
Micro Focus Fortify ScanCentral DAST

Software Version: 20.2.0
Windows®

Configuration and Usage Guide

Document Release Date: December 2020
Software Release Date: November 2020



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2020 Micro Focus or one of its affiliates

Trademark Notices

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

Documentation Updates

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

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

This document was produced on December 01, 2020. 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	10
Contacting Micro Focus Fortify Customer Support	10
For More Information	10
About the Documentation Set	10
 Change Log	 11
 Chapter 1: Introduction	 12
What is ScanCentral DAST?	12
Software Security Center	12
LIM	12
DAST API	13
DAST Global Service	13
ScanCentral DAST Database	13
WebInspect Sensor	13
Permissions in Fortify Software Security Center	13
Related Documents	14
All Products	15
Micro Focus Fortify ScanCentral DAST	15
Micro Focus Fortify Software Security Center	16
Micro Focus Fortify WebInspect	16
 Chapter 2: Setting Up the ScanCentral DAST Environment	 19
Before You Begin	19
Understanding the Installation Process	19
Setting Up Docker	21
Configuring the Database and Core Containers	21
About the ScanCentral DAST Configuration Tool	22
Installing and Launching the Configuration Tool	22
What's Next?	22
Configuring the Database Connection	22
Configuring the DBO-level Account	23

Configuring the Standard Account	23
What's Next?	23
Initializing the Database	24
Using the Default SecureBase	24
Using a Local SecureBase	24
What's Next?	24
Configuring SSL	24
About the Certificate Path	24
Generating an API SSL Certificate	25
Using an Existing Certificate	25
Not Using SSL	25
What's Next?	26
Configuring ScanCentral DAST Settings	26
Configuring SSC Settings	26
Configuring API Settings	26
Configuring LIM Settings	27
Configuring Proxy Settings	28
Creating a Sensor Service Token	28
Allowing Untrusted Certificates	28
Retaining Completed Scans on Sensor	28
Changing the SmartUpdate URL	29
Changing the Licensing URL	29
What's Next?	29
Generating Launch Artifacts	29
Understanding the Launch Artifacts	29
Generating the Launch Artifacts	30
What's Next?	30
Using the Compose File	30
Using PowerShell Scripts	31
Using One Script	31
Using Two Scripts	32
Using Fortify WebInspect on Docker	33
Using Fortify WebInspect with the Sensor Service	33
Important Information About Licenses	33
Important Information About Windows Server 2016	34
Configuring the Fortify WebInspect REST API	34
Installing and Configuring the DAST Sensor Service	36

Chapter 3: Understanding the User Interface	38
ScanCentral DAST User Interface	38
Filtering Data in Columns	38
Guidelines	39
Filtering by Application, Version, Name, or URL	39
Filtering by Date, Scan Status, or Scan Type	39
Clearing the Filter	40
Sorting Data in Columns	41
Chapter 4: Configuring a DAST Scan	42
What is a Scan?	42
Accessing Settings Configuration from Software Security Center	42
Accessing from the DAST Scans List	42
Accessing from the Settings List	43
What's Next?	43
Getting Started	43
What's Next?	44
Configuring a Standard Scan	44
What's Next?	45
Configuring a Workflow-driven Scan	46
Types of Macros Supported	46
Configuring a Workflow-driven Scan	46
What's Next?	47
Configuring an API Scan	47
What's Next?	49
Configuring Proxy Settings	49
What's Next?	51
Configuring Authentication	51
Configuring Site Authentication	51
Downloading the Macro Recorder Tool	51
Configuring Network Authentication	51
What's Next?	53
Configuring Scan Details	53
What's Next?	54
Adding and Managing Allowed Hosts	54

Adding Allowed Hosts	54
Editing or Removing Hosts	55
Scanning Single-page Applications	55
Technology Preview	55
The Challenge of Single-page Applications	55
Configuring SPA Support	56
Using Traffic Viewer (Traffic Monitor)	56
Proxy Server Included	56
Option Must be Enabled	56
Enabling Traffic Viewer (or Traffic Monitor)	56
Creating and Managing Exclusions	56
Creating Exclusions	57
Exclusion Examples	57
Editing or Removing Exclusions	58
Understanding and Creating Inclusive Exclusions	58
Understanding Inclusive Exclusion Regular Expressions	58
Example One	59
Example Two	59
Reviewing Scan Settings	60
Saving the Settings to Software Security Center	61
Scheduling a Scan	61
Running a Scan	63
Using the Scan Settings in the DAST API	63
Accessing the DAST API Swagger UI	63
Chapter 5: Working with DAST Scans	64
Accessing DAST Scans in Software Security Center	64
User Role Determines Capabilities	64
Understanding the Scans List	64
Understanding the Scan Detail Panel	66
Findings by Severity	67
Additional Scan Details	67
Working with Active Scans	68
Pausing a Scan	68
Stopping a Scan	68
Resuming a Scan	69
Re-importing a Scan	69

Managing the DAST Scans List	69
Starting a New Scan	69
Refreshing the Scans List	70
Publishing to Fortify Software Security Center	70
Deleting a Scan	70
Downloading DAST Scans, Settings, and Logs	70
File Types Available	71
Downloading a File	72
Chapter 6: Working with DAST Sensors	73
Accessing DAST Sensors in Software Security Center	73
User Role Determines Capabilities	73
Understanding the Sensor List	73
Understanding the Sensor Detail Panel	74
Enabling or Disabling Sensors	75
Facts About Disabled Sensors	75
Enabling or Disabling a Sensor	75
Chapter 7: Working with DAST Sensor Pools	76
Accessing DAST Sensor Pools in Software Security Center	76
User Role Determines Capabilities	76
Understanding the Sensor Pools List	76
Understanding the Pool Detail Panel	77
Creating a DAST Sensor Pool	77
Managing Sensor Pools	78
Facts About Managing Sensor Pools	78
Editing a Sensor Pool	78
Refreshing the Pools List	78
Deleting a Sensor Pool	79
Changing the Default Sensor Pool	79
Chapter 8: Working with DAST Settings	80
Accessing DAST Settings in Software Security Center	80
User Role Determines Capabilities	80
Understanding the Settings List	80

Understanding the Settings Detail Panel	81
Managing Settings	82
Creating New Settings	82
Editing Settings	82
Downloading Settings	83
Deleting Settings	83
Copying the Settings ID for Use in the API	83
Chapter 9: Working with DAST Scan Schedules	85
Accessing DAST Scan Schedules in Software Security Center	85
User Role Determines Capabilities	85
Understanding the Scan Schedules List	85
Understanding the Schedule Detail Panel	86
Managing Schedules	86
Creating a New Schedule	86
Editing a Schedule	87
Enabling or Disabling Schedules	87
Deleting a Schedule	87
Appendix A: Troubleshooting ScanCentral DAST	89
Locating Log Files	89
Log File Names	89
API Logs	89
Global Service Logs	89
Scan Configuration Tool Logs	90
Scanner Service Logs	90
Troubleshooting the Configuration Tool	90
Configuration Tool Fails to Launch	90
Troubleshooting the DAST API	91
Troubleshooting DAST Scans	92
Appendix B: Reference Lists	93
Policies	93
Best Practices	93
By Type	94
Custom	96

Hazardous	96
Deprecated Checks and Policies	96
Send Documentation Feedback	98

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

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

For More Information

For more information about Fortify software products:

<https://www.microfocus.com/solutions/application-security>

About the Documentation Set

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

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

Change Log

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

Software Release / Document Version	Changes
20.2.0 / December 4, 2020	Updated: <ul style="list-style-type: none">• Permissions for Application Security Tester and Security Lead to include running scans from existing settings templates. See "Permissions in Fortify Software Security Center" on page 13.• Installation process to include the trailing slash "/" after "/api" in the ScanCentral DAST URL in the ADMINISTRATION view in Fortify Software Security Center. See "Understanding the Installation Process" on page 19.• Configuring ScanCentral DAST settings to remove reference of trailing "/api". See "Configuring API Settings" on page 26.
20.2.0	Initial release of product.

