traffic Monitor	Indicates whether the Traffic Monitor is enabled in the settings. Possible values are **Enabled** and **Disabled**.
Submit for Triage	Indicates whether a scan run from these settings is uploaded to Fortify Software Security Center upon completion. Possible values are **Yes** and **No**.
SETTINGS IDENTIFIER	Indicates the settings identifier GUID that was assigned to the settings.

Understanding the Settings Logs Tab

ScanCentral DAST records event logs that are displayed in the **LOGS** tab of the detail panel. The event logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scan settings.

Managing Scan Settings

You can configure new scan settings, edit existing settings, download settings, and delete settings from the Settings List view.

Creating New Settings

You can access the Settings Configuration wizard from the Settings List view and create new settings.

To create new settings:

- Click **+ NEW SETTINGS**.
  The Settings Configuration wizard opens.

Editing Settings

You can access the Settings Configuration wizard from the settings detail panel and edit settings.

To edit settings:

1. In the **Settings List** view, select the settings to edit.
   The settings detail panel appears.
2. In the settings detail panel, click **EDIT**.
   The Settings Configuration wizard opens pre-populated with the selected scan settings.

Downloading Settings

You can download settings from the ScanCentral DAST database to your local machine.

Note: The download option may not be immediately available for newly created settings. The Settings Configuration wizard uses the Fortify WebInspect API to create the settings file. In some environments and situations, it might take several seconds to several minutes for the API to complete the process.

To download settings:

- Click the download icon ( ).
  By default, the file is downloaded to the folder on your local machine that is specified in your browser settings for downloads.

  Caution! Fortify WebInspect supports only Standard scan settings that are downloaded from ScanCentral DAST. Other types of scan settings may cause undesirable results in Fortify WebInspect.

Deleting Settings

To delete settings:

1. Do one of the following:
   - Select one or more check boxes for settings in the **Settings List** view, and then click **DELETE** at the bottom of the table.
   - Select the settings in the **Settings List** view to view the details, and then click **DELETE** at the bottom of the settings detail panel.

If the settings have dependencies, such as scheduled scans, a DELETE ERROR dialog box opens. In this case, you must resolve the dependencies before you can delete the settings.

2. To aid in resolving dependencies, in the **DELETE ERROR** dialog box, click **Copy list of dependencies**.

   A JSON string of the error summary is copied to the clipboard.

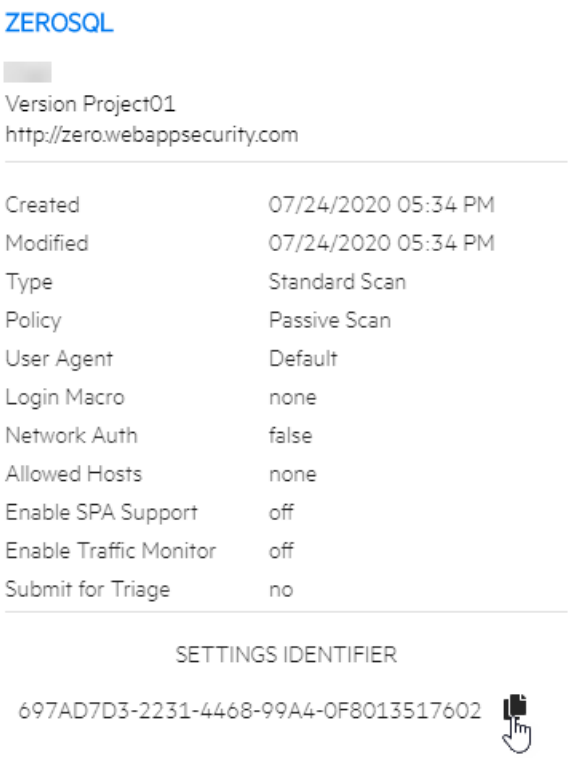
Copying the Settings ID for Use in the API

You can copy the settings identifier and use it to conduct a scan by way of the Fortify Software Security Center API.

To copy the settings identifier:

1. In the **Settings List** view, select the settings to copy.

   The settings detail panel appears.
2. In the settings detail panel, click the copy icon as shown below.



The scan settings identifier is copied to the clipboard.

Chapter 8: Working with Scan Schedules

You can view all of the scan schedules that are available in the ScanCentral DAST database in the Scan Schedules view. You can also configure a new scan schedule, edit an existing schedule, enable or disable schedules, and delete schedules. You can view whether a schedule is enabled, as well as other details, in the schedule detail panel. From the schedule detail panel, you can also enable or disable schedules.

Accessing DAST Scan Schedules in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST scan schedules directly in Fortify Software Security Center.

To access DAST scan schedules in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Scan Schedules**.
   The Scan Schedules view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Scan Schedules View

The Scan Schedules view displays in a table the scan schedules that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each schedule.

Column	Description
Application	Indicates the application for the scheduled scan.
Version	Indicates the version for the scheduled scan.
Name	Indicates the name of the schedule as assigned in the SETTINGS CONFIGURATION wizard.
Scan Settings	Indicates the name of the settings file that is used to conduct the scan.
Recurrence Type	Indicates how often the scheduled scan is run: **Daily**, **Weekly**, **Monthly**, or **Yearly**.
Last Occurrence	Indicates the last date and time that the scheduled scan ran.
Next Occurrence	Indicates the next date and time that the scheduled scan will be run.
Schedule Enabled	Indicates whether the schedule is enabled. Possible values are **Enabled** and **Disabled**.

Understanding the Schedule Detail Panel

When you click a scan schedule in the Scan Schedules view, the schedule detail panel appears to the right. The detail panel displays the same information that is displayed in the Scan Schedules view for the selected schedule, as well as the information described in the following table.

Item	Description
Start Date	Indicates the initial date and time that the schedule ran a scan.
End Date	Indicates the last date and time that the schedule will run a scan, based on the number of occurrences or actual date that was configured in the Settings Configuration wizard.

Understanding the Schedule Logs Tab

ScanCentral DAST records event logs that are displayed in the **LOGS** tab of the detail panel. The event logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scan schedules.

Managing Schedules

You can configure a new scan schedule, edit an existing schedule, enable or disable schedules, and delete schedules from the Scan Schedules view.

Creating a New Schedule

You can configure a new schedule from an existing template saved in Fortify Software Security Center or in a file.

To configure a new schedule:

1. On the **Scan Schedules** view, click **+ NEW SCHEDULE**.
   The SCAN SCHEDULE wizard opens.
2. In the **APPLICATIONS** area, select an application from the application **Name** list.

   Tip: To search for an application, type the application name in the **Application** box, and then click the search icon ( ).

   The APPLICATION VERSIONS area appears.
3. In the **APPLICATION VERSIONS** area, select a version from the application version **Name** list.

   Tip: To search for an application version, type the application version name in the **Application version** box, and then click the search icon ( ).

   The GETTING STARTED area appears with a START list that provides options for creating new settings or editing existing settings. A RECENT list also appears, displaying recently-opened scan settings for the specified application and version.
4. Do one of the following:
   - To use a template from Fortify Software Security Center, select **Open from SSC** in the **START** list, and then click **NEXT**.
   - To use a template saved to a file, select **Open file** in the **START** list, and then click **NEXT**.
   - To use a recently opened template, select a template under **RECENT**.

   The SCAN SCHEDULE dialog box opens.
5. Type a name for the scheduled scan in the **Name** box.
6. Enter a date for the scan to run in the **Start Date** box.

   Tip: To select a date from the calendar, click the calendar icon ( ).
7. Enter a time for the scan to start in the **Start Time** box.

   Note: The schedule uses the time zone from your browser.

8. To schedule a recurring scan, in the **Pattern** section specify how often to run the scan according to the following table.

To run...	Then...
Daily	a. Select **DAILY**. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. b. Select a recurrence in the **Occur every ___ week** box. c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

9. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

   Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.

10. Select a dynamic sensor from the **Sensor** list.

    The list of sensors comes from the Fortify Software Security Center sensor pools. **Any Available** is the default.

11. (Optional) If you select a sensor that is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
12. Click **OK**.

    The scan schedule is added to the ScanCentral DAST database.

Editing a Schedule

To edit a schedule:

1. On the **Scan Schedules** view, select the schedule to edit.

   The schedule detail panel appears.
2. In the settings detail panel, click **EDIT**.

   The SCHEDULE SCAN dialog box opens pre-populated with the selected schedule settings.
3. Follow the procedure for completing the SCAN SCHEDULE dialog box in "Creating a New Schedule" on page 244.

Enabling or Disabling Schedules

You can enable or disable schedules in the schedule detail pane. If a schedule is enabled, the scan runs as scheduled. If it is disabled, no additional scans are run.

To enable or disable a schedule:

1. On the **Scan Schedules** view, select the schedule to enable or disable.

   The schedule detail panel appears.
2. Do one of the following:
   - To enable the schedule, toggle the switch to **Enabled**.
   - To disable the schedule, toggle the switch to **Disabled**.

Deleting a Schedule

To delete a schedule, do one of the following:

- Select one or more check boxes for schedules in the **Scan Schedules** view, and then click **DELETE** at the bottom of the list.
- Select a schedule to view the schedule details, and then click **DELETE** at the bottom of the schedule detail panel.

Chapter 9: Working with Deny Intervals

A deny interval is a block of time during which scans are not permitted. ScanCentral DAST will not prevent you from scheduling a scan or attempting to start a scan manually during a blackout period. It will, however, place the job in the pending job queue and will start the scan when the deny interval ends.

Similarly, if a scan is running when a deny interval begins, the ScanCentral DAST will do one of the following:

- Pause the scan and finish it when the deny interval ends
- Force the scan to complete

Deny Intervals Apply to Applications

Deny intervals are applied to one or more applications. However, an application can have only one deny interval. If you create and apply a deny interval to an application with an existing deny interval, the existing deny interval is overwritten with the new one.

Deny Intervals are Global Settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools. For example, all scans that are running when a deny interval starts may be paused or forced to complete, depending on the deny interval settings.

Accessing Deny Intervals in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST deny intervals directly in Fortify Software Security Center.

To access DAST deny intervals in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Deny Intervals**.
   The Deny Intervals view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to deny intervals may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Deny Intervals View

The Deny Intervals view displays in a table the deny intervals that are stored in the ScanCentral DAST database. Deny intervals are applied to applications. If you create a deny interval and apply it to 100 applications, you will have 100 entries in the Deny Intervals view table.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each application that is configured with a deny interval.

Column	Description
Application	Identifies the application to which the deny interval applies.
Recurrence Type	Indicates how often the deny interval occurs: **Daily**, **Weekly**, **Monthly**, or **Yearly**. Sorting by the Recurrence Type column is not alphabetical. This column sorts by the length of the deny interval—either shortest to longest interval or longest to shortest interval.
Last Occurrence	Indicates the last date and time that the deny interval occurred.
Next Occurrence	Indicates the next date and time that the deny interval will occur.
Modified	Indicates the date and time that the deny interval was created, or if edited, the last date and time that the deny interval was changed.

Understanding the Deny Intervals Detail Panel

When you select an entry in the Deny Intervals view, the deny interval detail panel appears. The detail panel displays the information from the deny intervals list table for the selected deny interval.

The detail panel also provides options to edit and delete the selected deny interval.

Creating a Deny Interval

When you create a ScanCentral DAST deny interval, you must assign it to one or more applications. You create the deny interval and assign applications to it in the DENY INTERVAL wizard.

To create a deny interval:

1. On the **Deny Intervals** view, click **+ NEW DENY INTERVAL**.
   The DENY INTERVAL wizard opens.
2. On the **General** page, continue according to the following table.

To configure a...	Then...
Recurring deny interval **Note:** The **Recurring** option is selected by default.	a. Enter a date and time for the deny interval to start in the **Start Date** and **Start Time** boxes. b. In the **Duration** area, specify a duration in the **Days**, **Hours**, and **Minutes** boxes. **Tip:** To calculate the duration, click **CALCULATE DURATION**, enter a date and time for the deny interval to end in the **End Date** and **End Time** boxes, and then click **OK**. The duration is automatically calculated and added to the **Days**, **Hours**, and **Minutes** boxes.
Non-recurring deny interval	a. Clear the **Recurring** option. b. Enter a date and time for the deny interval to start in the **Start Date** and **Start Time** boxes. c. Enter a date and time for the deny interval to end in the **End Date** and **End Time** boxes. **Tip:** To select a date from the calendar, click the calendar icon ().

3. In the **Scan action** area, select an action. Options are:
   - **Pause scan** – the running scan is paused until the deny interval has ended.
   - **Force complete scan** – the running scan is forced to complete. If the **Submit for triage** option was selected in the scan settings, the scan results will be published to Fortify Software Security Center when the action is completed.
4. Click **NEXT**.

The Recurrence page appears. If you did not select the Recurring option on the General page, you cannot configure settings on the Recurrence page. Go to step 7.

5. To schedule a recurring deny interval, in the **Pattern** section specify how often to apply the deny interval according to the following table.

To apply...	Then...
Daily	a. Select **DAILY**. **Note:** If you selected a Duration longer than 24 hours from the Start Date and Start Time on the General page, then the Daily option is not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. **Note:** If you selected a Duration longer than a week from the Start Date and Start Time on the General page, then the Daily and Weekly options are not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ week** box. c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. **Note:** If you selected a Duration longer than a month from the Start Date and Start Time on the General page, then the Daily, Weekly, and Monthly options are not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**. **Note:** If you selected a Duration longer than a year from the Start Date and Start Time on the General page, then the Yearly option is visible on the Recurrence page. However, you cannot configure a duration that is

To apply...	Then...
	longer than the recurrence interval. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

6. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

     Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.
7. Click **NEXT**.

   The Application Select page appears, listing all available applications.
8. In the **APPLICATIONS** list, select one or more applications to which you want the deny interval to apply.

   The selected applications are added to the APPLICATIONS SELECTED area.
9. Click **NEXT**.

   The Review page appears.
10. Click **SAVE**.

    The deny interval is added to the ScanCentral DAST database for the applications selected.

Managing Deny Intervals

You can edit and delete deny intervals, and refresh the Deny Intervals view.

Facts About Editing a Deny Interval

Because each entry in the Deny Interval view is for a specific application, be aware of the following facts when editing a deny interval:

- When you select a deny interval from the Deny Interval view to edit, by default the changes apply only to the selected application. You can, however, apply changes to other applications while editing.
- Applications can have only one deny interval. When you edit a deny interval and apply it to an application, it replaces any existing deny interval already applied to that application.
- If you edit the start date and start time of an existing deny interval so that the current time is included in the deny interval, any scan that is currently running for the specified application will be paused or forced to complete.

Editing a Deny Interval

To edit a deny interval:

1. In the **Deny Interval** view, select the deny interval to edit.

   The deny interval detail panel appears.
2. Click **EDIT**.

   The DENY INTERVAL wizard opens with the deny interval settings visible for the selected application.

   Important! You are editing the settings for the selected application only. To apply your changes to multiple applications, you must select them in the **APPLICATIONS** list in the DENY INTERVAL wizard.
3. To make edits, follow the procedure in "Creating a Deny Interval" on page 249.

Deleting a Deny Interval

To delete a deny interval, do one of the following:

- Select one or more check boxes on the **Deny Intervals** view, and then click **DELETE** at the bottom of the table.
- Select a deny interval to view the deny interval details, and then click **DELETE** at the bottom of the deny interval detail panel.

Refreshing the Deny Intervals View

Generally, the changes that you make to deny intervals appear right away on the deny intervals view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Deny Intervals view:

- Click **REFRESH**.

Chapter 10: Working with Policies

You can import into the ScanCentral DAST database policies that have been customized using the Fortify WebInspect Policy Manager tool. Afterward, you can view the custom policies that are available in the ScanCentral DAST database in the Policies view. You can view the policy description, the applications to which the policy is assigned, and other details in the policy detail panel. From the policy detail panel, you can also edit and delete policies.

Accessing Policies in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST policies directly in Fortify Software Security Center.

To access DAST policies in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Policies**.
   The **Policies** view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to policies may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Policies View

The Policies view displays in a table the custom policies that have been imported into Fortify ScanCentral DAST from Fortify WebInspect.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each policy.

Column	Description
Name	Identifies the name of the imported policy.
Modified	Indicates the last date and time that the policy was edited. **Note:** You can only edit the name, description, and the applications to which the policy is assigned.

Understanding the Policy Detail Panel

When you select a policy in the Policies view, the policy detail panel appears. The policy name and description are displayed at the top.

The detail panel displays the same information that is displayed in the Policies view for the selected policy, as well as the information described in the following table.

Item	Description
ASSIGNED APPLICATIONS	Lists the applications to which the policy has been assigned.
Created	Indicates the date and time that the policy was imported into ScanCentral DAST.

Importing a Custom Policy

When you import a custom policy into ScanCentral DAST, you must assign it to one or more applications. You import the policy and assign applications to it in the CUSTOM POLICY wizard.

To import a policy:

1. On the **Policies** view, click **+ CUSTOM POLICY**.
   The CUSTOM POLICY wizard opens.
2. On the **General** page, click **IMPORT**.
3. Using the standard file-selection window, locate the `.policy` file and click **Open**.
   The **File** name, policy **Name**, and **Description** fields in the General page are populated.
4. Edit the **Name** and **Description** fields as needed.
5. Click **NEXT**.
   The Application Select page appears.
6. In the **APPLICATIONS** list, select one or more applications to which you want the policy to apply.

The selected applications are added to the APPLICATIONS SELECTED area.

7. Click **NEXT**.
   The Review page appears.
8. Click **SAVE**.
   The policy is added to the ScanCentral DAST database for the applications selected.

Managing Policies

You can edit and delete policies, and refresh the list on the Policies view.

Editing a Policy

To edit a policy:

1. In the **Policies** view, select the policy to edit.
   The policy detail panel appears.
2. Click **EDIT**.
   The CUSTOM POLICY wizard opens.
3. Edit the **Name** and **Description** fields as needed.
4. Click **NEXT**.
   The Application Select page appears.
5. In the **APPLICATIONS** list, select one or more applications to which you want the policy to apply.
   The selected applications are added to the APPLICATIONS SELECTED area.
6. Click **NEXT**.
   The Review page appears.
7. Click **SAVE**.
   The changes are saved in the ScanCentral DAST database.

Deleting a Policy

To delete a custom policy:

1. Do one of the following:
   - Select one or more check boxes for policies in the **Policies** view, and then click **DELETE** at the bottom of the table.
   - Select a policy to view the policy details, and then click **DELETE** at the bottom of the policy detail panel.

   A confirmation message appears with a prompt to select a replacement policy.

2. In the **Replacement policy** drop-down list, select a replacement policy to be used in all scan settings that contain the policy or policies being deleted.

   Important! If you are deleting multiple policies, then the replacement policy you choose will be used for all deleted policies.

Refreshing the Policies View

Generally, the changes that you make to policies appear right away on the Policies view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Policies view:

- Click **REFRESH**.

Chapter 11: Working with Base Settings

If you have Admin Role privileges in Fortify Software Security Center, you can create and edit base settings and apply them to applications. All users who have access to the selected applications can use these base settings as templates to create new settings or conduct a scan.

Differences Between Base Settings and Templates

A template from Fortify Software Security Center:

- Is a complete set of settings with all fields containing data
- Applies to one application and version

Base settings may:

- Be an incomplete set of settings with some fields missing data
- Apply to multiple applications and versions

Base Settings are Global Settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools. For example, base settings may apply to multiple applications and versions.

Accessing Base Settings in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST base settings directly in Fortify Software Security Center.

To access DAST base settings in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Base Settings**.
   The Base Settings view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to base settings

may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Restricting or Allowing Edits

If you have permissions to manage restricted scan settings, then you can restrict the editing of base settings. If a setting is already restricted, you can allow editing.

