opentext™

Fortify WebInspect Enterprise

Software Version: 23.2.0
Windows® operating systems

User Guide

Document Release Date: December 2023
Software Release Date: December 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

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

Trademark Notices

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 November 08, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Preface

Contacting Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

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

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	**Changes**
23.2.0	Updated: • List of policies with description of the PCI DSS 4.0 policy and with information about OAST-related checks. See "Policies List" on page 98 (Administrative Console) and "Policies List" on page 155 (WebConsole). • Information related to exporting scans with a known issue for XML files being imported to Fortify Software Security Center. See "Reviewing Scan Results" on page 182.
22.2.0	Removed: • References to **Enhance Coverage of Your Website** feature in Guided Scan.
21.2.0 / June 2022	Removed: • Scan Settings: Policy content.
21.2.0	Updated: • WebConsole scan list content with procedures for deleting selected scans and deleting multiple scans by date range. See "Reviewing the Scan List" on page 175.
21.1.0	Added: • Content for new scan settings page for User Agent. See "Scan Settings: User Agent" on page 399. Updated: • List of policies with description of the NIST-SP80053R5 policy. See "Policies List" on page 98 (Administrative Console) and "Policies List" on page 155 (WebConsole).

Software Release / Document Version	Changes
	• Site authentication content with support for masked variables in macros. See the following topics: ◦ "Configuring Web Site Scans Using a Predefined Template" on page 320 ◦ "Configuring Mobile Web Site Scans Using a Mobile Template" on page 332 ◦ "Configuring Native Scans Using a Mobile Template" on page 343 ◦ "Scan Settings: Authentication" on page 393 Removed: • References to Selenium IDE macros.

Chapter 1: About Fortify WebInspect Enterprise

OpenText™ Fortify WebInspect Enterprise employs a distributed network of OpenText™ Fortify WebInspect sensors controlled by a system manager with a centralized database. Optionally, you can integrate Fortify WebInspect Enterprise with OpenText™ Fortify Software Security Center to provide Fortify Software Security Center with information detected through dynamic scans of Web sites and Web services.

Benefits of Fortify WebInspect Enterprise

This innovative architecture enables you to:

- Conduct a large number of automated security scans using any number of sensors in various locations to scan Web applications and Web services.
- Manage large or small deployments of Fortify WebInspect sensors across your organization controlling product updates, scan policies, scan permissions, tools usage, and scan results, all centrally from the Fortify WebInspect Enterprise Administrative Console.
- Detect, track, and manage your new and existing Web applications and monitor all activity associated with them.
- Independently schedule scans and blackout periods, manually launch scans, and update repository information by using Fortify WebInspect or the Fortify WebInspect Enterprise Administrative Console.
- Limit exposure to enterprise-sensitive components and data by using centrally defined roles for users.
- Obtain an accurate snapshot of the organization's risk and policy compliance through a centralized database of scan results and trend analysis.
- Facilitate integration with third-party products and deployment of customized Web-based front ends using the WebServices application programming interface (API).

Fortify WebInspect Enterprise Components

Fortify WebInspect Enterprise comprises the following:

- The Fortify WebInspect Enterprise Administrative Console, also known as the Fortify WebInspect Enterprise Console. The Administrative Console is used for administrative and security functions.
- The Fortify WebInspect Enterprise Services Manager, also known as the Fortify WebInspect Enterprise Services Configuration Utility. This interface is used to configure or modify services associated with Fortify WebInspect Enterprise.

- The Fortify WebInspect Enterprise Web Console, also known as the Web Console. This is a browser-based interface designed for non-administrative functions such as running and managing scans, and for which this Help system is provided.
- The WebInspect Enterprise Desktop Application. This application enables you to perform the following tasks:
  - View scan results and the Traffic Monitor
  - Import a scan
  - Use Guided Scan
  - Generate reports
- Fortify WebInspect sensors. A Fortify WebInspect sensor is the Fortify WebInspect application when connected to Fortify WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans with no direct user interaction through the Fortify WebInspect graphical user interface. The sensor receives its instructions exclusively from the configurable connection to Fortify WebInspect Enterprise.
- Microsoft SQL Server.

A scan consists of a crawl and an audit, and you can also run only a crawl or only an audit. A crawl identifies the structure of the target Web site. An audit is the identification of vulnerabilities.

Fortify WebInspect Enterprise uses SmartUpdate technology to keep your threat protection current.

For information about system requirements, see the *Fortify Software System Requirements*. For information about installing or upgrading Fortify WebInspect Enterprise, see the *OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide*. You can access these documents from the **Resources** link on the Administrative Console.

Preparing Your System for Audit

OpenText Fortify WebInspect is an aggressive Web application analyzer that rigorously inspects your entire Web site for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. The scan policy and other options you select can affect server and application throughput and efficiency. When using the most aggressive policies, you should perform this analysis in a controlled environment while monitoring your servers.

Increased Network Traffic

The OpenText Fortify WebInspect Enterprise manager typically experiences a large amount of traffic from the Fortify WebInspect Enterprise Administrative Console and the Fortify WebInspect sensor.

Firewalls, Anti-virus Software, and Intrusion Detection Systems

The WebInspect sensor sends attacks to servers, and then analyzes and stores the results. Web application firewalls (WAF), anti-virus software, firewalls, and intrusion detection/prevention systems

(IDS/IPS) are in place to prevent these activities. Therefore, these tools can be problematic when conducting a scan for vulnerabilities.

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

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

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

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

Increased Form Input

Most Web applications contain HTML or JavaScript forms composed of special elements called input controls (text boxes, buttons, drop-down lists, etc.). Users generally “complete” a form by modifying its input controls (such as entering text or checking boxes) before submitting the form to an agent for processing. Usually, this processing will lead the user to another page or section of the application. For example, after completing a logon form, the user will proceed to the application's beginning page.

To conduct a thorough scan, Fortify WebInspect attempts to identify every page, form, file, and folder in your application. If you select the option to submit forms during a crawl of your site, Fortify WebInspect will complete and submit all forms it encounters.

To navigate through all possible links in the application, Fortify WebInspect submits appropriate data for each form by using a file containing the names of input controls and the associated values that need to be submitted during the scan. Fortify WebInspect includes a default Web form file containing sample name/value pairs. You can use the Web Form Editor to create and edit your own file containing web form values. The pre-defined forms enable Fortify WebInspect to navigate seamlessly through your application, but they may also produce the following consequences:

- When a user normally submits a form, if the application creates and sends email messages or bulletin board postings (to a product support or sales group, for example), Fortify WebInspect will also generate these messages as part of the audit.

  Tip: If your system generates email messages in response to user-submitted forms, you might want to disable your mail server. Alternatively, you could redirect all emails to a queue and then, after the audit, manually review and delete those emails that were generated in response to forms submitted by Fortify WebInspect.

- If normal form submission causes records to be added to a database, then forms submitted by Fortify WebInspect will create spurious records.

During the audit phase of a scan, Fortify WebInspect resubmits forms numerous times, manipulating every possible parameter to reveal problems in the application. This will greatly increase the number of messages and database records created.

Tip: For systems that write records to a back-end server (database, LDAP, etc.) based on forms submitted by clients, some users, before auditing their production system, create a backup copy of the database and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit, searching for and deleting records that contain one or more of the default form values used by Fortify WebInspect. You can determine these values by using the Web Form Editor.

Increased HTTP Requests and Invalid Input

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

Uploading of Files

Fortify WebInspect tests for certain vulnerabilities by attempting to upload files to your server. If your server allows such uploading, Fortify WebInspect will record this susceptibility and attempt to delete the uploaded file. Sometimes, however, the server will not allow a file to be deleted.

Tip: If your server allows uploading files, your post-scan maintenance should include searching for and deleting files whose name begins with "CreatedByHP."

Tip: In general, you can restrict the crawl and/or audit phases of a scan to a particular directory, or to a directory and its subdirectories in the directory tree, or to its parents in the directory tree. You can also specify particular URLs, host names, file extensions, and other entities to exclude from a crawl and/or an audit.

Related Documents

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

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

All Products

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

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

Fortify Software Security Center

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

Document / File Name	Description
OpenText™ Fortify Software Security Center User Guide SSC_Guide_<*version*>.pdf	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Fortify Software Security Center. It provides all of the information you need to acquire, install, configure, and use Fortify Software Security Center. It is intended for use by system and instance administrators,

Document / File Name	Description
	database administrators (DBAs), enterprise security leads, development team managers, and developers. Fortify Software Security Center provides security team leads with a high-level overview of the history and current status of a project.

Fortify WebInspect

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

Document / File Name	Description
OpenText™ Fortify WebInspect Installation Guide WI_Install_*<version>*.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
OpenText™ Fortify WebInspect User Guide WI_Guide_*<version>*.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect and OAST on Docker User Guide WI_Docker_Guide_*<version>*.pdf	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be

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

Fortify WebInspect Enterprise

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

Document / File Name	**Description**
OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Fortify Software Security Center and Fortify WebInspect, and troubleshooting the installation. It also describes how to configure the

Document / File Name	Description
	components of the Fortify WebInspect Enterprise system, which include the Fortify WebInspect Enterprise application, database, sensors, and users.
OpenText™ Fortify WebInspect Enterprise User Guide WIE_Guide_<*version*>.pdf	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of Fortify WebInspect sensors to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect Enterprise help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Chapter 2: WebInspect Enterprise Administrative Console

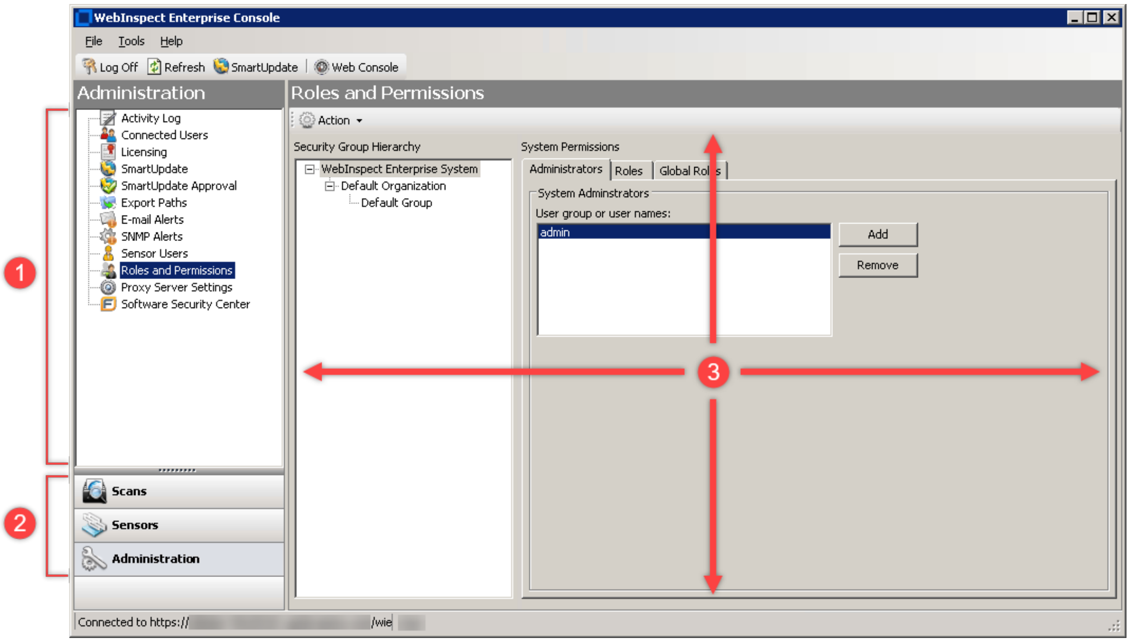
The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console, is used for administrative and security functions.

About the User Interface

The Administrative Console user interface comprises the following main areas:

- Menu bar
- Toolbar
- Shortcut pane
- Groups pane
- Form

The following image identifies the (1) Shortcuts, (2) Groups, and (3) Form.



About the Groups and Their Shortcuts

The buttons in the Groups pane represent groups of OpenText Fortify WebInspect Enterprise functions.

When you click a group button, the associated shortcuts appear above.

Click a shortcut to display a form containing related information or controls associated with the selected function.

In the screen capture above, the user selected the **Administration** group and then clicked the **Roles and Permissions** shortcut to display a form that enables you to manage the roles of administrative resources and the specific activities they are allowed to perform.

Scans Group

The **Scans** group has the following shortcuts:

- **Scan Queue** (See "About Controlling Scans Using the Scan Queue" on page 76.)
- **Scan Policies** (See "About Managing Scan Policies" on page 78.)

Sensors Group

The **Sensors** group has the following shortcut:

- **Sensors** (See "About Sensor Management " on page 83.)

Administration Group

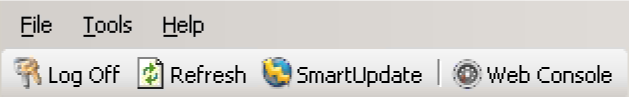
The **Administration** group has the following shortcuts:

- **Activity Log** (See "Managing the Activity Log" on page 97.)
- **Connected Users** (See "About Managing Connected Users" on page 95.)
- **Licensing** (See "Viewing License Information" on page 96.)
- **SmartUpdate** (See "Managing SmartUpdates" on page 40.)
- **SmartUpdate Approval** (See "Working with SmartUpdate Binary Files " on page 44.)
- **Export Paths** (See "Adding, Editing, and Deleting Export Paths for Saving Scans" on page 82.)
- **E-Mail Alerts** (See "Adding, Editing, and Deleting E-mail Alerts" on page 85.)
- **SNMP Alerts** (See "Adding, Editing, and Deleting SNMP Alerts" on page 89.)
- **Sensor Users** (See "Managing Sensor Users" on page 85.)
- **Roles and Permissions** (See "About Roles and Permissions" on page 47.)
- **Proxy Server Settings** (See "Managing Proxy Server Settings" on page 47.)
- **Software Security Center** (See "Configuring Settings for Fortify Software Security Center" on page 92.)

  Note: The **Software Security Center** shortcut is available only if Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

The procedures in this Help system describe how to use the form accessed by each shortcut. The availability of particular actions can depend on the permissions granted to you by your assigned role and on other factors (although system administrators have no restrictions on the functions they can perform).

Menu Bar and Toolbar



The menus and toolbar buttons are described in the following table.

Menu/Button	Description
File	Enables you to: - Log off from the Administrative Console. - Refresh the display. - Import to Fortify Software Security Center a set of applications that were sites discovered by the Web Discovery tool. (This option is also available when you select the **Software Security Center** shortcut in the **Administration** group.) **Note:** This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center. - Exit the application.
Tools	Enables you to: - Manually initiate a SmartUpdate. See "Managing SmartUpdates" on page 40. - Change the refresh rate for the console. See "Changing the Screen Refresh Rate " on page 37. - Launch various tools described in the *OpenText™ Fortify WebInspect Tools Guide*.
Help	Enables you to: - Open this Help file. - Open your e-mail application to send an e-mail to Fortify Customer Support. - Open the About WebInspect Enterprise Console dialog box.
Log On / Log Off	Log on to or log off from the Administrative Console.

Menu/Button	Description
Refresh	Refresh the screen.
SmartUpdate	Manually initiate a SmartUpdate. See "Managing SmartUpdates" on page 40.
Web Console	Log on to the Fortify WebInspect Enterprise Web Console, which enables you and authorized users to configure, run, and manage scans from a browser. The Web Console has its own, separate Help system.

See Also

"About Fortify WebInspect Enterprise" on page 25

"Logging On" below

"Changing the Screen Refresh Rate " on the next page

"Grouping and Sorting Items in Lists" on page 38

Logging On

To log on to the Administrative Console:

1. Click **Start > Fortify WebInspect Enterprise 23.2.0 Console**.

   The Log On to WebInspect Enterprise window appears.

   > **Note:** This window does not appear if you previously selected the option **Automatically log on when this application starts**.

2. Using the **Log on to** list, enter or select the URL of the OpenText Fortify WebInspect Enterprise manager.
3. Enter the **Username** and **Password** for an account that has permission to access the Administrative Console. This user is permitted to perform all restricted functions.
4. Select the option **Save password** as desired.
5. Select the option **Automatically log on when this application starts** if you want administrators not to have to enter login credentials in the future.
6. To go through a proxy server to reach the Fortify WebInspect Enterprise manager:
   a. Click the **Proxy** tab.
   b. Select one of the following:
      - **Use the System proxy** (to use the proxy server information from the local machine).
      - **Use the proxy below**, and then provide the proxy server's IP address and port number.
   c. Provide a valid **Username** and **Password**.
7. Click **OK**.

Tip: If you see a message indicating that the server refused the request, you may have entered your user name and password incorrectly, or your account has not been assigned to a role.

See Also

"About the User Interface" on page 33

Changing the Screen Refresh Rate

To specify a refresh rate for the OpenText Fortify WebInspect Enterprise Administrative Console:

1. After you log on, from the **Tools** menu, select **Options**.

   The WebInspect Enterprise Options window opens.
2. To refresh the display of Fortify WebInspect Enterprise information periodically, select **Automatically refresh display** and specify how often (in seconds) the display should be updated.
3. Click **OK**.

See Also

"About the User Interface" on page 33

Selecting Which Table Columns to Display

If a window includes a table that has configurable columns and you select the **Action > Column Setting** option, use the following buttons on the Column Setting dialog box to specify which columns should be displayed in the table.

Button	Description
-->>	Move all current column headings from the **Available** (left) section to the **Selected** (right) section to show all the columns in the table.
-->	Select specific column headings in the **Available** (left) section. Then click this button to move those column headings to the **Selected** (right) section and add them to the table. (You can select one column heading and then use `Shift` + click or `Ctrl` + click to select multiple headings.)
<--	Select specific column headings in the **Selected** (right) section. Then click this button to move those column headings to the **Available** (left) section and remove them from the table. (You can select one column heading and then use `Shift` + click or `Ctrl` + click to select multiple headings.)
<<--	Move all current column headings from the **Selected** (right) section to the **Available** (left) section to hide all the columns in the table.

You can also select the **Auto Resize Columns** check box to make the sum of all column widths automatically match the width of the window in which the table is displayed.

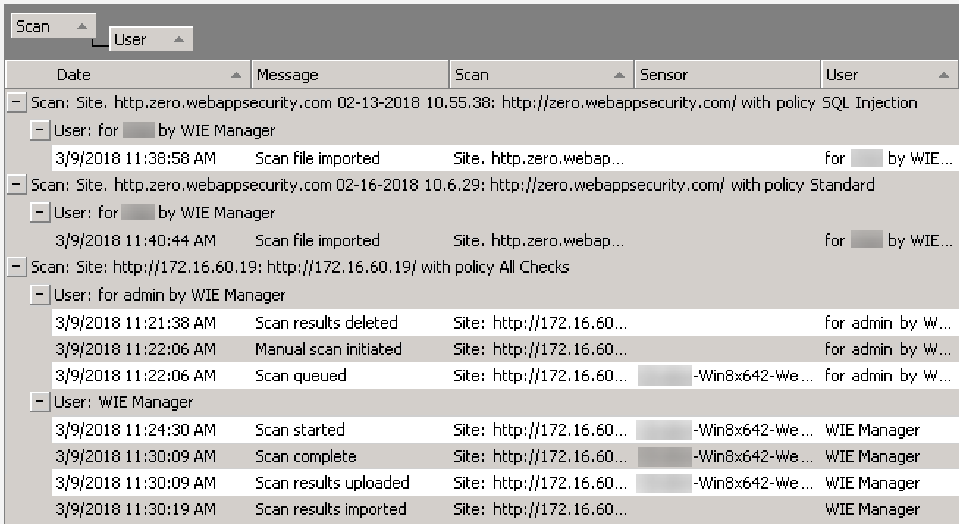
After you make your changes, click **OK**.