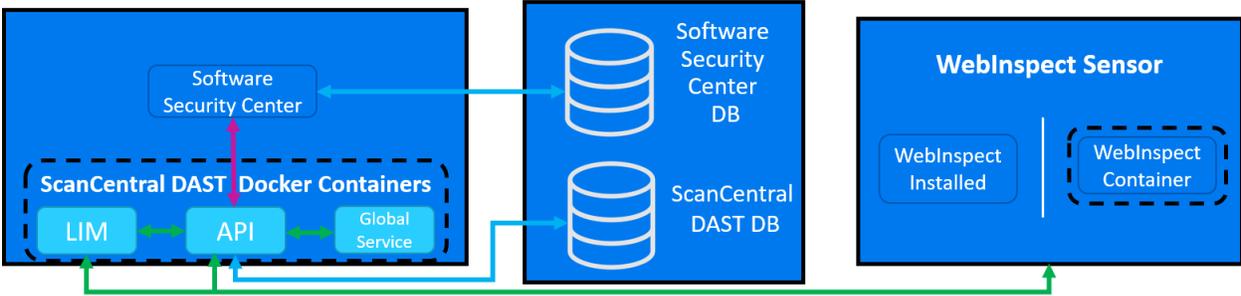
Chapter 1: Introduction

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.

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.

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, and scan schedules. 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 container 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*.

DAST API

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

The container name is `scancentral-dast-api`.

DAST Global Service

The ScanCentral DAST Global Service Docker container does the following:

- Starts scans (including scheduled scans)
- Communicates messages to and from the ScanCentral DAST Sensor Service
- Imports scan results to the Fortify Software Security Center database
- Performs additional background tasks

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

The container name is `scancentral-dast-globalservice`.

ScanCentral DAST Database

Configuration settings for ScanCentral DAST are stored in the ScanCentral DAST database. The ScanCentral DAST REST API and ScanCentral DAST Global Service connect to the database on start up to retrieve configuration settings.

WebInspect Sensor

The Fortify WebInspect sensor is either a Docker container or a Windows computer that runs the ScanCentral DAST Sensor Service and a Fortify WebInspect sensor. The sensor does the following:

- Starts and runs scans
- Reports scan statistics to the ScanCentral DAST Global Service
- Uploads the scan to the ScanCentral DAST Rest API

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

Permissions in Fortify Software Security Center

The permissions designated by your user role in Fortify Software Security Center determine the types of tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, and scan

schedules. The following table describes the default 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 settings templates	x	x		x	
Download artifacts (settings, scans, and logs)	x	x		x	

Related Documents

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

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

All Products

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

Document / File Name	Description
<i>About Micro Focus Fortify Product Software Documentation</i> About_Fortify_Docs_<version>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. Note: This document is included only with the product download.
<i>Micro Focus Fortify Software System Requirements</i> Fortify_Sys_Reqs_<version>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Micro Focus Fortify Software Release Notes</i> FortifySW_RN_<version>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
<i>What's New in Micro Focus Fortify Software <version></i> Fortify_Whats_New_<version>.pdf	This document describes the new features in Fortify Software products.

Micro Focus Fortify ScanCentral DAST

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

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

Micro Focus Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at

<https://www.microfocus.com/documentation/fortify-software-security-center>.

Document / File Name	Description
<i>Micro Focus Fortify Software Security Center User Guide</i> SSC_Guide_<version>.pdf	<p>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.</p> <p>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.</p>

Micro Focus Fortify WebInspect

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

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

Document / File Name	Description
<i>Micro Focus Fortify WebInspect Installation Guide</i> WI_Install_<version>.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
<i>Micro Focus Fortify WebInspect User Guide</i> WI_Guide_<version>.pdf	<p>This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services.</p> <p>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</p>

Document / File Name	Description
	<p>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.</p>
<p><i>Micro Focus Fortify WebInspect on Docker User Guide</i> WI_Docker_Guide_<version>.pdf</p>	<p>This document describes how to download, configure, and use Fortify WebInspect that is available as a container image on the Docker platform. This full version of the product is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center.</p>
<p><i>Micro Focus Fortify WebInspect Tools Guide</i> WI_Tools_Guide_<version>.pdf</p>	<p>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.</p>
<p><i>Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide</i> LIM_Guide_<version>.pdf</p>	<p>This document describes how to install, configure, and use the Fortify WebInspect License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.</p>
<p><i>Micro Focus Fortify WebInspect Agent Installation Guide</i> WI_Agent_Install_<version>.pdf</p>	<p>This document describes how to install the Fortify WebInspect Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.</p>
<p><i>Micro Focus Fortify WebInspect Agent Rulepack Kit Guide</i> WI_Agent_Rulepack_Guide_<version>.pdf</p>	<p>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</p>

Document / File Name	Description
	static ones.

Chapter 2: Setting Up the ScanCentral DAST Environment

You must install the DAST API and DAST Global Service containers on a VM, and each Fortify WebInspect sensor service on its own, separate VM. To assist you in setting up these Fortify ScanCentral DAST components, Fortify engineers have created a configuration tool, or wizard, that guides you through the process and prompts you for the information needed for a successful implementation.

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.
 - 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: <ul style="list-style-type: none">• Fortify ScanCentral DAST Server License (server-type license)• Fortify WebInspect Concurrent License
2.	Do the following:

Stage	Description
	<ol style="list-style-type: none"> 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. <p>For information about how to install the LIM and add licenses, see the <i>Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide</i>.</p>
3.	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Download and deploy Fortify Software Security Center 20.2.0 from the Micro Focus SSO download portal. 2. Create user accounts for users who will access Fortify ScanCentral DAST. <p>For information about how to install and configure Fortify Software Security Center, see the <i>Micro Focus Fortify Software Security Center User Guide</i>.</p>
4.	<p>Set up Docker on the host that will run the core ScanCentral DAST containers (DAST API and DAST Global Service). For more information, see "Setting Up Docker" on the next page.</p>
5.	<p>Download the ScanCentral DAST package from the Micro Focus SSO download portal.</p>
6.	<p>Use the ScanCentral DAST Configuration Tool to do the following:</p> <ul style="list-style-type: none"> • Configure and initialize the ScanCentral DAST database • Configure the settings that are used by the ScanCentral DAST API and the DAST Global Service, and generate a compose file or PowerShell script <p>For more information, see "Configuring the Database and Core Containers" on the next page.</p>
7.	<p>Use the compose file or PowerShell script to pull and launch the core ScanCentral DAST containers (DAST API and DAST Global Service).</p> <p>For more information, see "Generating Launch Artifacts" on page 29.</p>
8.	<p>Log in to Fortify Software Security Center and enable ScanCentral DAST in the ADMINISTRATION view.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Important! You must provide the ScanCentral DAST server URL to the Fortify Software Security Center administrator. The URL should be similar to the following:</p> <pre>http://<DAST_API_Hostname>:<Port>/api/</pre> <pre>http://<DAST_API_IP_Address>:<Port>/api/</pre> </div>

Stage	Description
	<p>The URL may use the https protocol instead.</p> <p>For more information, see the <i>Micro Focus Fortify Software Security Center User Guide</i>.</p>
9.	<p>Deploy the Fortify WebInspect on Docker container or deploy classic Fortify WebInspect with the sensor service.</p> <p>For more information, see "Using Fortify WebInspect on Docker" on page 33 or "Using Fortify WebInspect with the Sensor Service" on page 33.</p>

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 Docker for Windows.
2.	Optionally, if you plan to use a compose file to pull and run the core ScanCentral DAST containers (DAST API and DAST Global Service), download and install Docker Compose.
3.	Configure your machine for Docker containers.
4.	Register and start the Docker service.