To restrict editing:

- Click the restrict *<setting name>* icon ( ).

To allow editing:

- Click the allow *<setting name>* icon ( ).

If you do not have permissions to manage restricted scan settings, then you cannot edit any base settings with the restricted icon ( ).

For more information, see "Permissions in Fortify Software Security Center" on page 40.

Using Key Stores in Base Settings

To learn about using key store placeholders in base settings, see "Using Key Stores in Settings" on page 141.

Using Artifacts from a Repository in Base Settings

To learn about using artifacts from repositories in scan settings, see "Using Artifacts from a Repository in Settings" on page 143.

Understanding the Base Settings View

The Base Settings view displays in a table the base settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each base settings file.

Column	Description
Name	Indicates the name of the base settings file.
Scan Type	Indicates the type of scan to be conducted using the base settings. Types are:

Column	Description
	• **Standard Scan** • **Workflow-driven Scan** • **API Scan**
Modified	Indicates the date and time that the settings were created, or if edited, the last date and time that the settings were changed.

Understanding the Base Settings Detail Panel

When you click settings in the Base Settings view, the base settings detail panel appears to the right. The assigned applications that are configured in the base settings are listed at the top of the panel.

The detail panel displays the same information that is displayed in the Base Settings view for the selected settings, as well as the information described in the following table.

Item	Description
Created	Indicates the date and time that the settings were saved.
Policy	Identifies the dynamic policy to be used to conduct the scan.
User Agent	Indicates the user agent one or more of the following: • **Chrome** • **Chrome (Mobile Android)** • **Custom** • **Default** • **Edge** • **Safari** • **Safari (Mobile IOS)** **Note:** Default uses the user agent that is defined in Fortify WebInspect.
Login Macro	If applicable, indicates the file name of the login macro specified in the settings.
Has Network Auth	Indicates whether network authentication is specified in the settings. Possible values are **Yes** and **No**.

Item	Description
Allowed Hosts	If applicable, indicates the number of allowed hosts configured in the settings.
SPA Option	Indicates how SPA support is configured in the settings.
Traffic Monitor	Indicates whether Traffic Monitor is enabled in the settings. Possible values are **Enabled** and **Disabled**.
Submit for Triage	Indicates whether a scan run from these settings is uploaded to Fortify Software Security Center upon completion. Possible values are **Yes** and **No**.

Creating Base Settings

You create base settings in the Base Settings configuration wizard. To access this wizard from the ScanCentral DAST Base Settings view:

- Click **+ BASE SETTINGS**.

  The Base Settings configuration wizard opens to the Target page.

What's Next?

Do one of the following:

- To configure base settings for a standard scan, proceed with "Configuring Base Settings for a Standard Scan" below.
- To configure base settings for a workflow-driven scan, proceed with "Configuring Base Settings for a Workflow-driven Scan" on page 263.
- To configure base settings for an API scan, proceed with "Configuring Base Settings for an API Scan" on page 265.

Configuring Base Settings for a Standard Scan

A standard scan performs an automated analysis, beginning from the start URL.

To configure base settings for a standard scan:

1. On the Target page, click **STANDARD SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).

- **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.

3. Type the complete URL or IP address in the **Url** field.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, the sensor will not scan WWW.MYCOMPANY.COM or any other variation unless you specify alternatives in the **Allowed Hosts** setting. For more information, see "Adding and Managing Allowed Hosts in Base Settings" on page 285.

   An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

   Important! If the URL resolves to an IP address that is not in the valid range for scanning, then a warning appears. If you start the scan with an IP address that is not in the valid range, then the scan will stop and a reason will be provided.

   Scans by IP address will not follow links that use fully qualified URLs (as opposed to relative paths).

   Note: The sensor supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). You must enclose IPV6 addresses in brackets.

4. (Optional) To limit the scope of the scan to a specified area, select **Restrict to folder**, and from the list, select one of the following options:
   - **Directory only** – The sensor crawls and/or audits only the URL that you specify. For example, if you select this option and specify the URL www.mycompany/one/two/, the sensor will assess only the "two" directory.
   - **Directory and subdirectories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is higher in the directory tree.
   - **Directory and parent directories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is lower in the directory tree.
5. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

   Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in

the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.

   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's Next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring Proxy Settings in Base Settings" on page 271.
- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring Authentication in Base Settings for Standard and Workflow-driven Scans" on page 273.

Configuring Base Settings for a Workflow-driven Scan

A workflow-driven scan audits only those URLs included in a macro that you previously recorded. It does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, all of them will be included in the same scan.

Types of Macros Supported

You can use `.webmacro` files, HTTP archive (`.har`) files, or Burp Proxy captures.

Important! If you use a login macro in conjunction with a workflow macro or startup macro or both, all macros must be of the same type: all `.webmacro` files, all `.har` files, or all Burp Proxy captures. You cannot use different types of macros in the same scan. Likewise, `.webmacro` login and workflow files must have been created using the same version of Web Macro Recorder. You cannot use a login file that was recorded in the Event-based Web Macro Recorder and a workflow file that was recorded in the Session-based Web Macro Recorder.

Configuring Base Settings for a Workflow-driven Scan

To configure base settings for a workflow-driven scan:

1. On the Target page, click **WORKFLOW-DRIVEN SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.
3. Continue according to the following table.

To...	Then...
Add a macro to the scan settings	a. Click **MANAGE**. b. Type a name for the macro in the **Name** field. c. Click **IMPORT** and browse to locate the workflow to add to the scan settings. d. Click **OK**. e. Repeat steps a through d to add another macro to the scan settings.
Remove a macro from the list of macros	a. Select the macro in the macro list. b. Click **REMOVE**.

Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

You can use a key store placeholder for any field that displays the **Open key store** icon (🔑). For more information, see "Using Key Stores in Settings" on page 141.

4. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

5. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.
6. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.
   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (<system and browser information>) <platform> (<platform details>) <extensions>

What's Next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring Proxy Settings in Base Settings" on page 271.
- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring Authentication in Base Settings for Standard and Workflow-driven Scans" on page 273.

Configuring Base Settings for an API Scan

For Open API, OData, and Postman scans, the WebInspect sensor creates a macro from the REST API definition, and then performs an automated analysis. For GraphQL, gRPC, and SOAP scans, a more traditional scanning method is used.

Important! The DAST Utility Service container must be up and running to configure and run a Postman scan. Also, if the Postman scan requires a proxy, you must configure the proxy settings before you validate the Postman collection file(s). For more information, see "Configuring Proxy Settings" on page 157.

To configure base settings for an API scan:

1. On the **Target** page, click **API SCAN**.
2. In the **Type** list, select the API type to be scanned. The options are:
   - **GraphQL**
   - **GRPC**
   - **OData**
   - **Open API** (also known as Swagger)
   - **Postman**
   - **SOAP**

   Important! If you are configuring a Postman scan while using a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service, you must install prerequisite software on the sensor machine. For more information about this and other aspects of using Postman collection files, including configuring dynamic authentication using dynamic tokens, see "Scanning with a Postman Collection" on page 356.
3. Continue according to the following table.

For this API type...	Do this...

GraphQL
GRPC
OData
Open API
	To use a file:
	a. In the **Definition** list, select **File**.
	b. Click **IMPORT** and import the definition file.
	Tip: Alternatively, you can paste in the full path to a definition file that is saved on your local machine.
	Important! Open API definition files must specify the host, scheme, and service path. Otherwise, undesirable results may occur.
	To use a URL:
	a. In the **Definition** list, select **URL**.
	b. Provide the URL to the API definition file, as shown in the following examples:
	`http://172.16.81.36/v1`
	`http://myapi/protos/client.proto`
	`http://myapi/graphql/`
	c. If HTTP authorization credentials are needed to access the API

For this API type...	Do this...
	definition, enter them in the **Authentication Header** box, as shown in the following example: `Basic YWxhZGRpbjpvcGVuc2VzYW1l` **Important!** This authentication header is used only for accessing the API definition. It is not carried forward to the Authentication page of the Settings Configuration wizard. You must configure network authentication for the scan on the Authentication page. d. Click **VALIDATE** to verify that the DAST API can access the definition file and ensure that it is valid.
Postman	a. Do one of the following: ◦ To import a workflow collection, select **IMPORT** and then import the Postman collection file. ◦ To import an authentication collection, select **Authentication** from the **IMPORT** drop-down list, and then import the Postman collection file. ◦ To import an environment file, select **Environment** from the **IMPORT** drop-down list, and then import the Postman environment file. The file is added to the list of collection files. Repeat this Step to import additional files. **Important!** You can import only one authentication collection and one environment file. b. Click **VALIDATE** to validate the collection file(s). **Note:** At least one workflow collection must be imported before you can validate the files. The **VALIDATE** button is not available if only authentication and environment collections have been imported. Upon successful validation, the POSTMAN VALIDATION dialog box opens, displaying a list of sessions contained in the collection file(s). If authentication sessions are identified, they are preselected as **Auth**

For this API type...	Do this...
	sessions. All other sessions are preselected as **Audit** sessions. Additionally, the Postman Authentication Results area displays the type of authentication detected as **None**, **Static**, or **Dynamic**. **Note: Auth** sessions will be used for authentication for the scan. **Audit** sessions will be audited in the scan. c. (Optional) Select the **Auth** or **Audit** check box for a session to change its type as needed. d. (Optional) Make changes to the **Postman Authentication Results** as follows: ◦ For **Static** authentication, enter a token in the **Custom Header Token** box. ◦ For **Dynamic** authentication, do the following: • Select the **Regex (Custom)** option to the right of the **Response Token Name** box, and then enter a custom regular expression in the **Response Token Name** box. • Select the **Regex (Custom)** option to the right of the **Request Token Name** box, and then enter a custom regular expression in the **Request Token Name** box. • Clear the **Use Auto Detect** option to the right of the **Logout Condition** box, and then enter a new logout condition string in the **Logout Condition** box. e. Did you make changes to the Postman Authentication Results? ◦ If yes, click **VALIDATE** to validate the new authentication settings, and then click **OK**. **Note:** Clicking **VALIDATE** regenerates all sessions for the postman collection. It does not retain any previous changes to **Auth** or **Audit** sessions even if the collection and sessions are the same. ◦ If no, click **OK**. **Note:** After validation, an **EDIT** button is available. This button opens the POSTMAN VALIDATION dialog box for editing the sessions

For this API type...	Do this...
	contained in the collection file(s) as described previously in this procedure.

SOAP	To use a file:
	a. In the **Definition** list, select **File**.
	b. Click **IMPORT** and import the definition file.
	Tip: Alternatively, you can paste in the full path to a definition file that is saved on your local machine.
	c. In the **Version** list, select a version to allow filtering of operations by the specific version. Options are as follows:
	◦ **Legacy** – filters against the lowest supported version.
	◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available.
	◦ **Newest** – the default setting, filters against the latest version.
	To use a URL:
	a. In the **Definition** list, select **URL**.
	b. Provide the URL to the API definition file, as shown in the following example:
	`http://172.16.81.36/web-services/infoService?wsdl`
	c. In the **Version** list, select a version to allow filtering of operations by the specific version. Options are as follows:
	◦ **Legacy** – filters against the lowest supported version.
	◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available.
	◦ **Newest** – the default setting, filters against the latest version.
	d. If HTTP authorization credentials are needed to access the API definition, enter them in the **Authentication Header** box, as shown in the following example:
	`Basic YWxhZGRpbjpvcGVuc2VzYW1l`
	Important! This authentication header is used only for accessing the API definition. It is not carried forward to the Authentication

For this API type...	Do this...
	page of the Settings Configuration wizard. You must configure network authentication for the scan on the Authentication page. e. Click **VALIDATE** to verify that the DAST API can access the definition file and ensure that it is valid.

4. If you imported a definition file, the **API location is different from API definition location** option is selected. Specify the following:
   a. In the **API Scheme Type** list, select a type. Options are **HTTP**, **HTTPS**, and **HTTP/HTTPS**.
   b. In the **API Host** box, type the URL or hostname.
   c. In the **API Service Path** box, type the directory path for the API service.

Note: The GraphQL service location is always the same as the definition location. For SOAP, if the query string "?wsdl" value is removed, then the SOAP service location may or may not be the same as the definition location. The gRPC service location is always different from the definition location.

Note: If the service path is not defined for an Open API scan, then the sensor will use the basePath that is defined in the Open API definition contents. For Open API scans, select **API location is different from API definition location** unless your service is explicitly run at the same location as the docs folder for Open API. Optionally, you may choose to define a service path if it differs from the basePath.

5. (Optional) To submit the completed scan for triage in Fortify Software Security Center, select **Submit for triage**.

Note: Submitting for triage allows you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, do one of the following:
   - Select a policy from the **Policy** list.
   - Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 363. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

Tip: The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. However, you can choose another policy if needed.

7. Do one of the following:
   - To use a standard user agent, select it from the **User Agent** list.

     Note: Default uses the user agent that is defined in Fortify WebInspect.

   - To use a custom user agent, select **Custom** from the **User Agent** list, and then type the user-agent string in the **Custom User Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (<system and browser information>) <platform> (<platform details>) <extensions>

What's Next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring Proxy Settings in Base Settings" below.
- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring Authentication in Base Settings for API Scans" on page 275.

Configuring Proxy Settings in Base Settings

To configure proxy settings in the base settings:

1. On the Target page, click **PROXY SETTINGS**.
   The PROXY CONFIGURATION dialog box opens.
2. Select the **Use Proxy Server** option.
   The settings become available for you to configure.
3. Configure the settings according to the following table.

To...	Then...
Use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the web proxy settings	Select **Auto detect proxy settings**.
Import your proxy server information from Firefox	Select **Use Firefox proxy settings**. **Note:** Using browser proxy settings does not guarantee that you can access the

To...	Then...
	Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.
Load proxy settings from a Proxy Automatic Configuration (PAC) file	a. Select **Configure proxy settings using a PAC file**. b. In the **URL** box, type the URL location for the PAC file.
Access the Internet through a proxy server	a. Select **Explicitly configure proxy** settings. b. In the **Server** box, enter the URL or IP address of your proxy server. c. In the **Port** box, enter the port number (for example, 8080). d. From the **Type** list, select the protocol type for handling TCP traffic through the proxy server. The options are: **Standard**, **SOCKS4**, or **SOCKS5**. e. If authentication is required, select a type from the **Authentication** list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, or **Negotiate**. f. If your proxy server requires authentication, enter the qualifying user name in the **User Name** field and the qualifying password in the **Password** field. g. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass** field. Use semicolons to separate entries.

4. Click **OK**.
   The proxy settings are saved and the PROXY CONFIGURATION dialog box closes.

What's Next?

To configure authentication for the scan, click **NEXT** and proceed with "Configuring Authentication in Base Settings for Standard and Workflow-driven Scans" below or "Configuring Authentication in Base Settings for API Scans" on page 275.

Configuring Authentication in Base Settings for Standard and Workflow-driven Scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Configuring Site Authentication

You can use a recorded login macro containing one or more usernames and passwords that allow you to log in to the target site. The macro must also contain a "logout condition," which indicates when an inadvertent logout has occurred so that the sensor can rerun the macro to log in again.

To configure site authentication:

1. Select **Site Authentication**.
2. Do one of the following:
   - To import an existing login macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays the **Open key store** icon ( ). For more information, see "Using Key Stores in Settings" on page 141.
   - To record a login macro, click **Open Macro Recorder 23.1**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 23.1 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder Tool" below.

Downloading the Macro Recorder Tool

You can download the Event-based Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Windows-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, click **Download Macro Recorder 23.1**.

  The `MacroRecorder64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

  Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.

Using a Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

To use a client certificate:

1. Select **Use Client Certificate**.
2. Click **IMPORT**.

   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.

   The certificate file is added to the Client certificate box.
4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

   Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring Network Authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Network Authentication**.
2. Select an **Authentication Type**. Options are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Digest**

- **Kerberos**
- **NT LAN Manager (NTLM)**

3. Type the authentication username in the **Username** box.
4. Type the authentication password in the **Password** box.

Caution! The sensor crawls all servers granted access by this password (if the sites/servers are included in the Allowed Hosts setting). To avoid potential damage to your administrative systems, do not use credentials that have administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional.

What's Next?

To configure details for the scan, click **NEXT** and proceed with "Configuring Base Settings Details" on page 280.

Configuring Authentication in Base Settings for API Scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Options for configuring authentication include the following:

- "Using a Client Certificate" below
- "Configuring Network Authentication" on the next page
- "Using Custom Headers" on page 278
- "Configuring SOAP Settings" on page 279

Using a Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

Note: Client certificates do not apply to OData or Open API definition types.

To use a client certificate:

1. Select **Use API Client Certificate**.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.
   The certificate file is added to the Client certificate box.

4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring Network Authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Use API Network Authentication**.
2. Select an **Authentication Type**. The API Type determines the available authentication types. The complete list of authentication types is:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Bearer**
   - **Custom**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
3. Continue according to the following table.

For this authentication type...	Do this...
ADFS CBT **Automatic** **Basic** **Digest** **Kerberos** **NTLM**	a. Type the authentication username in the **Username** box. b. Type the authentication password in the **Password** box.

For this authentication type...	Do this...
Bearer	Optionally, type the JSON token, generally from a response to a login form, in the **Token Value** box. When using Bearer, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a Token Value" below.
Custom	a. Type the token name in the **Scheme** box. b. Optionally, type the token value in the **Parameter** box. When using Custom, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a Token Value" below.

Fetching a Token Value

You can use a custom regular expression to fetch the token value from a login or workflow macro. If a match to the regular expression occurs in the response, then the value is fetched and used as a bearer token. If the regular expression contains parentheses, then the value inside the parentheses will be extracted and used as a bearer token. Only the first value inside parentheses will be used.

Note: Fetching a token value does not apply to OData or Open API definition types.

To fetch a token value:

1. Select **Use Fetch Token**.
2. Do one of the following:
   - To import an existing macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays the **Open key store** icon ( ). For more information, see "Using Key Stores in Settings" on page 141.
   - To record a macro, click **Open Macro Recorder 23.1**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 23.1 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder Tool" on the next page.

3. Type a regular expression for pattern matching in the **Search Pattern** box.
4. Do one of the following:
   - To have each scan thread run its own fetch macro playback and apply the bearer token value to the thread, select the **Isolate state** check box.
   - To have only one fetch macro playback run for all scan threads and the single shared bearer token value apply to all threads, clear the **Isolate state** check box.

Downloading the Macro Recorder Tool

You can download the Event-based Web Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Windows-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, click **Download Macro Recorder 23.1**.

  The `MacroRecorder64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

  Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.

Using Custom Headers

You can configure multiple custom headers.

Important! Fortify recommends that you do not configure more than one custom header using the same HTTP header name.

To add a custom header:

1. Select **Use Custom Headers**.
2. Click the add icon (+).
3. In the **header name** box, type the custom HTTP header name. For example, `X-MyCustomAuth`.

   Important! The header must be unique and cannot be `Authorization`.
4. In the **header scheme** box, type the header value prefix name. For example, `CustomToken`.
5. In the **header value** box, type the custom header value.
6. Click the check icon (✔).
   The custom header is added to the list.

To edit a custom header:

- Click the edit icon ( ) for the custom header you want to edit.

To remove a custom header:

- Click the delete icon ( ) for the custom header you want to delete.

Configuring SOAP Settings

You can configure message-based authentication for SOAP scans.

To configure SOAP authentication settings:

1. Select **Use SOAP Configuration**.
2. Select that authentication method to use from the **SOAP Method** list. Options are **Username Token** and **Certificate Pair**.
3. Continue according to the following table.