See Also

"About the User Interface" on page 33

Grouping and Sorting Items in Lists

The OpenText Fortify WebInspect Enterprise Administrative Console enables you to group and sort listed items on some windows. Grouping is designed as a tree structure in the upper section of the window. When nothing is grouped, this area displays the text "Drag a column header here to group by that column."



Date	Message	Scan	Sensor	User
Scan: Site. http.zero.webappsecurity.com 02-13-2018 10.55.38: http://zero.webappsecurity.com/ with policy SQL Injection				
User: for [redacted] by WIE Manager				
3/9/2018 11:38:58 AM	Scan file imported	Site. http.zero.webap...		for [redacted] by WIE...
Scan: Site. http.zero.webappsecurity.com 02-16-2018 10.6.29: http://zero.webappsecurity.com/ with policy Standard				
User: for [redacted] by WIE Manager				
3/9/2018 11:40:44 AM	Scan file imported	Site. http.zero.webap...		for [redacted] by WIE...
Scan: Site: http://172.16.60.19: http://172.16.60.19/ with policy All Checks				
User: for admin by WIE Manager				
3/9/2018 11:21:38 AM	Scan results deleted	Site: http://172.16.60...		for admin by W...
3/9/2018 11:22:06 AM	Manual scan initiated	Site: http://172.16.60...		for admin by W...
3/9/2018 11:22:06 AM	Scan queued	Site: http://172.16.60...	[redacted]-Win8x642-We...	for admin by W...
User: WIE Manager				
3/9/2018 11:24:30 AM	Scan started	Site: http://172.16.60...	[redacted]-Win8x642-We...	WIE Manager
3/9/2018 11:30:09 AM	Scan complete	Site: http://172.16.60...	[redacted]-Win8x642-We...	WIE Manager
3/9/2018 11:30:09 AM	Scan results uploaded	Site: http://172.16.60...	[redacted]-Win8x642-We...	WIE Manager
3/9/2018 11:30:19 AM	Scan results imported	Site: http://172.16.60...		WIE Manager

To group listed items:

1. Drag the desired column header to the "Drag a column header..." area. The selected column header becomes the "root" of the tree view in the list.
2. Drag a second column header and place it to the left or right of the first header. Red arrows indicate the expected insertion point.
   - Place it to the right to create a subordinate branch.
   - Place it to the left to make the second header the root and the first header the subordinate branch.

To sort the listed items, click a column header in the tree.

Certain columns cannot be grouped. If you drag these columns, the program displays a circle with an X (rather than the red arrow indicators).

The same column header may be inserted in more than one spot on the grouping tree view, if desired.

You can also drag column headers to rearrange the order in which columns are listed.

See Also

"About the User Interface" on page 33

Performing Common Tasks

Each of the topics in the following bullets contains information about common tasks you can perform with the OpenText Fortify WebInspect Enterprise Administrative Console, along with links to other information you might find helpful. The topics are a subset of the topics shown in the Help **Contents** tab and are organized under the same headings.

Administrative Console User Interface

- "Logging On" on page 36
- "Changing the Screen Refresh Rate " on page 37

SmartUpdate Management

- "Managing SmartUpdates" on the next page
- "Working with SmartUpdate Binary Files " on page 44

Proxy Server Setting Management

- "Managing Proxy Server Settings" on page 47

Role and Permission Management

- "About Roles and Permissions" on page 47 and "Managing Roles and Permissions" on page 48
- "Adding, Removing, and Distributing Global Roles" on page 49
- "About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52
- "About Organization Administrators, Roles, and Permissions" on page 57
- "About Group Administrators, Roles, and Permissions" on page 66

Scan Management

- "About Controlling Scans Using the Scan Queue" on page 76 and "Controlling Scans Using the Scan Queue" on page 78
- "About Managing Scan Policies" on page 78 and "Managing Scan Policies" on page 79
- "Adding, Editing, and Deleting Export Paths for Saving Scans" on page 82

Sensor Management

- "About Sensor Management " on page 83and "Managing Sensors and Their Scans" on page 84

Sensor User Management

- "Managing Sensor Users" on page 85

E-Mail Alerts and SNMP Alert Management

- "Adding, Editing, and Deleting E-mail Alerts" on page 85
- "Adding, Editing, and Deleting SNMP Alerts" on page 89

Software Security Center (SSC) Interaction Management

- "Configuring Settings for Fortify Software Security Center" on page 92
- "Importing Applications into Fortify Software Security Center from a CSV File" on page 94

> **Note:** These topics apply only if Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

Activity Log Management

- "Managing the Activity Log" on page 97

Connected-User Management

- "About Managing Connected Users" on page 95 and "Managing Connected Users" on page 96

License Information

- "Viewing License Information" on page 96

Support

- Contacting Customer Support

Managing SmartUpdates

Fortify engineers uncover new vulnerabilities almost every day. They develop attack agents to search for these malicious threats and then update the OpenText corporate database so that you will always be on the leading edge of Web application security. Use SmartUpdate to obtain Fortify's latest adaptive agents and programs, as well as vulnerability and policy information.

Each time you log in to the OpenText Fortify WebInspect Enterprise Administrative Console, the Fortify WebInspect Enterprise server contacts the OpenText data center via the Internet and downloads any available binary updates, including new or updated adaptive agents, vulnerability checks, and policy information.

You can also obtain updates to the SecureBase, as well as binary updates for Fortify WebInspect Enterprise-connected products such as OpenText Fortify WebInspect, either manually or automatically on a schedule you specify.

If your Fortify WebInspect Enterprise server is not allowed to connect to the Internet, see "Performing a SmartUpdate (Offline)" on page 43.

> **Note:** If you need to use a proxy server to communicate with the OpenText SmartUpdate database, select the **Proxy Server Settings** shortcut in the **Administration** group in the Administrative Console.

> **Note:** Scans cannot start while sensors are receiving a SmartUpdate. Scheduled scans stay in "pending" state until SmartUpdate completes. This prevents sensors from picking up partial SmartUpdates when they update their local SecureBase from Fortify WebInspect Enterprise.

To display the SmartUpdate form, select **Administration** in the left pane and then select the **SmartUpdate** shortcut above.

The top section of the SmartUpdate form lists each update package that has been downloaded from OpenText. Each item includes (by default):

- The date and time the download started.
- The date and time the download completed.
- The status of the event.
- If applicable, an error message describing any problem that occurred.

Select an item in the SmartUpdate History list to display details about that event.

The bottom section of the SmartUpdate form lists any updates that are scheduled. Each item includes (by default):

- The name assigned to the update.
- How often it is scheduled to occur (if it is a recurring event).
- The date and time it last occurred (if it is a recurring event).
- The next date and time it is scheduled to occur.

Managing the SmartUpdate History and Schedules

To manage the SmartUpdate history and schedules:

1. Select **Administration** in the left pane and then select the **SmartUpdate** shortcut above.
2. Click **Action** and then click one of the following options:
    - **Clear Completed Updates.** Delete from the list the SmartUpdates that have been completed.
    - **Add Schedule**. Schedule a SmartUpdate. See "Adding a SmartUpdate Schedule " on the next page.
    - **Edit Schedule.** After you select a scheduled SmartUpdate in the SmartUpdate Schedules list, modify its settings in the SmartUpdate Settings window.
    - **Delete Schedule.** After you select a scheduled SmartUpdate in the SmartUpdate Schedules list, delete it.
    - **History Column Setting.** Open the Column Setting window, allowing you to specify which columns should appear in the SmartUpdate History section of the form.
    - **Schedule Column Setting.** Open the Column Setting window, allowing you to specify which columns should appear in the SmartUpdate Schedules section of the form.

> **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

Performing a Manual SmartUpdate

To perform a manual SmartUpdate:

1. In the Fortify WebInspect Enterprise Administrative Console, click **SmartUpdate** in the toolbar, or select **Administration** in the left pane and then select the **SmartUpdate** shortcut above.

   A message informs you that SmartUpdate was started.
2. Click **OK**.
3. To view the results of the update:
   a. Select **Administration** in the left pane and then select the **Activity Log** shortcut above.
   b. Examine the messages related to SmartUpdate.

Adding a SmartUpdate Schedule

To add a schedule for SmartUpdates:

1. Select **Administration** in the left pane and then select the **SmartUpdate** shortcut above.
2. Click the **Add Schedule** option in the **Action** menu.

   > **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

   The SmartUpdate Settings window opens.
3. Select the **General** form in the left pane.
   a. Type a name for the event in the **Scheduled SmartUpdate Name** field.
   b. In the **Start Time** field, specify the date and time when SmartUpdate should run.

      To change the date, click the drop-down arrow and select a date from the calendar.
   c. Select the **Time Zone** as needed.
   d. If you want only one SmartUpdate to occur, skip to Step 5 below.
4. If you want SmartUpdates to recur on a regular schedule:
   a. Select the **Recurrence** form in the left column.
   b. Select the **Recurring** check box.
   c. Use the **Pattern** group to select the frequency of the event (daily, every *x* days, every weekday, weekly, every *x* weeks, monthly, every *x* months, or yearly) and then provide the associated results.
   d. Use the **Range** group to specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the SmartUpdate should

occur.

5. Click **OK** to schedule the update.

Performing a SmartUpdate (Offline)

Follow this process to perform a SmartUpdate for Fortify WebInspect Enterprise that is offline.

Stage	Description
1.	Open a support case. Fortify Customer Support personnel will provide you with the offline FTP server URL and login credentials (if needed). For more information, see Contacting Customer Support in the "Preface" on page 22.
2.	On a machine that can access the Internet, access the offline FTP server.
3.	Navigate to the **WIE** directory.
4.	Download the **OfflineSmartupdater.exe** and the latest offline SmartUpdate package. **Note:** The SmartUpdate package has a `.smartupdate` file extension.
5.	Transport both files to the WebInspect Enterprise server.
6.	Run the OfflineSmartupdater.exe on the server and follow the prompts in the wizard. 1. When prompted for the update package, browse to the offline `.smartupdate` file you downloaded. 2. When prompted for database credentials, log in as a database user with permission to update the database schema. 3. On the last page of the wizard, click **Finish**.
7.	Wait for the update to complete, and then close the wizard.

See Also

"Working with SmartUpdate Binary Files " on the next page

"How Updates Occur on the Client" on page 46

Working with SmartUpdate Binary Files

Numerous binary update files are generally available to download for OpenText Fortify WebInspect Enterprise's client products, such as OpenText Fortify WebInspect and sensors. These files include older versions and foreign-language versions of the product, which you might not need or plan to use. Additionally, downloading all of these files could deplete a large amount of hard drive space.

You can review the available binary update files on the SmartUpdate Approval page, and select the ones you want to download. No binary file will be downloaded unless you choose to download it.

Updating the List of Available Binary Files

Upon initial installation, there will not be a list of available binary update files on the SmartUpdate Approval page. You will need to obtain the list of available files. For existing installations, if you have not performed a manual SmartUpdate or your scheduled SmartUpdate has not yet occurred, you will need to update the list of available files.

To obtain or update the list of available binary update files:

1. In the Fortify WebInspect Enterprise Administrative Console, click **SmartUpdate** in the toolbar.

   A message informs you that SmartUpdate was started.
2. Click **OK**.

Updates to SecureBase and SmartUpdater

Updates to SecureBase and the SmartUpdater are downloaded automatically.

Accessing the SmartUpdate Approval Form

To access the SmartUpdate Approval form and view the list of available updates:

- Select **Administration** in the left pane and then select **SmartUpdate Approval**.

You can group items in the list of available updates according to product, importance, or approval status.

Viewing Update Details

You can view the details of a particular binary update file in the Update Details section of the SmartUpdate Approval form. When you select a binary file in the list of available updates, the Update Details section is populated with a summary of the update, a list of features included, a list of prerequisites that must be installed prior to installing the update, and a list of files to be downloaded as part of the update. The size of each file to be downloaded is provided in parentheses after the file name.

Downloading Binary Update Files

You can download binary update files that have a Download Status of “Not Downloaded.”

To download one binary update file:

- Right-click the file to download and select **Download**.

  The selected update file is downloaded.

To download multiple binary update files:

1. Select multiple files to be downloaded.

   Note: All files selected must have the Download Status of “Not Downloaded.”

2. Right-click and select **Download**.

   The selected update file is downloaded.

Note: You might need to click Refresh to update the Download Status.

Approving or Declining Binary Update Files

None of the client applications can be updated until an administrator specifically approves the update.

The possible approval statuses are:

- **Not Approved** — Update has not yet been reviewed by the administrator.
- **Approved** — Update has been approved by the administrator and is available to clients.
- **Decline** — Update has been withheld by the administrator and is not available to clients.

After a file has been downloaded, you can approve it or decline it for installation on clients. To approve or decline a binary update file:

- Right-click a binary file that has a Download Status of “Downloaded” in the list and select one of the following options:
  - **Approve** — Make the binary update available to clients.
  - **Decline** — Withhold distribution of the binary update.

Note: The availability of particular options depends on the permissions granted to you by your assigned role.

For more information, see "How Updates Occur on the Client" on the next page.

Deleting a Downloaded File

If you have downloaded a file that you do not want or no longer need, you can delete it.

Important! Do not manually delete downloaded binary files from the WebInspect Enterprise Manager ProgramData folder. Delete downloaded files only on the SmartUpdate Approval page as described in this topic.

To delete a file:

- Right-click a binary file in the list with a Download Status of “Downloaded” and select **Delete Download**.

> **Note:** To prevent accidental deletion of a file you intend to make available to clients, you cannot delete a file with an Approval status of “Approved.” To delete the file, you must first change the Approval status to “Declined,” and then right-click the file and select **Delete Download**.

To delete multiple files:

1. Select multiple files to be deleted.

   > **Note:** All files selected must have the same Download status and Approval status. Otherwise, the delete option is not available.

2. Right-click and select **Delete Download**.

See Also

"Managing SmartUpdates" on page 40

"How Updates Occur on the Client" below

How Updates Occur on the Client

Once administrative approval is obtained, the update becomes available to client applications. For Fortify WebInspect, the SmartUpdate utility displays a window notifying users that an update is available. Users may either accept or reject the update. Updates for sensors (which do not have a user interface) are controlled by the Fortify WebInspect Enterprise Manager. If approved updates are available, a sensor will be required to download and apply the update before a scan can be assigned.

Typically, administrators prefer to update a single application instance and test it before performing a system-wide installation. This can be done by manually installing the updates on a test system. Sensor scans can be tested on a non-approved version of Fortify WebInspect (such as a special build developed for a specific customer) by selecting the specific sensor when configuring the scan in Fortify WebInspect Enterprise.

> **Note:** You can enable the **Can participate in "Any Available" sensor scans** option for any sensor. This includes sensors that are running a non-approved version of Fortify WebInspect, such as a special build developed for a specific customer.

SmartUpdate Affect on Scans

Scans cannot start while sensors are receiving a SmartUpdate. Scheduled scans stay in “pending” state until SmartUpdate completes. This prevents sensors from picking up partial SmartUpdates when they update their local SecureBase from Fortify WebInspect Enterprise.

See Also

"Managing SmartUpdates" on page 40

"Working with SmartUpdate Binary Files " on page 44

Managing Proxy Server Settings

If you use a proxy server to communicate with OpenText for SmartUpdates and licensing issues:

1. Select **Administration** in the left pane and then select the **Proxy Server Setting** shortcut above.
2. Select the **Use Proxy Server** option.
3. Provide the requested information.
4. Click **Save**.

> **Note:** SmartUpdates are not available if you use a SOCKS4 or SOCKS5 proxy server configuration. SmartUpdates are available through a proxy server only when using a standard proxy server.

About Roles and Permissions

A role is a named collection of permissions that administrators specify. From the Administrative Console, select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above to display the Roles and Permissions form. This form enables you to assign administrators and roles for three levels of Security Group Hierarchy—OpenText Fortify WebInspect Enterprise System, organization, and group. Each level has at least one administrator.

Administrators at each level can define roles, assign users to roles, and configure other security-related parameters. By assigning other users to roles, administrators can give them access to the Fortify WebInspect Enterprise system while limiting the functions they are allowed to perform, considering security. A user can be a member of more than one role.

You can specify one or more organizations, and each organization can have one or more subordinate groups. At installation, there is one organization named Default Organization, which contains one group named Default Group.

Each security level has categories of activities, and some of the categories are used in several levels. The set of activities in each category varies among categories. You can set the permission for an entire category or for its individual activities to Allowed, Unassigned, or Denied. Examples:

- Fortify WebInspect Enterprise System and organizations include the Policies category. Its activities are Can Import, Can View, Can Update, and Can Delete. When you create a role for Fortify WebInspect Enterprise System or an organization, you can set the permission to Allowed, Unassigned, or Denied for each Policies activity independently, or for the entire Policies category at once.
- Organizations and groups include the Blackout category. Its activities are Can Create, Can View, Can Update, and Can Delete. (Notice that this is a slightly different set of activities than the Policies category of the previous example.) When you create a role for an organization or a group, you can

set the permission to Allowed, Unassigned, or Denied for each Blackout activity independently, or for the entire Blackout category at once.

Note: Having the set of options Allowed, Unassigned, and Denied for permissions may seem ambiguous or redundant, but it enables Fortify WebInspect Enterprise to resolve conflicting permissions when a user is a member of more than one role. The role priorities are:

- Allowed outranks Unassigned—If the permission for a particular activity in Role A is Allowed and the permission for the same activity in Role B is Unassigned, then a user who is a member of both Role A and Role B *can* perform the activity.
- Denied outranks Allowed—If the permission for a particular activity in Role A is Allowed, and the permission for the same activity in Role B is “Denied,” then a user who is a member of both Role A and Role B *cannot* perform the activity.
- Unassigned (only) equals Denied—If a user’s permission for a particular activity is Unassigned and no other permissions are assigned to that user in another role for the same activity, then the user *cannot* perform the activity.

For information about managing roles and permissions at the Fortify WebInspect Enterprise System level, see "About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52.

For information about managing roles and permissions at the organization level, see "About Organization Administrators, Roles, and Permissions" on page 57.

For information about managing roles and permissions at the group level, see "About Group Administrators, Roles, and Permissions" on page 66.