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

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

Configuring the Database and Core Containers

Use the Fortify ScanCentral DAST Configuration Tool to configure the settings that are used by the ScanCentral DAST components.

About the ScanCentral DAST Configuration Tool

The ScanCentral DAST Configuration Tool helps you to configure the following components of the ScanCentral DAST environment:

- Connection settings and initialization of the ScanCentral DAST database
- SSL for DAST API
- Connection settings for Fortify Software Security Center and the License and Infrastructure Manager (LIM)
- Settings for SmartUpdate, DAST API, and proxy (if needed)

With these settings, the ScanCentral DAST Configuration Tool generates a compose file or a PowerShell script that you can run to pull the core containers (DAST API and DAST Global Service) from Docker Hub and run them on a host.

The ScanCentral DAST Configuration Tool is provided in the Fortify ScanCentral DAST software download package, which is a ZIP file that you download after purchase. The application and any required data are included in the ZIP file. You can extract the ZIP file and store its contents on your local machine.

You can run the configuration tool on one machine, and you can run the compose file or PowerShell script(s) that it generates on another. However, the configuration tool must have access to the database.

Installing and Launching the Configuration Tool

To install and launch the configuration tool:

1. Extract the files from the Fortify ScanCentral DAST software download package (a ZIP file).
2. To install the configuration tool, locate and double-click the file named `DAST Config Tool Setup <version>.exe`.
The installer launches, installs the application, and adds a shortcut to the desktop.
3. To launch the configuration tool, double-click the **DAST Config Tool** shortcut.
The configuration tool opens to the Database Connection page.

What's Next?

Proceed with ["Configuring the Database Connection"](#) below.

Configuring the Database Connection

You can configure connections to an existing database or have the configuration tool create a new database with the information you provide on the **Database connection** page.

Important! You must provide credentials for existing accounts on the database server. The

configuration tool does not create user accounts for the database.

Configuring the DBO-level Account

You must configure a connection to the database using a 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.

To configure a database connection for the DBO-level account:

1. In the **DBO-LEVEL ACCOUNT** area, type the database server name in the **Server** field.
2. For authentication to the server, do one of the following:
 - To use the credentials of the user who is currently logged into Windows, select **Use Windows authentication**.
 - To use the credentials for another account, then type the user name in the **User name** field and the password in the **Password** field.

Important! The user account must be a database owner (DBO) server-level account that has full access to the database.

3. Do one of the following:
 - To create a new database, select **Create new database** and type a name for the new database in the **Database** field.
 - To use an existing database, select **Use existing database** and select the database from the **Database** list.
4. To verify that you can access the database with the credentials provided, click **Validate**.

Configuring the Standard Account

You must configure a second connection to the database for a standard user 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.

To configure a database connection for the standard user account:

1. In the **STANDARD ACCOUNT** area, type the user name in the **User name** field and the password in the **Password** field.
2. Type the password in the **Confirm Password** field.
3. To verify that you can access the database with the credentials provided, click **Validate**.
4. Click **Next**.

What's Next?

Proceed with ["Initializing the Database" on the next page](#).

Initializing the Database

When initializing the database, you can use the default SecureBase ZIP file that is packaged with the ScanCentral DAST configuration tool or you can use a local version of SecureBase content to seed the database on the **Database initializer** page.

Using the Default SecureBase

To initialize the database using the zipped SecureBase that is included in the ScanCentral DAST configuration tool:

1. Ensure that **Use default SecureBase zip** is selected.
2. Click **Initialize database**.
Depending on your network configuration, it might take several minutes to initialize the database. When initialization is complete, a message indicates success.
3. Click **Next**.

Using a Local SecureBase

To use a version of SecureBase that you have locally:

1. Click **select**, and then locate and select the SecureBase file.
2. Click **Initialize database**.
Depending on your network configuration, it might take several minutes to initialize the database. When initialization is complete, a message indicates success.
3. Click **Next**.

What's Next?

Proceed with ["Configuring SSL" below](#).

Configuring SSL

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

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.

Generating an API SSL Certificate

You can provide the information needed to generate a certificate on the Generate Certificate tab. The certificate is generated when the configuration tool creates and downloads launch artifacts.

To generate a self-signed API SSL certificate:

1. Select the **Generate Certificate** tab.
2. In the **Certificate path** field, type the directory path where you want the certificate to be stored upon creation.

Note: Alternatively, click **select** and navigate to the location.

3. In the **Generate Self-Signed Certificate** area, continue according to the following table.

For this field...	Do this...
Host	Type the IP address of the machine running the DAST API service container.
Password	Optionally, type the password for the private key. Note: The password is encrypted and stored in the database.
Confirm Password	Optionally, retype the password for the private key.
Validity	Enter the number of days the certificate will be valid.

Using an Existing Certificate

You can use an existing certificate by specifying the directory path to the certificate on the Use Existing Certificate tab.

To use an existing certificate:

1. Select the **Use Existing Certificate** tab.
2. In the **Certificate file** field, type the directory path to the existing certificate.

Note: Alternatively, click **select** and navigate to the certificate.

3. Optionally, in the **Certificate password** field, type the password for the private key.
4. Optionally, in the **Certificate confirm password** field, retype the password for the private key.

Not Using SSL

Important! Encrypted communication for the DAST API service is not required, but Fortify highly recommends it.

To not use encrypted communication for the DAST API service:

1. Select the **Do Not Use SSL** tab.
2. Select the **Run the ScanCentral DAST API without SSL** check box.

What's Next?

After you have configured SSL details, click **Next**. Proceed with "[Configuring ScanCentral DAST Settings](#)" below.

Configuring ScanCentral DAST Settings

You can configure the various settings needed to deploy your Fortify ScanCentral DAST environment on the **Settings configuration** page.

Configuring SSC Settings

You must configure the connection between Fortify ScanCentral DAST and Fortify Software Security Center in the **SSC SETTINGS** area.

To configure your Fortify Software Security Center settings:

1. In the **SSC URL** field, type the URL for your Fortify Software Security Center application.

Important! You cannot use localhost for the SSC URL. You must use a routable IP address or hostname. The URL must use the following format:

```
https://<ip_address>:<port>/ssc  
https://<hostname>:<port>/ssc
```

2. In the **Service account username** field, type 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 13.

3. In the **Service account password** field, type the password for the account.
4. To verify that you can access Fortify Software Security Center with the credentials provided, click **Validate**.

Configuring API Settings

You must configure the URL for the DAST API in the **API SETTINGS** area. You can also configure cross-origin resource sharing (CORS) settings in this area.

To configure API settings:

1. In the **DAST API URL** field, type 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:

```
http://<DAST_API_Hostname>:<Port>
```

```
http://<DAST_API_IP_Address>:<Port>
```

The URL may use the `https` protocol instead.

Make note of this URL. It is required to enable Fortify ScanCentral DAST in Fortify Software Security Center.

2. By default, **Allow all origins for CORS policy** is not selected. The Fortify Software Security Center URL is the only one that is automatically allowed. To change this behavior, do one of the following:

- To add an allowed URL, type the URL in the **URL** field, and then click **Add**.

The URL is added to the Allowed CORS origins list.

Note: The Fortify Software Security Center URL is not visible in the list, but is allowed by default.

- To allow traffic from all URLs, select the **Allow all origins for CORS policy** option.

Configuring LIM Settings

During the database initialization, a sensor pool named "default" is created in the database. You must configure a LIM and LIM pool to associate with the default sensor pool for licensing. You configure these details in the **LIM SETTINGS** area.

To configure the LIM settings:

1. In the **LIM URL** field, type the LIM service URL.

Important! The URL must use the following format:

```
https://<server_url>/<service-directory>
```

where

server_url is the root web site.

service-directory is the service virtual directory name. The default name is `limservice`.