For this authentication method...	Do this...
Username Token	a. In the **Username** box, type the user name whose credentials are used to access the SOAP service. b. In the **Password** box, type the password for the user name. c. In the **Username Token Type** list, select the type of token. Options are **Text** and **Hash**. d. In the **Timestamp** list, select an option for when the Username Token was created and when it expires. Options are **Created**, **Full**, and **None**. e. If nonce is enabled for the token, select **Includes nonce**. **Important!** Nonce is required for hash tokens because it helps the server to recalculate the hash and compare it to the data the client sent.
Certificate Pair	a. Click **IMPORT** to the right of the **Client Certificate** box. A standard Windows file selection dialog box opens. b. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Client Certificate box. c. In the **Client Certificate Password** box, type the password. d. Click **IMPORT** to the right of the **Server Certificate** box.

For this authentication method...	Do this...
	A standard Windows file selection dialog box opens. e. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Server Certificate box. f. If the server certificate requires a password, select **Requires password** and type the password in the **Server Certificate Password** box.

4. Optionally, to identify the Web Services Addressing (WS-Addressing) schema version used by the SOAP service, select **Use WS Addressing** and continue as follows:
   a. In the **Schema Version** list, select the version. Options are **NONE**, **WSA0408**, and **WSA0508**.
   b. In the **WSA: To** box, enter the URL override for the Web service host.

   Note: SOAP services may be exposed by way of a load balancer or reverse proxy. This configuration may prevent the sensor from getting the correct information for the internal Web service host name. The "WSA: To" URL override provides the correct address into WS Addressing.

   The URL override uses the following format:

   `https://<host_name><service_path>/<port_name>`

What's Next?

To configure details for the scan, click **NEXT** and proceed with "Configuring Base Settings Details" below.

Configuring Base Settings Details

You can configure the following settings on the Base Settings Details page:

- Content and filters (API scans only. For more information, see "Configuring API Content and Filters in Base Settings" on the next page.)
- Allowed hosts (For more information, see "Adding and Managing Allowed Hosts in Base Settings" on page 285.)
- Scan priority (For more information, see "Configuring Scan Priority in Base Settings" on page 286.)
- Data retention (For more information, see "Configuring Data Retention in Base Settings" on page 287.)
- Single-page application (SPA) support (Standard and Workflow-driven scans only. For more information, see "Scanning Single-page Applications in Base Settings" on page 287.)

- Traffic Monitor (For more information, see "Enabling Traffic Monitor in Base Settings" on page 288.)
- Exclusions (For more information, see "Creating and Managing Exclusions in Base Settings" on page 288.)
- Redundant page detection (Standard and Workflow-driven scans only. For more information, see "Configuring Redundant Page Detection in Base Settings" on page 290.)

What's Next?

After you configure the scan details, click **NEXT** and proceed with "Applying Base Settings to Applications" on page 291.

Configuring API Content and Filters in Base Settings

When configuring API scans, you can use the Content and Filters page to configure the preferred content type, as well as operations and parameter names and types to include or exclude during the scan.

Specifying the Preferred Content Type

The preferred content type setting specifies the preferred content type of the request payload. If the preferred content type is in the list of supported content types for an operation, then the generated request payload will be of that type. Otherwise, the first content type listed in an operation will be used. By default, the preferred content type is application/json.

To change the preferred type:

- Type the preferred content type in the **Preferred Content Type** box.

Defining Specific Operations to Include

The Include feature defines an allow list of operation IDs that should be included in the output.

To define a specific operation to include:

1. Select **Specific Operations**.
2. Select **Include**.
3. Click the add icon (+).
4. In the **Operation to add** box, type the operation ID.
5. Click the check icon (✔).
   The operation ID is added to the allow list.

Defining Specific Operations to Exclude

The Exclude feature defines a deny list of operation IDs that should be excluded from the output.

To define a specific operation to exclude:

1. Select **Specific Operations**.
2. Select **Exclude**.
3. Click the add icon (+).
4. In the **Operation to add** box, type the operation ID.
5. Click the check icon (✔).
   The operation ID is added to the deny list.

Editing Specific Operations

To edit a specific operation in the allow or deny list:

1. Do one of the following:
   - To edit an operation in the allow list, select **Include**.
   - To edit an operation in the deny list, select **Exclude**.
2. Click the edit icon (✎) for the operation ID you want to edit.

Removing Specific Operations

To remove a specific operation from the allow or deny list:

1. Do one of the following:
   - To remove an operation from the allow list, select **Include**.
   - To remove an operation from the deny list, select **Exclude**.
2. Click the delete icon (✕) for the operation ID you want to remove.

Defining Parameter Rules

Parameter rules define a default value to use for a parameter when the parameter name and type are encountered. You can also specify operations to determine whether a specific parameter rule should or should not apply to those operations.

Important! If you configure a parameter rule and then change the API definition type for which the parameter rule type becomes invalid, the invalid parameter rule type will be changed to **Any**. The invalid parameter rule will be highlighted in the Parameter Rules list, and a warning message will be displayed below the list.

To add a parameter rule:

1. Select **Parameter Rules**.
2. Click **Add**.
   The PARAMETER RULE dialog box appears.
3. In the **Parameter Rule Name** box, type a name for the rule.

4. In the **Parameter Rule Type** list, select a type. Available options depend on the API type and may include the following:
   - **Any**
   - **Boolean**
   - **Date**
   - **File**
   - **Guid**
   - **Number**
   - **String**

   For more information on the Parameter Rule Types and their equivalents based on API type, see "Understanding Parameter Type Matches" on page 171.
5. Continue according to the following table:

For this Rule Type...	Do this...
Any	In the **Value** box, type any value.
Boolean	In the **Boolean Value** list, select **true** or **false**.
Date	To enter any string value as the date: • Type the string in the **Date** box. **Note:** You may enter a duration, time span, formatted date, or formatted time in the **Date** box. To select a date/time format and use a calendar and clock to generate a formatted string: a. Click **GENERATE DATE**. The GENERATE DATE STRING dialog box opens. b. From the **Date Type** list, select a format. Options are **Date and time**, **Date**, and **Time**. c. In the **Date** box, enter a date using the preferred format defined in your Fortify Software Security Center. **Tip:** To select a date from the calendar, click the calendar icon ( ). d. In the **Time** box, enter a time using the preferred format

For this Rule Type...	Do this...
	defined in your Fortify Software Security Center. **Tip:** To select a date from the calendar, click the clock icon ( ). e. Click **OK**.
File	a. Click **IMPORT** and browse to locate the file to add to the scan settings. b. Click **Open**.
Guid	In the **Value** box, enter a GUID.
Number	In the **Number Value** box, enter a numerical value.
String	In the **Value** box, type any value.

6. For Open API scans, in the **Parameter Rule Location** list, select a location where the parameter is found in the request. Options are:
   - **Any**
   - **Body**
   - **Header**
   - **Path**
   - **Query**
7. Optionally, select **Inject Parameter** to include the defined parameter in the request.

   Important! The **Inject Parameter** option does not work with schema-based APIs, such as SOAP, gRPC, and Postman. Those API types do not accept forced parameters. For GraphQL, **Inject Parameter** only works with the query operation if the property is in the query schema.
8. Optionally, to specify operations to which this parameter rule should or should not apply, select **Specific Operations** and perform steps 2-5 of "Defining Specific Operations to Include" on page 281 or "Defining Specific Operations to Exclude" on page 281.
9. Click **OK**.

   The rule is added to the Parameter Rules list.

Editing a Parameter Rule

To edit a rule in the Parameter Rules list:

- Select the check box for the rule to edit, and then click **EDIT**.

  The PARAMETER RULE dialog box appears. For more information about using this dialog box, see "Defining Parameter Rules" on page 282.

Removing a Parameter Rule

To remove a rule from the Parameter Rules list:

- Select the check box for the rule to remove, and then click **REMOVE**.

Adding and Managing Allowed Hosts in Base Settings

Use the **Allowed Hosts** setting to add and manage domains to crawl and audit. If your Web application uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the scan.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As the sensor scans the target site, if it encounters a link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, the sensor would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Adding Allowed Hosts

To add allowed hosts:

1. Click **MANAGE**.
2. In the SPECIFY ALLOWED HOST dialog box, type a URL in the **Name** box.

   Important! When you specify the URL, do not include the protocol designator (such as http:// or https://).

3. (Optional) To use a regular expression to represent a URL, select **Use Regular Expression**.

4. Do one of the following:
   - To save the allowed host to the list, click the check mark icon (✔).
     The URL is added to the allowed hosts list. To add another allowed host, return to Step 2.
   - To clear the fields and start over, click the retry icon (↻) and return to Step 2.
5. When the list of allowed hosts is complete, click **OK**.

Editing or Removing Hosts

To edit or remove an allowed host:

1. Select a host from the **Allowed Hosts** list.
2. Do one of the following:
   - To edit the host name or regular expression, click **MANAGE**.
     The SPECIFY ALLOWED HOST dialog box opens. For more information about using this dialog box, see "Adding Allowed Hosts" on the previous page.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Configuring Scan Priority in Base Settings

Scans are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Before starting a scan, the Global Service determines if there is a higher-priority scan that needs to be started. If there is, the lower-priority scan will remain in the queue. Additionally, a lower-priority scan that is running will be paused for a higher-priority scan if no other sensor is available.

If Advanced Scan Prioritization is enabled, the Global Service may move scans to other sensors, depending on scan priority and other settings. For more information about Advanced Scan Prioritization, see "Understanding Advanced Scan Prioritization" on page 174.

Note: Applications are configured with a default priority level in the application settings. For more information, see "Understanding the Application Settings View" on page 296.

Changing the Priority

To select a priority other than the default setting for the scan:

- Select a priority from 0 to 10 in the **Priority** list.

  Note: If you set a priority that differs from the Application Settings, the lower of the two settings will be used.

Tip: You cannot disable scan priority. However, you can set all applications and scans to the same priority to accomplish something similar.

Configuring Data Retention in Base Settings

If data retention is enabled for the application being scanned, then a default number of days for scan retention is configured in the application settings. In such cases, the default number of days for scan retention is displayed in the Details page. For more information, see "Working with Application Settings" on page 295.

To set a number of days other than the default setting for the scan:

- Enter the number of days in the **Data Retention** box.

Note: If you set a number of days that differs from the Application Settings, the lower of the two settings will be used.

Scanning Single-page Applications in Base Settings

This topic describes single-page application (SPA) support for crawling and auditing the Document Object Model (DOM) of an application.

The Challenge of Single-page Applications

Developers use JavaScript frameworks such as Angular, Ext JS, and Ember.js to build SPAs. These frameworks make it easier for developers to build applications, but more difficult for security testers to scan those applications for security vulnerabilities.

Traditional sites use simple back-end server rendering, which involves constructing the complete HTML web page on the server side. SPAs and other Web 2.0 sites use front-end DOM rendering, or a mix of front-end and back-end DOM rendering. With SPAs, if the user selects a menu item, the entire page can be erased and recreated with new content. However, the event of selecting the menu item does not generate a request for a new page from the server. The content update occurs without reloading the page from the server.

With traditional vulnerability testing, the event that triggered the new content might destroy other events that were previously collected on the SPA for audit. Through its SPA support, the dynamic sensor offers a solution to the challenge of vulnerability testing on SPAs.

Configuring SPA Support

When SPA support is enabled, the DOM script engine finds JavaScript includes, frame and iframe includes, CSS file includes, and AJAX calls during the crawl, and then audits all traffic generated by those events.

To configure SPA support:

- Under **Single-Page Applications** on the Details page, select one of the following options:
  - **Automatic** - If the sensor detects a SPA framework, it automatically switches to SPA-support mode.
  - **Disabled** - Indicates that SPA frameworks are not used in the target application.

- **Enabled** - Indicates that SPA frameworks are used in the target application.

  Caution! Enable SPA support for single-page applications only. Enabling SPA support to scan a non-SPA website results in a slow scan.

Enabling Traffic Monitor in Base Settings

The site tree of a scan normally displays only the hierarchical structure of the website or web service, plus those sessions in which a vulnerability was discovered. If traffic monitor is enabled, then the Traffic Viewer tool and the Traffic table in the scan results allow you to view every HTTP request sent by the sensor and the associated HTTP response received from the web server.

Note: The Traffic Viewer tool is not included with ScanCentral DAST. However, if you have Fortify WebInspect installed locally, you can use the tool that is included with your local installation.

Option Must be Enabled

To see all traffic in the Traffic Viewer tool or in the Traffic table in the scan results, you must enable Traffic Monitor logging in the scan settings.

Note: The Traffic table is always available in the scan results in ScanCentral DAST. However, enabling Traffic Monitor logging includes all of the scan traffic.

Enabling Traffic Monitor Logging

To enable traffic monitor logging:

- Under **Traffic Analysis** on the Details page, select **Enable Traffic Monitor**.

Creating and Managing Exclusions in Base Settings

You can exclude URLs and sessions—based on criteria in their requests or responses—from being crawled and audited. Excluding URLs means that the sensor will not examine the specified URL or host for links to other resources. Excluding sessions means that sensor will not process the sessions that meet the exclusion criteria.

To exclude these items from your scan, you must create a list of Basic Exclusions. Each exclusion in the list identifies one or more targets in which the criteria for exclusion is found.

Note: You can add multiple targets to each entry in the Basic Exclusions list.

Creating Exclusions

To create one or more exclusions:

1. Under **Basic Exclusions** on the Details page, click **CREATE**.
   The MANAGE EXCLUSIONS dialog box opens.
2. Type a name for the exclusion in the **Name** box.

3. From the **Target** list, select one of the following target types to configure for exclusion:
   - **Extension** - Excludes file extensions that match the exclusion criteria
   - **Host** - Excludes hosts that match the exclusion criteria
   - **Post parameter** - Excludes sessions with a POST request parameter that matches the exclusion criteria
   - **Query parameter** - Excludes sessions with a query parameter in the URL that matches the exclusion criteria
   - **Request** – Excludes sessions with a request that matches the exclusion criteria
   - **Response** – Excludes sessions with a response that matches the exclusion criteria
   - **Response header** - Excludes sessions with a response header that matches the exclusion criteria
   - **Status code** - Excludes sessions with a response status code that match the exclusion criteria
   - **URL** – Excludes URLs that match the exclusion criteria
4. Type a name for the target in the **Name** box.
5. Select one of the following types of exclusion for the target from the **Type** list:
   - **Matches Regex** – Matches the regular expression you specify in the **String** box
   - **Matches Regex extension** – Matches the regular expression extension you specify in the **String** box
   - **Matches** - Matches the specified criteria in the **String** box
   - **Contains** – Contains the text string you specify in the **String** box
6. Type the string to match in the **String** box.
   For examples of Target, Type, and String settings, see "Exclusion Examples" below.
7. Do one of the following:
   - To save the exclusion to the list, click the check mark icon (✔).
     The exclusion is added to the list. To create another exclusion, return to Step 2.
   - To clear the fields and start over, click the retry icon (↻) and return to Step 2.
8. When the list of exclusions is complete, click **OK**.

Exclusion Examples

The following table provides examples of exclusions.

To...	Create the following exclusion...
Ensure that you never send requests to any resource at Microsoft.com	URL contains `Microsoft.com`

To...	Create the following exclusion...

Exclude the following directories:
 	
`http://www.test.com/W3SVC55/`
`http://www.test.com/W3SVC5/`
`http://www.test.com/W3SVC550/`
	URL matches regex `/W3SVC[0-9]*/`

Ensure that you never process session responses with 404 Not Found	Response contains `Not Found`

For more information about creating exclusions, see "Understanding and Creating Inclusive Exclusions" on page 179.

Editing or Removing Exclusions

To edit or remove an entry in the **Basic Exclusions** list:

1. Select an entry from the **Basic Exclusions** list.
2. Do one of the following:
   - To edit the exclusion settings, click **MANAGE**.

     The MANAGE EXCLUSIONS dialog box opens. For more information about using this dialog box, see "Creating Exclusions" on page 288.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Configuring Redundant Page Detection in Base Settings

Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, the sensor would never be able to finish the scan. The **Perform redundant page detection** option compares page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources.

Important! Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.

To configure redundant page detection:

1. Select the **Perform redundant page detection** check box.
2. Configure settings as described in the following table.

Setting	Description
Page Similarity Threshold (%)	Indicates how similar two pages must be to be considered redundant. Enter a percentage from 1 to 100, where 100 is an exact match. The default setting is 95 percent.

Setting	Description
Tag attributes to include	Identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes in this list adds those attributes and their values in the page structure. By default, `id` and `class` tag attributes are included. To add tag attributes: a. Type the attribute name in the **Tag item** box. Do not include tag brackets (< and >). b. Click **ADD**. The tag attribute is added to the **Tag attributes to include** list. **Tip:** Certain sites may be primarily composed of one type of tag, such as `<div>`. Including these attributes creates a more rigid page match. Excluding these attributes creates a less strict match.

Enabling SAST Correlation in Base Settings

SAST correlation correlates the static and dynamic findings for your web application in Fortify Software Security Center. Correlation allows you to see the static findings that were also found in a dynamic scan. It can help you to prioritize which issues to fix and help verify that those issues are not false positives.

To enable SAST correlation:

- Select **Enable SAST Correlation**.

Applying Base Settings to Applications

Base settings are applied at the application level. Therefore, when configuring base settings, you must select one or more applications to which the settings will apply.

To select applications:

- In the **APPLICATIONS** list on the **Applications** page, select the check box(es) for the application (s) to which you want to apply the settings.

  The selected applications are added to the APPLICATIONS SELECTED list.

What's Next?

After you selected applications, click **NEXT** and proceed with "Reviewing and Saving Base Settings" on the next page.

Reviewing and Saving Base Settings

On the Review page, you can review a summary of the base settings that you configured and save the settings for others to use.

To save the base settings:

1. On the **Review** page, type a name for the base settings in the **Name** box.
2. Click **SAVE**.

   The base settings are added to the DAST database and appear in the base settings list. For more information, see "Understanding the Base Settings View" on page 259.

Using Advanced Settings in Base Settings

You can edit advanced settings in the Base Settings wizard.

Accessing Advanced Settings

At any time while configuring base settings, you can access the advanced settings.

To access the advanced settings:

- Click **Advanced Settings** in the bottom left navigation.

  The ADVANCED SETTINGS panel opens.

Editing Advanced Settings

The following settings are available for editing:

- "Advanced Settings: Crawl and Audit Mode" below
- "Advanced Setting: Requestor Performance" on the next page

When you have finished editing the advanced settings, click the hide icon ( ) to close the ADVANCED SETTINGS panel.

Advanced Settings: Crawl and Audit Mode

The crawl and audit mode advanced setting is available only if the SCAN MODE is set to **Crawl and Audit**.

Tip: If you selected **Crawl Only** or **Audit Only** on the Target page in the Base Settings wizard, you can change it in the advanced settings to enable the crawl and audit mode advanced setting.

To change the crawl and audit mode advanced setting:

- In the **CRAWL AND AUDIT MODE** area, select one of the options described in the following table.

Option	Description
Simultaneously	As the sensor maps the site's hierarchical data structure, it audits each resource (page) as it is discovered, rather than crawling the entire site and then conducting an audit. This option is most useful for extremely large sites where the content could change before the crawl can be completed. **Note:** This is the default setting.
Sequentially	The sensor crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.

Advanced Setting: Requestor Performance

The requestor performance advanced setting allows you to configure shared or separate requestors, as well as the maximum number of threads per requestor.

Using a Shared Requestor

With this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This option is suitable for use when maintaining state is not a significant consideration.