See Also

"Managing Roles and Permissions" below

"About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52

"About Organization Administrators, Roles, and Permissions" on page 57

"About Group Administrators, Roles, and Permissions" on page 66

Managing Roles and Permissions

To manage roles and permissions functions that can be accessed from the **Action** menu items in the **Roles and Permissions** shortcut:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an entry in the Security Group Hierarchy (WebInspect Enterprise System, an organization, or a group).

3. Click **Action** or right-click the selected item in the Security Group Hierarchy, and then click one of the following options:

   - **Add Organization.** After you select WebInspect Enterprise System in the Security Group Hierarchy, create an organization. See "Adding, Removing, and Renaming Organizations" on page 58.
   - **Rename Organization.** After you select an organization in the Security Group Hierarchy, change its name. See "Adding, Removing, and Renaming Organizations" on page 58.
   - **Remove Organization.** After you select an organization in the Security Group Hierarchy, remove (delete) it. See "Adding, Removing, and Renaming Organizations" on page 58.
   - **Add Group.** After you select an organization in the Security Group Hierarchy, add a new group to it. See "Adding, Removing, and Renaming Groups" on page 68.
   - **Rename Group.** After you select a group in the Security Group Hierarchy, change its name. See "Adding, Removing, and Renaming Groups" on page 68.
   - **Remove Group.** After you select a group in the Security Group Hierarchy, remove (delete) it. See "Adding, Removing, and Renaming Groups" on page 68.
   - **Add User(s) to Roles.** After you select an item in the Security Group Hierarchy, add a user to multiple roles simultaneously. See "Adding a User Or Group To Multiple Roles" on page 51.
   - **Role Membership and Removal.** After you select an item in the Security Group Hierarchy, click the option, specify a user name or group name, and display members in the role, optionally remove a user or group from a role. See "Displaying or Removing Roles of Users or Groups" on page 52.

> **Note:** The availability of particular options depends on the type of item selected in the Security Group Hierarchy and on the permissions granted to you by your assigned role.

See Also

"About Roles and Permissions" on page 47

Adding, Removing, and Distributing Global Roles

A global role is one that defines permissions for all three hierarchical levels (OpenText Fortify WebInspect Enterprise System, organization, and group). When it is created, Fortify WebInspect Enterprise automatically copies the role to all levels (that is, to the Fortify WebInspect Enterprise System, to every organization, and to every group). However, you may subsequently remove the global role from specific organizations. Users can be added independently at each level, but permissions can be changed only at the Fortify WebInspect Enterprise System level, and only on the **Global Roles** tab. Any and all changes to a global role are propagated to each copy at all hierarchical levels.

Adding a Global Role

To add a global role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Global Roles** tab.
4. Click **Add** (the button above **Rename**).
5. On the New Role dialog box, enter a name for the role, select the default permission category that will be assigned to each activity, and click **OK**.
6. In the **Permissions** list, expand the System, Organization and Group permissions and select the **Unassigned, Allowed,** or **Denied** permission for each category of activities or for particular activities in each category, as desired.

Removing a Global Role

To remove a global role from specific organizations:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Global Roles** tab.
4. Select a role.
5. If the **All Organizations** check box is selected, clear it.
6. Select an organization from which the selected role should be deleted.
7. Click **Remove**.

Distributing an Existing Global Role to All Organizations

To distribute a global role to all organizations if it is currently restricted to particular organizations:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Global Roles** tab.
4. Select a role assigned to specific organizations.
5. Select **All Organizations**.

Note: Whenever you create an organization, Fortify WebInspect Enterprise automatically distributes to that organization all the global roles for which the All Organizations option is selected.

See Also

"About Roles and Permissions" on page 47

"About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on the next page

Adding a User Or Group To Multiple Roles

You can add a user or group to roles in individual organizations or groups, repeating the process as often as necessary until the user or group has been inserted into all desired roles. Although this is quick and easy when dealing with one user or group and one role, it can be repetitious and time-consuming for multiple users or groups and roles. The **Action** menu option **Add User(s) to Roles** enables you to add a user or group to multiple roles simultaneously.

To add a user or group to multiple roles simultaneously:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Click **Action** and select **Add User(s) to Roles**.

   The Add User to Roles dialog box opens.
3. Do one of the following:
   - If OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, type a user name or group name in the **User/Group name** text box, or click **Browse** to open the Select SSC Users or Groups dialog box and select a user or group.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     i. Click **Advanced**.

        The Select Users or Groups window appears.
     ii. Search for and select the user or group name you want to add to roles, and click **OK**.
     iii. Click **OK**.
4. Select a role from the **Roles** list.

   For information about global roles, which include “(global)” as a suffix, see "Adding, Removing, and Distributing Global Roles" on page 49.

   “All Custom Roles” are the roles that have been added at all levels—Fortify WebInspect Enterprise System, organizations, and groups.
5. Continue as follows:
   - If you selected a global role, under **Permission Hierarchy** select which organizations and groups containing that role are to be updated to include the user or group you selected.
   - If you selected **(All Custom Roles)**, under **Permission Hierarchy** select the roles to which the user or group you selected is to be assigned.
6. Click **Apply**.

See Also

"About Roles and Permissions" on page 47

Displaying or Removing Roles of Users or Groups

The Role Membership and Removal form displays the roles to which the user or group you specify is assigned. You can then remove the user or group from that role.

To display and optionally remove roles assigned to a user or group:

1. Select Administration in the left pane and then select the Roles and Permissions shortcut above.
2. Click **Action** and select **Role Membership and Removal**.

   The Role Membership and Removal dialog box appears.
3. Type a user or group name, or click **Browse** to find and select a user or group.
4. Click **Search**.

   If you entered your own user name or the name of a group to which you belong, OpenText Fortify WebInspect Enterprise displays all the roles to which you are assigned.

   If you entered a user name or group name other than your own, you must be an administrator to see their roles. Fortify WebInspect Enterprise displays the roles to which the specified user or group is assigned, but only for those organizations and groups for which you are an administrator.
5. To remove a user or group (that is, a member) from a role, select the check boxes for the roles from which they are to be removed and click **Remove**.

See Also

"About Roles and Permissions" on page 47

About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions

OpenText Fortify WebInspect Enterprise system administrators have all permissions with no IP restrictions. No one else can log on until the initial system administrator assigns other users to roles during or after the installation procedures. A Fortify WebInspect Enterprise system administrator can:

- Add other users as Fortify WebInspect Enterprise system administrators.
- Create, rename, and delete organizations.
- Create roles that allow access to certain Fortify WebInspect Enterprise Administrative Console features and assign users to those roles (thereby limiting the functions a specific user may perform).

Fortify WebInspect Enterprise System roles have the following categories of activities:

- Activity Log
- Licensing

- SmartUpdate
- E-mail Alerts
- SNMP Alerts
- Export Paths
- Sensors
- Policies

When you select **WebInspect Enterprise System** from the Security Group Hierarchy pane, the following tabs appear in the System Permissions section:

- **Administrators**. Use this tab to add or remove system administrators. See "Adding and Removing Fortify WebInspect Enterprise System Administrators" below.
- **Roles**. Use this tab to add a Fortify WebInspect Enterprise System role, assign groups or users to a Fortify WebInspect Enterprise System role, or copy a Fortify WebInspect Enterprise System role for use at the Fortify WebInspect Enterprise System level, the organization level, or the group level. See "Managing Fortify WebInspect Enterprise System Roles and Permissions" on the next page.
- **Global Roles**. Use this tab to add or remove global roles, and to distribute a global role to all organizations if it is currently restricted to particular organizations. See "Adding, Removing, and Distributing Global Roles" on page 49.

Adding an Organization

Every system must have at least one organization. You can add an organization with any of the tabs selected. For more information, see "Adding, Removing, and Renaming Organizations" on page 58.

See Also

"About Roles and Permissions" on page 47

Adding and Removing Fortify WebInspect Enterprise System Administrators

OpenText Fortify WebInspect Enterprise system administrators have all permissions with no IP restrictions. No one else can log on until the initial system administrator assigns other users to roles during or after the installation procedures. A Fortify WebInspect Enterprise system administrator can:

- Add other users as Fortify WebInspect Enterprise system administrators.
- Create, rename, and delete organizations.
- Create roles that allow access to certain Fortify WebInspect Enterprise Administrative Console features and assign users to those roles (thereby limiting the functions a specific user may perform).

This topic describes how to add and remove Fortify WebInspect Enterprise System administrators.

Adding a Fortify WebInspect Enterprise System Administrator

To add a Fortify WebInspect Enterprise system administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Click **Add**.
5. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     1. Click **Advanced**.

        The Select Users or Groups window appears.
     2. Search for and select the user or group name you want to add to roles, and click **OK**.
     3. Click **OK**.
6. Click **OK**.

Removing a Fortify WebInspect Enterprise System Administrator

To remove a Fortify WebInspect Enterprise system administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Select a user group or user name.
5. Click **Remove**.

See Also

"About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52

Managing Fortify WebInspect Enterprise System Roles and Permissions

This topic describes the following tasks:

- "Adding a Fortify WebInspect Enterprise System Role " on the next page
- "Assigning Groups or Users to a Fortify WebInspect Enterprise System Role " on page 56

- "Copying a Fortify WebInspect Enterprise System Role " on the next page

  The copy can be used at the Fortify WebInspect Enterprise System level, the organization level, or the group level.

Adding a Fortify WebInspect Enterprise System Role

To add a Fortify WebInspect Enterprise System role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Click **Add** (to the right of the **Role Name** pane).
5. On the New Role dialog box, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.
6. In the **Permissions** list, expand the nodes to view the activities associated with each category.

   > **Note:** Having the set of options Allowed, Unassigned, and Denied for permissions enables Fortify WebInspect Enterprise to resolve conflicting permissions when a user is a member of more than one role. The role priorities are:
   >
   > - Allowed outranks Unassigned—If the permission for a particular activity in Role A is Allowed and the permission for the same activity in Role B is Unassigned, then a user who is a member of both Role A and Role B *can* perform the activity.
   > - Denied outranks Allowed—If the permission for a particular activity in Role A is Allowed, and the permission for the same activity in Role B is “Denied,” then a user who is a member of both Role A and Role B *cannot* perform the activity.
   > - Unassigned (only) equals Denied—If a user’s permission for a particular activity is Unassigned and no other permissions are assigned to that user in another role for the same activity, then the user *cannot* perform the activity.

7. To assign the same permission to all activities within a single category:
   a. Click the category name (such as “Activity Log”).
   b. Click the drop-down arrow that appears on the far right end of the row.
   c. Select a permission.
8. To change permission for a single activity:
   a. Expand a category.
   b. Click the activity name (such as “Can view log”).
   c. Click the drop-down arrow that appears on the far right end of the row.
   d. Select a permission.

Assigning Groups or Users to a Fortify WebInspect Enterprise System Role

To assign groups or users to a Fortify WebInspect Enterprise System role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a name in the **Role name** list.
5. Click **Add** (on the far right of the **User group or user names** pane).
6. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     i. Click **Advanced**.

        The Select Users or Groups window appears.

     ii. Search for and select the user or group name you want to add to roles, and click **OK**.
     iii. Click **OK**.
7. Click **OK**.

Copying a Fortify WebInspect Enterprise System Role

You can copy a Fortify WebInspect Enterprise System role and keep it at the Fortify WebInspect Enterprise System level or assign it to an organization or group. You must be an administrator of an organization or group to copy a Fortify WebInspect Enterprise System role to it.

To copy a Fortify WebInspect Enterprise System role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Copy/Move**.
6. On the Copy/Move Role dialog box, specify the **Role Name** for the copy and select the organization or group to which the role will be assigned.

   The same role can be assigned to multiple organizations and groups.
7. To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role in the copy.
8. To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying a Fortify WebInspect Enterprise System role to an organization or a

group.

9. Select the organization or group to which the Fortify WebInspect Enterprise System role will be copied.
10. Click **OK**.

See Also

"About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52

About Organization Administrators, Roles, and Permissions

The system administrator who creates an organization automatically becomes an administrator for that organization. An organization administrator can:

- Assign other users as organization administrators.
- Determine which objects are available to that organization (for example, select which of the available scanning policies may be used by applications within an organization).
- Set the maximum priority level that can be assigned to scans conducted by this organization.
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the OpenText Fortify WebInspect Enterprise Web Console.
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one organization to another.
- Create, rename, and delete applications.

You are not required to configure multiple organizations. If you prefer, you may associate all applications with a single organization.

Organization roles have the following categories of activities:

- Blackouts
- Policies
- E-mail Alerts
- SNMP Alerts
- Reports

Security within the Fortify WebInspect Enterprise system is arranged according to a hierarchy of organizations and groups. A Fortify WebInspect Enterprise system can have one or more organizations, and each organization can have one or more subordinate groups. At installation, there is one organization named Default Organization, which contains one group named Default Group.

When you select an organization from the Security Group Hierarchy pane, the following tabs appear in the Organization Permissions section:

- **Administrators**. Use this tab to add or remove organization administrators. See "Adding and Removing Organization Administrators" on page 59.

- **Configuration**. Use this tab to set the maximum scan priority for an organization and to enable or disable the Retest feature, which enables you to view the server's response as rendered in a browser. See "Configuring Organization Options" on page 60.
- **Roles**. Use this tab to add groups or users to an organization role. See "Managing Organization Roles And Permissions" on page 61.
- **Resources**. From this tab, you can make export paths, policies, and sensors available or unavailable to a selected organization. See "Specifying Resources Available to Organizations" on page 64.
- **Move/Copy Objects**. Use this tab to copy an organization role to any hierarchy level or to move a role from one organization to another. See "Moving or Copying Objects to Groups or Other Organizations" on page 65.

> **Note:** When Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center and an application version is created in Fortify Software Security Center, it is also created automatically in Fortify WebInspect Enterprise, where it is added to the Default Group in the Default Organization. If you want a different group in the same or a different organization to have access to a particular application version in Fortify WebInspect Enterprise, use the Administrative Console to move that application version to that group. See "About Group Administrators, Roles, and Permissions" on page 66.

See Also

"About Roles and Permissions" on page 47

Adding, Removing, and Renaming Organizations

This topic describes how to add an organization, remove an organization, and rename an organization.

Adding an Organization

To add an organization:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Click **Action** and select **Add Organization**.

   The Create Organization dialog box appears.
5. In the **Name** field, type a name for the organization.
6. Click **OK**.

> **Note:** Whenever you create an organization, OpenText Fortify WebInspect Enterprise automatically distributes to that organization all global roles for which the **All Organizations** option is selected.

Removing an Organization

To remove an organization:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click **Action** and select **Remove Organization**.
4. Confirm that you want to remove the organization.

Renaming an Organization

To rename an organization:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click **Action** and select **Rename Organization**.

   The Rename Organization dialog box appears.
4. Type a new name for the organization.
5. Click **OK**.

See Also

"About Fortify WebInspect Enterprise System Administrators, Roles, and Permissions" on page 52

"About Organization Administrators, Roles, and Permissions" on page 57

Adding and Removing Organization Administrators

The system administrator who creates an organization automatically becomes an administrator for that organization. An organization administrator can:

- Assign other users as organization administrators.
- Determine which objects are available to that organization (for example, select which of the available scanning policies may be used by applications within an organization).
- Set the maximum priority level that can be assigned to scans conducted by this organization.
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the OpenText Fortify WebInspect Enterprise Web Console.
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one organization to another.
- Create, rename, and delete applications.

This topic describes how to add or remove organization administrators.

Adding an Organization Administrator

To add an organization administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Click **Add**.
5. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     1. Click **Advanced**.

        The Select Users or Groups window appears.
     2. Search for and select the user or group name you want to add to roles, and click **OK**.
     3. Click **OK**.
6. Click **OK**.

Removing an Organization Administrator

To remove an organization administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Select a user group or user name.
5. Click **Remove**.

See Also

"About Organization Administrators, Roles, and Permissions" on page 57

Configuring Organization Options

To configure the organization options:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Configuration** tab.

Configuring Option: Organization Maximum Security Priority

If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. For each organization, you can specify the maximum priority level that may be assigned to scans.

Select the highest priority level that a user in this organization may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

A group administrator can limit the members of the group to running scans of the same or lower (but not higher) maximum priority than is specified for the parent organization. For example, if the maximum priority for an organization is 3, the administrator of a group within that organization can set the group maximum priority to 3, 4 or 5, but not to 1 or 2.

Configuring Option: Disable Retest Browser Tab

The Retest feature enables you to view the server’s response as rendered in a browser. Retesting a cross-site scripting vulnerability, however, may cause the script to loop infinitely on the Browser tab when using Microsoft Internet Explorer. If you are concerned about executing a cross-site scripting attack that may be embedded in your application, select the **Disable Retest Browser Tab** option to disable the Retest feature.

See Also

"About Organization Administrators, Roles, and Permissions" on page 57

Managing Organization Roles And Permissions

This topic describes how to:

- Add an organization role
- Add groups or users to an organization role
- Copy or move an organization role

  > **Note:** A copy can be used at the OpenText Fortify WebInspect Enterprise System level, the organization level, or the group level, and you can move a role from one organization to another.

- Remove an organization role
- Rename an organization role

Adding an Organization Role

To add an organization role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.

3. Click the **Roles** tab.
4. Click **Add** (to the right of the **Role Name** pane).
5. On the New Role dialog box, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.
6. In the **Permissions** list, expand the nodes to view the activities associated with each category.

> **Note:** Having the set of options Allowed, Unassigned, and Denied for permissions enables Fortify WebInspect Enterprise to resolve conflicting permissions when a user is a member of more than one role. The role priorities are:
>
> - Allowed outranks Unassigned—If the permission for a particular activity in Role A is Allowed and the permission for the same activity in Role B is Unassigned, then a user who is a member of both Role A and Role B *can* perform the activity.
> - Denied outranks Allowed—If the permission for a particular activity in Role A is Allowed, and the permission for the same activity in Role B is “Denied,” then a user who is a member of both Role A and Role B *cannot* perform the activity.
> - Unassigned (only) equals Denied—If a user’s permission for a particular activity is Unassigned and no other permissions are assigned to that user in another role for the same activity, then the user *cannot* perform the activity.

7. To assign the same permission to all activities within a single category:
   a. Click the category name (such as “Blackouts" or "Policies”).
   b. Click the drop-down arrow that appears on the far right end of the row.
   c. Select a permission.
8. To change permission for a single activity:
   a. Expand a category.
   b. Click the activity name (such as “Can create" or "Can view”).
   c. Click the drop-down arrow that appears on the far right end of the row.
   d. Select a permission.

Adding Groups or Users to an Organization Role

> **Note:** To save time when assigning a user to multiple roles, see "Adding a User Or Group To Multiple Roles" on page 51.

To add groups or users to an organization role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a name in the **Role name** list.
5. Click **Add** (on the far right of the **User group or user names** pane).

6. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     i. Click **Advanced**.

        The Select Users or Groups window appears.

     ii. Search for and select the user or group name you want to add to roles, and click **OK**.

     iii. Click **OK**.
7. Click **OK**.