2. In the **Service account username** field, type a LIM account username.
3. In the **Service account password** field, type the password for the account.
4. In the **Default LIM Pool Name** field, type the LIM pool name to associate with the default sensor pool for licensing.
5. In the **Default LIM Pool Password** field, type the password for the LIM pool.
6. To verify that you can access the LIM with the credentials provided, click **Validate**.

Configuring Proxy Settings

If you need to use a proxy in your Fortify ScanCentral DAST environment, you can configure it in the **PROXY SETTINGS** area. 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, and OpenAPI and OData definition URLs.

To configure proxy settings:

1. To enable proxy settings, select **Use proxy**.
2. In the **Proxy address** field, type the URL or IP address and port number of your proxy server.
3. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), type the addresses or URLs in the **Proxy bypass list** field.

Tip: This field accepts a comma separated list of regular expressions. For example:

```
localhost, [a-z]+\.\myestore\.net$
```

4. If your proxy server requires authentication, type the qualifying user name in the **Proxy username** field.
5. If your proxy server requires authentication, type the qualifying password in the **Proxy password** and **Confirm password** fields.

Creating a Sensor Service Token

You must create a sensor service token, which is a shared secret for all of your sensors to use to authenticate with the ScanCentral DAST API.

To create a sensor service token:

- In the **Sensor Service Token** field in the **Sensor Settings** area, type a string with a minimum of 10 characters.
The value is encrypted.

Allowing Untrusted Certificates

To allow Fortify ScanCentral DAST components to accept self-signed (untrusted) certificates when communicating with other Fortify products:

- In the **OTHER SETTINGS** area, select **Allow untrusted server certificates**.

Retaining Completed Scans on Sensor

By default, scans are not saved in the sensor container after the sensor completes the scan and uploads the data to the DAST database.

To save completed scans in the sensor container:

- In the **OTHER SETTINGS** area, select **Retain completed Scans**.

Changing the SmartUpdate URL

To change the URL for the SmartUpdate service:

- In the **SmartUpdate URL** field in the **OTHER SETTINGS** area, type the URL for the SmartUpdate service.

The default URL is `https://smartupdate.fortify.microfocus.com/`.

Changing the Licensing URL

To change the URL for the licensing service:

- In the **Licensing URL** field in the **OTHER SETTINGS** area, type the URL for the licensing service.

The default URL is `https://licenseservice.fortify.microfocus.com/`.

What's Next?

After you have configured ScanCentral DAST settings, click **Next**. Proceed with "[Generating Launch Artifacts](#)" below.

Generating Launch Artifacts

Using the settings you configured in the Fortify ScanCentral DAST Configuration Tool, you can generate the files needed to launch your Fortify ScanCentral DAST environment.

Understanding the Launch Artifacts

The configuration tool creates and downloads the following files to your local machine:

- `appsettings.json` - This file configures the sensor service. Use this file to run the Fortify ScanCentral DAST Sensor Service and a Fortify WebInspect sensor.
- `docker-compose.yml` - This file pulls images and starts containers for the DAST API and DAST Global Service.
- `edast-api.pfx` - If you generated a certificate using the configuration tool, 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.

- `pull-and-start-containers.ps1` - This PowerShell script pulls the DAST Global Service and DAST API images from Docker Hub, and then starts the containers.
- `pull-and-start-sensor-container.ps1` - This PowerShell script pulls the Fortify WebInspect image from Docker Hub, and then starts the container.
- `pull-images.ps1` - This PowerShell script pulls the DAST Global Service and DAST API images from Docker Hub, but does not start the containers.
- `pull-sensor-container.ps1` - This PowerShell script pulls the Fortify WebInspect image from

Docker Hub, but does not start the container.

- `service-token.txt` - This text file contains the shared secret that all your DAST sensors must use to authenticate with the DAST API.
- `start-containers.ps1` - This PowerShell script starts the DAST Global Service and DAST API containers, but does not pull the images.
- `start-sensor-container.ps1` - This PowerShell script starts the Fortify WebInspect container, but does not pull the image.

For more information about the DAST components mentioned here, ["What is ScanCentral DAST?" on page 12.](#)

Generating the Launch Artifacts

To generate and download the launch artifacts:

- On the Generate compose file page, click **Download launch artifacts**.
The configuration tool prompts you for the location to save the ZIP file containing the launch files.

What's Next?

After you have downloaded the launch artifacts, you can use them to pull the DAST API, DAST Global 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 the Compose File

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 21.](#)

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

Use the following process to use the compose file.

Stage	Description
1.	Copy the following files to the host where you want to run the DAST Global Service and DAST API containers: <ul style="list-style-type: none">• <code>edast-api.pfx</code> (Required only if generated by the configuration tool)• <code>docker-compose.yml</code>

Stage	Description
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 <code>docker-compose up</code> , and press Enter . The DAST Global Service and DAST API images are pulled and the containers are started.

Using PowerShell Scripts

The configuration tool creates and downloads three PowerShell scripts. These scripts offer the following options:

- Use one script to pull images of the DAST API and DAST Global 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 and DAST Global Service containers.

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 Global Service and DAST API containers: <ul style="list-style-type: none">• <code>edast-api.pfx</code> (Required only if generated by the configuration tool)• <code>pull-and-start-containers.ps1</code>
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 <code>pull-and-start-containers.ps1</code> script: <ol style="list-style-type: none">1. Copy the contents from the <code>pull-and-start-containers.ps1</code> script.2. Paste the contents in the PowerShell ISE script pane.3. Click the Run Selection icon. <p>Note: Alternatively, you can set the execution policy to allow all scripts, and then run</p>

Stage	Description
	<p>the script as follows:</p> <pre>& "<drive>:<path_to_script>\pull-and-start-containers.ps1"</pre> <p>For more information about setting the execution policy, refer to your Windows PowerShell documentation.</p> <p>The DAST Global Service and DAST API images are pulled and the containers are started.</p>

Using Two Scripts

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

Stage	Description
1.	<p>Copy the following files to the host where you want to run the DAST Global Service and DAST API containers:</p> <ul style="list-style-type: none">• <code>edast-api.pfx</code> (Required only if generated by the configuration tool)• <code>pull-images.ps1</code>• <code>start-containers.ps1</code>
2.	<p>On this same host, start Windows PowerShell ISE as Administrator. For more information about using PowerShell, refer to your Windows PowerShell documentation.</p>
3.	<p>Pull the images.</p> <p>To avoid errors regarding non-digitally signed scripts, run the contents of the <code>pull-images.ps1</code> script:</p> <ol style="list-style-type: none">1. Copy the contents from the <code>pull-images.ps1</code> script.2. Paste the contents in the PowerShell ISE script pane.3. Click the Run Selection icon. <p>Note: Alternatively, you can set the execution policy to allow all scripts, and then run the script as follows:</p> <pre>& "<drive>:<path_to_script>\pull-images.ps1"</pre> <p>For more information about setting the execution policy, refer to your Windows PowerShell documentation.</p> <p>The DAST Global Service and DAST API images are pulled.</p>

Stage	Description
4.	<p>Start the containers.</p> <p>To avoid errors regarding non-digitally signed scripts, run the contents of the <code>start-containers.ps1</code> script:</p> <ol style="list-style-type: none">1. Copy the contents from the <code>start-containers.ps1</code> script.2. Paste the contents in the PowerShell ISE script pane.3. Click the Run Selection icon. <p>Note: Alternatively, if you set the execution policy to allow all scripts as described in Stage 3, you can run the script as follows:</p> <pre>& "<drive>:<path_to_script>\start-containers.ps1"</pre> <p>The DAST Global Service and DAST API containers are started.</p>

Using Fortify WebInspect on Docker

The Fortify WebInspect on Docker image is available for download on the Docker container platform. The image includes the full version of Fortify WebInspect software, and is packaged with a running mode that enables it to run as a Fortify ScanCentral DAST sensor. For information on how to pull and run the image as a DAST sensor, see the *Micro Focus Fortify WebInspect on Docker User Guide*.