To use a shared requestor:

1. In the **REQUESTOR PERFORMANCE** area, select **Shared** from the **Requestor Performance Type** drop-down list.
2. In the **Requestor thread count** box, enter the maximum number of threads (up to 75).

Using Separate Requestors

With this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl Requestor Thread Count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5.

The **Audit Requestor Thread Count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

To use separate requestors:

1. In the **REQUESTOR PERFORMANCE** area, select **Separate** from the **Requestor Performance Type** drop-down list.
2. In the **Crawl Requestor Thread Count** box, enter the maximum number of threads (up to 25).
3. In the **Audit Requestor Thread Count** box, enter the maximum number of threads (up to 50).

Chapter 12: Working with Application Settings

Application settings apply to applications and generally override settings that are made in scan settings. Application settings such as scan priority, data retention, SAST correlation, domain restrictions, and private data settings are created and maintained by Fortify Software Security Center users who have permission to manage ScanCentral DAST deny intervals and other global settings.

Application Settings are Global Settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools.

Priority

Scans for an application are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Applications are configured with a default priority level in the application settings. For more information, see "Configuring Scan Priority" on page 173 or "Configuring Scan Priority in Base Settings" on page 286.

Data Retention

When a scan is run, it creates several artifacts, including scan logs, an FPR, a site tree, and a scan file. Configuring data retention settings for an application can aid in preventing your ScanCentral DAST database from becoming full. Purging the scan data from ScanCentral DAST does not delete the FPR from Fortify Software Security Center.

Applicable Scans for Domain Restrictions

Domain restrictions allow the scanning of a specific IP address, range of IP addresses, or a domain or host. Application setting domain restrictions apply only to Standard scans or API scans that use a start URL.

Accessing the Application Settings

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with DAST application settings directly in Fortify Software Security Center.

To access DAST application settings in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Application Settings**.
   The Application Settings view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Application Settings View

The Application Settings view displays in a table the settings for each of the applications in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each application.

Column	Description
Application	Identifies the application to which the settings apply.
Priority	Specifies the default priority of scans that are run for the application. For more information, see "Configuring Scan Priority" on page 173 or "Configuring Scan Priority in Base Settings" on page 286.
Data Retention	Indicates whether data retention is configured for scans of the application. Settings are **Enabled** and **Disabled**.
Retention Days	Specifies the number of days to retain scan data in the ScanCentral DAST database.

Column	Description
Sast Correlation	Indicates whether SAST correlation is configured for scans of the application. Settings are **Enabled** and **Disabled**.
Global Restrictions	Indicates whether global restrictions are configured for scans of the application. Settings are **Enabled** and **Disabled**. For more information, see "Working with Global Restrictions" on page 321.
Has Domain Restrictions	Indicates whether domain restrictions are configured for scans of the application. Settings are **Yes** and **No**.
Global Private Data Settings	Indicates whether global private data settings are configured for scans of the application. Settings are **Enabled** and **Disabled**. For more information, see "Working with Private Data Settings" on page 324.
Has Private Data Settings	Indicates whether private data settings are configured for scans of the application. Settings are **Yes** and **No**.

Understanding the Application Setting Detail Panel

When you select an entry in the Application Settings view, the application settings detail panel appears. The detail panel displays the information from the Application Settings table for the selected application.

If global restrictions are enabled, the detail panel displays the list of allowed IP addresses or hosts or both. If specific domain restrictions are configured for the application, the detail panel displays the list of allowed IP addresses or hosts or both.

Important! For domain restrictions, ScanCentral DAST merges the global and application-level restrictions. If the URL passes either the global or application-level restrictions, the scan will run.

Additionally, the detail panel provides an option to edit the settings for the selected application.

Managing Application Settings

You can edit existing application settings and refresh the settings that are displayed in the Application Settings view.

Editing Application Settings

To edit application settings:

1. In the **Application Settings** view, select one or more check boxes for the application settings to edit.
2. Click **EDIT**.

   The APPLICATION SETTINGS wizard opens pre-populated with the selected application settings.

   Note: If you select multiple application settings to edit, then the APPLICATION SETTINGS wizard will display default settings rather than those of the selected applications.

3. On the **Getting Started** page, continue according to the following table.

To...	Then...
Edit scan priority	In the **Priority** drop-down list, select a new priority.
Enable data retention	a. Slide the **Data Retention Disabled** toggle to **Data Retention Enabled**. b. In the **Number of days for retention** box, select a number of days to retain scans in the database.
Disable data retention	Slide the **Data Retention Enabled** toggle to **Data Retention Disabled**.
Enable SAST correlation	Slide the **SAST Correlation Disabled** toggle to **SAST Correlation Enabled**.
Disable SAST correlation	Slide the **SAST Correlation Enabled** toggle to **SAST Correlation Disabled**.

4. On the **Domain Restrictions** page, continue according to the following table.

To...	Then...
Enable global restrictions	Slide the **Global Domain Restrictions Disabled** toggle to **Global Domain Restrictions Enabled**.
Disable global restrictions	Slide the **Global Domain Restrictions Enabled** toggle to **Global Domain Restrictions Disabled**.
Create an application domain	a. Click **NEW**.

To...	Then...
restriction	b. Continue with the steps in "Creating or Editing an Application Domain Restriction" on the next page.
Edit an existing application domain restriction	a. In the **APPLICATION DOMAIN RESTRICTIONS** area, select the restriction to edit. b. Click **EDIT**. c. Continue with the steps in "Creating or Editing an Application Domain Restriction" on the next page.
Delete an application domain restriction	a. In the **APPLICATION DOMAIN RESTRICTIONS** area, select the restriction to delete. b. Click **DELETE**.

5. On the **Private Data Settings** page, continue according to the following table.

To...	Then...
Enable global private data settings	Slide the **Global Private Data Settings Disabled** toggle to **Global Private Data Settings Enabled**.
Disable global private data settings	Slide the **Global Private Data Settings Enabled** toggle to **Global Private Data Settings Disabled**.
Create an application private data setting	a. Click **NEW**. b. Continue with the steps in "Creating or Editing an Application Private Data Setting" on page 301.
Edit an existing application private data setting	a. In the **APPLICATION PRIVATE DATA SETTINGS** area, select the data setting to edit. b. Click **EDIT**. c. Continue with the steps in "Creating or Editing an Application Private Data Setting" on page 301.
Delete an application private data setting	a. In the **APPLICATION PRIVATE DATA SETTINGS** area, select the data setting to delete. b. Click **DELETE**.

6. Click **OK**.

Refreshing the Application Settings View

Generally, the changes that you make to the application settings appear right away on the Application Settings view. However, if other users have access to the same applications, any changes they make will not be updated in your view. To see such changes, you can manually refresh the Application Settings view.

To refresh the Application Settings view:

- Click **REFRESH**.

Creating or Editing an Application Domain Restriction

You can create or edit an application domain restriction in the DOMAIN RESTRICTION dialog box of the APPLICATION SETTINGS wizard. For information about accessing this wizard, see "Managing Application Settings" on page 297.

To create or edit an application domain restriction in the DOMAIN RESTRICTION dialog box:

1. Optionally, in the **Restriction Name** box, type a name for the restriction.
2. Continue according to the following table.

To allow a...	Do this...
Specific IP address	a. In the **Domain Restriction Type** list box, select **IP address**. b. In the **IP Address** box, type the IP address to restrict.
Range of IP addresses	a. In the **Domain Restriction Type** list box, select **IP address range**. b. In the **From** box, type the first IP address in the range. c. In the **To** box, type the last IP address in the range.
Domain or host	a. In the **Domain Restriction Type** list box, select **Host**. b. In the **Host** box, type the domain or host name. **Note:** You can enter only one domain or host name. To allow additional hosts, you must create a domain restriction for each host.

3. Click **OK**.

Creating or Editing an Application Private Data Setting

You can create or edit an application private data setting in the PRIVATE DATA CONFIGURATION dialog box of the APPLICATION SETTINGS wizard. For information about accessing this wizard, see "Managing Application Settings" on page 297.

To create or edit an application private data setting in the PRIVATE DATA CONFIGURATION dialog box:

1. In the **Type** list, select a type of data to use for matching on information in the scan and log files. Options are **Regex** or **Literal**.
2. In the **Match** box, do one of the following:
   - For **Regex** type matches, construct a regular expression as match criteria.
   - For **Literal** type matches, type the exact text to use as match criteria.
3. In the **Replace** box, type the value to use for masking private data that is found.
4. Click **OK**.

Chapter 13: Working with Two-factor Authentication

Two-factor authentication augments the standard password, which is defined as the "something you know" factor, with one of the following:

- Something you have, such as a one-time passcode (OTP) sent by SMS or email
- Something you are, such as your fingerprint, face, or retina

While this second factor of authentication improves security, it adds a layer of complexity when conducting an automated scan of web applications that implement it.

Fortify engineers have developed a method and process that enable Fortify WebInspect sensors and the Event-based Web Macro Recorder to automate the "something you have" factor of two-factor authentication.

How Scanning with Two-factor Authentication Works

Fortify ScanCentral DAST includes a 2FA Server Docker image that you configure for a control center to process the SMS and email responses coming from your application server. There is also a mobile application that forwards SMS responses to the control center. The control center queues the responses and forwards them to the appropriate TruClient browser when needed for authentication. For more information about the 2FA Server Docker image and container, see "ScanCentral DAST with Two-factor Authentication" on page 39.

Recommendation

Fortify strongly recommends that you use test phones and test email addresses only. For privacy concerns, do not use personal phones and email addresses.

Known Limitations

The following known limitations apply to the two-factor authentication feature:

- Only POP3 servers that support unique ID listing (UIDL) are supported.
- Currently, only Android mobile phones are supported.
- The mobile phone requires a Wi-Fi connection in the same subnet where the Fortify WebInspect sensor is installed.

Configuring Two-factor Authentication in ScanCentral DAST

The following table describes the process for configuring two-factor authentication in your ScanCentral DAST environment.

Stage	Description
1.	Prepare the Windows, Ubuntu Linux, or Red Hat Linux host machine. For more information, see "ScanCentral DAST with Two-factor Authentication" on page 39.
2.	Do the following: 1. Pull the Windows or Linux 2FA Server image from the Docker hub. 2. Generate a master token to use as an environment variable in the Docker run command for the 2FA Server container. 3. Run the 2FA Server container. For more information, see "Running the 2FA Server" on the next page. **Note:** PowerShell and bash scripts are available for generating the master token, pulling the image, and running the container on a host machine. For instructions on using the PowerShell script, see "Using PowerShell Scripts for the 2FA Server" on page 306. For information about executing the bash scripts, refer to your Linux distribution documentation.
3.	Configure the 2FA server in ScanCentral DAST. For more information, see "Creating a 2FA Server" on page 310.

Conducting a Scan Using Two-factor Authentication

After you have configured two-factor authentication in ScanCentral DAST, you can conduct a scan using two-factor authentication. The following table describes the process for conducting such a scan.

Stage	Description
1.	In the Event-based Web Macro Recorder, record a login macro and modify it as follows: 1. Add and configure a **Two-factor authentication** group step.

Stage	Description
	Note: You must configure the group step for SMS or email responses. The group step includes a **Wait for 2FA** step that you must also configure. 2. Configure the **Wait for 2FA** step. 3. Add a **Generic Object Action** step and configure it as a **Type** step. 4. Add a **Generic Object Action** step and configure it as a **Click** step. For more information, see the *Micro Focus Fortify WebInspect Tools Guide*.
2.	In the Web Macro Recorder, replay the login macro.
3.	In ScanCentral DAST, run a scan using the macro. For more information, see "Configuring a Scan" on page 137.

Running the 2FA Server

After installing the Docker Engine on your Linux or Windows host machine and starting the Docker service, you can pull an image of the 2FA Server from the Fortify Docker repository and run it in a container.

Note: PowerShell and bash scripts are available for generating the master token, pulling the image, and running the container on a host machine. For instructions on using the PowerShell script, see "Using PowerShell Scripts for the 2FA Server" on page 306. For information about executing the bash scripts, refer to your Linux distribution documentation.

Pulling the 2FA Server Image

To pull the current Ubuntu Linux version of the Fortify 2FA Server image:

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

```
docker pull fortifydocker/fortify-2fa:23.1.alpine.3.14.6
```

To pull the current Red Hat Linux version of the Fortify 2FA Server image:

- At the terminal prompt on the Red Hat Linux Docker host machine, enter the following command:

```
docker pull fortifydocker/fortify-2fa:23.1.ubi.8
```

To pull the current Windows version of the Fortify 2FA Server image:

- In PowerShell on the Windows host machine, enter the following command:

```
docker pull fortifydocker/fortify-2fa:23.1.nanoserver.1809
```

Generating a Master Token

You must provide a master token to use as an environment variable in the Docker run command and in the ScanCentral DAST user interface when configuring the 2FA Server. You can generate a master token in Linux or Windows for this purpose.

Important! The master token is not stored on the host machine. Be sure to save it for use in running the container and configuring the 2FA Server in ScanCentral DAST.

To generate a master token in Linux:

1. At the terminal prompt, enter the following commands:

   ```
   MASTER_TOKEN=$(uuidgen)
   echo $(uuidgen)
   ```

   Linux returns a GUID.

   ```
   90fc1ea9-723f-4cc9-8a65-d231c7af73d4
   ```

2. Copy the GUID to use when running the container and configuring the 2FA Server in ScanCentral DAST.

To generate a master token in Windows:

1. In PowerShell, enter the following commands:

   ```
   $MASTER_TOKEN = [guid]::NewGuid().ToString()
   echo $MASTER_TOKEN
   ```

   Windows returns a GUID.

   ```
   373ceaf2-4ad9-4dc4-ab57-fa6d7bf5b54e
   ```

2. Copy the GUID to use when running the container and configuring the 2FA Server in ScanCentral DAST.

Running the 2FA Server Container

Using the GUID created previously, you can run the 2FA Server container.

Note: Some environments do not allow environment variable names that begin with a number. For this reason, the Docker run commands include the optional "FORTIFY_" prefix for the 2FA image environment variables.

To run the container in Linux:

- At the terminal prompt, enter the following command:

```
docker run --name "<container_name>" -d \
-p 443:443 \
-e "FORTIFY_2FA_MASTER_TOKEN=<master_token>" \
"<image_name>"
```

If your security policy prevents services from running on ports below 1024, you may add `-e "FORTIFY_2FA_API_PORT=8443" \` to the command and publish the assigned port as shown in the following example.

```
docker run --name "<container_name>" -d \
-p 8443:8443 \
-e "FORTIFY_2FA_MASTER_TOKEN=<master_token>" \
-e "FORTIFY_2FA_API_PORT=8443" \
"<image_name>"
```

Tip: The backslash (\) indicates the end of line for the Linux OS.

To run the container in Windows:

- In PowerShell, enter the following command:

```
docker run --name "<container_name>" -d `
-p 443:443 `
-e "FORTIFY_2FA_MASTER_TOKEN=<master_token>" `
"<image_name>"
```

Using PowerShell Scripts for the 2FA Server

The Configuration Tool CLI creates and downloads PowerShell scripts for the 2FA Server. (For more information, see "Understanding the Launch Artifacts" on page 96.) These scripts offer the following options:

- Use one script to pull the 2FA Server image, and then start the container.
- Use two scripts: one to pull the 2FA Server image, and then another to start the container.

You use the script or scripts on the host where you want to run the 2FA Server container.

Using One Script

Use the following process to use a single PowerShell script to pull images and start the containers.

Stage	Description
1.	Copy the `pull-and-start-twofactorauth-container.ps1` to the host where you want to run the 2FA Server container.
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information about using PowerShell, refer to your Windows PowerShell documentation.
3.	To avoid errors regarding non-digitally signed scripts, run the contents of the script as follows: 1. Copy the contents from the `pull-and-start-twofactorauth-container.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-and-start-twofactorauth-container.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The 2FA Server image is pulled and the container is started.

Using Two Scripts

Use the following process to use separate pull and start PowerShell scripts.

Stage	Description
1.	Copy the following files to the host where you want to run the 2FA Server container: • `pull-twofactorauth-image.ps1` • `start-twofactorauth-container.ps1`
2.	On this same host, start Windows PowerShell ISE as Administrator. For more information

Stage	Description
	about using PowerShell, refer to your Windows PowerShell documentation.
3.	Pull the image. To avoid errors regarding non-digitally signed scripts, run the contents of the `pull-twofactorauth-image.ps1` script as follows: 1. Copy the contents from the `pull-twofactorauth-image.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows: `& "<drive>:<path_to_script>\pull-twofactorauth-image.ps1"` For more information about setting the execution policy, refer to your Windows PowerShell documentation. The 2FA Server image is pulled.
4.	Start the container. To avoid errors regarding non-digitally signed scripts, run the contents of the `start-twofactorauth-container.ps1` script as follows: 1. Copy the contents from the `start-twofactorauth-container.ps1` script. 2. Paste the contents in the PowerShell ISE script pane. 3. Click the **Run Selection** icon. **Note:** Alternatively, if you set the execution policy to allow all scripts as described in Stage 3, you can run the script as follows: `& "<drive>:<path_to_script>\start-twofactorauth-container.ps1"` The 2FA Server container is started.

Accessing the Two Factor Authentication View

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can set up and manage two-factor authentication for your scans directly in Fortify Software Security Center. Two-factor authentication servers that are configured in ScanCentral DAST appear in the Two Factor Authentication view.

To access the Two Factor Authentication view in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Two Factor Authentication**.
   The Two Factor Authentication view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules.

Understanding the Two Factor Authentication View

The Two Factor Authentication view displays in a table the two-factor authentication servers that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each two-factor authentication server.

Column	Description
Name	Indicates the name of the two-factor authentication server.
Root URL	Indicates the hostname and port where the 2FA Server Docker container is running.
Status	Indicates the current status of the 2FA Server container. Possible statuses are: • **Online** – The server is running and capable of processing SMS or email responses or both. • **Offline** – The server is not running. • **Unknown** – The status of the server cannot be determined. • **InvalidAuthToken** – The access token is not valid. **Note:** This is *not* the master token used in the run command for the 2FA Server container. During 2FA Server configuration, ScanCentral DAST creates an access token to authenticate communication with the 2FA server. InvalidAuthToken refers to this access token.

Column	Description
Status Time	The date and time when the 2FA Server container entered its current status.
Access Token Created	The date and time when the access token was created by ScanCentral DAST for the 2FA Server.
Access Token Expiration	The date and time when the access token for the 2FA Server expires. **Important!** Upon expiration, ScanCentral DAST automatically creates a new token. After this date, however, you must generate a new QR code and scan it to update the settings on your mobile phone. For more information, see "Configuring a Mobile Device" on page 319.

Understanding the Two-factor Authentication Detail Panel

When you select a server in the Two Factor Authentication view, the two-factor authentication detail panel appears. The server name and root URL appear at the top of the panel, along with the information from the Two Factor Authentication table for the selected 2FA Server.

The detail panel also provides options to edit and delete the selected 2FA Server, as well as join a mobile device to the server.

Creating a 2FA Server

You can use the TWO FACTOR AUTHENTICATION wizard to create a 2FA Server that will process the SMS and email responses coming from your application server. During creation, you must assign the 2FA Server to sensor pools.

Important! If the 2FA Server Docker image has not been downloaded and started in a container, then you cannot verify the server configuration.

To create a 2FA Server:

1. On the **Two Factor Authentication** page, click **+ NEW 2FA SERVER**.
   The TWO FACTOR AUTHENTICATION wizard opens.
2. On the **Getting Started** page, enter the following information:
   - In the **2FA Server Name** box, enter a name for the server.
   - In the **Root URL** box, enter the URL and port number for the 2FA server.

     Tip: This is the URL for the host running the 2FA Server. The default port is 443.