Copying or Moving an Organization Role

You can copy an organization role to any level (system, organization, or group). You can also move a role from one organization to another, which will remove it from the original organization. You must be an administrator of the target organization to copy or move an organization role to it.

To move or copy an organization role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Copy/Move**.
6. On the Copy/Move Role dialog box, specify the **Role Name** for the copy and select the organization or group to which the role will be assigned.

   The same role can be assigned to multiple organizations and groups. The permissions associated with a role can be copied or moved only between similar levels (that is, from one group to another or from one organization to another).
7. To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role in the copy.
8. To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying an organization role and assigning it to a group or to the system.
9. Select the system, organization, or group to which the organization role will be copied or moved.
10. Do one of the following:
    - Click **OK** to copy the organization role.
    - Click **Move** to move the organization role. This option is available only if you move the organization role, along with its users and permissions, to another organization.

Removing an Organization Role

Note: You cannot remove a global role.

To remove an organization role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Remove**.
6. Confirm that you want to remove the organization role.

Renaming an Organization Role

Note: You cannot rename a global role.

To rename an organization role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Rename**.
6. Type a new name for the organization role.
7. Click **OK**.

See Also

"About Organization Administrators, Roles, and Permissions" on page 57

Specifying Resources Available to Organizations

You can specify which resources—export paths, policies, or sensors—are available to an organization. For example, the OpenText Fortify WebInspect Enterprise system contains approximately 20 scanning policies. Your organization administrator can choose to allow members of the organization to use only particular policies.

Note: A group administrator can further restrict which resources are available to a group in the organization.

To manage resources that are available to organizations:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Click the **Resources** tab.
4. Select an item in the **Object Type** list. On the **Resources** tab, organizations have the following object types:
   - Export Paths
   - Policies
   - Sensors

   Objects of the selected type that are not allowed appear in the **Available** column. Objects that are allowed appear in the **Allowed** column.
5. Do one of the following to make one or more objects available (but not allowed), or allowed:
   - To move particular objects from the **Available** column to the **Allowed** column, select one or more of them and click [>].
   - To move all objects from the **Available** column to the **Allowed** column, click [>>].
   - To move particular objects from the **Allowed** column to the **Available** column, select one or more of them and click [<].
   - To move all objects from the **Allowed** column to the **Available** column, click [<<].

See Also

"About Organization Administrators, Roles, and Permissions" on page 57

Moving or Copying Objects to Groups or Other Organizations

You can assign a particular user-created object to a different organization (and optionally to a group) by either moving it or copying it. Moving an object removes it from its currently assigned location. Copying an object retains its current location while also placing a copy in a new location.

To move or copy an object from an organization to a different organization and optionally to a group:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select an organization in the Security Group Hierarchy pane.
3. Select the **Move/Copy Objects** tab.

4. Select an item in the **Object Type** list. On the **Move/Copy Objects** tab, organizations have the following object types:
    - Blackouts
    - E-mail Alerts
    - Policies
    - Scan Templates
    - SNMP Alerts
5. Click **Retrieve**.

    All user-created objects of the selected type appear in the **Object Results** list.
6. Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.
7. Click **Move** or **Copy**.
8. On the Move Objects or Copy Objects window, select an organization from the **Target Organization** list.
9. (Optional) Select a group from the **Security Group** list.
10. If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list. Examples:
    - You are not allowed to move a user-created (custom) policy from Organization A to Organization B if that policy is to be used for a scheduled scan in Organization A.
    - If you are moving a user-created scan template from one organization to another, and that template uses a scan policy that is not in the target organization, then you must also move (or copy) the scan policy.

    For each dependent object, click the drop-down arrow in the Action column under Object Dependencies and select the appropriate action (such as **Move to, Copy to,** or **Allow**).
11. Click **Move** or **Copy**.
12. When a dialog box appears informing you that all dependencies have been satisfied and prompting you to commit the move or copy, click **Yes**.

See Also

"About Organization Administrators, Roles, and Permissions" on page 57

About Group Administrators, Roles, and Permissions

An organization administrator who creates a group automatically becomes an administrator for that group. A group administrator can:

- Assign other users as group administrators.
- Determine which objects are available to that group (for example, select which of the scanning policies made available to the organization may be used by this group).

- Set the maximum priority level that can be assigned to scans conducted by this group (within the limits established for the organization’s maximum priority level).
- Specify which URLs or IP addresses may be scanned by this group.
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the OpenText Fortify WebInspect Enterprise Web Console.
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one group to another.

Group roles have the following categories of activities:

- Application Versions
- Scans
- Scan Templates
- Scheduled Scans
- E-mail Alerts
- SNMP Alerts
- Blackouts
- Fortify Toolkit

Security within the Fortify WebInspect Enterprise system is arranged according to a hierarchy of organizations and groups. A Fortify WebInspect Enterprise system can have one or more organizations, and each organization can have one or more subordinate groups. At installation, there is one organization named Default Organization, which contains one group named Default Group.

When you select a group from the Security Group Hierarchy pane, the following tabs appear in the Group Permissions section:

- **Administrators**. Use this tab to add or remove group administrators. See "Adding and Removing Group Administrators" on page 69.
- **Configuration**. Use this tab to set the maximum scan priority for a group and to configure group IP and host permissions. See "Configuring Group Options" on page 70.
- **Roles**. Use this tab to add groups or users to a group role. See "Managing Group Roles And Permissions" on page 71.
- **Resources**. From this tab, you can make export paths, policies, and sensors available or unavailable to a selected group. See "Specifying Resources Available to Groups" on page 74.
- **Move/Copy Objects**. Use this tab to copy a group role to any hierarchy level or to move a role from one group to another. See "Moving or Copying Objects to Organizations or Other Groups" on page 75.

Each group must be associated with an organization. If you don't want a certain user to see certain sites or scans, you must create separate groups and assign the user to a role in one group or the other.

Note: When Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center and an application version is created in Fortify Software Security Center, it is also created automatically in Fortify WebInspect Enterprise, where it is added to the Default Group in the Default Organization. If you want a different group in the same or a different organization to have access to a particular application version in Fortify WebInspect Enterprise, use the Administrative Console to move that application version to that group.

See Also

"About Roles and Permissions" on page 47

Adding, Removing, and Renaming Groups

This topic describes how to add a group, remove a group, and rename a group.

Adding a Group

To add a group:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. In the Security Group Hierarchy pane, select the organization to which you want to add a group.
3. Click the **Administrators** tab.
4. Click **Action** and select **Add Group**.

   The Create Group dialog box appears.
5. In the **Name** field, type a name for the group.
6. Select the highest priority level that a user in this group may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

   If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. Your choices may be restricted by your organization.
7. In the **Scan Permissions** section, click **Add**.
8. In the **Host** field, type a host name (wild cards are allowed), IP address, or IP address range, and click **OK**.

   To specify a range of addresses, enter the lowest numerical address, followed by a dash (-), and then followed by the highest numerical address, such as 134.55.33.4-134.55.33.244.

   You can also use wild cards, such as 134.55.33.* and www.mysite.*. Enter only an asterisk (*) to allow all possible IP addresses.
9. In the **Properties** pane, you can:
   - Change the IP address or the host name.
   - Change permissions for running a Web Site scan and Web Service scan.
10. Click **OK**.

Note: A user who creates a group is automatically assigned as an administrator of that group.

Removing a Group

To remove a group:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click **Action** and **Remove Group**.
4. Confirm that you want to remove the group.

Renaming a Group

To rename a group:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click **Action** and select **Rename Group**.

   The Rename Group dialog box appears.

4. Type a new name for the group.
5. Click **OK**.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Adding and Removing Group Administrators

An organization administrator who creates a group automatically becomes an administrator for that group. A group administrator can:

- Assign other users as group administrators.
- Determine which objects are available to that group (for example, select which of the scanning policies made available to the organization may be used by this group).
- Set the maximum priority level that can be assigned to scans conducted by this group (within the limits established for the organization’s maximum priority level).
- Specify which URLs or IP addresses may be scanned by this group.
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the OpenText Fortify WebInspect Enterprise Web Console.
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one group to another.

This topic describes how to add or remove group administrators.

Adding a Group Administrator

To add a group administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Click **Add**.
5. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     1. Click **Advanced**.

        The Select Users or Groups window appears.
     2. Search for and select the user or group name you want to add to roles, and click **OK**.
     3. Click **OK**.
6. Click **OK**.

Removing a Group Administrator

To remove a group administrator:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Administrators** tab.
4. Select a user group or user name.
5. Click **Remove**.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Configuring Group Options

To configure the group options:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Configuration** tab.

Configuring Option: Group Maximum Security Priority

If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. For each group, you can specify the maximum priority level that may be assigned to scans.

Select the highest priority level that a user in this group may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).

A group administrator can limit the members of the group to running scans of the same or lower (but not higher) maximum priority than is specified for the parent organization. For example, if the maximum priority for an organization is 3, the administrator of a group within that organization can set the group maximum priority to 3, 4 or 5, but not to 1 or 2.

Configuring Option: Group IP and Host Permissions

For each group, the ability to scan web sites is restricted to those IP addresses or hosts specified as follows:

1. Click **Add**.
2. Enter an IP address or host name and click **OK**.

   To specify a range of addresses, enter the lowest numerical address, followed by a dash (-), and then followed by the highest numerical address, such as 134.55.33.4-134.55.33.244.

   You can also use wild cards, such as 134.55.33.* and www.mysite.*. Enter only an asterisk (*) to allow all possible IP addresses.
3. In the Properties pane, select **Can Run Scan**, click the drop-down arrow that appears, and select **Unassigned, Allowed,** or **Denied**.
4. Repeat this procedure to specify additional targets.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Managing Group Roles And Permissions

This topic describes how to:

- Add a group role
- Add groups or users to a group role
- Copy or move a group role

  > **Note:** A copy can be used at the Fortify WebInspect Enterprise System level, the organization level, or the group level, and you can move a role from one group to another.

- Remove a group role
- Rename a group role

Adding a Group Role

To add a group role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Click **Add** to the right of the **Role Name** pane).
5. On the New Role dialog box, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.
6. In the **Permissions** list, expand the nodes to view the activities associated with each category.

   > **Note:** Having the set of options Allowed, Unassigned, and Denied for permissions enables Fortify WebInspect Enterprise to resolve conflicting permissions when a user is a member of more than one role. The role priorities are:
   >
   > - Allowed outranks Unassigned—If the permission for a particular activity in Role A is Allowed and the permission for the same activity in Role B is Unassigned, then a user who is a member of both Role A and Role B *can* perform the activity.
   > - Denied outranks Allowed—If the permission for a particular activity in Role A is Allowed, and the permission for the same activity in Role B is “Denied,” then a user who is a member of both Role A and Role B *cannot* perform the activity.
   > - Unassigned (only) equals Denied—If a user’s permission for a particular activity is Unassigned and no other permissions are assigned to that user in another role for the same activity, then the user *cannot* perform the activity.

7. To assign the same permission to all activities within a single category:
   a. Click the category name (such as “Blackouts").
   b. Click the drop-down arrow that appears on the far right end of the row.
   c. Select a permission.
8. To change permission for a single activity:
   a. Expand a category.
   b. Click the activity name (such as “Can Create" or "Can View”).
   c. Click the drop-down arrow that appears on the far right end of the row.
   d. Select a permission.

Adding Groups or Users to a Group Role

> **Note:** To save time when assigning a user to multiple roles, see "Adding a User Or Group To Multiple Roles" on page 51.

To add groups or users to a group role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a name in the **Role name** list.
5. Click **Add** (on the far right of the **User group or user names** pane).
6. Do one of the following:
   - If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, on the Select SSC Users or Groups dialog box, select users from the **Select Users** list.
   - For installations without Fortify Software Security Center integration, on the Select Users or Groups window:
     i. Click **Advanced**.

        The Select Users or Groups window appears.

     ii. Search for and select the user or group name you want to add to roles, and click **OK**.

     iii. Click **OK**.
7. Click **OK**.

Copying or Moving a Group Role

You can copy a group role to any level (system, organization, or group). You can also move a role from one group to another, which will remove it from the original group. You must be an administrator of the target group to copy or move a group role to it.

To move or copy a group role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Copy/Move**.
6. On the Copy/Move Role dialog box, specify the **Role Name** for the copy and select the organization or group to which the role will be assigned (or select the WebInspect Enterprise system).

   The same role can be assigned to multiple organizations and groups. The permissions associated with a role can be copied or moved only between similar levels (that is, from one group to another or from one organization to another).
7. To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role in the copy.
8. To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying a group role and assigning it to an organization or to the system.

9. Select the system, organization, or group to which the group role will be copied or moved.
10. Do one of the following:
    - Click **OK** to copy the group role.
    - Click **Move** to move the group role. This option is available only if you move the group role, along with its users and permissions, to another group.

Removing a Group Role

Note: You cannot remove a global role.

To remove a group role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Remove**.
6. Confirm that you want to remove the group role.

Renaming a Group Role

Note: You cannot rename a global role.

To rename a group role:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Roles** tab.
4. Select a role from the **Role name** list.
5. Click **Rename**.
6. Type a new name for the group role.
7. Click **OK**.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Specifying Resources Available to Groups

You can specify which resources—export paths, policies, or sensors—are available to a group. For example, the OpenText Fortify WebInspect Enterprise system contains approximately 20 scanning policies. Your organization administrator can choose to allow members of the organization to use only particular policies. Of those, you can allow even fewer to be used in your group.

To manage resources that are available to groups:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Click the **Resources** tab.
4. Select an item in the **Object Type** list. On the **Resources** tab, groups have the following object types:
   - Export Paths
   - Policies
   - Sensors

   Objects of the selected type that are not allowed appear in the **Available** column. Objects that are allowed appear in the **Allowed** column.
5. Do one of the following to make one or more objects available (but not allowed), or allowed:
   - To move particular objects from the **Available** column to the **Allowed** column, select one or more of them and click >.
   - To move all objects from the **Available** column to the **Allowed** column, click >>.
   - To move particular objects from the **Allowed** column to the **Available** column, select one or more of them and click <.
   - To move all objects from the **Allowed** column to the **Available** column, click <<.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Moving or Copying Objects to Organizations or Other Groups

You can assign a particular user-created object to a different group (and optionally to an organization) by either moving it or copying it. Moving an object removes it from its currently assigned location. Copying an object retains its current location while also placing a copy in a new location.

To move or copy an object from a group to a different group and optionally to an organization:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
2. Select a group in the Security Group Hierarchy pane.
3. Select the **Move/Copy Objects** tab.

4. Select an item in the **Object Type** list. On the **Move/Copy Objects** tab, groups have the following object types:
   - Blackouts
   - E-mail Alerts
   - Scan Templates
   - SNMP Alerts
   - Applications
   - Deleted Applications
5. Click **Retrieve**.

   All user-created objects of the selected type appear in the **Object Results** list.
6. Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.
7. Click **Move** or **Copy** (or **Recover** if you are restoring deleted application versions).
8. On the Move Objects or Copy Objects window, select a group from the **Target Group** list.
9. (Optional) Select a group from the **Security Group** list.
10. If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list.

    For each dependent object, click the drop-down arrow in the Action column under Object Dependencies and select the appropriate action (such as **Move to, Copy to,** or **Allow**).
11. Click **Move** or **Copy**.
12. When a dialog box appears informing you that all dependencies have been satisfied and prompting you to commit the move or copy, click **Yes**.

See Also

"About Group Administrators, Roles, and Permissions" on page 66

Managing Scans, Sensors, and Sensor Users

The following pages provide information on:

- Scan management
- Sensor Management
- Sensor User Management

About Controlling Scans Using the Scan Queue

This topic describes the capabilities provided by the Scan Queue form to control scans. For procedures, see "Controlling Scans Using the Scan Queue" on page 78.

When you resume a suspended scan, if the sensor that started the scan is available, then that sensor will reload the scan data and resume scanning. If the sensor that started the scan is now running a different scan, then that sensor will compare the priority of both scans. If the first (suspended) scan has a lower priority, the sensor will place it back in the queue and continue running the current scan. If the first scan has a higher priority, the sensor will suspend the second scan (placing it in the queue), reload the data from the first scan, and resume scanning. In any case, resumed scans are always assigned to the same sensor on which they began.

When you select a scan on the Scan Queue form, you can:

- Stop the scan if it is running, and remove the scan request from the queue. This is useful if, for example, the scan is taking too long to run. Scan results, though incomplete, are available for inspection.
- Suspend the scan at its current point and later resume it where it left off.

  When you resume a suspended scan, if the sensor that started the scan is available, then that sensor will reload the scan data and resume scanning. If the sensor that started the scan is now running a different scan, then that sensor will compare the priority of both scans. If the first (suspended) scan has a lower priority, the sensor will place it back in the queue and continue running the current scan. If the first scan has a higher priority, the sensor will suspend the second scan (placing it in the queue), reload the data from the first scan, and resume scanning. In any case, resumed scans are always assigned to the same sensor on which they began.
- Remove the scan results and request from the OpenText Fortify WebInspect Enterprise database.

Note: The availability of particular options depends on the status of the selected scan and on the permissions granted to you by your assigned role.

For each scan that is running or waiting to run, the Scan Queue form displays (by default):

- The name assigned to the scan
- The scan's priority
- The date and time the scan request was created
- The sensor conducting the scan
- The scan's status
- The organization and group

For procedures, see "Controlling Scans Using the Scan Queue" on the next page.

See Also

"Scan Status Messages List" on page 103

Controlling Scans Using the Scan Queue

To control the running of scans in the queue:

1. Select **Scans** in the left pane and then select the **Scan Queue** shortcut above.
2. Select a scan request in the queue (unless you plan to change which columns to display in the form).
3. Click **Action** or right-click the selected scan request, and then click one of the following options:
    - **Stop.** Stop the scan if it is running, and remove the scan request from the queue. The results, although incomplete, are available for inspection.
    - **Suspend.** Suspend the scan so that you can resume it later.
    - **Resume.** Resume the scan where it left off when it was suspended.
    - **Delete.** Remove the scan from the OpenText Fortify WebInspect Enterprise database.
    - **Column Setting.** Specify which columns to display in the form.

> **Note:** The availability of particular options depends on the status of the selected scan and on the permissions granted to you by your assigned role.

See Also

"About Controlling Scans Using the Scan Queue" on page 76

About Managing Scan Policies

This topic describes the capabilities provided by the Scan Policies form to manage scan policies. For procedures, see "Managing Scan Policies" on the next page and "Creating Custom and Master Scan Policies" on page 80. For a list of each policy and its purpose, see "Policies List" on page 98.

OpenText Fortify WebInspect Enterprise provides many standard system policies that determine which types of vulnerabilities the scan should focus on. Each policy is kept current using the SmartUpdate function, ensuring that scans are accurate and can detect the most recent discovered threats. One or more of these policies can meet your needs well.

As a system administrator operating at the WebInspect Enterprise system permissions level, you can copy a system policy and modify it as needed, making it a custom policy. You can create multiple custom policies and assign each one to a different organization and groups as needed.