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.

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 Information About Windows Server 2016

You can install Fortify WebInspect on Windows Server 2016. However, if you install the DAST sensor service on Windows Server 2016, you must first install ASP.NET Core Runtime 3.1.x (Hosting Bundle). 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. If you choose Basic for authentication, you must provide user name(s) and

Setting	Value
	<p>password(s). To do this:</p> <ol style="list-style-type: none"> Click the Edit passwords button and select a text editor. The <code>wircserver.keys</code> file opens in the text editor. The file includes sample user name and password entries: <pre>username1:password1 username2:password2</pre> 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. Save the file. <p>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.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Tip: You can use a tool, such as the MakeCert utility in the Windows Software Development Kit (SDK), to create your client certificate.</p> </div>
Use HTTPS	<p>Select this check box to access the server over an HTTPS connection.</p> <p>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:</p> <pre>\$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 certhash=\$(\$rootcertID)appid="{160e1003-0b46-47c2-a2bc-01ea1e49b9dc}"</pre> <p>The preceding script creates a certificate for the local host and the computer</p>

Setting	Value
	<p>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.</p> <p>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.</p>
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 ["Generating Launch Artifacts" on page 29](#).

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

```
sc create ScannerWorkerService binpath= "<PathToScannerService>  
  \EDAST.ScannerWorkerService.exe" start= auto
```

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

```
sc create ScannerWorkerService binpath= "C:\ScannerService  
  \EDAST.ScannerWorkerService.exe" start= auto
```

The `ScannerWorkerService` is created and automatically starts each time the computer is restarted.

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. Configure the service to run automatically.
- d. Apply the changes.

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

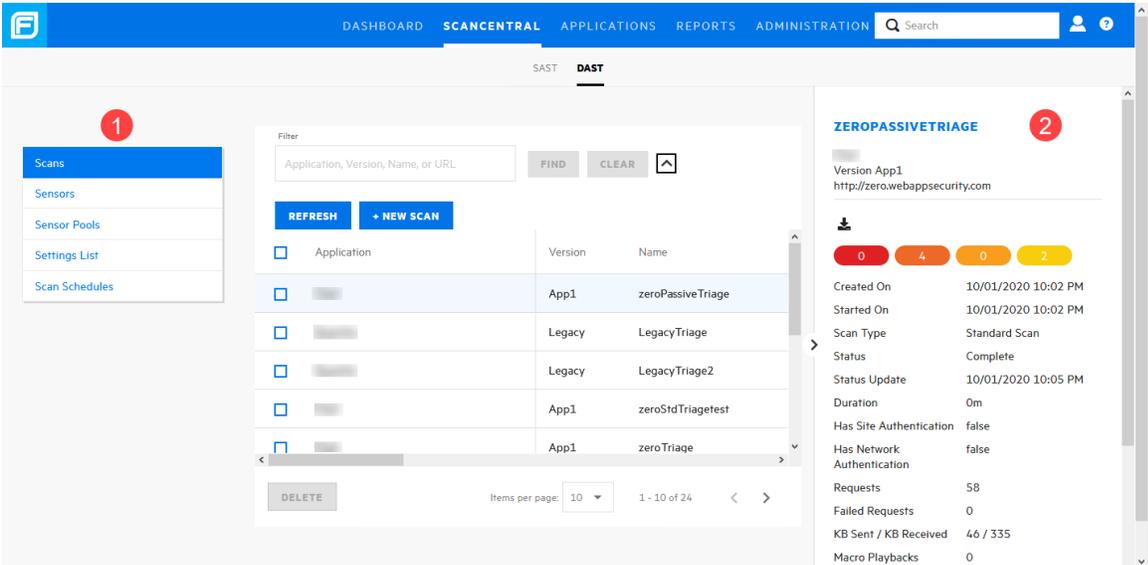
The service starts and polls the Fortify WebInspect API for instructions.

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 DAST scans, sensors, sensor pools, settings, and scan schedules directly in Fortify Software Security Center.

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 list.

Filtering Data in Columns

You can filter the columns in the Scans list 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 the columns in the Settings List 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 filtering:

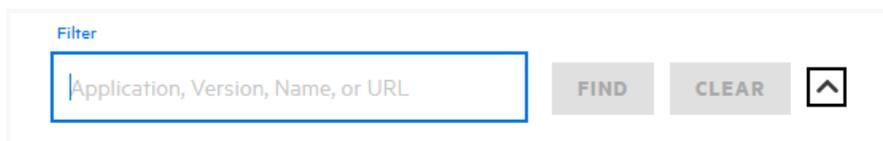
- You can use partial words for filtering. For example, using the filter criteria "che" includes the application named "OnlineParcheesi" and scans named "Allchecks" in the filter results.
- You cannot use wildcard characters, such as the asterisk (*), as placeholders.
- You cannot use regular expressions.

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 list. 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. This procedure illustrates filtering in the Scans list, but it works in the Settings List too.

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

- Type the filter criteria into the **Filter** box, and then click **FIND**.



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

The list 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 **FIND**.

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

To filter by date or Scan Status or Scan Type:

1. Click the down arrow to the right of the **FIND** button.
The date and status (or scan type) filter fields appear.

The screenshot shows a filter interface. At the top, there is a search bar labeled 'Filter' with the placeholder text 'Application, Version, Name, or URL'. To the right of the search bar are three buttons: 'FIND', 'CLEAR', and a dropdown arrow. Further right are two blue buttons: 'REFRESH' and '+ NEW SCAN'. Below the search bar, there are four filter fields: 'Date Range' (a dropdown menu with 'Select date' as the selected option), 'Start date' (a text field with a calendar icon), 'End date' (a text field with a calendar icon), and 'Scan Status' (a dropdown menu with 'Status' as the selected option).

2. 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.

3. Click **FIND**.

Clearing the Filter

To clear the filter and show all scans or all settings:

- Click **CLEAR**.

Sorting Data in Columns

By default, columns of text are listed in alphabetical order, columns of dates are in chronological order, and columns of numerical data are in numerical order.

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.

Version Name ↑ URL

To reverse the current sort order:

- Click the column name again.

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

Version Name ↓ URL

To clear the sorting:

- Click the column name a third time.

The arrow next to the column name disappears.

Version Name URL

Chapter 4: Configuring a DAST Scan

Use the Settings Configuration wizard to configure a Fortify ScanCentral DAST scan of your Web application to assess potential security flaws. A Fortify ScanCentral DAST scan is an automated scan of your Web application, 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 uses two basic modes for determining the security weaknesses of your Web application:

- **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.

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 list appears.
2. On the **Scans** list, click **+ NEW SCAN**.
The Settings Configuration wizard opens to the Getting Started page.

Accessing from the Settings List

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

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

What's Next?

Proceed with "[Getting Started](#)" below.

Getting Started

To configure a ScanCentral DAST scan:

1. On the Getting Started page, select an application from the **Application Name** list.
2. From the **Application Version** list, select a version.
The **START** list appears, providing 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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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.

Note: If you import Fortify WebInspect settings, you will not be able to edit any settings that are not displayed in the

If you want to...	Then...
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.	
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" below](#).
- To configure a workflow-driven scan, proceed with ["Configuring a Workflow-driven Scan" on page 46](#).
- To configure an API scan, proceed with ["Configuring an API Scan" on page 47](#).

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 54](#).

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/`.

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 issue.

6. Select a policy from the **Audit Depth (Policy)** list.

Note: The policies are stored in Securebase. For more information about the list of policies, see ["Policies" on page 93](#).

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 49](#).
- To configure authentication for the scan, click **NEXT** and proceed with ["Configuring Authentication" on page 51](#).

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, Burp Proxy captures, or a Selenium IDE macro.

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 Burp Proxy captures, or all Selenium macros. You cannot use different types of macros in the same scan.