Important! For SMS two-factor authentication, you must enter the public network IP address of the Docker host. For email two-factor authentication, you may enter the Docker container's internal IP address.

- In the **Token** box, enter the master token GUID that you previously generated for the server. For more information, see "Generating a Master Token" on page 305.

3. Click **VERIFY**.

   Connection to the 2FA Server is validated.

   Tip: If you are unable to validate a connection to the server, ensure that the 2FA Server Docker image has been downloaded and started in a container.

4. Click **NEXT**.

   The Sensor Pools page appears.

5. In the **SENSOR POOLS** list, select one or more check boxes to assign to the 2FA Server.

   Important! Only sensors in the selected pools will run scans that use two-factor authentication.

6. Click **NEXT**.

   The Review page appears.

7. Click **NEXT**.

   The Join mobile device page appears.

8. Do one of the following:
   - If your application server sends email responses only, then click **CANCEL**.
   - If your application server sends SMS responses, then proceed with "Configuring a Mobile Device" below.

Configuring a Mobile Device

If your application server sends SMS responses, then you must install the **Fortify2FA** mobile application on a mobile device and download your two-factor authentication settings to it. After configuration, the mobile application receives the SMS response and forwards it to the 2FA Server.

Note: Currently, the mobile application is available only for Android operating systems.

To configure the mobile application on the **Join mobile device** page:

1. Have you already downloaded and installed the **Fortify2FA** mobile application on the mobile device?
   - If *yes*, start the application on the mobile device, and then go to step 2.
   - If *no*, go to step 2.
2. In the **Mobile Phone** field, enter the phone number that will receive SMS responses.

3. Click **GENERATE QR CODE**.

   The 2FA Server generates a quick response (QR) code that includes the two-factor authentication settings and a link to download the mobile application.
4. Do one of the following:
   - To configure the application, use the mobile phone's camera to scan the QR code.
   - To install and configure the mobile application, proceed to "Installing and Configuring the Fortify2FA Mobile App" below.

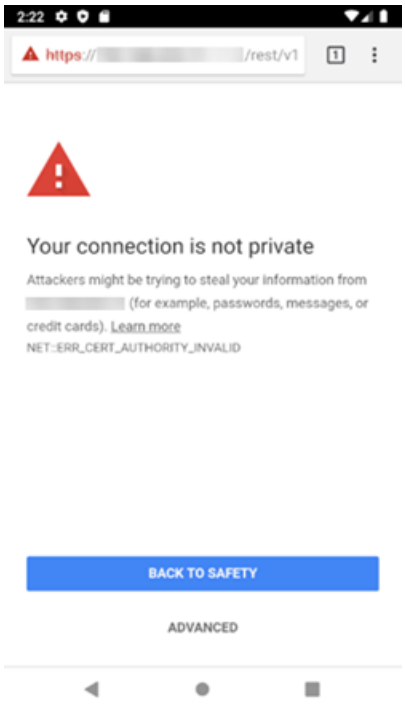
Installing and Configuring the Fortify2FA Mobile App

To install and configure the mobile application on a phone that will receive SMS responses:

1. Use the mobile phone's camera to scan the QR code on the **Join mobile device** page.

   A link appears.
2. Click the link (or **Open** button) to access the site for downloading the app.

   A warning about the self-signed certificate appears.

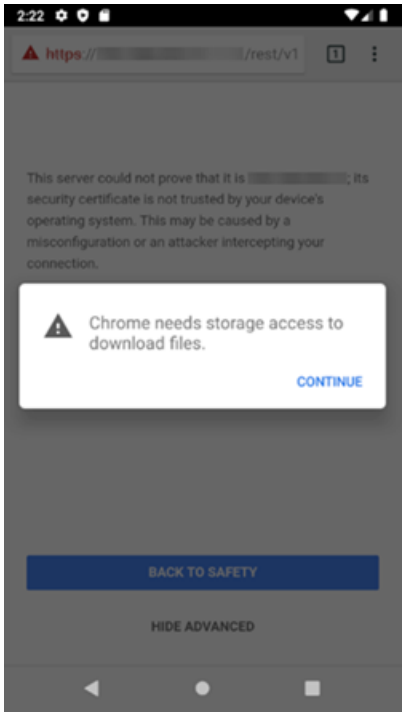


3. Click **ADVANCED**.

Additional information is provided along with a link to proceed.

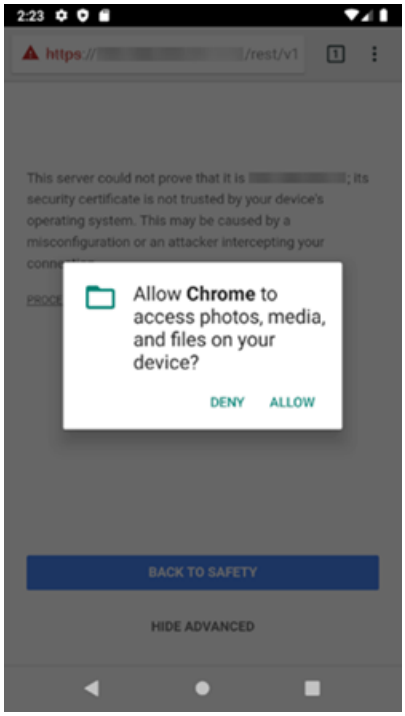
4. Click **PROCEED TO *<ip_address>* (UNSAFE)**.

   A prompt requests storage access to download files.



5. Click **CONTINUE**.

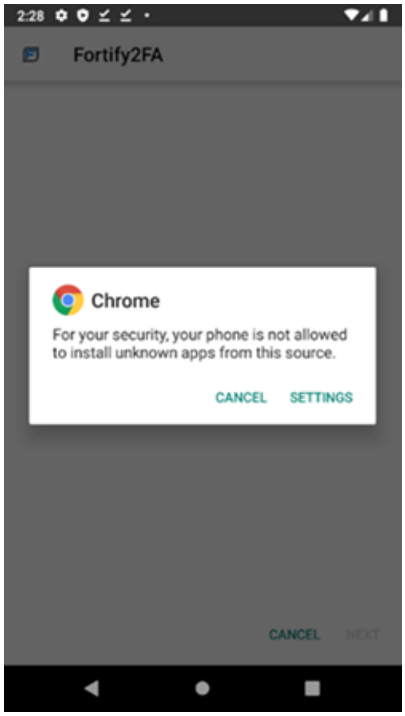
A prompt requests access to photos, media, and files on the device.



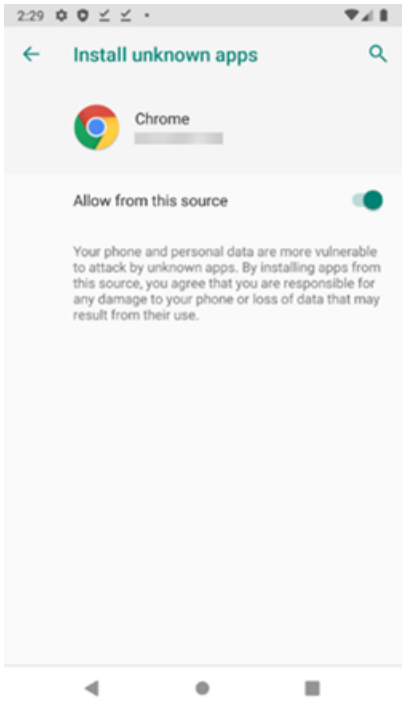
6. Click **ALLOW**.
   The fortify-2fa.apk file is downloaded.

7. Click **OPEN**.

A prompt advises about installing unknown apps.

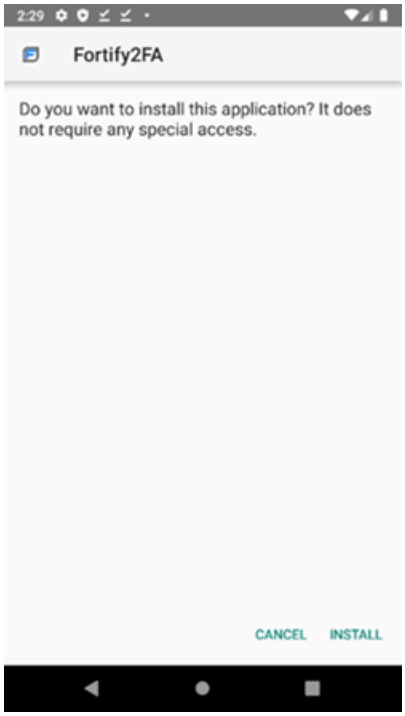


8. Click **SETTINGS**.
   The Install unknown apps setting appears.



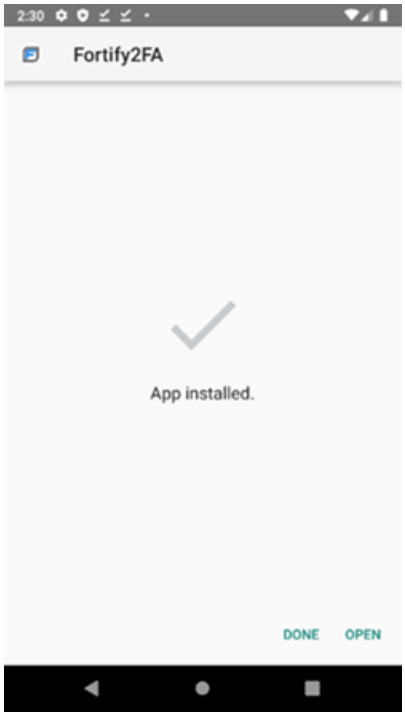
9. Enable **Allow from this source**.

A prompt asks if you want to install the application.



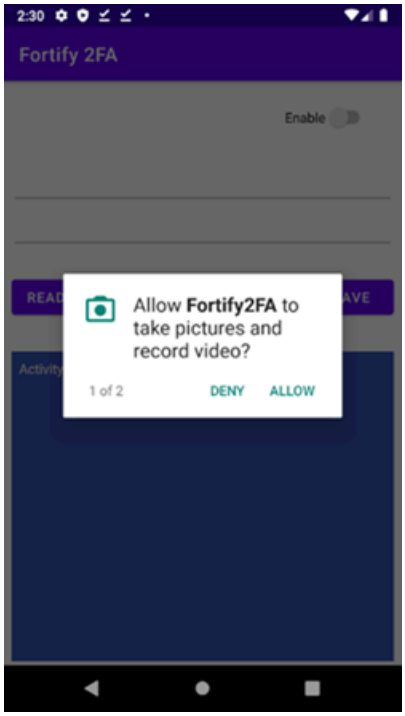
10. Click **INSTALL**.

    A message indicates that the app is installed.



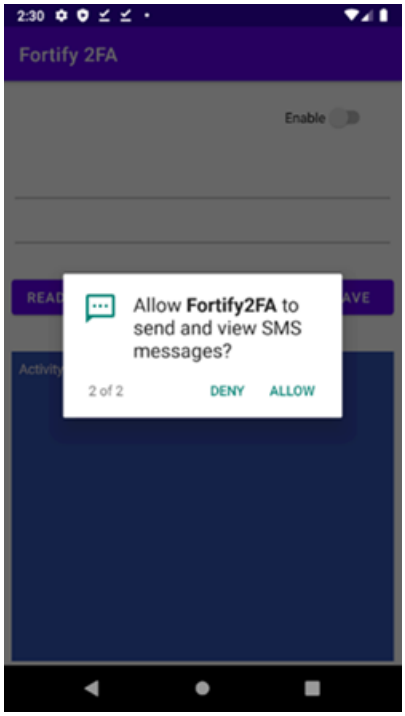
11. Click **OPEN**.

A prompt requests permission to take pictures and record video.



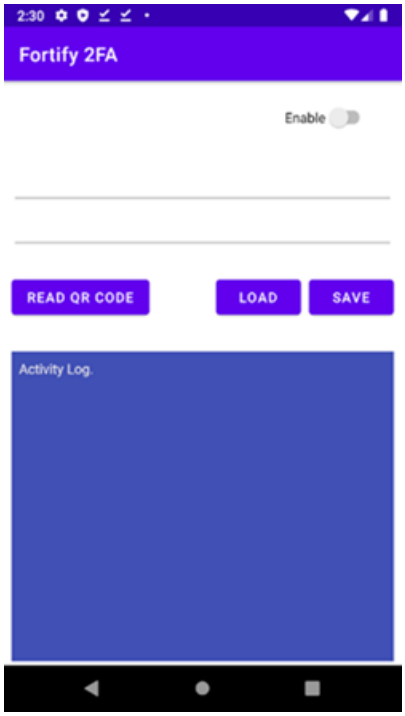
12. Click **ALLOW**.

A prompt requests permission to send and view SMS messages.



13. Click **ALLOW**.

The app is ready to be configured.



14. Click **READ QR CODE** to scan the QR code on the **Join mobile device** page.
    The two-factor authentication settings are configured in the **Fortify2FA** mobile application.

Managing 2FA Servers

You can edit and delete 2FA Servers, and refresh the servers that are displayed on the Two Factor Authentication view. Additionally, you can configure a new mobile device or update settings for an existing device on the two-factor authentication detail panel.

Editing a 2FA Server

To edit a 2FA Server:

1. In the **Two Factor Authentication** view, select the 2FA Server to edit.
   The two-factor authentication detail panel appears.
2. Click **EDIT**.
   The TWO FACTOR AUTHENTICATION wizard opens with the settings visible for the selected 2FA Server.
3. To make edits, follow the procedure in "Creating a 2FA Server" on page 310.

Deleting a 2FA Server

To delete a 2FA Server, do one of the following:

- Select one or more check boxes for 2FA Servers in the **Two Factor Authentication** view, and then click **DELETE** at the bottom of the table.
- Select a 2FA Server to view the two-factor authentication details, and then click **DELETE** at the bottom of the two-factor authentication detail panel.

Refreshing the 2FA Server List

Generally, the changes that you make to 2FA Servers appear right away on the Two Factor Authentication view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Two Factor Authentication view:

- Click **REFRESH**.

Configuring a Mobile Device

If your application server sends SMS responses, then you must install the **Fortify2FA** mobile application on a mobile device and download your two-factor authentication settings to it. After configuration, the mobile application receives the SMS response and forwards it to the 2FA Server.

Note: Currently, the mobile application is available only for Android operating systems.

During 2FA Server configuration, ScanCentral DAST creates an access token to authenticate communication with the 2FA server. By default, the access token is valid for one year. Upon expiration, ScanCentral DAST automatically creates a new access token. When this occurs, you must generate a new QR code and scan it to update the existing settings on your mobile phone.

You can configure a new mobile device or update settings for an existing device on the two-factor authentication detail panel.

To configure the mobile application:

1. In the **Two Factor Authentication** view, select the 2FA Server to edit.

   The two-factor authentication detail panel appears.
2. Click **JOIN MOBILE DEVICE**.

   The JOIN MOBILE DEVICE dialog box appears.
3. Have you already downloaded and installed the **Fortify2FA** mobile application on the mobile device?
   - If *yes*, start the application on the mobile device, and then go to step 4.
   - If *no*, go to step 4.

4. Click **GENERATE QR CODE**.

   The 2FA Server generates a quick response (QR) code that includes the two-factor authentication settings and a link to download the mobile application.
5. Do one of the following:
   - To configure the mobile application, use the mobile phone's camera to scan the QR code.
   - To install and configure the mobile application, proceed to "Installing and Configuring the Fortify2FA Mobile App" on page 312.

Chapter 14: Working with Global Restrictions and Private Data Settings

You can configure global restrictions and private data settings that apply globally to all scans. You can disable the global aspect of these restrictions and settings, and apply them to individual applications in the Application Settings view. The following pages describe creating, viewing, and managing global restrictions and private data settings.

Working with Global Restrictions

You can configure global restrictions that limit a user's ability to scan by host, IP address, or range of IP addresses. Global restrictions *allow* scanning of the specified IP addresses or hosts. By default, global restrictions apply to all scans. However, you can disable global restrictions for individual applications in the Application Settings view. For more information, see "Managing Application Settings" on page 297.

Important! For domain restrictions, ScanCentral DAST merges the global and application-level restrictions. If the URL passes either the global or application-level restrictions, the scan will run.

Applicable Scans

Global Restrictions apply only to Standard scans or API scans that use a start URL.

Accessing Global Restrictions in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with global restrictions directly in Fortify Software Security Center.

To access global restrictions in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Global Restrictions**.
   The Global Restrictions view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to global

restrictions may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Global Restrictions View

The Global Restrictions view displays in a table the global domain restrictions that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each domain restriction.

Column	Description
Name	Optionally, indicates the name given to the restriction upon creation.
Restriction Type	Indicates the type of restriction. Options are: • **Single** – A single IP address is allowed. • **Range** – A range of IP addresses is allowed. • **Host** – A single domain or host name is allowed.
Restriction	Specifies the restriction value—an IP address, a range of IP addresses, or a host name.

Creating a Global Restriction

You can create a global restriction for an IP address, range of IP addresses, or host name. Restrictions for IP addresses support Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

Tip: You can use an asterisk (*) as a wild card character at the beginning of a domain name, such as *.webappsecurity.com, or at the end of an IP address, such as 172.16.*.*.

To create a global restriction:

1. On the **Global Restrictions** view, click **+ RESTRICTION**.
   The DOMAIN RESTRICTION dialog box opens.
2. Optionally, in the **Restriction Name** box, type a name for the restriction.
3. Continue according to the following table.

To allow a...	Do this...
Specific IP address	a. In the **Domain Restriction Type** list box, select **IP address**.

To allow a...	Do this...
	b. In the **IP Address** box, type the IP address to restrict.
Range of IP addresses	a. In the **Domain Restriction Type** list box, select **IP address range**. b. In the **From** box, type the first IP address in the range. c. In the **To** box, type the last IP address in the range.
Domain or host	a. In the **Domain Restriction Type** list box, select **Host**. b. In the **Host** box, type the domain or host name. **Note:** You can enter only one domain or host name. To allow additional hosts, you must create a domain restriction for each host.

4. Click **OK**.
   The restriction is added to the Global Restrictions view and applied to all applications that have Global Domain Restrictions enabled.

Managing Global Restrictions

You can edit and delete global restrictions, and refresh the Global Restrictions view.

Editing a Global Restriction

To edit a global restriction:

1. In the **Global Restrictions** view, select the global restriction to edit.
2. Click **EDIT**.
   The DOMAIN RESTRICTION dialog box opens.
3. Edit the fields as needed.

   Note: For a description of the fields, see "Creating a Global Restriction" on the previous page.
4. Click **OK**.
   The changes are saved in the ScanCentral DAST database.

Deleting a Global Restriction

To delete a global restriction:

- Select one or more check boxes for global restrictions in the **Global Restrictions** view, and then click **DELETE** at the bottom of the table.

Refreshing the Global Restrictions View

Generally, the changes that you make to global restrictions appear right away on the Global Restrictions view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Global Restrictions view:

- Click **REFRESH**.

Working with Private Data Settings

You can configure private data settings that remove personally identifiable information from the scan and log data upon scan completion. By default, private data settings apply to all scans. However, you can disable private data settings for individual applications in the Application Settings view. For more information, see "Managing Application Settings" on page 297.

Accessing Private Data Settings

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with private data settings directly in Fortify Software Security Center.

To access private data settings in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Private Data Settings**.
   The Private Data Settings view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to private data settings may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Private Data Settings View

The Private Data Settings view displays in a table the private data settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each private data setting.

Column	Description
Private Data Type	Indicates the type of data used for matching on information in the scan. Possible values are **Regex** and **Literal**.
Match	Specifies the regular expression or literal text used as match criteria to identify private data.
Replace	Specifies the value used for masking the private data in scans and log files.