A system administrator can designate one custom policy as the *master* policy, and any changes to it will be automatically propagated to the organizations and groups, eliminating the need to update each individual copy of that policy in each organization and group.

When you select a *standard* system policy on the Scan Policies form, you can:

- View it, but not edit it.
- Copy it and rename it to make it a custom policy.

When you select a *custom* policy on the Scan Policies form, you can:

- Edit it.
- Delete it.
- Specify whether or not it is the master policy.

All sensors connected to Fortify WebInspect Enterprise access common policies from the database. If you want to run OpenText Fortify WebInspect independent of Fortify WebInspect Enterprise and incorporate the results of the Fortify WebInspect scans into Fortify WebInspect Enterprise, you can import a standard or custom policy into Fortify WebInspect Enterprise from Fortify WebInspect or export a custom policy from Fortify WebInspect Enterprise to Fortify WebInspect.

The Scan Policies form displays:

- Each policy that is configured in your environment
- The product to which each policy applies
- Whether or not the policy is a pre-packaged (system) policy
- When the policy was last updated
- For custom policies, the organization to which the policy is assigned

For procedures, see:

- "Managing Scan Policies" below
- "Creating Custom and Master Scan Policies" on the next page

See Also

"Policies List" on page 98

Managing Scan Policies

For details about the Policy Manager tool described in this topic, see the *OpenText™ Fortify WebInspect Tools Guide* or the Help system for that tool.

To manage system scan policies (that is, policies provided with OpenText Fortify WebInspect Enterprise) or custom scan policies (which are created by administrators):

1. Select **Scans** in the left pane and then select the **Scan Policies** shortcut above.
2. Select a scan policy (unless you plan to import or export a policy).
3. Click **Action** or right-click the selected policy, and then click one of the following options:
    - **Edit.** (Custom policies only) Open the Policy Manager tool, allowing you to view and modify the selected policy. (You can double-click the policy name instead.)

- **View.** (System policies only) Open the Policy Manager tool, allowing you to view the selected policy. (You can double-click the policy name instead.)

- **Copy.** Copy the selected policy. After you rename the policy, the Policy Manager tool opens and loads the selected policy, allowing you to edit it. When you then save the policy, it is added to the list of policies as a custom policy. For more details about creating a custom policy, which you can optionally specify to be a master policy, see "Creating Custom and Master Scan Policies" below.

- **Delete.** (Custom policies only) Delete the selected policy.

- **Rename.** (Custom policies only) Rename the custom policy.

- **Import.** Import a policy from OpenText Fortify WebInspect.

- **Export.** (Custom policies only) Export a custom policy to Fortify WebInspect.

Note: The availability of particular options depends on whether the policy is a system policy or a custom policy and on the permissions granted to you by your assigned role.

See Also

"About Managing Scan Policies" on page 78

"Creating Custom and Master Scan Policies" below

"Policies List" on page 98

Creating Custom and Master Scan Policies

As a system administrator operating at the OpenText Fortify WebInspect Enterprise system permissions level, you can copy a system policy and modify it as needed, making it a custom policy. You can create multiple custom policies and assign each one to a different organization and groups as needed.

A system administrator can designate one custom policy as the master policy, and any changes to it will be automatically propagated to the organizations and groups, eliminating the need to update each individual copy of that policy in each organization and group.

When you select a standard system policy on the Scan Policies form, you can:

- View it, but not edit it.
- Copy it and rename it to make it a custom policy.

When you select a *custom* policy on the Scan Policies form, you can:

- Edit it.
- Delete it.
- Specify whether or not it is the master policy.

To create a custom policy, optionally make it a master policy, and then make the new policy available to an organization you select:

1. Enable the required permissions:
   a. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
   b. Select **WebInspect Enterprise System** in the Security Group Hierarchy pane.
   c. Click the **Roles** tab.
   d. Select or create a role.
   e. In the Permissions area, select **Policies**.
   f. Select **Allowed** for all Policies permissions.
2. Create a custom policy:
   a. Select **Scans** in the left pane and then select the **Scan Policies** shortcut above.
   b. Select a policy that you want to use as the template for the new custom policy.
   c. Click **Copy** in the **Action** menu or in the shortcut menu that appears when you right-click the selected policy.

      Note: The availability of particular options depends on the permissions granted to you by your assigned role.

      Fortify WebInspect Enterprise checks for and downloads any updates to the policy.
   d. In the Copy Policy dialog box, enter a name for the new policy and assign it to an organization.
   e. If you want the new policy to be a master policy, select the **Use as Master** option.
   f. Click **OK**.

      The Policy Manager tool opens.
   g. Modify the policy as needed.
   h. When finished, save the new custom policy and close the Policy Manager.

      The custom policy now appears in the list of Scan Policies.
3. Add the custom policy to an organization:
   a. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
   b. Select an organization in the Security Group Hierarchy pane.
   c. Click the **Resources** tab.
   d. Select **Policies** from the **Object Type** list.
   e. To add the new custom policy to the list of allowed policies, select the policy from the **Available** list and click >.

See Also

"About Managing Scan Policies" on page 78

"Managing Scan Policies" on page 79

"Policies List" on page 98

Adding, Editing, and Deleting Export Paths for Saving Scans

The Export Paths form displays a list of destinations (paths) that may be used for saving scan results. OpenText Fortify WebInspect Enterprise uses these paths to populate the drop-down list from which Fortify WebInspect Enterprise Web Console users select a location for storing the data.

To manage paths that can be used for saving scan results:

1. Click **Administration** in the left pane and then select the **Export Paths** shortcut above.
2. If you plan to edit or delete an existing export path, select it in the Export Paths list.
3. Click **Action** and then click one of the following options:

   > **Note:** When specifying a path for the **Add** and **Edit** options, use the Universal Naming Convention (or click the **Browse** button and select a folder).
   >
   > If you browse for a folder and select a local (rather than a network) folder, the selection refers to the hard drive of the machine on which the Fortify WebInspect Enterprise server is installed.
   >
   > The Fortify WebInspect Enterprise server must have access to any location you designate as an export path.

   - **Add.** Open the Export Path Settings window and add a path.
   - **Edit.** Open the Export Path Settings window and modify the selected path.
   - **Delete.** Delete the selected path. You cannot delete an export path that is currently being used or that is associated with a scheduled scan.

   > **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

4. If you have added or edited a path, click **OK** in the Export Path Settings window.

See Also

"Specifying Export Paths for Saving Scans" below

Specifying Export Paths for Saving Scans

The Export Path Settings dialog box opens when you add or edit an export path from the Export Paths form, which displays a list of destinations (paths) that may be used for saving scan results. OpenText Fortify WebInspect Enterprise uses these paths to populate the drop-down list from which Fortify WebInspect Enterprise Web Console users select a location for storing the data.

When specifying a path for the **Add** and **Edit** options, use the Universal Naming Convention (or click the **Browse** button and select a folder).

If you browse for a folder and select a local (rather than a network) folder, the selection refers to the hard drive of the machine on which the Fortify WebInspect Enterprise server is installed.

The Fortify WebInspect Enterprise server must have access to any location you designate as an export path.

> **Note:** When specifying a path for the **Add** and **Edit** options, use the Universal Naming Convention (or click the **Browse** button and select a folder).
>
> If you browse for a folder and select a local (rather than a network) folder, the selection refers to the hard drive of the machine on which the Fortify WebInspect Enterprise server is installed.
>
> The Fortify WebInspect Enterprise server must have access to any location you designate as an export path.

For detailed information about adding, editing, and deleting export paths, see "Adding, Editing, and Deleting Export Paths for Saving Scans" on the previous page.

About Sensor Management

This topic describes the capabilities provided by the Sensors form to manage sensors. For procedures, see "Managing Sensors and Their Scans" on the next page.

A sensor is defined as OpenText Fortify WebInspect that is connected to OpenText Fortify WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans with no direct user interaction.

For each sensor in the system, the Sensors form displays:

- Sensor name
- Host name
- Sensor status
- Sensor version
- Status message, indicating the result of the most recent action attempted.

If necessary, click the **Sensor Detail** tab (at the bottom of the form) to display additional information about the selected sensor. This includes the option **Can participate in "Any Available" sensor scans**. Ordinarily, sensors that are running a non-approved version of Fortify WebInspect (such as a special build developed for a specific customer) will not be selected to run a scan when you choose the **Can participate in "Any Available" sensor scans** option. You can remove that restriction, however, by selecting the non-approved sensor on the Sensors form and then selecting the option **Can participate in "Any Available" sensor scans**. Sensors that are newer than the latest approved SmartUpdate are then eligible to be selected.

> **Note:** If you do not see a list of installed sensors, you must install the required version of Microsoft .NET Framework.

For procedures, see "Managing Sensors and Their Scans" on the next page.

Managing Sensors and Their Scans

To manage sensors and their scans:

1. Select **Sensors** in the left pane and then select the **Sensors** shortcut above.
2. Select a sensor.
3. Click **Action** or right-click the selected sensor, and then click one of the following options:
   - **Edit Sensor Details.** Modify the name, location, and description of the sensor.
   - **Stop Scan.** Stop the scan. The job cannot be resumed.
   - **Suspend Scan.** Interrupt the scan. The scan can be resumed from the point where it was interrupted.
   - **Pause Sensor.** Temporarily halt the sensor. If a scan is running on that sensor, the scan will be suspended. Use this option to conduct maintenance on the machine with the sensor or to prevent the sensor from accepting any scans.

     > **Note:** This feature is a transient state held in memory on the sensor; it will not be remembered if the sensor service is ever restarted. For a long-term status, disable the sensor.

   - **Continue Sensor.** Enable the sensor after pausing. "Paused" must appear in the Status column. If the sensor was running a scan when it was paused, the scan will resume automatically.
   - **Enable/Disable.** Disassociate the sensor from the OpenText Fortify WebInspect Enterprise system. Turn the server on or off. You must be a member of the security administrator's group to enable a new sensor.
   - **Rename Sensor.** Change the sensor name.
   - **Migrate Sensor.** Reassign all schedules, pending scans, etc., from one sensor to another. Used primarily when installing a replacement sensor.
   - **Delete Sensor.** Disassociate the sensor from the Fortify WebInspect Enterprise system. To enable this option, you must stop the Fortify WebInspect Sensor service (**Start > Control Panel > Administrative Tools > Services**), taking the sensor offline.

   > **Note:** The availability of particular options depends on the permissions granted to you by your assigned role and on the status of the selected sensor.

See Also

"About Sensor Management " on the previous page

Managing Sensor Users

The Sensor Users form lists all OpenText Fortify WebInspect sensor users, which exist to run scans on behalf of OpenText Fortify WebInspect Enterprise users. To run scans, at least one Windows user account must be assigned as a sensor user. Prior to or during the installation of Fortify WebInspect Enterprise, at least one Windows user account should have been created for use as a Fortify WebInspect Enterprise sensor user.

To make a Windows user account a Fortify WebInspect Enterprise sensor user:

1. Select **Administration** in the left pane and then select the **Sensor Users** shortcut above.
2. Click **Add** in the right pane of the Sensor Users form.
3. In the Select Users or Groups dialog box, type the name of a Windows user to add, in the format of localhost\user or domain\user. If you specify only the user, you can click **Check Names** to help identify the localhost or domain.

   Click **Advanced** on the Select Users or Groups dialog box to search for users or groups.
4. Click **OK**.
5. Verify that the sensor user you specified has been added to the list of Sensor Users in the dialog box.

To remove a sensor user:

1. Select a sensor user from the list.
2. Click **Remove**.

Managing E-mail and SNMP Alerts

The following pages describe how to set up and manage e-mail messages and Simple Network Management Protocol (SNMP) messages that are sent to recipients you specify whenever certain WebInspect Enterprise events occur.

Adding, Editing, and Deleting E-mail Alerts

You can direct OpenText Fortify WebInspect Enterprise to send an e-mail message to recipients you specify whenever certain Fortify WebInspect Enterprise events occur. Such a message is called an e-mail alert.

The E-mail Alerts form lists all e-mail alerts configured for the system. Each item includes:

- The name of the alert
- The address of the e-mail recipient
- The IP addresses of scanned sites that may elicit an alert
- The event or action that will trigger the alert

- The organization
- The group

To add, edit, or delete e-mail alerts:

1. Click **Administration** in the left pane and then select the **E-mail Alerts** shortcut above.
2. Click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings as needed for sending e-mail alerts for specific Fortify WebInspect Enterprise events:
   - **SMTP Server:** The name of the server used for outgoing e-mail.
   - **SMTP Port:** The port number used for outgoing e-mail.
   - **Sender:** The text that will appear in the "From" field of the e-mail. It need not be a valid e-mail account, but it must be in the format *Sender text1@text2.text3*, where the *Sender* and *text* fields are any text you want to use, such as WebInspect Enterprise alerts@microfocus.com.
   - **Use SSL:** Select this check box if you want to use Secure Sockets Layer (SSL) protocol.
   - **Authentication:** If your server requires authentication, select **Basic** or **NTLM**, and then provide a user name and password.
3. If you plan to edit or delete an existing e-mail alert, select it in the E-mail Alerts list.
4. Click **Action** and then click one of the following options:
   - **Add.** Open the E-Mail Alert Settings window and add an e-mail alert.
   - **Edit.** Open the E-Mail Alert Settings window and modify the selected e-mail alert.
   - **Delete.** Delete the selected e-mail alert.

   Note: The availability of particular options depends on the permissions granted to you by your assigned role.
5. If you are adding or editing an e-mail alert, complete the fields in the E-Mail Alert Settings window as follows:
   a. Enter a name for the alert in the **Name** field.
   b. Select **System**, **Organization**, or **Security Group**.
   c. If you selected **Organization** or **Security Group**, select an organization or group from the drop-down list.
   d. In the **Recipient e-mail address** field, enter the e-mail address of the person who should receive the alert. To specify multiple recipients, insert a semicolon between e-mail addresses.
   e. If the alert should be sent only when selected actions occur related to a host name or specific IP address or range of IP addresses, in the **Host name, address, or IP Address Range** field, enter the host name or IP address. You can specify multiple addresses or a range of addresses.

      For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254).

Separate multiple addresses or ranges with a semicolon.

Enter an asterisk (*) to allow alerts for all IP addresses.

f. Select one or more actions that will trigger the alert.

   System alerts can be sent for:

   - Sensor error
   - SmartUpdate completed
   - SmartUpdate failed

   Organization or security group alerts can be sent for:

   - Scan completed
   - Scan started
   - Scan failed
   - Critical vulnerability detected

g. Click **OK**.

Specifying E-mail Alert Settings

To add or edit an e-mail alert, complete the fields in the E-Mail Alert Settings window as follows:

1. Enter a name for the alert in the **Name** field.
2. Select **System**, **Organization**, or **Security Group**.
3. If you selected **Organization** or **Security Group**, select an organization or group from the drop-down list.
4. In the **Recipient e-mail address** field, enter the e-mail address of the person who should receive the alert. To specify multiple recipients, insert a semicolon between e-mail addresses.
5. If the alert should be sent only when selected actions occur related to a host name or specific IP address or range of IP addresses, in the **Host name, IP address, or IP Address Range** field, enter the host name or IP address. You can specify multiple addresses or a range of addresses.

   For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254).

   Separate multiple addresses or ranges with a semicolon.

   Enter an asterisk (*) to allow alerts for all IP addresses.
6. Select one or more actions that will trigger the alert.

   System alerts can be sent for:

   - Sensor error
   - SmartUpdate completed
   - SmartUpdate failed

Organization or security group alerts can be sent for:

- Scan completed

  Note: The Scan Completed email notification includes the total number of vulnerabilities found in each severity level—Critical, High, Medium, Low, Best Practice, and Info—and a Total Risk Score. For more information, see "Understanding Assigned Risks and the Total Risk Score" below.

- Scan started
- Scan failed
- Critical vulnerability detected

7. Click **OK**.

Note: You must also configure the SMTP Settings on the **SMTP Alerts** form by clicking **SMTP Settings** (at the bottom of the form). For detailed information about adding, editing, and deleting e-mail alerts, including configuring the SMTP Settings, see "Adding, Editing, and Deleting E-mail Alerts" on page 85.

Understanding Assigned Risks and the Total Risk Score

Each vulnerability in the OpenText SecureBase has an associated severity level ranging from critical to informational. For example, most SQL Injection vulnerabilities are rated as critical, while Statistics Information Disclosure is considered a low risk.

Assigned Risks

Each severity level is assigned a risk value as shown in the following table.

Severity Level	**Assigned Risk**
Critical	5
High	4
Medium	3
Low	2
Best Practice	1
Info	0

Total Risk Score

OpenText Fortify WebInspect Enterprise uses the assigned risks and the following calculation to determine the Total Risk Score:

(#Criticals * 5) + (#Highs * 4) + (#Mediums * 3) + (#Lows * 2) + (#BestPractices * 1) = Total Risk Score

The Info severity level has an assigned risk of “0” and is not included in the Total Risk Score.

For example, suppose a completed scan has the following vulnerability Severity Level counts:

- Critical – 54
- High – 13
- Medium – 4
- Low – 21
- Best Practice – 31
- Info - 5 (not included in the Total Risk Score)

The scan would have a Total Risk Score as determined by the following calculation:

(54 * 5) + (13 * 4) + (4 * 3) + (21 * 2) + (31 * 1) = Total Risk Score

(270) + (52) + (12) + (42) + (31) = 407

Where Total Risk Score Appears

The Scan Completed email notification includes the total number of vulnerabilities found in each severity level—Critical, High, Medium, Low, Best Practice, and Info—and a Total Risk Score. For more information, see "Specifying E-mail Alert Settings" on page 87.

Adding, Editing, and Deleting SNMP Alerts

You can direct OpenText Fortify WebInspect Enterprise to send a Simple Network Management Protocol (SNMP) message to IP addresses you specify whenever certain Fortify WebInspect Enterprise events occur. Such a message is called an SNMP alert.

The SNMP Alerts form lists all SNMP alerts configured for the system. Each item includes:

- The name of the alert
- The IP address of the SNMP alert recipient
- The action or event that will trigger the alert
- The organization
- The group

To add, edit, or delete SNMP alerts:

1. Click **Administration** in the left pane and then select the **SNMP Alerts** shortcut above.
2. Click **SNMP Settings** (at the bottom of the form) and configure SNMP settings as needed for sending SNMP alerts for specific Fortify WebInspect Enterprise events:
   - **SNMP Host:** The IP address of the server that will receive the alert and forward it to the intended recipient.
   - **SNMP Port:** The port number for SNMP alerts on the SNMP host.
   - **Community:** An SNMP community is a text string that acts as a password for authenticating messages sent between the management station (the SNMP manager) and the device (the SNMP agent). There are typically two types of community names:
     - A read-only community name that allows queries of the agent
     - A read-write community name that allows an NMS to perform set operations
3. If you plan to edit or delete an existing SNMP alert, select it in the SNMP Alerts list.
4. Click **Action** and then click one of the following options:
   - **Add.** Open the SNMP Alert Settings window and add an SNMP alert.
   - **Edit.** Open the SNMP Alert Settings window and modify the selected SNMP alert.
   - **Delete.** Delete the selected SNMP alert.