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...
Add a macro to the scan settings	<ol style="list-style-type: none">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	<ol style="list-style-type: none">a. Select the macro in the macro list.

To...	Then...
macros	b. Click REMOVE .

- (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 issue.

- Select a policy from the **Audit Depth (Policy)** list.

Note: The policies are stored in Securebase. For more information about the list of policies, see ["Policies" on page 93](#).

- 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 49](#).
- To configure authentication for the scan, click **NEXT** and proceed with ["Configuring Authentication" on page 51](#).

Configuring an API Scan

An API scan creates a macro from a REST API definition and performs an automated analysis.

To configure an API scan:

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

3. Continue according to the following table.

For this API type...	Do this...
Open API	<p>a. In the Definition list, select File or URL, and continue as follows:</p> <ul style="list-style-type: none"> ○ If you selected File, click IMPORT and import the definition file. ○ If you selected URL, provide the URL to the API definition file, as shown in the following example: <code>http://172.16.81.36/v1</code> <p>Tip: Alternatively, you can paste in the full path to a definition file that is saved on your local machine.</p> <p>b. If HTTP authorization credentials, such as a bearer token, are needed to access the API definition, enter them in the Authentication Header box, as shown in the following example: <code>Basic YWxhZGRpbjpvGVuc2VzYW11</code></p>
Postman	<p>Click IMPORT and import the Postman collection file.</p> <p>Important! You must include the authorization credentials in the collection file.</p>
OData	<p>In the Definition list, select File or URL, and continue as follows:</p> <ul style="list-style-type: none"> ● If you selected File, click IMPORT and import the definition file. ● If you selected URL, provide the URL to the API definition file, as shown in the following example: <code>http://172.16.81.36/v1</code> <p>Tip: Alternatively, you can paste in the full path to a definition file that is saved on your local machine.</p>

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 issue.

5. Select a policy from the **Audit Depth (Policy)** list.

Note: The policies are stored in Securebase. For more information about the list of policies, see ["Policies" on page 93](#).

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" below](#).
- To configure authentication for the scan, click **NEXT** and proceed with ["Configuring Authentication" on page 51](#).

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

To...	Then...
	will not be used.
Load proxy settings from a Proxy Automatic Configuration (PAC) file	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 commas 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](#)" below.

Configuring Authentication

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.
 - To record a login macro, click **Open Macro Recorder 5.0**.

Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 5.0 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 Macro Recorder with Macro Engine 5.0 tool from the ScanCentral DAST REST API container.

To download the Macro Recorder tool:

- Under **Site Authentication**, click **Download Macro Recorder 5.0**.

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**.

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

Active Directory Federation Services Channel Binding Token authentication helps protect against man-in-the-middle (MITM) attacks in which an attacker intercepts a client's credentials and forwards them to a server. Protection against such attacks is made possible when a Channel Binding Token (CBT) is required or allowed by the server when establishing communications with clients. In some servers, such as IIS, ADFS CBT is called "Extended Protection for Authentication."

It is similar to NTLM authentication, but ADFS CBT authentication builds a CBT token based on the hash of the HTTPS site server certificate. This authentication type is usually used for HTTPS sites. For an HTTP site, it works similar to NTLM but the token is empty.

Note: Most servers require the domain name to be entered along with the user name in the Username field, such as DOMAIN/username or username@domainname.com. Consider this possibility if you have difficulty connecting to your server with the credentials you provide.

Automatic

Allow the sensor to determine the correct authentication type.

Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance will be noticeably improved.

Basic

A widely used, industry-standard method for collecting user name and password information.

- a. The Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials.
- b. The Web browser then attempts to establish a connection to a server using the user's credentials.
- c. If a user's credentials are rejected, the browser displays an authentication window to re-enter the user's credentials.
- d. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.

The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.

Digest

The Windows Server operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is

always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

Kerberos

Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

NT LAN Manager (NTLM)

NTLM is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and the sensor has to pass through a proxy server to submit its requests to the Web server, the sensor may not be able to crawl or audit that Web site.

Caution! After configuring the sensor for NTLM authentication and scanning the NTLM-protected sites, you might want to disable the NTLM authentication settings to prevent any potential problem.

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" below](#).

Configuring Scan Details

You can configure the following settings on the Details page:

- Add and manage allowed hosts (For more information, see ["Adding and Managing Allowed Hosts" on the next page.](#))
- Enable single-page application (SPA) support (For more information, see ["Scanning Single-page Applications" on page 55.](#))
- Enable Traffic Monitor (For more information, see ["Using Traffic Viewer \(Traffic Monitor\)" on page 56.](#))

- Create and manage exclusions (For more information, see ["Creating and Managing Exclusions" on page 56.](#))

What's Next?

After you configure the scan details, click **NEXT** and proceed with ["Reviewing Scan Settings" on page 60.](#)

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 "Wlexample.com," you would need to add "Wlexample2.com" and "Wlexample3.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**.

Scanning Single-page Applications

This topic describes single-page application (SPA) support for crawling and auditing the Document Object Model (DOM) of an application.

Important! This version of SPA support is provided as a technology preview.

Technology Preview

Technology preview features are currently unsupported, may not be functionally complete, and are not suitable for deployment in production. These features are provided as a courtesy and the primary objective is to gain wider exposure for the feature with the goal of full support in the future.

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.

Using Traffic Viewer (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. The Traffic Viewer (or Traffic Monitor) allows you to display and review every HTTP request sent by the sensor and the associated HTTP response received from the web server.

Proxy Server Included

The Traffic Viewer includes a self-contained proxy server that you can configure and run on your desktop. With it, you can monitor traffic from your browser as it submits HTTP requests and receives responses from a web server. The Traffic Viewer proxy is a tool for debugging and penetration assessment; you can see every request and server response while browsing a site.

Option Must be Enabled

To use the Traffic Viewer, you must enable Traffic Monitor logging in the scan settings. Otherwise, the Traffic Viewer is not available for a scan.

Enabling Traffic Viewer (or Traffic Monitor)

To enable the Traffic Viewer (or Traffic Monitor):

- 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:
 - **URL** – Excludes a host or 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
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.
 - **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
Exclude the following directories:	URL matches regex /W3SVC[0-9]*/

To...	Create the following exclusion...
http://www.test.com/W3SVC55/ http://www.test.com/W3SVC5/ http://www.test.com/W3SVC550/	
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:

```
site\.tld/sub/sub[0-9]+
```

Adding the negative look ahead to include sub1 results in this regular expression:

```
site\.tld/sub/sub(?!1)[0-9]+
```

This regular expression matches and excludes everything in the previous list of URLs that does not include sub1.