Default Private Data Settings

There are three default private data settings:

- Credit or debit card number
- IP address
- Social Security Number

You can delete these default settings. However, in the case of accidental deletion, you must recreate them. There is no way to restore private data settings.

Creating Private Data Settings

You can create a private data setting that applies to all applications that have Global Private Data Settings enabled.

To create a private data setting:

1. On the **Private Data Settings** view, click **+ PRIVATE DATA SETTING**.
   The PRIVATE DATA CONFIGURATION dialog box opens.
2. In the **Type** list, select a type of data to use for matching on information in the scan and log files. Options are **Regex** or **Literal**.
3. In the **Match** box, do one of the following:
   - For **Regex** type matches, construct a regular expression as match criteria.
   - For **Literal** type matches, type the exact text to use as match criteria.

4. In the **Replace** box, type the value to use for masking private data that is found.
5. Click **OK**.

The private data setting is added to the Private Data Settings view and applied to all applications that have Global Private Data Settings enabled.

Managing Private Data Settings

You can edit and delete private data settings, and refresh the Private Data Settings view.

Editing a Private Data Setting

To edit a private data setting:

1. In the **Private Data Settings** view, select the private data setting to edit.
2. Click **EDIT**.
   The PRIVATE DATA CONFIGURATION dialog box opens.
3. Edit the fields as needed.

   Note: For a description of the fields, see "Creating Private Data Settings" on the previous page.
4. Click **OK**.
   The changes are saved in the ScanCentral DAST database.

Deleting a Private Data Setting

To delete a private data setting:

- Select one or more check boxes for private data settings in the view, and then click **DELETE** at the bottom of the table.

Refreshing the Private Data Setting View

Generally, the changes that you make to private data settings appear right away on the Private Data Setting view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Private Data Settings view:

- Click **REFRESH**.

Chapter 15: Working with Key Stores and Artifacts Repositories

Key stores and artifacts repositories help you streamline the management of values in scan settings and the files used in settings, such as workflow macros, login macros, and client certificates. The following pages describe key stores and artifacts repositories.

Understanding Key Stores

Key stores provide a way to create variables that you can use in scan settings, base settings, and macro parameters. Creating a key store generates placeholder text that you can use in settings fields that accept string data. Values for the placeholder text are stored in key store entries. When a scan starts in ScanCentral DAST using the settings file, the placeholder text is replaced with the latest values from the key store.

When you save scan settings that use key store placeholder text, a background process generates a Fortify WebInspect XML settings file that you can download. This XML file includes the latest values from the key store entries. However, the key store references are removed and the values in this file are static.

When you edit a key store, a background process uses the latest values to generate new Fortify WebInspect XML settings files for any scan settings that use the updated key store. When the settings are regenerated, the Modified date for the settings is updated.

Benefit of Using Key Stores

Key stores allow you to manage scan settings values in a single location. For example, if scan settings use an API token that changes frequently, you can use a key store to store the token value. Scan settings can reference the key store entry by using the placeholder text instead of the API token. When the token changes, a single change to the key store entry is all that is needed.

Key Store Placeholder Format

The format for key store entry placeholder text is as follows:

```
${DAST_KS_KeyStoreName_KeyStoreEntryName}
```

Any entry in a field that includes the format `${DAST_KS_KeystoreName_KeyStoreEntryName}` is identified by ScanCentral DAST as a key store placeholder. If you manually edit this placeholder to include two sequential underscore characters, such as `${DAST_KS_KeystoreName__KeyStoreEntryName}`, or any other change that alters the format, it will no longer be identified by ScanCentral DAST as a key store placeholder.

Placeholder Text in Exported/Imported Settings

When you export scan settings that use key store placeholder text from ScanCentral DAST, the placeholder text is replaced with the actual values from the key store. Importing the scan settings back into ScanCentral DAST uses the key store values at the time the settings were created, rather than the key store placeholder text.

Types of Key Store Entries and Their Usage

There are two types of key store entries:

- URL
- Text

You can use URL types only in fields that accept URLs. You can use text types in any field that accepts string input, except for the Policy ID field.

You cannot use key store entries in the names of base settings or scan settings.

URL Key Store Entry Validation

URL fields require key store entry values to be valid URLs. Therefore, URL fields are validated against the value of the selected key store entry rather than the placeholder text.

Accessing Key Stores in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with key stores directly in Fortify Software Security Center.

To access key stores in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Key Stores**.
   The Key Stores view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to key stores may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Key Stores View

The Key Stores view displays in a table the key stores that are in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each key store.

Column	Description
Name	Identifies the name of the key store.
Description	Provides a description of the key store.
Is Hidden	Indicates whether the key store and its entries are visible for selection in the user interface. Options are **Yes** and **No**.
All Application Access	Indicates whether all applications have access to the values in key store entries. Options are **Yes** and **No**.

Understanding the Key Store Detail Panel

When you select a key store in the Key Stores view, the key store detail panel appears.

The detail panel displays the same information that is displayed in the Key Stores view for the selected key store, as well as the list of applications to which the key store is assigned.

Understanding the Key Store Usage Tab

The detail panel includes a usage tab that shows the usage data for the selected key store. The usage data is categorized into the following groups:

- **Scan Settings** – a list of scan settings that use values from the key store
- **Base Scan Settings** – a list of base scan settings that use values from the key store
- **Scans** – a list of scans that use values from the key store

A group is displayed only if there is usage associated with the group.

The following table describes the data that is provided in each group.

Data	Description
Name	Identifies the name of the settings file or scan.

Data	Description
Settings ID or **Scan ID**	Indicates the integer ID in the ScanCentral DAST database for the settings file or scan.
Property	Identifies the settings property, such as `ScanSettings.StartUrls` or `ScanSettings.ProxyPACUrl`, that uses the key store entry.
Entry Name	Identifies the name of the key store entry.

Creating a Key Store

When you create a key store, you can assign it to individual applications or to all applications. These assignments determine which applications can use the key store placeholders in their scan settings.

To create a key store:

1. On the **Key Stores** view, select **+ KEY STORE**.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. Configure the GENERAL settings as follows:
   a. To make the key store visible so that it can be selected when configuring scan settings, slide the toggle to **Key Store Visible**.

      Tip: You cannot delete a key store after it has been created. However, you can hide it so that it is not visible to users when configuring scan settings. To hide the key store, slide the toggle to **Key Store Hidden**.

   b. In the **Key Store Name** box, type a name that will become part of the placeholder text used in settings.

      Important! This field is required and cannot be the same as any existing key store. After the key store is created, you cannot change the key store name.

   c. Optionally, in the **Key Store Description** box, type a useful description.
3. Click **NEXT**.
   The Application Select page appears.
4. Do one of the following:
   - To assign the key store to all existing and future applications, slide the toggle to **Grant all application access**.
   - To assign the key store to individual applications, slide the toggle to **Assign individual applications**, and then select individual application check boxes in the **APPLICATIONS** list.

     Note: Only selected applications will have access to the key store. The key store must have at least one assigned application.

5. Click **NEXT**.

   The Key Store Values page appears.

   Note: The key store must have at least one key store entry.

   Tip: To view updated key store entries that other administrators may be creating in the same key store, click **REFRESH** to update the list of key store entries.

6. To add a key store entry, select **+ KEY STORE ENTRY**.

   The KEY STORE ENTRY dialog box opens.

7. Continue as follows:
   a. To make the key store entry visible so that it can be selected when configuring scan settings, slide the toggle to **Key Store Entry Visible**.

      Tip: You cannot delete a key store entry. However, you can hide it so that it is not visible to users when configuring scan settings. To hide the key store entry, slide the toggle to **Key Store Entry Hidden**.

   b. In the **Key Store Entry Name** box, type a name that will become part of the placeholder text used in settings.

      Important! The name cannot contain underscores or spaces, exceed 255 characters, or match any existing key store entry names. After the entry is saved, you cannot change the key store entry name.

   c. Optionally, in the **Key Store Entry Description** box, type a useful description.
   d. From the **Type** list, select either **Text** or **Url**.

      Note: Entries of URL type are available only for settings fields that require a URL. Text type entries are not available for settings fields that require a URL.

   e. In the **Key Store Entry Value** box, type the value that will replace the placeholder text in the scan settings.

      Note: The maximum length is 4,000 characters.

   f. Click **OK**.

      The new entry is added to the KEY STORE ENTRIES list.

      Tip: To make the entry values in the list visible, click **REVEAL VALUES**. You cannot sort on the **Entry Value** column because these values are encrypted.

      Note: You cannot delete a key store entry that has been saved. However, you can remove one that has not yet been saved by clicking the remove icon (×) for the entry. Only unsaved entries have the remove icon.

   g. Optionally, to add another key store entry, select **+ KEY STORE ENTRY** and return to Step a.
8. Click **NEXT**.

The Review page appears.

9. Click **SAVE**.

Managing Key Stores

You can edit a key store, hide a key store, and view hidden key stores.

Editing a Key Store

To edit a key store:

1. In the **Key Stores** view, click the edit icon (✎) for the key store you want to edit.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. To make edits, follow the procedure listed in "Creating a Key Store" on page 330.

Hiding a Key Store

You cannot delete a key store, but you can hide it from view in the user interface. Placeholders in a hidden key store are not available for selection in the scan settings and base settings user interfaces.

Note: Although a hidden placeholder is not available for selection in the user interface, you can manually enter the placeholder in a relevant field. If the placeholder is formatted correctly, ScanCentral DAST will accept it without further validation. Ensure that manually entered placeholders are valid. Otherwise, the scan settings may not be valid. For more information, see "Key Store Placeholder Format" on page 327.

To hide a key store:

1. In the **Key Stores** view, click the edit icon (✎) for the key store you want to hide.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. To hide the key store so that it cannot be selected when configuring scan settings, slide the toggle to **Key Store Hidden**.
3. In the left navigation, select **Review**.
   The Review page appears.
4. Click **SAVE**.

Viewing Hidden Key Stores

By default, hidden key stores are not visible in the Key Stores view. However, you can view them if needed.

To view hidden key stores:

- On the **Key Stores** view, select the **Show hidden** check box.
  All key stores become visible in the Key Stores view.

Managing Key Store Entries

You cannot delete a key store entry that has been saved. However, you can edit or hide a key store entry.

Editing a Key Store Entry

To edit a key store entry:

1. In the **Key Stores** view, click the edit icon ( ) for the key store whose entries you want to edit.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. In the left navigation, select **Key Store Values**.
   The Key Store Values page appears.
3. Click the edit icon ( ) for the entry you want to edit.
   The KEY STORE ENTRY dialog box opens.

   Tip: To make the value visible, click **REVEAL VALUE**.
4. Edit the values as described in Step 7 of "Creating a Key Store" on page 330.

Hiding a Key Store Entry

You cannot delete a key store entry, but you can hide it from view in the user interface.

To hide a key store entry:

1. In the **Key Stores** view, click the edit icon ( ) for the key store whose entries you want to hide.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. In the left navigation, select **Key Store Values**.
   The Key Store Values page appears.
3. Click the edit icon ( ) for the entry you want to hide.
   The KEY STORE ENTRY dialog box opens.
4. Slide the toggle to **Key Store Entry Hidden**.

Understanding Artifacts Repositories

Artifacts repositories provide a way to specify repositories where scan artifacts reside. When a scan is run that references an artifact in a repository, either a tagged version or the latest copy of the artifact is pulled and used to configure and run the scan.

Benefits of Using Artifacts Repositories

When artifacts are stored in the ScanCentral DAST database and updated frequently, such as Postman collections, you must manually reconfigure scan settings after each update. Creating a reference to artifacts in a repository eliminates the need to manually update scan settings. The latest version of the artifacts are automatically pulled from the repository and used to run the scan each time the settings are used.

Supported Artifacts

Any file that you can import into ScanCentral DAST to configure settings or start a scan can be placed in a repository and referenced. Such artifacts include client certificates, login macros, workflow macros, HAR files, Burp files, Postman collections, and so forth.

Supported Repositories

Supported repositories are GitHub, GitHub Enterprise, and JFrog Artifactory.

Using a Proxy with the Repository

If a proxy is required for communication with the repository, the DAST API will use the proxy that is configured in ScanCentral DAST.

Artifacts in XML Settings Files

Artifacts from the repository will be included in Fortify WebInspect XML settings files that are downloaded from ScanCentral DAST.

Accessing Artifacts Repositories in Software Security Center

After you configure your Fortify ScanCentral DAST environment and enable DAST in the ADMINISTRATION view in Fortify Software Security Center, you can work with artifacts repositories directly in Fortify Software Security Center.

To access artifacts repositories in Fortify Software Security Center:

1. Select **SCANCENTRAL** > **DAST**.
   The Scans view appears.
2. In the left panel, select **Artifacts Repositories**.
   The Artifacts Repositories view appears.

User Role Determines Capabilities

Your user role and permissions in Fortify Software Security Center determine which tasks you can perform on DAST scans, sensors, sensor pools, settings, and scan schedules. Access to artifacts repositories may also be restricted. For more information, see "Permissions in Fortify Software Security Center" on page 40.

Understanding the Artifacts Repositories View

The Artifacts Repositories view displays in a table the repositories that are in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with Tables" on page 124.

The following table describes the columns of information provided for each repository.

Column	Description
Repository Name	Identifies the name of the repository.
Description	Provides a description of the repository.
Repository Type	Indicates the type of repository. Possible values are: • **GitHub** • **GitHub Enterprise** • **JFrog Artifactory**
Root Api Url	Indicates the URL for the location of the repository.
All Application Access	Indicates whether all applications have access to the artifacts in the repository. Options are **Yes** and **No**.
Repository Status	Indicates the current status of the repository, including the migration status during the deletion process. Possible statuses are:

Column	Description
	• **Active** – The repository is currently active and usable in the UI. • **Migrate Artifacts Queued** – A user deleted the repository and chose to migrate artifacts that are being used from the selected repository to the DAST database. • **Migrating Artifacts** – Artifacts are currently migrating from the repository during the deletion process. • **Migrating Artifacts Failed** – Artifact migration failed. You can retry a delete with migration or delete without migration. • **Canceling Migration** – A user canceled the migration and the migration process is currently being stopped. • **Migration Canceled** – A user canceled the migration, stopping the migration and deletion process. The artifacts that were migrated remain in the DAST database. The artifacts repository remains active and usable in the UI.

Understanding the Artifacts Repositories Detail Panel

When you select a repository in the Artifacts Repositories view, the artifacts repository detail panel appears.

The detail panel displays the same information that is displayed in the Artifacts Repositories view for the selected repository, as well as the list of applications to which the repository is assigned.

Understanding the Artifacts Repositories Usage Tab

The detail panel includes a usage tab that shows the usage data for the selected repository. The usage data is categorized into the following groups:

- **Scan Settings** – a list of scan settings that use artifacts from the repository
- **Base Scan Settings** – a list of base scan settings that use artifacts from the repository
- **Scans** – a list of scans that use artifacts from the repository

A group is displayed only if there is usage associated with the group.

The following table describes the data that is provided in each group.

Data	Description
Name	Identifies the name of the settings file or scan.

Data	Description
Settings ID or **Scan ID**	Indicates the integer ID in the ScanCentral DAST database for the settings file or scan.
Property	Identifies the settings property, such as `ScanSettings.LoginMacroBinaryField` or `ScanSettings.TruClientMacroParameters.MacroBinaryField`, that uses the artifact.
Artifact Path	Indicates the path to the artifact in the repository.

Understanding the Artifacts Repositories Logs Tab

ScanCentral DAST records event logs that are displayed in the **LOGS** tab of the detail panel. The event logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with artifacts repositories.

Creating an Artifacts Repository

When you create an artifacts repository, you can assign it to individual applications or to all applications. These assignments determine which applications can use artifacts from the repository.

Before You Begin

You must generate an access token for your repository to configure access to the repository in ScanCentral DAST. The token must have read access at minimum. If additional requirements are needed, refer to your GitHub, GitHub Enterprise, or JFrog Artifactory documentation.

Creating an Artifacts Repository

To create an artifacts repository:

1. On the **Artifacts Repositories** view, select **+ ARTIFACTS REPOSITORY**.
   The ARTIFACTS REPOSITORY CONFIGURATION wizard opens to the Getting Started page.
2. Configure the GENERAL settings as follows:
   a. In the **Repository Name** box, type a name for the repository.
   b. Optionally, in the **Repository Description** box, type a useful description.
3. Click **NEXT**.
   The DETAILS page appears.
4. Continue as follows:

a. From the **Repository Type** list, select the type of repository to configure. Options are:
   - **GitHub**
   - **GitHub Enterprise**

     Important! Be sure to select the correct GitHub type for your repository. ScanCentral DAST will validate connection to the root API URL regardless of the selected type. However, if the wrong type is selected, ScanCentral DAST will not be able to retrieve artifacts from the repository when configuring settings.
   - **JFrog Artifactory**

b. In the **Root API URL** box, type the URL for the location of the repository.
c. In the **Access Token** box, enter the access token that you created for the repository.

5. If you are configuring a GitHub or GitHub Enterprise repository type, provide the following information:
   a. In the **Owner** box, type the name of the owner or owner group for the repository.
   b. In the **Branch** box, type the name of the repository branch to be used.

      Important! If you create a connection to a specific branch and then create a new branch from your original branch, you must edit the previous connection to use the new branch or create a new repository using the new branch.
6. Optionally, click **VALIDATE** to validate the connection using the configuration settings.

   A dialog displays whether the connection to the repository succeeded or failed.
7. Click **NEXT**.

   The Application Select page appears.
8. Do one of the following:
   - To assign the repository to all existing and future applications, slide the toggle to **Grant all application access**.
   - To assign the repository to individual applications, slide the toggle to **Assign individual applications**, and then select individual application check boxes in the **APPLICATIONS** list.

     Note: Only selected applications will have access to the repository. The repository must have at least one assigned application.
9. Click **NEXT**.

   The Review page appears.
10. Click **SAVE**.

Managing Artifacts Repositories

You can edit an existing repository, validate the repository connection, and delete the repository.

Editing a Repository

To edit a repository:

1. In the **Artifacts Repositories** view, click the edit icon (✎) for the repository you want to edit.
   The ARTIFACTS REPOSITORY CONFIGURATION wizard opens to the Getting Started page.
2. To make edits, follow the procedure listed in "Creating an Artifacts Repository" on page 337.

Validating a Repository Connection

You can validate the connection to an existing repository from the artifacts repository details panel.

To validate a repository connection:

1. In the **Artifacts Repositories** view, select the repository whose connection you want to validate.
   The artifacts repository details panel opens.
2. In the details panel, click **VALIDATE**.
   A dialog displays whether the connection to the repository succeeded or failed.

Deleting a Repository

If you delete a repository, ScanCentral DAST prompts you to migrate the artifacts that are referenced in scan settings and base settings from the repository to the DAST database. If you select this option, ScanCentral DAST will migrate only the referenced artifacts from the repository. During migration, ScanCentral DAST validates the files. Depending on your environment and network, it may take some time to migrate.

Caution! When you delete a repository and do not migrate the artifacts, all scan settings and base settings that reference the repository become invalid. Additionally, you cannot restore a deleted repository. You must recreate the artifact repository.

To delete a repository:

1. In the **Artifacts Repositories** view, select the repository to delete.
   The artifacts repository details panel opens.
2. In the details panel, click **DELETE**.
   The DELETE REPOSITORY dialog box opens.
3. Optionally, to see which scan settings, base settings, and scans reference artifacts in the repository, click **See Usage**.
   The information displayed here is the same as in the USAGE tab on the repository details panel. For more information, see "Understanding the Artifacts Repositories Usage Tab" on page 336.
4. By default, the **Migrate artifacts** check box is selected. Do one of the following:

- Leave the check box selected so that all artifacts specified in the usage list will be downloaded to the DAST database before the repository is deleted. With this option, all scan settings and base settings that reference the repository remain valid.
- Clear the check box so that referenced artifacts will *not* be downloaded to the DAST database before the repository is deleted. With this option, all scan settings and base settings that reference the repository become invalid upon deletion.