   Note: The availability of particular options depends on the permissions granted to you by your assigned role.

5. If you are adding or editing an SNMP alert, complete the fields in the *SNMP Alert Settings* window as follows:
   a. Enter a name for the alert in the **Name** field.
   b. Select **System**, **Organization**, or **Security Group**.
   c. If you selected **Organization** or **Security Group**, select an organization or group from the drop-down list.
   d. In the **Host name, IP address, or IP Address Range** field, enter the host name or IP address of the SNMP-compliant device that should receive the alert. You can specify multiple addresses or a range of addresses.

      For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254).

      Separate multiple addresses or ranges with a semicolon.

      Enter an asterisk (*) to allow alerts for all IP addresses.
   e. Select one or more actions that will trigger the alert.

      System alerts can be sent for:
      - Sensor error
      - SmartUpdate completed
      - SmartUpdate failed

Organization or security group alerts can be sent for:

- Scan completed
- Scan started
- Scan failed
- Critical vulnerability detected

f. Click **OK**.

Specifying SNMP Alert Settings

To add or edit an SNMP alert, complete the fields in the SNMP Alert Settings window as follows:

1. Enter a name for the alert in the **Name** field.
2. Select **System**, **Organization**, or **Security Group**.
3. If you selected **Organization** or **Security Group**, select an organization or group from the drop-down list.
4. In the **Host name, IP address, or IP Address Range** field, enter the host name or IP address of the SNMP-compliant device that should receive the alert. You can specify multiple addresses or a range of addresses.

   For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254).

   Separate multiple addresses or ranges with a semicolon.

   Enter an asterisk (*) to allow alerts for all IP addresses.
5. Select one or more actions that will trigger the alert.

   System alerts can be sent for:

   - Sensor error
   - SmartUpdate completed
   - SmartUpdate failed

   Organization or security group alerts can be sent for:

   - Scan completed
   - Scan started
   - Scan failed
   - Critical vulnerability detected
6. Click **OK**.

Note: You must also configure the SNMP Settings on the **SNMP Alerts** form by clicking **SNMP Settings** (at the bottom of the form). For detailed information about adding, editing, and deleting SNMP alerts, including configuring the SNMP Settings, see "Adding, Editing, and Deleting SNMP Alerts" on page 89.

Working with Fortify Software Security Center

The following pages describe how to configure OpenText Fortify Software Security Center settings in the Fortify WebInspect Enterprise Administrative Console for automatic publishing of scans to Fortify Software Security Center and importing applications into Fortify Software Security Center.

Configuring Settings for Fortify Software Security Center

> **Note:** This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

The settings in the Software Security Center form in the Fortify WebInspect Enterprise Administrative Console must be configured to do the following:

- Publish scans to Fortify Software Security Center. When Fortify Software Security Center settings are correctly configured, scans are automatically published to Fortify Software Security Center by default.

  > **Note:** To disable automatic publishing, see "Disabling Automatic Publishing of Scans to Fortify Software Security Center" on the next page.

- Import applications into Fortify Software Security Center from a `.csv` file that was created by using the Web Discovery tool.

Initial settings for Fortify Software Security Center are established during installation of Fortify WebInspect Enterprise. If necessary, use the Software Security Center form to modify the settings as follows:

1. Click **Administration** in the left pane and then select the **Software Security Center** shortcut above.
2. Enter the following information:
   - **WebInspect Enterprise URL:** The URL of the Fortify WebInspect Enterprise server.
   - **Software Security Center URL:** The URL of the Fortify Software Security Center server.
   - **Administrator: User Name** and **Password:** The user name and password of a general Fortify Software Security Center administrator account created in Fortify Software Security Center.

     Web Console users, when publishing scans to Fortify Software Security Center, will be required to enter their own credentials.

     > **Note:** If the Fortify Software Security Center administrator's password expires or he changes it, or if a new Fortify Software Security Center administrator is chosen for interaction with Fortify WebInspect Enterprise, a Fortify WebInspect Enterprise administrator will need to rerun the Initialization Wizard (**Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Initialize**) and specify the new credentials for the Fortify Software Security Center administrator. The

> Initialization Wizard will detect that your newly specified Fortify Software Security Center administrator exists in Fortify Software Security Center but she is not a System Administrator in Fortify WebInspect Enterprise. In this case, the Wizard will display the Administrator Role Page, which enables you to add her to Fortify WebInspect Enterprise with the System Administrator role by selecting the **Add Current User to System Administrator Role** check box and clicking **Next**.

- **WebInspect Enterprise Service Account: User Name** and **Password**: The user name and password of an account in Fortify Software Security Center with the role of Fortify WebInspect Enterprise System. This service controls the sharing of application versions with Fortify WebInspect Enterprise and obtains lists of completed and running scans from Fortify WebInspect Enterprise.
- **Security Group:** The organization/group to which new application versions are assigned when created by Fortify Software Security Center. To change the organization/group for new application versions, select a different entry from the dropdown list.

3. To verify the settings for connection to Fortify Software Security Center, click **Test**.
4. To save the settings, click **Save**.
5. (Optional) Click **Action** and then click one of the following options:
   - **Import Applications to SSC:** Import applications into Fortify Software Security Center from a `.csv` file created from IP addresses found using the Web Discovery tool. See "Importing Applications into Fortify Software Security Center from a CSV File" on the next page
   - **Synchronize Applications:** Synchronize applications between Fortify WebInspect Enterprise and Fortify Software Security Center. This process generally occurs automatically.
   - **Unregister WebInspect Enterprise:** Disconnect Fortify WebInspect Enterprise from Fortify Software Security Center. Use this option only if you are moving to another instance of Fortify Software Security Center.

> **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

Disabling Automatic Publishing of Scans to Fortify Software Security Center

To disable automatic publishing of scans to Fortify Software Security Center:

1. If you are authorized to do so, open the following file:

   ```
   C:\Program Files\Fortify\Fortify WebInspect Enterprise
   23.2.0\ManagerWS\web.config
   ```
2. Change the value in

   ```
   <add key="AutoPublishScans" value="true" />
   ```
   from `true` to `false`
3. Save and close the file.

Importing Applications into Fortify Software Security Center from a CSV File

Note: This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

You can use the Web Discovery tool to discover sites over a range of IP addresses and convert the discovered sites to applications in a `.csv` file. Then you can edit the data and import the applications into Fortify Software Security Center (SSC), as follows:

1. Run the Web Discovery tool against the desired range of IP addresses. See the "Web Discovery" chapter in the *OpenText™ Fortify WebInspect Tools Guide*.

   In the Web Discovery tool, you will click **File > Export > To CSV File** to save the set of discovered sites, and specify the desired name and location for the `.csv` file.
2. Open the `.csv` file in Microsoft Excel.
3. Review the `.csv` file. Adjust the widths and edit the values of the following columns as desired. For example, you can specify Fortify Software Security Center application and version names that are meaningful to you.
   - **SSC Application (required):** The name to be given to the application to be imported into Fortify Software Security Center. By default, the value is the IP address that was discovered.
   - **SSC Version (optional):** The name to be given to the version to be imported into Fortify Software Security Center. By default, the value is **Production**.
   - **URL (optional):** By default, the value is the URL to be used for a scan.
   - **Server Information (optional):** By default, the value is the web platform of the detected server. It appears in application version properties in Fortify WebInspect Enterprise, but does not appear in Fortify Software Security Center.
   - **Finish Using Application (optional):** In conjunction with the following field, specify the application and version with the application template attributes that will be used to finish the application version to be imported into Fortify Software Security Center.
   - **Finish Using Application Version (optional):** In conjunction with the preceding field, specify the application and version with the application template attributes that will be used to finish the application version to be imported into Fortify Software Security Center.
4. Save the edited file.
5. In the Fortify WebInspect Enterprise Administrative Console, click **File > Import Applications to SSC**.

   The Create Application Versions from imported CSV file dialog box opens.
6. Browse to the `.csv` file location and select the file.

7. Select the appropriate option:
   - WebInspect Enterprise Admin Console is running on the same machine as the WIE server
   - WebInspect Enterprise Admin Console is running on a remote machine

   > **Note:** If you indicate the WIE server is running on the same machine but it is actually remote, the task will fail and an error message will be written to the `TaskService_trace.log` file.

8. Click **OK**.

   The applications and application versions are queued for import into Fortify Software Security Center.

Managing Users and the Activity Log

The following pages describe how to manage users who are currently logged in to the WebInspect Enterprise system and the Activity Log that lists significant WebInspect Enterprise events. It also describes accessing and viewing the license information.

About Managing Connected Users

This topic describes the capabilities provided by the Connected Users form to manage users who are currently logged in to the OpenText Fortify WebInspect Enterprise system. You can release a user license to make it available to another user. For procedures, see "Managing Connected Users" on the next page.

The Connected Users form lists each logged-in user.

Each item in the form includes (by default):

- Application Type, such as WebInspect Enterprise (WIE) or WebInspect
- Application Subtype, such as Console or Console-Web
- Application Version
- The user's name
- The user's IP Address
- The time and date when the user connected to the system
- Status
- Message

A summary at the bottom of the from shows the total number of user licenses in use, the total number of available user licenses, and the logon session timeout period (which you can edit).

For procedures, see "Managing Connected Users" on the next page.

See Also

"Viewing License Information" on the next page

Managing Connected Users

To control the set of connected (logged-in) users:

1. Select **Administration** in the left pane and then select the **Connected Users** shortcut above.
2. Select a user (unless you plan to change which columns to display in the form).
3. Click **Action** or right-click the selected user, and then click one of the following options:
   - **Release User License.** Intended for use with licenses that permit multiple users. Disassociate the selected user from the license, allowing another user to occupy that position.
   - **Column Setting.** Specify which columns to display in the form.

> **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

See Also

"About Managing Connected Users" on the previous page

Viewing License Information

To display the following license information, select **Administration** in the left pane and then select the **Licensing** shortcut above:

- **Activation ID:** The unique identifier for the license issued by OpenText.

  If you upgrade from a trial version or if you otherwise modify the conditions of your license, click **Update** to update your license.
- **User Information:** Information about the person to whom the license is granted.
- **License Information**
  - **Licensed IP or Host Ranges:** The IP addresses or hosts to which scans are restricted.
  - **Bypass DNS:** Indicates if the application is allowed to bypass a domain name server.
  - **Valid To:** The ending date of the period for which the license is valid.
  - **Maintenance End Date:** The date on which the maintenance contract terminates.
  - **Total available sensor licenses:** The maximum number of sensors that may be connected to OpenText Fortify WebInspect Enterprise.
  - **Total Scan Count:** The maximum number of scans that may be conducted.
- **License Usage Information**
  - **Available Scan Count:** Remaining number of scans allowed.
  - **Total in use sensor licenses:** Number of licensed sensors in use.
  - **Total in use concurrent user licenses:** Number of concurrent licensed sensors in use.

> **Note:** If the Fortify WebInspect Enterprise Administrative Console is installed on a machine that does not have Internet access, see the *OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide* for instructions on activating the application.

See Also

"About Managing Connected Users" on page 95

Managing the Activity Log

The Activity Log lists significant OpenText Fortify WebInspect Enterprise events. Each item includes (by default):

- The date and time the event occurred
- A message indicating the event or activity
- For scan-related events, the URL or IP address or the job name associated with this activity
- The sensor associated with this activity
- The name of the user
- The IP address of the workstation

You can display all entries in the Activity Log or restrict the listing to those activities that occurred on or after a specific date.

To limit the size of the Activity Log, click **Activity Log Settings** (at the bottom of the form) and set the desired limits.

To manage the activity log in other ways:

1. Select **Administration** in the left pane and then select the **Activity Log** shortcut above.
2. Click **Action** and then click one of the following options:
   - **Export Activity Log to TSV.** Save the activity log to a text file using a tab-separated format.
   - **Export Activity Log to CSV.** Save the activity log to a text file using a comma-separated format.
   - **Export Activity Log to XML.** Save the activity log to a text file using an XML format.
   - **Clear Activity Log.** Delete all entries in the activity log.
   - **Copy Message(s) to Clipboard.** Copy the text in all columns of all selected list entries.
   - **Column Setting.** Specify which columns to display in the form.

   > **Note:** The availability of particular options depends on the permissions granted to you by your assigned role.

Reference Lists

The following pages provide lists of policies, scan status messages, HTTP status codes, and sensor statuses.

Policies List

Fortify WebInspect provides various policies that you can use with your scans and crawls to determine the vulnerability of your Web application. Each policy is kept current using the SmartUpdate function, ensuring that assessments are accurate and capable of detecting the most recently discovered threats. The policies described here are listed by group.

> **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.

About OAST-related Checks

For networks that have Internet access, the Fortify WebInspect sensor uses a public DNS service when running OAST-related checks. Ensure that your firewall does not block access to **fortify-oast.net**. For networks lacking Internet access, the Fortify OAST on Docker image is available. For more information, see the *OpenText™ Fortify WebInspect and OAST on Docker User Guide*.

Best Practices

The Best Practices group contains policies designed to test applications for the most pervasive and problematic web application security vulnerabilities.

- **API**: This policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.
- **CWE Top 25 *<version>***: The Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25) is a list created by MITRE. The list demonstrates the most widespread and critical software weaknesses that can lead to vulnerabilities in software.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **Best Practices** group.
- **General Data Protection Regulation (GDPR)**: The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and provides a framework for organizations on

how to handle personal data. The GDPR articles that pertain to application security and require businesses to protect personal data during design and development of their products and services are as follows:

- Article 25, data protection by design and by default, which requires businesses to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.
- Article 32, security of processing, which requires businesses to protect their systems and applications from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

This policy contains a selection of checks to help identify and protect personal data specifically related to application security for the GDPR.

- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 - (NIST SP 800-53 Rev.5) provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. This policy contains a selection of checks that must be audited to meet the guidelines and standards of NIST SP 800-53 Rev.5.
- **OWASP Application Security Verification Standard (ASVS)**: The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test, and verify secure applications.

  This policy uses OWASP ASVS suggested CWE mapping for each category of SecureBase checks to include. Because CWE is a hierarchical taxonomy, this policy also includes checks that map to additional CWEs that are implied from OWASP ASVS suggested CWE using a "ParentOf" relationship.
- **OWASP Top 10 <*year*>**: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about the most critical web application security flaws. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. Multiple releases of the OWASP Top Ten policy may be available. For more information, consult the OWASP Top Ten Project.
- **SANS Top 25<*year*>**: The SANS Top 25 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software. These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to take over the software completely, steal data, or prevent the software from working altogether.
- **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers.

By Type

The By Type group contains policies designed with a specific application layer, type of vulnerability, or generic function as its focus. For instance, the Application policy contains all checks designed to test an application, as opposed to the operating system.

- **Aggressive Log4Shell**: This policy performs a comprehensive security assessment of your web application for JNDI Reference injections in vulnerable versions of Apache Log4j libraries. In vulnerable versions, Log4j does not restrict JNDI features. This allows an attacker who can control log messages to inject JNDI references that point to an attacker-controlled server. This can lead to remote code execution on the vulnerable target. Compared with other policies that include Log4Shell agent, this policy performs a more accurate and decisive job, but produces a significant number of requests and has a longer scan time.
- **Aggressive SQL Injection**: This policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs a more accurate and decisive job, but has a longer scan time.
- **Apache Struts**: This policy detects supported known advisories against the Apache Struts framework.
- **Blank**: This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Client-side**: This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.
- **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.
- **Cross-Site Scripting**: This policy performs a security scan of your web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a website to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **By Type** group.
- **Mobile**: A mobile scan detects security flaws based on the communication observed between a mobile application and the supporting backend services.

- **NoSQL and Node.js**: This policy includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL, such as MongoDB, and server side infrastructures based on JavaScript, such as Node.js.
- **OAST**: This policy includes all checks that use Out-of-band Application Security Testing (OAST) technology in scanning logic.
- **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **PCI DSS 4.0**: The Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0) provides a baseline of technical and operational requirements designed to protect account data. This policy contains a selection of checks that need to be audited to meet the secure coding requirements of PCI DSS 4.0.
- **PCI Software Security Framework *<version>* (PCI SSF *<version>*)**: The PCI SSF provides a baseline of requirements and guidance for building secure payment systems and software that handle payment transactions. This policy contains a selection of checks that must be audited to meet the secure coding requirements of PCI SSF.
- **Privilege Escalation**: The Privilege Escalation policy scans your web application for programming errors or design flaws that allow an attacker to gain elevated access to data and applications. The policy uses checks that compare responses of identical requests with different privilege levels.
- **Server-side**: This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQL Injection**: The SQL Injection policy performs a security scan of your web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database.
- **Transport Layer Security**: This policy performs a security assessment of your web application for insecure SSL/TLS configurations and critical transport layer security vulnerabilities, such as Heartbleed, Poodle, and SSL Renegotiation attacks.
- **WebSocket**: This policy detects vulnerabilities related to WebSocket implementation in your application.

Custom

The Custom group contains all user-created policies and any custom policies modified by a user.

Hazardous

The Hazardous group contains a policy with potentially dangerous checks, such as a denial-of-service attack, that could cause production servers to fail. Use this policy against non-production servers and systems only.

- **All Checks**: An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the database. This scan includes all checks that are listed in the compliance reports that are available in Fortify web application and web services vulnerability scan products. This includes checks for known and unknown vulnerabilities at the web server, web application server, and web application layers.

  > **Caution!** An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. We strongly recommend 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.

See Also

"About Managing Scan Policies" on page 78

Scan Status Messages List

The following table describes the status messages that may be returned by OpenText Fortify WebInspect.

Status	Definition
Pending	A user has created a job by scheduling a scan or attempting to start a scan manually when the sensor is not available. The job appears in the Queued Scans list and will be started automatically when the sensor becomes available (if it is not preempted by a job with a higher priority).
Running	A sensor is conducting the scan. The job appears in the Running Scans list.
Suspended	A user has started or scheduled another scan with a higher priority; the suspended scan has been placed in the Queued Scans list and will be resumed

Status	Definition
	when the sensor becomes available.
Complete	The scan has finished without error. The job appears in the Completed Scans list.
Failed	The sensor encountered an error that prevented the scan from completing.
Aborted	A user has stopped a scan.
Offline	The sensor conducting the scan is no longer connected to the Fortify WebInspect Enterprise system. This can occur because of network disruption or if a console user stopped the Fortify WebInspect Enterprise Sensor service (Start/Settings/Control Panel/Administrative Tools/Services), taking the sensor offline.
Suspended_ Manual	A user has temporarily interrupted a running scan. The suspended scan appears in the Queued Scans list, but will not be resumed until the user enters the command to do so.
Suspending_ Manual	A user has temporarily interrupted a running scan. The sensor is in the process of suspending the scan and placing it in the queue.
Imported	The user's attempt to import the scan was successful.
Blackout_ Pending	A user has created a job by scheduling a scan or attempting to start a scan manually, but a blackout period prohibits the job from starting. The scan appears in the Queued Scans list and will be started automatically when the blackout period expires and a sensor becomes available.
Blackout_ Suspended	The scan was running when a blackout period started. The scan has been placed in the Queued Scans list and will be resumed automatically when the blackout period expires and a sensor becomes available.
Blackout_ Suspending	The scan was running when a blackout period started. The sensor is in the process of suspending the scan and placing it in the Queued Scans list.