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
```

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.

Note: 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 63.](#))
- Use the settings in the API (For instructions, see ["Using the Scan Settings in the DAST API" on page 63.](#))

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 SCHEDULE SCAN dialog box opens.
2. Type a name for the scheduled scan in the **Name** box.
3. Enter a date and time for the scan to start in the **Start Date** and **Start Time** boxes.

Tip: To select a date from the calendar, click the calendar icon (📅).

4. Select your time zone from the **Timezone** list.
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	<ol style="list-style-type: none">a. Select DAILY.b. Select a recurrence in the Occur every ___ day box.
Weekly	<ol style="list-style-type: none">a. Select WEEKLY.b. Select a recurrence in the Occur every ___ week box.c. Select the days to run each week.

To run...	Then...
Monthly	a. Select MONTHLY . b. Select a recurrence in the Occur every ___ month box. c. Do one of the following: <ul style="list-style-type: none"> o Select Occur on day and enter a date in the box. o Select Occur on the, and then select an interval from the Interval list and a day from the Day list. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Note: Interval options are First, Second, Third, Fourth, and Last.</div>
Yearly	a. Select YEARLY . b. Do one of the following: <ul style="list-style-type: none"> o Select Occur on, and then select a month from the Month list and enter a date in the Day box. o 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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Note: Interval options are First, Second, Third, Fourth, and Last.</div>

6. Under **Range**, do one of the following:
 - To leave the schedule 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.

Settings Identifier: 8c27261d-8f0a-4ebe-897e-0538bf988c77

The above Settings Identifier can be used to run this scan template from any automation platform by performing a POST request against `http://[hostname]/api/scans/start-scan-cicd`. The request should include the Settings Identifier as the `cicdToken` in the JSON payload, and should include an Authorization header using an encoded `CIToken` from SSC | Administration | Users | Token Management. For more information, see `http://[hostname]/api/swagger`.

Copy CURL example to clipboard 

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

For more information about using the DAST API, access the Swagger UI at the URL referenced on the Review page.

Chapter 5: Working with DAST Scans

You can view the scans that are available in the ScanCentral DAST database in the Scans list. You can also start a new scan, refresh the scan list, 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 list appears.

User Role Determines Capabilities

Your user role in Fortify Software Security Center determines 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 13](#).

Understanding the Scans List

The Scans list displays the scans that are available in the ScanCentral DAST database. The following table describes the columns of information provided for each scan.

Column	Description
Application	Indicates the application that was selected when the scan was configured for the target URL.
Version	Indicates the version that was selected when the scan was configured for the target URL.
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.

Column	Description
Critical High Medium Low	Indicates the number of findings for each severity category in the scan.
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	<p>Indicates the current status of the scan. Possible statuses are as follows:</p> <ul style="list-style-type: none"> • 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. <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <ul style="list-style-type: none"> • 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. • 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 into Fortify Software Security Center. • Import Failed – Something went wrong during the import process. • Failed to Start – A sensor accepted the scan, but the scan failed to start. Possible reasons include: <ul style="list-style-type: none"> • The Fortify Software Security Center DAST API is not running. • The connection to the ScanCentral DAST database has been lost.

Column	Description
	<ul style="list-style-type: none">• 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 waiting for the sensor to become available.• Forced Complete – The user paused a scan and subsequently clicked Complete. The scan 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.

Understanding the Scan Detail Panel

When you click a scan in the Scans list, the scan detail panel appears to the right.

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 following table describes the additional information that is provided in this panel.

Item	Description
Created On	Indicates the date and time that the scan was created in the dynamic scan database and queued to be run.
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.
Scan Type	Indicates the type of scan selected during scan configuration: Standard Scan , Workflow-Driven Scan , or API Scan .
Status	Indicates the current status of the scan. For more information, see "Understanding the Scans List" on page 64 .
Status Update	Indicates the date and time that the sensor last reported its status.
Duration	Indicates how long the scan ran before completion. For more information, see "Understanding the Scans List" on page 64 .
Has Site Authentication	Indicates whether site authentication was used to conduct the scan. Possible values are true and false .
Has Network Authentication	Indicates whether network authentication was used to conduct the scan. Possible values are true and false .
Requests	Shows the total number of requests that were sent during the scan.
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.

Item	Description
Macro Playbacks	Indicates the number of times that macros have been played during the scan.
Pool	Identifies the pool to which the sensor belongs in Fortify Software Security Center.
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 List" on page 64 .
Sensor	Indicates the name of the dynamic sensor that conducted the scan.
Publish Status	Indicates whether the scan has been published to Fortify Software Security Center, where you can perform audit analysis of the findings.
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.

Working with Active Scans

You can pause, stop, resume, and re-import active scans in the Scans list. 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 list, 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 list, 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 list, 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 list 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 list, 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.

Managing the DAST Scans List

You can configure and submit a new scan, refresh the scans list, publish to and delete scans from the scans list on the Scans page.

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 list.

To configure settings or use existing settings for a new scan:

- Click **+ NEW SCAN**.

The SETTINGS CONFIGURATION wizard opens.

Refreshing the Scans List

You must manually refresh the scans list to see new scans that have been queued or scan statuses that have changed.

To view an updated list of scans:

- 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 list, 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 list 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 list, and then click **DELETE** at the bottom of the list.
- Select a scan to view the scan details, and then click **DELETE** at the bottom of the scan details panel.

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 list. Depending on the status of the associated scan, you can also download a log file or the site tree (.csv format) to examine, or the scan results (.scan or .fpr format) to view the findings and other scan details that are not available in Fortify Software Security Center.

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.

File Types Available

The following table describes the file types that are available for download for each scan status.

Scan Status	File Types Available for Download		
	Scan Settings	Scan Result / Site Tree / FPR	Scan Logs
Queued	x		
Pending	x		
Not Running	x		
Running	x		
Complete	x	x	x
Interrupted	x		x
Unknown	x		
Importing	x		
Import Failed	x		
Failed to Start	x		
Pausing	x		
Resuming	x		
Completing Scan	x		
Resume Scan Queued	x		
Forced Complete	x	x ¹	x

¹Scans 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.

For more information about the scan statuses, see ["Understanding the Scans List" on page 64](#).

Downloading a File

To download a file for a scan:

1. Do one of the following:
 - In the scans list, 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.

Note: The available file types to download depend on the scan status. For details, see ["File Types Available" on the previous page](#).

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.

Chapter 6: Working with DAST Sensors

You can view all of the sensors that are stored in the ScanCentral DAST database in the Sensors list. 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 list appears.
2. In the left panel, select **Sensors**.
The Sensors list appears.

User Role Determines Capabilities

Your user role in Fortify Software Security Center determines 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 13.

Understanding the Sensor List

The Sensors list shows all sensors that are stored in the ScanCentral DAST database. The following table describes the columns of information provided for each sensor.

Column	Description
Name	Identifies the sensor name.
Pool	Identifies the pool to which the sensor belongs.
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

Column	Description
	ScanCentral DAST database.
Enabled	Indicates whether the sensor is enabled to perform scans. Possible values are true and false .
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 list, the sensor detail panel appears. The sensor details show the sensor's status and whether it is enabled. The following table describes the additional information that is provided for the selected sensor.

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.
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 list 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 list.

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 list.

The sensor details panel appears.

The screenshot shows the details for a sensor named 'WIN10X64'. At the top, there is a blue bar with the sensor name. Below it, the status is 'Online'. A toggle switch is currently in the 'Enabled' position. Below the toggle, there is a table of sensor attributes:

IP Address	[Redacted]
Pool	Default
Current Scan ID	
Last Connect	10/05/2020 02:11 PM
Operating System	Microsoft Windows
Version	10.0.18363
Application Version	20.2.229.0
WebInspect Version	20.2.0.125

2. Do one of the following:
 - To enable the sensor, toggle the switch to **Enabled**.
 - To disable the sensor, toggle the switch to **Disabled**.

Chapter 7: Working with DAST 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.

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 list appears.
2. In the left panel, select **Sensor Pools**.
The Sensors Pools list appears.

User Role Determines Capabilities

Your user role in Fortify Software Security Center determines 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 13](#).

Understanding the Sensor Pools List

The Sensor Pools list displays the ScanCentral DAST sensor pools that are configured in the ScanCentral DAST database. The following table describes the columns of information provided 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).

Column	Description
Default	Indicates whether the pool is designated as the default pool. Possible values are true or false . 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.

Understanding the Pool Detail Panel

When you select a pool in the Sensor Pools list, 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 the next page](#).

The following table describes the additional information provided for each pool.

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.

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 CREATE NEW POOL dialog box opens.
2. In the **Name** field, type a name for the pool.
3. In the **Description** field, 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** field, 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 **ASSIGN SENSORS** at the top of the dialog box or click **NEXT**.

- The YOUR SENSORS list appears.
8. Select one or more sensors to add to the pool.
The sensor(s) are added to the SELECTED SENSORS list.
 9. Click **ASSIGN APPLICATIONS** at the top of the dialog box or click **NEXT**.
The YOUR APPLICATIONS list appears.
 10. Select one or more applications to add to the pool.
The application(s) are added to the SELECTED APPLICATIONS list.
 11. 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.

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 the previous page](#).

Refreshing the Pools List

Generally, the changes that you make to the sensor pools appear right away on the Sensor Pools page. 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 list.

To view an updated pools list:

- 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 list, and then click **DELETE** at the bottom of the list.
- 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.

Chapter 8: Working with DAST Settings

You can view the settings that are available in the ScanCentral DAST database in the Settings List. 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, you can also configure new scan settings, edit existing settings, download settings, and delete settings.

Accessing DAST 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 settings directly in Fortify Software Security Center.

To access DAST settings in Fortify Software Security Center:

1. Select **SCANCENTRAL > DAST**.
The Scans list appears.
2. In the left panel, select **Settings List**.
The Settings list appears.

User Role Determines Capabilities

Your user role in Fortify Software Security Center determines 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 13](#).

Understanding the Settings List

The Settings List displays the settings that are available in the ScanCentral DAST database. The following table describes the columns of information provided for each settings file in the list.

Column	Description
Name	Indicates the name of the settings file. This is the name that was assigned at 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:

Column	Description
	<ul style="list-style-type: none">• 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 Settings Detail Panel

When you click a settings file in the Settings List, 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 following table describes the additional information that is provided in this panel.

Item	Description
Created	Indicates the date and time that the settings were saved.
Modified	Indicates the date and time that the settings were created, or if edited, the last date and time that the settings were changed.
Type	Indicates the type of scan to be conducted using the settings. Types are: <ul style="list-style-type: none">• Standard Scan• Workflow-driven Scan• API Scan
Policy	Identifies the dynamic policy to be used to conduct the scan.
User Agent	Indicates the user agent one or more of the following: <ul style="list-style-type: none">• Chrome• Chrome (Mobile Android)• Custom• Default• Edge• Safari• Safari (Mobile IOS)

Item	Description
	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.
Network Auth	Indicates whether network authentication is specified in the settings.
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.
Enable Traffic Monitor	Indicates whether Traffic Monitor is enabled in the settings.
Submit for Triage	Indicates whether a scan run from these settings is uploaded to Fortify Software Security Center upon completion.
SETTINGS IDENTIFIER	Indicates the settings identifier GUID that was assigned to the settings.

Managing Settings

You can configure new scan settings, edit existing settings, download settings, and delete settings from the Settings List.

Creating New Settings

You can access the Settings Configuration wizard from the Settings List 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**, 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.

Deleting Settings

To delete settings, do one of the following:

- Select one or more check boxes for settings in the **Settings List**, and then click **DELETE** at the bottom of the list.
- Select the settings in the **Settings List** to view the details, and then click **DELETE** at the bottom of the settings detail panel.

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**, select the settings to copy.
The settings detail panel appears.

2. In the settings detail panel, click the copy icon as shown below.

ZEROSQL

Version Project01
<http://zero.webappsecurity.com>

Created	07/24/2020 05:34 PM
Modified	07/24/2020 05:34 PM
Type	Standard Scan
Policy	Passive Scan
User Agent	Default
Login Macro	none
Network Auth	false
Allowed Hosts	none
Enable SPA Support	off
Enable Traffic Monitor	off
Submit for Triage	no

SETTINGS IDENTIFIER

697AD7D3-2231-4468-99A4-0F8013517602 

The scan settings identifier is copied to the clipboard.

Chapter 9: Working with DAST Scan Schedules

You can view all of the scan schedules that are available in the ScanCentral DAST database in the Scan Schedules list. 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 list appears.
2. In the left panel, select **Scan Schedules**.
The Scan Schedules list appears.

User Role Determines Capabilities

Your user role in Fortify Software Security Center determines 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 13](#).

Understanding the Scan Schedules List

The Scan Schedules list displays the scan schedules that are available in the ScanCentral DAST database. 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.

Column	Description
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.
Enabled	Indicates whether the schedule is enabled. Possible values are true and false .

Understanding the Schedule Detail Panel

When you click a scan schedule in the Scan Schedules list, the schedule detail panel appears to the right. The following table describes the additional information that is provided for the selected schedule.

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.

Managing Schedules

You can configure a new scan schedule, edit an existing schedule, enable or disable schedules, and delete schedules from the Scan Schedules list.

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** page, click **+ NEW SCHEDULE**.
The SCAN SETTINGS TEMPLATE dialog box opens.

2. Select an application from the **Application Name** list.
3. Select a version from the **Application Version** list.

A START list and a list of recently opened settings templates, if applicable, appear at the bottom of the dialog box.

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 **+ NEW SCHEDULE**.
 - To use a template saved to a file, select **Open file** in the **START** list, and then click **+ NEW SCHEDULE**.
 - To use a recently opened template, select a template under **RECENT**.

The SCHEDULE SCAN dialog box opens.

5. Follow the procedure described in ["Scheduling a Scan" on page 61](#).

Editing a Schedule

To edit a schedule:

1. Select the schedule in the list.
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 described in ["Scheduling a Scan" on page 61](#).

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. Select the schedule in the list.
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 schedules list, 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.

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.

Log File Names

The log file name is in the format of YYYY-MM-DD.log, such as 2020-10-14.log. There is one log file per day. If you run the configuration tool more than once during a single day, the file is appended with new entries for each successive run.

A maximum of seven log files per service is kept. 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.

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 container, enter the following command:

```
docker stop scancentral-dast-api  
The API container stops.
```

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

```
run "docker cp scancentral-dast-api:/app/logs/ c:\<Directory>"  
The API logs are copied to the directory you specify in the command.
```

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 container, enter the following command:

```
docker stop scancentral-dast-globalservice  
The Global Service container stops.
```

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

```
run "docker cp scancentral-dast-globalservice:/app/logs/ c:\<Directory>"  
The Global Service logs are copied to the directory you specify in the command.
```

Scan Configuration Tool Logs

You can find the DAST Configuration Tool log files in the following location:

```
c:\Users\<CurrentUser>\AppData\Local\Programs\edas-t.-configuration-  
tool\resources\bin\logs
```

Scanner Service Logs

You can find the scanner service log files in the following location:

```
c:\<ServiceExtractionPath>\logs
```

Troubleshooting the Configuration Tool

If the DAST Configuration Tool fails to create and seed the database or fails at any other point, review the tool log file for errors.

Tip: If you need to uninstall the DAST Configuration Tool, an uninstaller is located at:

```
C:\Users\<user>\AppData\Local\Programs\edas-t.-configuration-  
tool\Uninstall DAST Config Tool
```

Configuration Tool Fails to Launch

The following table describes possible causes and solutions when the configuration tool fails to launch.

Error or Symptom	Possible Cause	Possible Solution
The configuration tool application does not launch.	Your OS may have the environment variable for HTTP_PROXY set for proxy use.	The configuration tool requires that the environment variable for NO_PROXY be set to localhost. Refer to your OS documentation and change this environment

Error or Symptom	Possible Cause	Possible Solution
		variable.

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 DYNAMIC API"	ScanCentral DAST might be using an untrusted or self-signed certificate.	To resolve this issue, do one of the following: <ul style="list-style-type: none"> 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.
	The ScanCentral DAST API URL may be configured improperly.	Do the following: <ol style="list-style-type: none"> Navigate to Administration > Configuration > ScanCentral DAST. Update the URL.
	The ScanCentral DAST API might be inaccessible from the current browser.	Verify the following: <ul style="list-style-type: none"> 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	Ask your administrator to navigate to Administration >

Error or Symptom	Possible Cause	Possible Solution
	(CSP) might be too restrictive.	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 "Configuring API Settings" on page 26.

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 33.

Appendix B: Reference Lists

The following pages provide a list of policies that are available for use in Fortify ScanCentral DAST.

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:** 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.

- **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 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.
- **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 Software Security Framework 1.0 (PCI SSF 1.0):** The PCI SSF 1.0 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 1.0.
- **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.

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 20.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!