5. Click **OK**.

   If **Migrate artifacts** is enabled, the migration process will start, followed by the deletion of the repository configuration. For more information, see "Migrating Artifacts" below.

Migrating Artifacts

During the artifacts migration process, a **Cancel Migration** button is displayed in the details panel. Clicking this button cancels the migration, but any artifacts that have been downloaded to the DAST database will remain there. The **Delete** button is not available while artifacts are being migrated. If the migration fails or is canceled, the **Delete** button will become available again. If the migration fails, you can retry migrating artifacts or deleting the repository.

Appendix A: Troubleshooting ScanCentral DAST

If you encounter issues when setting up your Fortify ScanCentral DAST environment or with using it after a successful set up, the following pages might help determine possible causes and solutions.

Locating Log Files

This topic provides information about log files generated by the various DAST components, including where to find logs for each component and how to extract log files if necessary.

Event Log Files in the UI

You can view event log files for scans, settings, scan schedules, and artifacts repositories in their respective detail panels. For more information, see the following:

- "Understanding the Scan Detail Panel" on page 203
- "Understanding the Scan Settings Detail Panel" on page 238
- "Understanding the Schedule Detail Panel" on page 243
- "Understanding the Artifacts Repositories View" on page 335

Log File Names

The log file name is in the format of `YYYY-MM-DD.log`, such as `2023-05-04.log`. There is one log file per day. If you run the Configuration Tool CLI more than once during a single day, the file is appended with new entries for each successive run.

ScanCentral DAST keeps a maximum of seven log files per service. A new log file is created daily or when a log file reaches 100 MB. The 100 MB limit prevents log files from becoming too large.

Extracting Log Files

You must use the Docker `cp` command to copy log files from the DAST API, DAST global service, Fortify WebInspect on Docker, DAST utility service, and DAST Configuration Tool CLI Docker containers to your local file system. If any of the directory paths contain spaces, then you must enclose the path within quotation marks in the Docker `cp` command as shown in the following example:

```
docker cp <ContainerName>:"C:\Program Files\Fortify\<ServiceName>\logs"
<Drive>:\<Directory>
```

Note: The Docker `stop` and `cp` commands in the examples in this topic use the default image names as the container names. Your container names might be different.

API Logs

To obtain log files for the DAST API, you must extract them while the container is *not* running.

To extract the log files:

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

   ```
   docker stop scancentral-dast-api
   ```

   The API container stops.
2. Enter the following command to extract the log files:

   ```
   docker cp scancentral-dast-api:\app\logs <Drive>:\<Directory>
   ```

   The API logs are copied to the directory you specify in the command.

DAST Configuration Tool CLI Logs

You can find log files for the DAST Configuration Tool CLI executable version in the directory where the `DAST.ConfigurationToolCLI.exe` file is located.

When using the DAST Configuration Tool CLI Docker version, mapping the volume to the `C:\app\logs` or `/app/logs` directory on the host system in the Docker run command exposes the log files to your workstation. For more information, see "Using the Windows TAR File" on page 85 and "Using the Linux TAR File" on page 87.

Global Service Logs

To obtain log files for the DAST global service, you must extract them while the container is *not* running.

To extract the log files:

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

   ```
   docker stop scancentral-dast-globalservice
   ```

   The global service container stops.
2. Enter the following command to extract the log files:

   ```
   docker cp scancentral-dast-globalservice:\app\logs <Drive>:\<Directory>
   ```

   The global service logs are copied to the directory you specify in the command.

Scanner Service Logs

If you are using the Fortify WebInspect on Docker image, then you must extract the scanner service logs while the container is *not* running.

To extract the log files:

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

   ```
   docker stop <ContainerName>
   ```

   The container stops.
2. Enter the following command to extract the log files:

   ```
   docker cp <ContainerName>:"C:\Program Files\Fortify\DAST-
   ScannerService\logs" <Drive>:\<Directory>
   ```

   The scanner service logs are copied to the directory you specify in the command.

If you are using a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service, then you can find the scanner service log files in the following location:

```
C:\Program Files\Fortify\DAST-ScannerService\logs
```

Utility Service Logs

To obtain log files for the DAST utility service, you must extract them while the container is *not* running.

To extract the log files:

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

   ```
   docker stop scancentral-dast-utilityservice
   ```

   The utility service container stops.
2. Enter the following command to extract the log files:

   ```
   docker cp scancentral-dast-utilityservice:"C:\Program
   Files\Fortify\DAST-UtilityService\logs" <Drive>:\<Directory>
   ```

   The utility service logs are copied to the directory you specify in the command.

Troubleshooting the Configuration Tool CLI

If the DAST Configuration Tool CLI fails to create and seed the database or fails at any other point, review the tool log file for errors.

CLI Return Codes

When the Configuration Tool CLI finishes, it provides the return codes described in the following table.

Return Code	Description
0	The command completed normally.
-1 or another negative number	An error occurred. Check the log file for specific error messages.

Troubleshooting Tips

The following table describes possible causes and solutions related to the Configuration Tool CLI.

Error or Symptom	Possible Cause	Possible Solution
You configured a proxy in the Configuration Tool CLI, but do not want to access Fortify Software Security Center through the proxy. Now the Configuration Tool CLI cannot validate a connection to Fortify Software Security Center using the host name, machine name, or container name.	The Fortify Software Security Center host name, machine name, or container name is not in the `proxyBypassList` parameter.	Do the following: 1. Add the Fortify Software Security Center host name, machine name, or container name to the `proxyBypassList` parameter in the JSON or YML settings file. For more information, see "Environment Settings" on page 73. 2. If your OS has an `HTTP_PROXY` or `HTTPS_PROXY` environment variable or both, then add the Fortify Software Security Center host name, machine name, or container name in a comma-separated list to the `NO_PROXY` variable. For example, if the Fortify Software Security Center URL is `http://MySSCMachine:8080/ssc`, then the comma-separated list in the `NO_PROXY` variable would be as follows:

Error or Symptom	Possible Cause	Possible Solution
		`localhost,MySSCMachine` If the previous steps do not correct the issue, then use the Fortify Software Security Center IP address instead of the host name, machine name, or container name as follows: • In the `proxyBypassList` parameter in the JSON or YML settings file • In the `sscRootUrl` in the JSON or YML settings file
You configured a proxy in the Configuration Tool CLI, but do not want to access the LIM through the proxy. Now the Configuration Tool CLI cannot validate a connection to the LIM using the host name, machine name, or container name.	A known issue prevents using the host name, machine name, or container name in the `proxyBypassList` parameter.	When configuring ScanCentral DAST settings, do one of the following: • Use the LIM IP address in the `proxyBypassList` parameter in the JSON or YML settings file. • Set the `useProxy` parameter to `false` in the JSON or YML settings file, and configure `HTTP_PROXY` and `NO_PROXY` environment variables instead. For more information, see "Environment Settings" on page 73.

Troubleshooting Upgrade Issues

If you perform an incomplete upgrade, you may encounter compatibility issues when attempting to use Fortify ScanCentral DAST. The following table describes possible causes and solutions related to upgrade issues.

Important! When upgrading your ScanCentral DAST environment, follow these requirements:

- Use the ScanCentral DAST Configuration Tool CLI that is packaged with the version of ScanCentral DAST software that you downloaded. Do *not* use a previous version of the tool.
- Upgrade your Fortify Software Security Center to the current compatible version. For version compatibility, see "Software Integrations for Fortify ScanCentral DAST" in the *Micro Focus Fortify Software System Requirements*.

- Upgrade all ScanCentral DAST components, including the DAST database, DAST API container, DAST Global Service container, DAST Utility Service container, and the Fortify WebInspect on Docker image or the classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service.

Error or Symptom	Possible Cause	Possible Solution
The following error appears in the global service log file: `IsVersionCompatible failed. ProcessName = DAST.GlobalWorkerService, Version = <DAST Version>, Type = DAST`	The global service attempted to start, but it is not compatible with the database. The DAST database was updated, but the global service container was not.	Do one of the following: • Use the `docker-compose.yml` file that the Configuration Tool created when you upgraded your DAST database to upgrade all containers to the same version as your DAST database. For more information, see "Using the Compose File" on page 99. • Use the PowerShell scripts that the Configuration Tool created when you upgraded your DAST database to upgrade all containers to the same version as your DAST database. For more information, see "Using PowerShell Scripts" on page 100.
The following warning appears in the scanner service log file: `Scanner application version is not compatible and will have limited functionality. Version = <dastVersion>`	The scanner service started, but it is not compatible with the database. The DAST database was updated, but the scanner service was not. The service cannot start new scans or create scan settings.	Do one of the following: • Pull and run a compatible version of the Fortify WebInspect on Docker image. For more information, see the *Micro Focus Fortify WebInspect*

Error or Symptom	Possible Cause	Possible Solution
		and OAST on Docker User Guide. • Upgrade your classic Fortify WebInspect installation and upgrade the Fortify ScanCentral DAST sensor service to compatible versions. For more information, see "Using Fortify WebInspect with the Sensor Service" on page 103.
The following error appears in the scanner service log file: `IsVersionCompatible failed. ProcessName = DAST.ScannerWorkerService, Version = <webInspectVersion>, Type = WebInspect`	The scanner service attempted to start, but it is not compatible with the database. The DAST database was updated, but the scanner service was not.	Do one of the following: • Pull and run a compatible version of the Fortify WebInspect on Docker image. For more information, see the *Micro Focus Fortify WebInspect and OAST on Docker User Guide*. • Upgrade your classic Fortify WebInspect installation and upgrade the Fortify ScanCentral DAST sensor service to compatible versions. For more information, see "Using Fortify WebInspect with the Sensor Service" on page 103.
One of the following errors appears in the utility service log file: `IsVersionCompatible failed. ProcessName = DAST.UtilityWorkerService,`	The utility service attempted to start, but it is not compatible with the database. The DAST database was	Do one of the following: • Use the `docker-compose.yml` file that the Configuration Tool

Error or Symptom	Possible Cause	Possible Solution

`Version = <DAST Version>, Type = DAST`
 	
`IsVersionCompatible failed. ProcessName = DAST.Web.API, Version = <DAST Version>, Type = DAST`
	updated, but the utility service was not.	created when you upgraded your DAST database to upgrade all containers to the same version as your DAST database. For more information, see "Using the Compose File" on page 99.
		• Use the PowerShell scripts that the Configuration Tool created when you upgraded your DAST database to upgrade all containers to the same version as your DAST database. For more information, see "Using PowerShell Scripts" on page 100.

Troubleshooting the DAST API

The following table describes possible causes and solutions when you cannot connect to the DAST API from Fortify Software Security Center.

Error or Symptom	Possible Cause	Possible Solution
In Fortify Software Security Center, you receive the following error on the ScanCentral DAST page: "UNABLE TO CONNECT TO SCANCENTRAL DAST API"	ScanCentral DAST might be using an untrusted or self-signed certificate.	To resolve this issue, do one of the following: • Ask your administrator to redeploy using a trusted certificate. • Navigate to the *<ScanCentral DAST API Swagger>*, export the certificate, and add it to your trusted certificate store.

Error or Symptom	Possible Cause	Possible Solution
	The ScanCentral DAST API URL may be configured improperly.	Do the following: 1. Navigate to **Administration** > **Configuration** > **ScanCentral DAST**. 2. Update the URL.
	The ScanCentral DAST API might be inaccessible from the current browser.	Verify the following: • The <*ScanCentral DAST API Swagger*> is not blocked by firewall rules. • The host is resolvable by way of DNS. • The API service is running properly.
	Fortify Software Security Center's content security policy (CSP) might be too restrictive.	Ask your administrator to navigate to **Administration** > **Configuration** > **Security** to adjust the CSP policy.
	Cross-origin resource sharing (CORS) might have been misconfigured when ScanCentral DAST was deployed.	Ask your administrator to run the ScanCentral DAST Configuration Tool to validate CORS is configured properly, and to adjust if necessary. For more information, see "DAST API Settings" on page 63.

Troubleshooting DAST Scans

The following table describes possible causes and solutions when a DAST scan fails to start or fails to complete.

Error or Symptom	Possible Cause	Possible Solution
You are running Fortify WebInspect with the DAST sensor service and a scan status is "Failed to Start."	The WebInspect REST API might not be running.	Verify that the WebInspect REST API is configured and started. For more information, see "Using Fortify WebInspect with the Sensor Service" on page 103.
A scan is stuck in one of the following transitional states: • Queued • Resume Scan Queued • Resume Scan Queued Deny Interval	If the transitional state persists, it could be due to network errors or the scanner service being down. In such cases, the command to resume the scan will not have been sent or the scanner service will not have acknowledged receiving the resume command.	You may see network-related errors in the scanner service log files. Also check the DAST global service log files for any errors. For more information, see "Locating Log Files" on page 341.
		To determine if the scanner service is down: 1. Check the sensor status in the Sensors list. If the status is **Offline**, then correct this issue first. For more information, see "Understanding the Sensors View" on page 224. 2. Ensure that the WebInspect API service is running. For more information, see "Checking and Restarting the WebInspect REST API Service" on page 353. 3. Restart the sensor service. For more information, see "Troubleshooting the Sensor Service" on page 354.

Error or Symptom	Possible Cause	Possible Solution
A scheduled scan fails to start, and the following entry appears in the global service log file: `Failed to process scan schedule. The scanner assigned is no longer active. ScanScheduleId = <Id>, ScannerId = <ScannerId>`	The scheduled scan was configured with the **Use this sensor only** option, but the original sensor container that was assigned to the scheduled scan no longer exists due to upgrading the ScanCentral DAST components.	Edit the scheduled scan settings to use the new sensor container. For more information, see "Editing a Schedule" on page 246.
A scan using a client certificate fails upon startup.	The certificate must be a valid CER, PEM, or PFX format.	Update the scan settings with a valid client certificate.
	The certificate might not be installed on the machine where the sensor service is running or the private key might not be exportable.	Do one of the following: • Install the certificate on the machine where the sensor service is running. • Verify that the certificate's private key is exportable.
	If the certificate is password protected, the password provided might be incorrect.	Update the scan settings with the correct certificate password.

Troubleshooting Alerts

Alerts do not always indicate that there is a scan quality issue. Some alerts may be false positive. However, alerts may provide insight into issues that could adversely affect the scan.

Disabling Alerts

You cannot currently disable alerts in the ScanCentral DAST user interface. For assistance in disabling individual alerts, contact Micro Focus Fortify Customer Support. For more information, see "Preface" on page 24.

Alerts Troubleshooting Table

Important! Any solutions involving changes to scan settings must be made for a future scan. You cannot change the scan settings for the current scan.

The following table describes possible causes and solutions for alerts.

Alert	Possible Cause	Possible Solution
EXCESSIVE LOGIN	The login macro has been played an excessive number of times for the number of requests made. The login credentials may be incorrect or the logout signature may be invalid.	Do one of the following: • Perform troubleshooting procedures on the macro. • Record a new login macro. For more information, see the *Micro Focus Fortify WebInspect Tools Guide*.
REDUNDANT CONTENT	Redundant content has been detected.	You might be able to improve performance in a future scan by enabling redundant page detection. For more information, see "Configuring Redundant Page Detection" on page 182 or "Configuring Redundant Page Detection in Base Settings" on page 290.
RESPONSE TIME	Responses coming from the Web server are taking longer than average or longer than expected. A longer response time may result in a slower scan.	Check your network connectivity or the performance of the application under test (AUT).
WAF DETECTED	A Web application firewall (WAF) signature has been detected.	Disable the WAF that is protecting the AUT.

Checking and Restarting the WebInspect REST API Service

You can check to see whether the WebInspect REST API service is running, and then stop and/or restart the service if needed.

Checking the WebInspect REST API Service Status in a Classic Fortify WebInspect Installation

To check the service status:

- Right-click the **Micro Focus Fortify Monitor** icon.
  If the service is running, you will see the "Stop WebInspect API" option in the menu.

Restarting the Service in a Classic Fortify WebInspect installation

If the service is currently running, but you need to stop it:

- Right-click the **Micro Focus Fortify Monitor** icon, and then click **Stop WebInspect API**.

To restart the service:

- Right-click the **Micro Focus Fortify Monitor** icon, and then click **Start WebInspect API**.

  Note: The start option may not be available until the service has fully stopped.

Checking the WebInspect REST API Service Status in Fortify WebInspect on Docker

To check the service status:

- In Windows PowerShell, enter the following command:

```
Get-Service -Name "WebInspect API"
```

Restarting the Service for Fortify WebInspect on Docker

Tip: If you need to restart both the WebInspect API and the sensor service, restarting the container restarts both.

If the service is currently running, but you need to stop it:

- In Windows PowerShell, enter the following command:

  ```
  net stop "WebInspect API"
  ```

To start the service again:

- In Windows PowerShell, enter the following command:

  ```
  net start "WebInspect API"
  ```

Troubleshooting the Sensor Service

The following table describes possible causes and solutions when the sensor service fails to start.

Error or Symptom	Possible Cause	Possible Solution
The sensor service fails to start, and the following entry appears in the scanner service log file: `The remote certificate is invalid because of errors in the certificate chain: UntrustedRoot`	Encrypted communication is used for the DAST API service, but the API SSL certificate is not installed in the Trusted Store on the DAST sensor service machine.	1. Copy the API SSL certificate from the Configuration Tool artifacts. 2. Add the certificate to the Trusted Store on the machine where the DAST sensor service will run. For more information, see "Using Fortify WebInspect with the Sensor Service" on page 103.

You can check to see whether the sensor service is running, and then stop and/or restart the service if needed, as described in the following paragraphs.

Checking the Sensor Service Status in a Classic Fortify WebInspect Installation

To check the service status:

1. Open Windows Services Manager (`services.msc`). For more information, refer to your Windows documentation.
2. In Windows Services Manager, look for the service named **ScannerWorkerService**.
3. Check the **Status** column.

Restarting the Sensor Service in a Classic Fortify WebInspect Installation

If the service is currently running, but you need to stop it:

- In Windows Services Manager, right-click the service named **ScannerWorkerService**, and then select **Stop**.

To restart the service:

- In Windows Services Manager, right-click the service named **ScannerWorkerService**, and then select **Start**.

Checking the Sensor Service Status in Fortify WebInspect on Docker

To check the service status:

- In Windows PowerShell, enter the following command:

  ```
  get-process -Name "DAST.ScannerWorkerService"
  ```

  If the service is running, you will see statistics for a process named "DAST.ScannerWorkerService."
  If the service is not running, you will get the following error:

  ```
  get-process : Cannot find a process with the name "WebInspect". Verify the
  process name and call the cmdlet again.
  ```

Restarting the Sensor Service in Fortify WebInspect on Docker

Tip: If you need to restart both the WebInspect API and the sensor service, restarting the container restarts both.

If the service is currently running, but you need to stop it:

- In Windows PowerShell, enter the following command:

  ```
  stop-process -Name "DAST.ScannerWorkerService.exe"
  ```

To start the service again:

- In Windows PowerShell, enter the following command:

  ```
  start-process -Name "DAST.ScannerWorkerService.exe"
  ```

Appendix B: Scanning with a Postman Collection

You can use your existing Postman automation test scripts, also known as collections, to conduct scans of REST API applications. This section provides general information about Postman, tips for creating a good Postman collection, and instructions for manually configuring dynamic tokens for authentication.