See Also

"About Controlling Scans Using the Scan Queue" on page 76

HTTP Status Codes List

The following list of status codes was extracted from the Hypertext Transfer Protocol version 1.1 standard (RFC 2616). You can view the complete standard at http://www.w3.org/Protocols/rfc2616/rfc2616.html.

Code	Definition
100	Continue.
101	Switching Protocols.
200 OK	Request has succeeded.
201 Created	Request fulfilled and new resource being created.
202 Accepted	Request accepted for processing, but processing not completed.
203 Non-Authoritative Information	The returned metainformation in the entity-header is not the definitive set as available from the origin server, but is gathered from a local or a third-party copy.
204 No Content	The server has fulfilled the request but does not need to return an entity-body, and might want to return updated metainformation.
205 Reset Content	The server has fulfilled the request and the user agent should reset the document view which caused the request to be sent.
206 Partial Content	The server has fulfilled the partial GET request for the resource.
300 Multiple Choices	The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent-driven negotiation information (section 12) is being provided so that the user (or user agent) can select a preferred representation and redirect its request to that location.
301 Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.
302 Found	The requested resource resides temporarily under a different URI.
303 See Other	The response to the request can be found under a different URI and should be retrieved using a GET method on that resource.
304 Not Modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server should respond with this status code.
305 Use Proxy	The requested resource MUST be accessed through the proxy given by the Location field.

Code	Definition
306 Unused	Unused.
307 Temporary Redirect	The requested resource resides temporarily under a different URI.
400 Bad Request	The request could not be understood by the server due to malformed syntax.
401 Unauthorized	The request requires user authentication. The response MUST include a WWW-Authenticate header field (section 14.47) containing a challenge applicable to the requested resource.
402 Payment Required	This code is reserved for future use.
403 Forbidden	The server understood the request, but is refusing to fulfill it.
404 Not Found	The server has not found anything matching the Request-URI.
405 Method Not Allowed	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.
406 Not Acceptable	The resource identified by the request is only capable of generating response entities which have content characteristics not acceptable according to the accept headers sent in the request.
407 Proxy Authentication Required	This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.
408 Request Timeout	The client did not produce a request within the time that the server was prepared to wait.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server and no forwarding address is known.
411 Length Required	The server refuses to accept the request without a defined Content-Length.
412 Precondition	The precondition given in one or more of the request-header fields

Code	Definition
Failed	evaluated to false when it was tested on the server.
413 Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
414 Request-URI Too Long	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415 Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416 Requested Range Not Satisfiable	A server should return a response with this status code if a request included a Range request-header field (section 14.35), and none of the range-specifier values in this field overlap the current extent of the selected resource, and the request did not include an If-Range request-header field.
417 Expectation Failed	The expectation given in an Expect request-header field (see section 14.20) could not be met by this server, or, if the server is a proxy, the server has unambiguous evidence that the request could not be met by the next-hop server.
500 Internal Server Error	The server encountered an unexpected condition which prevented it from fulfilling the request.
501 Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
502 Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503 Service Unavailable	The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
504 Gateway Timeout	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server specified by the URI (e.g., HTTP, FTP, LDAP) or some other auxiliary server (e.g., DNS) it needed to access in attempting to complete the request.

Code	Definition
505 HTTP Version Not Supported	The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.

Sensor Status List

The following table describes the statuses that a sensor can display.

Status	Definition
Offline	The sensor is not connected.
Initializing	The sensor is initializing.
Idle	The sensor is not busy.
Starting	The sensor is starting a new scan.
Running	The sensor is conducting a scan.
Complete	The current scan has completed, but the sensor is not ready to start another scan.
Aborting	The sensor is aborting the current scan, but is not ready to start another scan.
Aborted	The current scan has been aborted.
Paused	The sensor is not available; scans may not be passed to this sensor.
Suspending	The sensor is suspending the current scan, but is not ready to start another scan.
Suspended	The current scan has been suspended.
Resuming	The sensor is resuming a suspended scan.
Warning	An error occurred on the sensor, but it was not severe enough to abort the current scan.
Error	A fatal error occurred on the sensor.
Unlicensed	A license is not assigned to this sensor.

Chapter 3: WebInspect Enterprise Services Manager

This chapter describes how to use the WebInspect Enterprise Services Manager to configure or modify the scan uploader service, task service, and scheduler service.

About the Fortify WebInspect Enterprise Services Manager

Use the OpenText™ Fortify WebInspect Enterprise Services Manager, also known as the Fortify WebInspect Enterprise Services Configuration Utility, to configure or modify the following services associated with Fortify WebInspect Enterprise:

- The scan uploader service, which handles the transfer of scans from OpenText Fortify WebInspect to Fortify WebInspect Enterprise. For more information, see "Configuring the Scan Uploader Service" below.
- The task service, which monitors the queue for various background tasks. For more information, see "Configuring the Task Service" on page 111.
- The scheduler service, which handles the scheduling of scans, discovery scans, and smart updates. For more information, see "Configuring the Scheduler Service" on page 114.

To start the utility, click **Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Services Manager**.

To access information about configuring the services, click its button in the left column.

Configuring the Scan Uploader Service

If the OpenText Fortify WebInspect Enterprise Scan Uploader Service was installed, OpenText Fortify WebInspect can scan a website and export the scan results to a location called a "dropbox." The Scan Uploader Service accesses each dropbox periodically and, if files exist, it uploads those files to the Fortify WebInspect Enterprise Manager.

Service Status

This area of the interface reports the current status of the Scan Uploader service. You can start, stop, restart, or configure the service.

To configure the service:

1. Click **Configure** in the Service Status section.

   The Configure Service dialog box appears.
2. Select which credentials should be used for logging on to the service:
   - **Local system account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.
   - **This account** - An account identified by the credentials you specify.
3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Fortify WebInspect Enterprise Configuration

This area of the interface reports the Fortify WebInspect Enterprise configuration.

To configure Fortify WebInspect Enterprise:

1. Click **Configure** in the WebInspect Enterprise Configuration section.

   The WebInspect Enterprise Configuration dialog box appears.
2. Enter the URL of the Fortify WebInspect Enterprise Manager.
3. Provide the Fortify WebInspect Enterprise Manager's authentication credentials.
4. To verify that the user name and password are correct, click **Test**.
5. If the Scan Uploader service uses a proxy, select **Enable Proxy** and provide the requested information.
6. Click **OK**.

Dropbox Configuration

Fortify WebInspect can scan a Web site and export the scan results to a location called a "dropbox." The purpose of the Fortify WebInspect Enterprise Uploader Service is to access each dropbox periodically and, if files exist, to upload those files to the Fortify WebInspect Enterprise Manager.

To create a dropbox:

1. Click **Add** in the Dropbox Configuration section.

   The Configure Dropbox dialog box appears.
2. Enter a dropbox name.
3. Enter the full path and name of the folder that will be used as the dropbox (or click **Browse** to select or create a folder).

   Be sure to select or create a folder that will not be used for any other purpose.

4. Enter the application version that will be serviced by this dropbox.
5. Click **OK**.

Logging Configuration

This area of the interface reports current settings for the logging function.

To configure logging:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration dialog box appears.
2. The logging output is contained in `UploaderService_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location** - For Windows Server 2008 or Windows Server 2012, the default location is:

     `\ProgramData\HP\WIE\UploaderService`
   - **Enter location for log file** - Type a path to the folder that will contain the logs, or click **Browse** to select a location.
3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.

   When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `UploaderService_trace.log`, `UploaderService_trace.log.1`, etc.
6. Click **OK**.

Starting the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Configuring the Task Service

Configure the Task Service to monitor the queue for database and logging background tasks. If OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, the Task Service also handles the background tasks for application version updates and issue synchronization with Fortify Software Security Center.

Service Status

This area of the interface reports the current status of the Task service.

To configure the service:

1. Click **Configure** in the Service Status section.

   The Configure Service dialog box appears.

2. Select which credentials should be used for logging on to the service:

   - **Local system account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.

   - **This account** - An account identified by the credentials you specify.

3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Database Configuration

This area of the interface reports the database server name and database name.

To configure the database:

1. Click **Configure** in the Database Configuration section.

   The Database Configuration dialog box appears.

2. Enter a server name.
3. Specify the account under which Fortify WebInspect Enterprise will connect to the database.

   - **Windows Authentication** - The name and password specified in the Fortify WebInspect Enterprise Manager’s user account is used to authenticate to the database. When working in a domain environment, the Fortify WebInspect Enterprise Manager’s user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the Fortify WebInspect Enterprise Manager and the database computers.

   - **SQL Authentication** - Enter the SQL Server user name and password.

4. Enter or select a database.
5. Click **OK**.

Logging Configuration

This area of the interface reports current settings for the logging function.

To configure logging:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration dialog box appears.

2. The logging output is contained in `TaskService_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location** - For Windows Server 2008 or Windows Server 2012, the default location is:

     `\ProgramData\HP\WIE\TaskService`
   - **Enter location for log file** - Type a path to the folder that will contain the logs, or click **Browse** to select a location.
3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.

   When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `TaskService_trace.log`, `TaskService_trace.log.1`, etc.
6. Click **OK**.

Fortify Software Security Center Poll Interval

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center (SSC), this area of the interface determines how often Fortify WebInspect Enterprise contacts Fortify Software Security Center for updates.

To configure settings:

1. In the **SSC application version updates polling interval** field, specify (in seconds) how frequently Fortify WebInspect Enterprise contacts Fortify Software Security Center to check for application version name changes or deletions.
2. In the **SSC issue synchronization interval** field, specify (in minutes) how frequently Fortify WebInspect Enterprise contacts Fortify Software Security Center to check for changes to audit information, comments, attachments, and “not an issue” and “suppressed” status.
3. Click **Apply**.

Starting the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Configuring the Scheduler Service

Service Status

This area of the interface reports the current status of the Scheduler service. You can start, stop, restart, or configure the service.

To configure the service:

1. Click **Configure** in the Service Status section.

   The Configure Service dialog box appears.
2. Select which credentials should be used for logging on to the service:
   - **Local system account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.
   - **This account** - An account identified by the credentials you specify.
3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Fortify WebInspect Enterprise Manager

If the OpenText Fortify WebInspect Enterprise Manager URL is changed using IIS or another tool, change the URL here as well.

Logging Configuration

This area of the interface reports current settings for the logging function.

To configure logging:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration dialog box appears.
2. The logging output is contained in `Scheduler_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location** - For Windows Server 2008 or Windows Server 2012, the default location is:

     `\ProgramData\HP\WIE\Scheduler`
   - **Enter location for log file** - Type a path to the folder that will contain the logs, or click **Browse** to select a location.
3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).

4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.

   When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `Scheduler_trace.log`, `Scheduler_trace.log.1`, etc.
6. Click **OK**.

Starting the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Chapter 4: WebInspect Enterprise Web Console

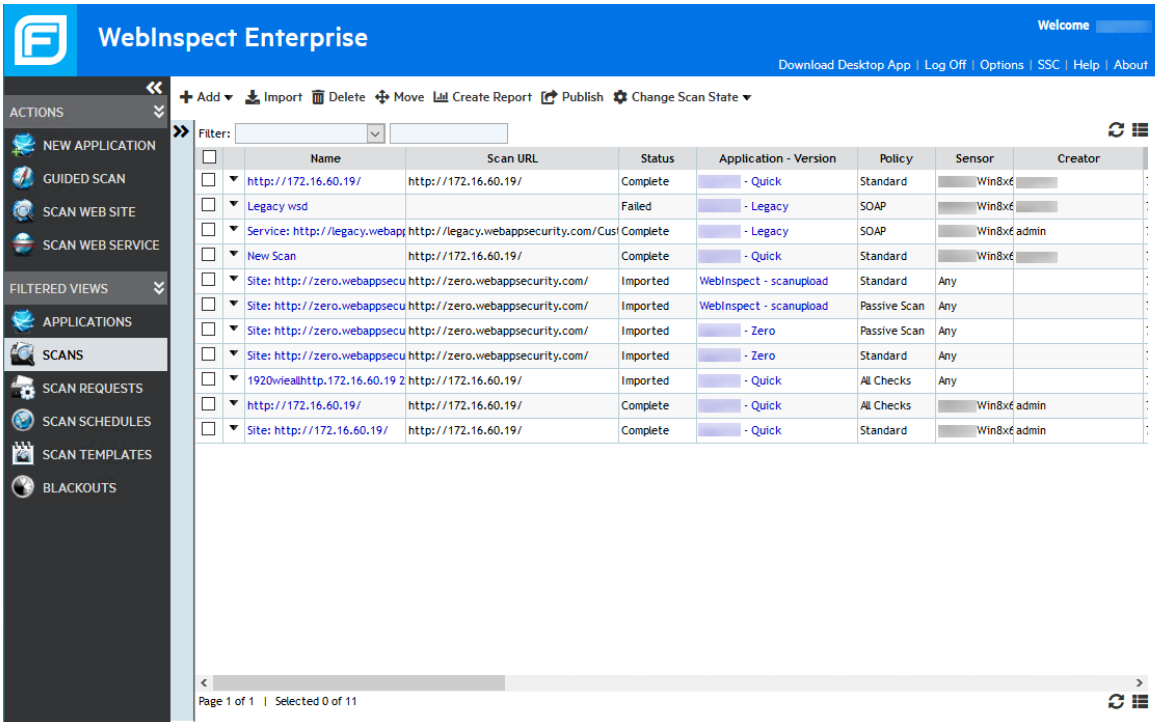
The WebInspect Enterprise Web Console, also known as the Web Console, is a browser-based interface designed for non-administrative functions such as running and managing scans.

Using the Interface

The OpenText Fortify WebInspect Enterprise Web Console user interface comprises the following main areas:

- **Toolbar** - Links in the upper right of the page to capabilities that are available for all Fortify WebInspect Enterprise Web Console screens
- **Navigation pane** - Left pane to select the action to take or the associated view or form to display in the right pane.
- **Views** and **forms** - Displays the view or form selected in the navigation pane.

In the following screen capture, the **Scans** option in the Navigation pane on the left has been selected and a form containing a list of all scans in the Fortify WebInspect Enterprise system is displayed. (For more information about displaying and managing scans, see "Reviewing the Scan List" on page 175.)



☐		Name	Scan URL	Status	Application - Version	Policy	Sensor	Creator
☐	▼	http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	[redacted]
☐	▼	Legacy wsd		Failed	[redacted] - Legacy	SOAP	[redacted] Win8x6	[redacted]
☐	▼	Service: http://legacy.webapp	http://legacy.webappsecurity.com/Cust	Complete	[redacted] - Legacy	SOAP	[redacted] Win8x6	admin
☐	▼	New Scan	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	[redacted]
☐	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	WebInspect - scanupload	Standard	Any	
☐	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	WebInspect - scanupload	Passive Scan	Any	
☐	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	[redacted] - Zero	Passive Scan	Any	
☐	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	[redacted] - Zero	Standard	Any	
☐	▼	1920wieallhttp.172.16.60.19 2	http://172.16.60.19/	Imported	[redacted] - Quick	All Checks	Any	
☐	▼	http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	All Checks	[redacted] Win8x6	admin
☐	▼	Site: http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	admin

Page 1 of 1 | Selected 0 of 11

Navigation Pane

The Navigation pane contains the following groups and commands:

- **Actions**
  - New Application (if the user has Administrator privileges) - See "Creating New Application Versions" on page 160
  - Guided Scan (Launches Guided Scan, the preferred method for performing a website scan. See the Guided Scan Help system for information about the Guided Scan client application.) - See "Configuring a Guided Scan " on page 319
  - Scan Web Site (appears only if **Enable "New Scan" Action** in **Options** has been selected) - See "Configuring a Web Site Scan" on page 125
  - Scan Web Service (appears only if **Enable "New Web Service" Action** in **Options** has been selected) - See "Configuring a Web Service Scan" on page 130
  - New Scan Schedule (appears only if **Enable "New Scan Schedule" Action** in **Options** has been selected) - See "Enabling New Scan Schedules" on page 124
  - New Blackout (appears only if **Enable "New Blackout" Action** in **Options** has been selected) - See "Enabling New Blackout Periods" on page 124
- **Filtered Views**
  - Applications - See "Viewing Application Versions" on page 161
  - Scans - See "Reviewing the Scan List" on page 175
  - Scan Requests (appears only if Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center) - See "Using Scan Requests from Fortify Software Security Center" on page 139
  - Scan Schedules - See "Scan Schedules" on page 136
  - Scan Templates - See "Using Scan Templates" on page 143
  - Blackouts - See "Using Blackouts" on page 149
- **Administration**
  - Deleted Applications (appears only after an application has been removed) - See "Managing Deleted Applications" on page 170

Click a command to display a form containing related information or controls, or to initiate a function.

Toolbar

The OpenText Fortify WebInspect Enterprise Web Console toolbar at the top right contains the links described in the following table.

Link	Description
Download Desktop App	Downloads the WebInspect Enterprise Desktop Application to the local machine. This application enables you to perform the following tasks: • View scan results and the Traffic Monitor • Import a scan • Use Guided Scan • Generate reports For more information, see "About the WebInspect Enterprise Desktop Application" on the next page.
Log Off	Logs you off the Fortify WebInspect Enterprise Web Console application.
Options	Opens the Configure Options window, allowing you to select a default group, choose a time zone for the web console, and enable or disable other options. For more information, see "Configuring Toolbar Options" on page 120.
SSC	Opens the connected OpenText Fortify Software Security Center in the current browser window. **Note:** This link appears only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.
Help	Opens the Help file for the Web Console.
About	Opens a window that displays the Fortify WebInspect Enterprise manager version and the database schema version.

In addition, you can click the Fortify logo to return to the home page of the Fortify WebInspect Enterprise application.