For information about configuring a Postman scan, see "Configuring an API Scan" on page 151.

What is Postman?

Postman is an API development environment that allows you to design, collaborate on, and test APIs. Postman lets you create collections for your API calls, where each collection can be organized into subfolders and multiple requests. You can import and export collections, making it easy to share files across your development and testing environment. Using a Collection Runner such as Newman, tests can be run in multiple iterations, saving time on repetitive tests.

Benefits of a Postman Collection

A REST API application does not expose all the endpoints in a format that a human with a browser or an automated tool can consume. It is often simply a collection of endpoints that accepts various posts, puts, and gets with a specific set of request data. To successfully audit these endpoints, the ScanCentral DAST sensor needs to understand key details about the API. A well-defined Postman collection can expose these endpoints so that the sensor can audit the API application.

Known Limitations with Postman Variables

ScanCentral DAST does not support Global variables or Data variables in Postman. However, it does support Environment and Collection variables, as well as Local variables in a collection.

As a workaround, you can specify Global variables and Data variables in an Environment, which is a set of variables that you can use in your Postman requests.

Postman Prerequisites

A Postman collection version 2.0 or 2.1 is required for conducting scans in ScanCentral DAST. The remaining prerequisite software is installed on the Fortify WebInspect Docker image.

However, if you are using a classic Fortify WebInspect installation with the Fortify ScanCentral DAST sensor service, you must install Newman command-line collection runner, Node.js, and Node Package Manager (NPM). For specific version information and additional instructions, see the *Micro Focus Fortify Software System Requirements*.

Tips for Preparing a Postman Collection

This topic provides tips for creating a good Postman collection.

Ensure Valid Responses

To get valid responses, the collection must be complete and executable. Requests must include:

- A valid request URL
- The correct HTTP method (POST, GET, PUT, PATCH, or DELETE)
- Valid parameter data that allows proper exercising of the API

  For example, if you have a “name” parameter, then you must provide actual sample data such as "King Lear" or "Hamlet," rather than the default data type “string.”

Order of Requests

Remember that the order of operations or requests is important. For example, you must create (or POST) sample data to a parameter before you can do a GET or a DELETE operation on the data.

Tip: To avoid URL errors while running the collection in the ScanCentral DAST sensor, after bundling the API requests in the correct order in your collection, save each request individually by clicking the request and then clicking **Save**.

Handling Authentication

If your API requires authentication, you must configure it in the Postman collection. Follow these guidelines when configuring authentication:

- The user credentials must be current and not expired.
- If you use an environment to specify authentication information, select the type of authentication environment in the Postman collection.
- It is possible that not all requests in the collection require authentication or not all requests require the same type of authentication. If this is the case in your collection, be sure to specify the appropriate authentication type for each request in the collection.

  Important! If session state is lost while using various authentication types in a scan, it will not be restored correctly. For proper restoration of session state, use a login macro or Postman login collection with a single type of authentication.

Using Static Authentication

When using static authentication, you must hard-code user credentials as a name/value pair in the Postman collection. When the ScanCentral DAST sensor parses the collection file, it determines the type of authentication being used and retrieves the key name and value from the collection. These values are then added to the scan settings.

The ScanCentral DAST sensor supports the following types of static authentication:

- API Key
- Basic
- Bearer Token
- Digest
- NTLM
- Oauth 1.0
- Oauth 2.0

Using Dynamic Authentication

When using dynamic authentication, you must store the Bearer token or API key authentication variables in either a Postman environment file or a collection file. For example, a Bearer Token may use a variable such as `{{bearerToken}}`.

You must use regular expressions in a response state rule to dynamically supply the Bearer token or API key during the scan. The response state rule provides search and replace options that enable the token or key to be retrieved from a response and then used in future sessions.

Using a Postman Login Macro

You can provide a login macro and a workflow macro in the form of Postman collection files when configuring scan settings. For example, you can specify a login macro file such as `LoginBearer.json`. When using a login macro, however, you must also specify a logout condition, such as the regular expression `The\stoken\sis\snot\svalid`.

Postman Auto-configuration

Auto-configuration for static authentication is supported when the authentication values are known, such as when the username and password are hard-coded in the authentication section of the collection. If auto-configuration is not disabled, ScanCentral DAST checks the authentication portion of the collection file for valid values that are then applied to the scan settings.

Auto-configuration for dynamic authentication attempts to automatically provide a login macro and response state rule. It is useful when the Bearer token or API key is stored in a variable. If successfully validated, the authentication sessions are added to the sessions table. If a Bearer token was detected

but a stable configuration was not created, then no authentication sessions are added to the sessions table.

Important! Auto-configuration for dynamic authentication works only for simple cases using Bearer token authentication.

If auto-configuration fails, you must manually configure authentication. For more information, see "Manually Configuring Postman Login for Dynamic Tokens" below.

Sample Postman Scripts

Sample code for leveraging the Postman API can be found at https://github.com/fortify/WebInspectAutomation.

A sample Postman collection is available for download on the Fortify repository on GitHub at https://github.com/fortify/WebInspectAutomation/tree/master/PostmanSamples.

Manually Configuring Postman Login for Dynamic Tokens

This topic describes how to configure dynamic authentication manually if auto-configuration fails for a Postman scan. Dynamic authentication uses dynamic tokens.

What are Dynamic Tokens?

Dynamic tokens are authentication tokens that are generated by software and are unique for each instance of authentication. Tokens can be created for a short period of time, and each instance is renewed individually.

Before You Begin

You must know the following to configure manual login:

- The type of authentication used in your application (such as Bearer, API key, OAuth1.0, OAuth 2.0, Cookie)
- How to create regular expression search arguments

Process Overview

The process to manually configure login is described in the following table.

Stage	Description
1.	Identify and isolate the login request or requests in a separate Postman collection. For more information, see "Identifying and Isolating the Login Request" below.
2.	Create a logout condition regular expression. For more information, see "Creating a Logout Condition with Regular Expressions" below
3.	Create a response state rule. For more information, see: • "Creating a Response State Rule for a Bearer Token" on the next page • "Creating a Response State Rule for an API Key" on the next page **Note:** A response state rule is not needed for cookie session management.

Identifying and Isolating the Login Request

To identify and isolate the login request:

1. Examine the Postman collection contents to identify the login request.

   Tip: Typically, the login request is the first request in the Postman collection that obtains an authentication token. However, authentication could involve several requests.

2. Copy this request or multiple requests.
3. Paste the request(s) in a separate file.
4. Save the file as a Postman collection.

Creating a Logout Condition with Regular Expressions

To create a logout condition:

1. Find several requests that require authentication.
2. Do one of the following:
   - For a bearer token, replace the auth token with an incorrect value and send it to the application.
   - For an API key, send an incorrect APIKey value to the application.
3. Use the reply from these requests to create a regular expression that matches these responses and does not match a valid session.

   For example, if you see the word “unauthorized” in most cases, then it is the best word to use in the regular expression, such as:

   ```
   [STATUSCODE]200 AND [BODY]unauthorized
   ```

If an incorrect APIKey value gets a reply of “{"status": "Access Deny"}”, then the best regular expression would be:

```
[BODY]Access\sDeny
```

Creating a Response State Rule for a Bearer Token

To create a response state rule for a bearer token, you must create two regular expressions.

The first regular expression searches all responses for an authentication token update. Typically, this token will be in response to the login request that was identified in Stage 1 of the process.

For example, in the following response, we see a reference to "token."

```
"{"success":true,"message":"Authentication
      successful!","token":"eyJhbGciOiJIUzI1NiIs
      InR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluI
      iwiaWF0IjoxNTg1NzQzNzkzLCJleHAiOjE1ODU3NDc
      zOTN9.i8uXa20JQt00tlOjd1twRD76jTnsG-0xiU97
      QWy6jkg"}"
```

For this response, we can create the following regular expression:

```
"token":"(?<Token>[-a-zA-Z0-9._~+/]+?=*)"}$
```

In this regular expression, the `(?<Token>[-a-zA-Z0-9._~+/]+?=*)` identifies the value of the token.

Note: XML uses character escaping. When you use regular expressions that include < and > symbols in XML format, the < symbol escapes with `<` and the > symbol escapes with `>`.

The second regular expression indicates where to store this token. For a bearer token, it will be in the “Authorization: Bearer ….” header.

The following is an example for a bearer token:

```
"Authorization:\sBearer\s(?<Token>[^\r\n]*)\r\n"
```

In this second regular expression, the `(?<Token>[^\r\n]*)` identifies the value that should be replaced with the value from the first regular expression.

Creating a Response State Rule for an API Key

To create a response state rule for an API key, you must create two regular expressions.

The first regular expression searches all responses for an authentication token update. Typically, this token will be in response to the login request that was identified in Stage 1 of the process.

For example, assume that you have a header API key type of auth. A request sends the username and password to the path "/Login" and returns a response similar to the following:

```
"{"success":true,"APIToken":
      "tp8989ieupgrjynsfbnfgh9ysdopfghsprohjo"}"
```

All protected requests send an "APIKey: ...." header to authorize access.

For this response, we can create the following regular expression:

```
"APIToken":"(?<APIToken>[a-zA-Z0-9]+?)"}$
```

Note: XML uses character escaping. When you use regular expressions that include < and > symbols in XML format, the < symbol escapes with `<` and the > symbol escapes with `>`.

The second regular expression indicates where to store this token. For an APIKey, it could be a custom header name and value or a custom query parameter name and value.

```
APIKey:\s(?<APIToken>[^\r\n]*)\r\n
```

Appendix C: Reference Lists

The following pages provide a list of policies that are available for use in Fortify ScanCentral DAST, as well as HTTP status codes for reference.

Policies

A policy is a collection of vulnerability checks and attack methodologies that the Fortify WebInspect sensor deploys against a Web application. Each policy is kept current through SmartUpdate functionality, ensuring that scans are accurate and capable of detecting the most recently discovered threats.

Fortify ScanCentral DAST contains the following packaged policies that you can use to determine the vulnerability of your Web application.

Note: This list might not match the policies that you see in your product. SmartUpdate might have added or deprecated policies since this document was produced.

Best Practices

The Best Practices group contains policies designed to test applications for the most pervasive and problematic web application security vulnerabilities.

- **API**: This policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.
- **CWE Top 25 *<version>***: The Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25) is a list created by MITRE. The list demonstrates the most widespread and critical software weaknesses that can lead to vulnerabilities in software.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **Best Practices** group.
- **General Data Protection Regulation (GDPR)**: The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and provides a framework for organizations on how to handle personal data. The GDPR articles that pertain to application security and require businesses to protect personal data during design and development of their products and services

are as follows:

- Article 25, data protection by design and by default, which requires businesses to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.
- Article 32, security of processing, which requires businesses to protect their systems and applications from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

This policy contains a selection of checks to help identify and protect personal data specifically related to application security for the GDPR.

- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 - (NIST SP 800-53 Rev.5) provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. This policy contains a selection of checks that must be audited to meet the guidelines and standards of NIST SP 800-53 Rev.5.
- **OWASP Application Security Verification Standard (ASVS)**: The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test, and verify secure applications.

  This policy uses OWASP ASVS suggested CWE mapping for each category of SecureBase checks to include. Because CWE is a hierarchical taxonomy, this policy also includes checks that map to additional CWEs that are implied from OWASP ASVS suggested CWE using a "ParentOf" relationship.
- **OWASP Top 10 *<year>***: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about the most critical web application security flaws. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. Multiple releases of the OWASP Top Ten policy may be available. For more information, consult the OWASP Top Ten Project.
- **SANS Top 25*<year>***: The SANS Top 25 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software. These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to take over the software completely, steal data, or prevent the software from working altogether.
- **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers.

By Type

The By Type group contains policies designed with a specific application layer, type of vulnerability, or generic function as its focus. For instance, the Application policy contains all checks designed to test an application, as opposed to the operating system.

- **Aggressive Log4Shell**: This policy performs a comprehensive security assessment of your web application for JNDI Reference injections in vulnerable versions of Apache Log4j libraries. In vulnerable versions, Log4j does not restrict JNDI features. This allows an attacker who can control log messages to inject JNDI references that point to an attacker-controlled server. This can lead to remote code execution on the vulnerable target. Compared with other policies that include Log4Shell agent, this policy performs a more accurate and decisive job, but produces a significant number of requests and has a longer scan time.
- **Aggressive SQL Injection**: This policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs a more accurate and decisive job, but has a longer scan time.
- **Apache Struts**: This policy detects supported known advisories against the Apache Struts framework.
- **Blank**: This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Client-side**: This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.
- **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.
- **Cross-Site Scripting**: This policy performs a security scan of your web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a website to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **By Type** group.
- **Mobile**: A mobile scan detects security flaws based on the communication observed between a mobile application and the supporting backend services.

- **NoSQL and Node.js**: This policy includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL, such as MongoDB, and server side infrastructures based on JavaScript, such as Node.js.
- **OAST**: This policy includes all checks that use Out-of-band Application Security Testing (OAST) technology in scanning logic.
- **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **PCI DSS 4.0**: The Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0) provides a baseline of technical and operational requirements designed to protect account data. This policy contains a selection of checks that need to be audited to meet the secure coding requirements of PCI DSS 4.0.
- **PCI Software Security Framework *<version>* (PCI SSF *<version>*)**: The PCI SSF provides a baseline of requirements and guidance for building secure payment systems and software that handle payment transactions. This policy contains a selection of checks that must be audited to meet the secure coding requirements of PCI SSF.
- **Privilege Escalation**: The Privilege Escalation policy scans your web application for programming errors or design flaws that allow an attacker to gain elevated access to data and applications. The policy uses checks that compare responses of identical requests with different privilege levels.
- **Server-side**: This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQL Injection**: The SQL Injection policy performs a security scan of your web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database.
- **Transport Layer Security**: This policy performs a security assessment of your web application for insecure SSL/TLS configurations and critical transport layer security vulnerabilities, such as Heartbleed, Poodle, and SSL Renegotiation attacks.
- **WebSocket**: This policy detects vulnerabilities related to WebSocket implementation in your application.

Custom

The Custom group contains all user-created policies and any custom policies modified by a user.

Hazardous

The Hazardous group contains a policy with potentially dangerous checks, such as a denial-of-service attack, that could cause production servers to fail. Use this policy against non-production servers and systems only.

- **All Checks**: An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the database. This scan includes all checks that are listed in the compliance reports that are available in Fortify web application and web services vulnerability scan products. This includes checks for known and unknown vulnerabilities at the web server, web application server, and web application layers.

  Caution! An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. Fortify strongly recommends using the All Checks policy only in test environments.

Deprecated Checks and Policies

The following policies and checks are deprecated and are no longer maintained.

- **Application (Deprecated)**: The Application policy performs a security scan of your web application by submitting known and unknown web application attacks, and only submits specific attacks that assess the application layer. When performing scans of enterprise level web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your scan in terms of speed and memory usage.
- **Assault (Deprecated)**: An assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web application server, and web application layers. An assault scan includes checks that can create denial-of-service conditions. It is strongly recommended that assault scans only be used in test environments.
- **Deprecated Checks**: As technologies go end of life and fade out of the technical landscape it is necessary to prune the policy from time to time to remove checks that are no longer technically necessary. Deprecated checks policy includes checks that are either deemed end of life based on current technological landscape or have been re-implemented using smart and efficient audit algorithms that leverage latest enhancements of core WebInspect framework.
- **Dev (Deprecated)**: A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web application layer only. The policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **OpenSSL Heartbleed (Deprecated)**: This policy performs a security assessment of your web application for the critical TLS Heartbeat read overrun vulnerability. This vulnerability could potentially disclose critical server and web application data residing in the server memory at the time a malicious user sends a malformed Heartbeat request to the server hosting the site.
- **OWASP Top 10 Application Security Risks - 2010 (Deprecated)**: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about what the most critical web application security flaws are. Adopting the OWASP Top 10 is

perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. This policy includes elements specific to the 2010 Top Ten list. For more information, consult the OWASP Top Ten Project.

- **Platform (Deprecated)**: The Platform policy performs a security scan of your web application platform by submitting attacks specifically against the web server and known web applications. When performing scans of enterprise-level web applications, use the Platform Only policy in conjunction with the Application Only policy to optimize your scan in terms of speed and memory usage.
- **QA (Deprecated)**: The QA policy is designed to help QA professionals make project release decisions in terms of web application security. It performs checks for both known and unknown web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
- **Quick (Deprecated)**: A Quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the web server, web application server and web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **Safe (Deprecated)**: A Safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown vulnerabilities at the web server, web application server and web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.
- **Standard (Deprecated)**: Standard (Deprecated) policy is copy of the original standard policy before it was revamped in R1 2015 release. A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web application server and web application layers. A standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

HTTP Status Codes

The following list of status codes was extracted from the Hypertext Transfer Protocol version 1.1 standard (RFC 2616). You can find more information at http://www.w3.org/Protocols/.

Code	Definition
100	Continue
101	Switching Protocols
200 OK	Request has succeeded
201 Created	Request fulfilled and new resource being created
202 Accepted	Request accepted for processing, but processing not completed.
203 Non-Authoritative	The returned metainformation in the entity-header is not the definitive

Code	Definition
Information	set as available from the origin server, but is gathered from a local or a third-party copy.
204 No Content	The server has fulfilled the request but does not need to return an entity-body, and might want to return updated metainformation.
205 Reset Content	The server has fulfilled the request and the user agent should reset the document view which caused the request to be sent.
206 Partial Content	The server has fulfilled the partial GET request for the resource.
300 Multiple Choices	The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent-driven negotiation information (section 12) is being provided so that the user (or user agent) can select a preferred representation and redirect its request to that location.
301 Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.
302 Found	The requested resource resides temporarily under a different URI.
303 See Other	The response to the request can be found under a different URI and should be retrieved using a GET method on that resource.
304 Not Modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server should respond with this status code.
305 Use Proxy	The requested resource MUST be accessed through the proxy given by the Location field.
306 Unused	Unused.
307 Temporary Redirect	The requested resource resides temporarily under a different URI.
400 Bad Request	The request could not be understood by the server due to malformed syntax.
401 Unauthorized	The request requires user authentication. The response MUST include a WWW-Authenticate header field (section 14.47) containing a challenge applicable to the requested resource.

Code	Definition
402 Payment Required	This code is reserved for future use.
403 Forbidden	The server understood the request, but is refusing to fulfill it.
404 Not Found	The server has not found anything matching the Request-URI.
405 Method Not Allowed	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.
406 Not Acceptable	The resource identified by the request is only capable of generating response entities which have content characteristics not acceptable according to the accept headers sent in the request.
407 Proxy Authentication Required	This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.
408 Request Timeout	The client did not produce a request within the time that the server was prepared to wait.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server and no forwarding address is known.
411 Length Required	The server refuses to accept the request without a defined Content-Length.
412 Precondition Failed	The precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.
413 Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
414 Request-URI Too Long	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415 Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.

Code	Definition
416 Requested Range Not Satisfiable	A server should return a response with this status code if a request included a Range request-header field (section 14.35), and none of the range-specifier values in this field overlap the current extent of the selected resource, and the request did not include an If-Range request-header field.
417 Expectation Failed	The expectation given in an Expect request-header field (see section 14.20) could not be met by this server, or, if the server is a proxy, the server has unambiguous evidence that the request could not be met by the next-hop server.
500 Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.
501 Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
502 Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503 Service Unavailable	The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
504 Gateway Timeout	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server specified by the URI (e.g., HTTP, FTP, LDAP) or some other auxiliary server (e.g., DNS) it needed to access in attempting to complete the request.
505 HTTP Version Not Supported	The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.

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 Micro Focus Fortify 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 Configuration and Usage Guide (Fortify ScanCentral DAST 23.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!