About the WebInspect Enterprise Desktop Application

The WebInspect Enterprise Desktop Application enables you to perform the following tasks:

- View scan results and the Traffic Monitor
- Import a scan
- Use Guided Scan
- Generate reports

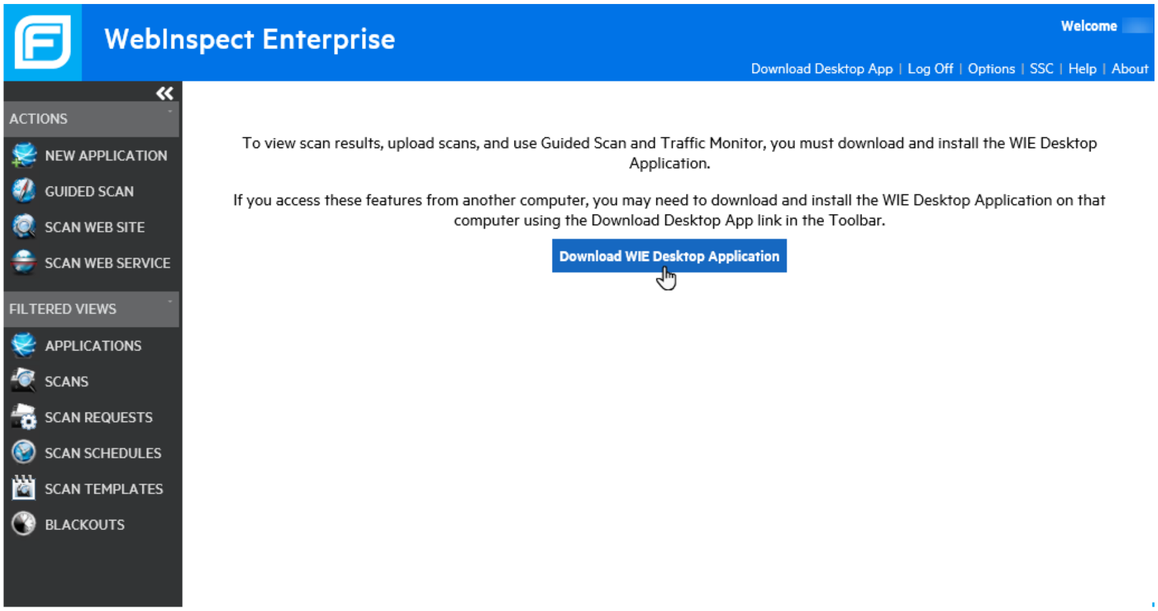
Before you can use these features, however, you must download and install the application.

Downloading from Initial Prompt

The first time you access the Web Console, you are prompted to download the WebInspect Enterprise Desktop Application.

To download the application from the prompt:

1. Click **Download WIE Desktop Application**.



To view scan results, upload scans, and use Guided Scan and Traffic Monitor, you must download and install the WIE Desktop Application.

If you access these features from another computer, you may need to download and install the WIE Desktop Application on that computer using the Download Desktop App link in the Toolbar.

   The `WIEDesktop64.exe` file is downloaded to the local machine.

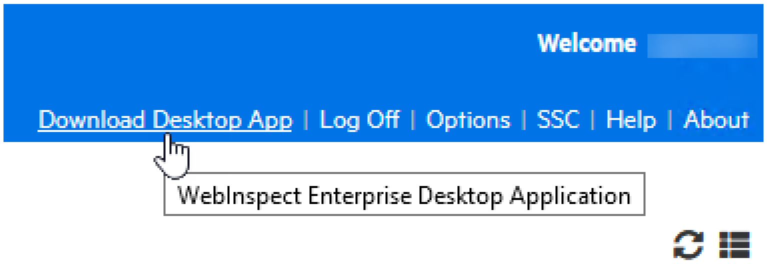
2. Navigate to the download location, right-click the file and select **Run as administrator** to launch the installation wizard.
3. Follow the prompts in the installation wizard to install the application.

Downloading from Toolbar

If you do not download the application when you first access the Web Console, you can download it at anytime from the Web Console toolbar.

To download the application from the toolbar:

1. Click **Download Desktop App** in the Web Console toolbar.


Welcome
Download Desktop App | Log Off | Options | SSC | Help | About
WebInspect Enterprise Desktop Application

   The `WIEDesktop64.exe` file is downloaded to the local machine.
2. Navigate to the download location, right-click the file and select **Run as administrator** to launch the installation wizard.
3. Follow the prompts in the installation wizard to install the application.

Configuring Toolbar Options

Click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar to configure the following options.

Option	Description
Default Group	Select a group that will be used by client applications that cannot specify a group. A client application is OpenText Fortify WebInspect or any application that uses the Fortify WebInspect Enterprise application programming interface (API). Each user account is associated with a default group. If Fortify WebInspect Enterprise receives a call to create an object and the calling client application is not aware of the Fortify WebInspect Enterprise "group" category, Fortify WebInspect Enterprise will use the default group specified here.
Web Console Time Zone	Select the time zone in which you work.
Enable "Scan Web Site" Action	This option enables you to initiate a Web Site scan from the Web Console, using the Scan Web Site function in the Actions group. If not selected, **Scan Web Site** does not appear in the Actions group in the navigation pane. This option is selected by default.
Enable "Scan Web Service" Action	This option enables you to initiate a Web Service scan from the Web Console, using the Scan Web Service function in the Actions group. If not selected, **Scan Web Service** does not appear in the Actions group in the navigation pane. This option is selected by default.

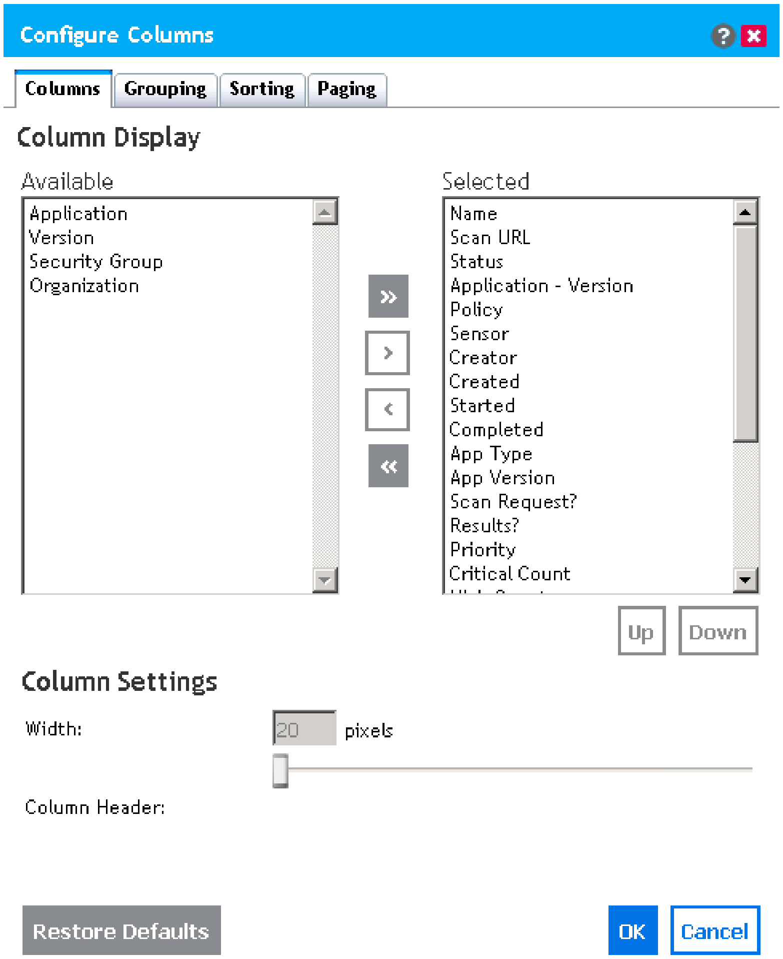
Option	Description
Enable "New Scan Schedule" Action	This option enables you to schedule a scan from the Web Console, using the New Scan Schedule function in the Actions group. If not selected, **New Scan Schedule** does not appear in the Actions group in the navigation pane. This option is not selected by default.
Enable "New Blackout" Action	This option enables you to create and modify blackout periods from the Web Console. If not selected, **New Blackout** does not appear in the Actions group in the navigation pane. This option is not selected by default.

Configuring Form Layouts

Most forms contain an Edit Layout icon that, when clicked, displays the Configure Columns dialog box that enables you to change the number of rows on the page, modify column widths, specify which columns are displayed, and sort data by columns.

This dialog box has four tabs:

- Columns
- Grouping
- Sorting
- Paging



Column Display

Available

- Application
- Version
- Security Group
- Organization

Selected

- Name
- Scan URL
- Status
- Application - Version
- Policy
- Sensor
- Creator
- Created
- Started
- Completed
- App Type
- App Version
- Scan Request?
- Results?
- Priority
- Critical Count

Column Settings

Width: 20 pixels

Column Header:

Columns

Use this tab to specify which columns are displayed on the grid. Column headers listed in the **Selected** list will be displayed. Use the controls illustrated below to move column headers between the **Selected** list and the **Available** list.

Control	Description
»	Add all
›	Add selected
‹	Remove selected
«	Remove all

To change the column width:

1. Select a column header.
2. Enter a value in the **Width** field (or use the slider to select a width).
3. Click **OK**.

Grouping

You can group objects in views (applications, scans, and scan schedules) according to the available column names. Any grouping you define is applied to every tab on the form you are viewing.

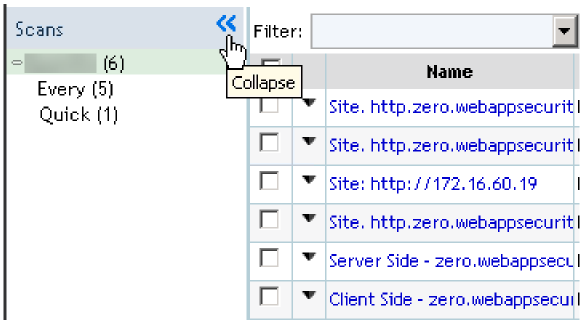
In the following example, vulnerabilities are grouped by severity and then by check name within each severity category.

1. In the Navigation pane, click **Scans**.
2. Click the Edit Layout icon ☰ .
3. On the Configure Columns dialog box, click the **Grouping** tab.
4. In the **Available** list, select **Security Group** and click **>**.
5. Select **Policy** and click **>**.

   Both column headers are now removed from the **Available** list and appear in the **Selected** list.
6. Click **OK**.

When you return to the **Scans** tab, the Group pane displays the grouped results. When you select a group name (such as DEV Group, in this example), OpenText Fortify WebInspect Enterprise displays only those scans belonging to that group. Redundant items (policy names, in this example) are combined and the number of instances is reported in parentheses following the policy name.

You can open or close the pane using the Group pane toggle.



Name
Site. http.zero.webappsecurit
Site. http.zero.webappsecurit
Site: http://172.16.60.19
Site. http.zero.webappsecurit
Server Side - zero.webappsecu
Client Side - zero.webappsecu

Sorting

To arrange the column data alphabetically, select one or more column headers and then select either **Ascending** or **Descending**.

Paging

To specify the number of rows displayed on a page, select a value from the **Page Size** list.

Enabling New Scan Schedules

The New Scan Schedule action enables you to specify settings (options) for a scan and designate the time when the scan should begin.

This feature does not appear in the Actions group in the navigation pane unless **Enable "New Scan Schedule" action** is selected in the toolbar options. To enable or disable this feature, click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar. (It is disabled by default.) See "Using the Interface" on page 116 and "Configuring Toolbar Options" on page 120 if necessary.

See Also

"Configuring a Scheduled Scan" on page 133

"Legacy Scheduled Scan - Schedule: General" on page 250

"Legacy Scheduled Scan - Schedule: Recurrence" on page 251

Enabling New Blackout Periods

The New Blackout action enables you to specify settings (options) for a blackout period.

This feature does not appear in the Actions group in the navigation pane unless **Enable "New Blackout" action** is selected in the toolbar options. To enable or disable this feature, click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar. (It is disabled by default.) See "Using the Interface" on page 116 and "Configuring Toolbar Options" on page 120 if necessary.

Conducting Scans

The following pages describe scanning a web site, Guided Scan, scan schedules, scan templates, and blackout periods.

Accessing Guided Scan

To use Guided Scan, you must download and install the WebInspect Enterprise Desktop Application. For more information, see "About the WebInspect Enterprise Desktop Application" on page 119.

Launching Guided Scan

To launch Guided Scan in Internet Explorer:

1. In the Fortify WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A message appears asking if you want to allow the program to open.
2. Click **Allow**.

To launch Guided Scan in Chrome:

1. In the Fortify WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A message appears asking if you want to open the program.
2. Click **Open WIE.Desktop**.

To launch Guided Scan in Firefox:

1. In the Fortify WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A Launch Application window appears.
2. Select **WIE.Desktop**, and then click **Open Link**.

Configuring a Web Site Scan

Use the New Scan page to configure a web site scan.

Note: This feature does not appear in the Actions group in the navigation pane unless **Enable "Scan Web Site" action** is selected in the toolbar options. To enable or disable this feature, click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar. (It is enabled by default.) See "Using the Interface" on page 116 and "Configuring Toolbar Options" on page 120 if necessary.

Accessing the New Scan Page

To access the New Scan page in the Fortify WebInspect Enterprise Web Console, do one of the following:

- In the Actions group on the navigation pane, click **SCAN WEB SITE**.
- In the Filtered Views group on the navigation pane, click **SCANS**, and then click **Add > Create a Web Site Scan**.

Specifying the Application Version

To specify the application version:

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

Configuring General Settings

To configure the general settings for the scan:

1. Click **GENERAL** in the navigation pane.
2. In the **Scan Name** field, type a name or brief description for the scan.
3. To use an existing scan template with configured settings, select a template from the **Template** list.

4. Select one of the following scan modes:
   - **Crawl Only**: This option completely maps a site's hierarchical data structure.
   - **Crawl & Audit**: Fortify WebInspect maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see "Legacy Scan Settings: Method" on page 218.
   - **Audit Only**: Fortify WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.
5. Select one of the following scan types:

   Standard Scan

   Fortify WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

   a. In the **Start URL** field, type or select the complete URL or IP address of the site you want to examine.

      If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, Fortify WebInspect will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

      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 pursue links that use fully qualified URLs (as opposed to relative paths).

      Fortify WebInspect supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets. See "Internet Protocol Version 6" on page 130.

   b. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:
      - **Directory only (self)** - Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.
      - **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
      - **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

   List-Driven Scan

   Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility.

If you select **List-Driven Scan**, do one of the following:

- Click **Import** and select a text file or XML file containing the list of URLs you want to scan.
- Click **Manage** to create or modify a list of URLs.

Workflow-Driven Scan

Fortify WebInspect audits only those URLs included in the macro that you previously recorded and 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, they will all be included in the same scan.

If you select **Workflow-Driven Scan**, do one of the following:

- Click **Import** to select a macro containing the URLs you want to you want to scan.
- Click **Manage** to import or remove a macro, and to specify allowed hosts.
- If you have access to the Fortify WebInspect Enterprise Administrative Console, click **Tools > Workflow Macro Recorder** to create a workflow macro. See the *OpenText™ Fortify WebInspect Tools Guide*.

Configuring Authentication

To configure authentication for the scan:

1. Click **AUTHENTICATION** in the navigation pane.
2. If you need to access the target site through a proxy server, select **Network Proxy** and then choose an option from the **Proxy Profile** list.

   Note: Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the browser connection settings are not configured for proxy, then a proxy server will not be used.

   - **Auto Detect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use the file to configure the browser's Web proxy settings.
   - **Use System proxy settings on the sensor machine**: Import proxy server information from the sensor machine, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured, not on the local system.
   - **Use PAC file**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **EDIT** to enter the location (URL) of the PAC.
   - **Use Explicit Proxy Settings**: Specify proxy server settings. If you select this option, click **EDIT** to enter proxy information.
   - **Use Firefox proxy settings on the sensor machine**: Import your proxy server information from Firefox, to use it for the user account running the sensor that attempts to run a scan.

     Note: The sensor should run on a user account that has proxy settings configured, not on the local system.

3. Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.
4. Select **Site Authentication** to use a recorded login macro containing a user name and password that allows you to log on to the target site. The macro must also contain a logout condition, which indicates when an inadvertent logout has occurred so Fortify WebInspect Enterprise can rerun the macro to log on again.

   Do one of the following:

   - To use a login macro from the macro repository:
     1. Click **Select**.
     2. Select a macro from the **Macro Name** drop-down list.
     3. Click **OK**.
   - To use a local copy of a login macro, click **Import** to select a macro.
   - To erase the macro name, clear the **Site Authentication** check box.

   If input parameters were used when the login macro was recorded, a list of **Login Macro Parameters** appears. You can edit the inputs in this list. When scanning the application page that contains the input control associated with a parameter, Fortify WebInspect will substitute the input from this list. For more information, see the *OpenText™ Fortify WebInspect Tools Guide*.

   > **Tip:** If parameters were masked when the macro was recorded, the input will be masked in the parameters list. You can edit masked inputs, but the new values will also be masked.

Configuring Coverage

To configure coverage and thoroughness for the scan:

1. Click **COVERAGE** in the navigation pane.
2. Select a policy from the **Policy** list.

   For descriptions of policies, see "Policies List" on page 155.
3. If you want Fortify WebInspect to submit values for input controls on forms it encounters while scanning the target site:
   a. Select **Auto fill web forms during crawl**. Fortify WebInspect will extract the values from a file that you create using the Web Form Editor.
   b. Click **Load** to locate and load the file.
4. If you want to capture traffic session data to view in the Traffic Viewer tool, select **Enable Traffic Monitor**.
5. If your site is case-sensitive, select the **Case-Sensitive URL** option to ensure the URL is treated as case-sensitive during the scan.

   > **Example:** Some servers (such as IIS) do not differentiate between www.mycompany.com/samplepage and www.mycompany.com/SamplePage.

Configuring Priority

Configuring priority for the scan determines the order of the scan in the scan queue. To configure priority for the scan:

1. Click **PRIORITY** in the navigation pane.
2. If you want to create a template containing the settings you configured for this scan, select **Create Scan Template** and type a name for the new template in the **Template Name** field.
3. Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.
4. Select the sensor to run the scan. You can choose a specific sensor or select **Any Available** from the list.

Starting or Canceling the Scan

To start the scan:

- Click **SCAN**.

> **Note:** Even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

To cancel the scan:

- Click **CANCEL**.

> **Note:** If you selected **Create Scan Template**, but cancel the scan, the template will not be created.

Scan Dependencies

Certain objects in OpenText Fortify WebInspect Enterprise are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object.

For example, if a scan uses a scan template, you cannot delete the template until you either delete all scans that use that template or modify those scan settings to use a different template. If the scan is currently running, you must cancel it.

Internet Protocol Version 6

OpenText Fortify WebInspect Enterprise supports Internet Protocol version 6 (IPv6) addresses in web site and web service scans. When you specify the Start URL, you must enclose the IPv6 address in brackets. For example:

- http://[::1]

  Fortify WebInspect Enterprise scans "localhost."
- http://[fe80::20c:29ff:fe32:bae1]??/subfolder/?

  Fortify WebInspect Enterprise scans the host at the specified address starting in the "subfolder" directory.
- http://[fe80::20c:29ff:fe32:bae1]??:8080/subfolder/??

  Fortify WebInspect Enterprise scans a server running on port 8080 starting in "subfolder."

About Web Services

Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most Web services use Simple Object Access Protocol (SOAP) to send XML data between the Web service and the client Web application that initiated the information request. Unlike HTML, which only describes how Web pages are displayed, XML provides a framework to describe and contain structured data. The client Web application can readily understand the returned data and display that information to the end user.

A client Web application that accesses a Web service receives a Web Services Description Language (WSDL) document so that it understands how to communicate with the service. The WSDL document describes the programmed procedures included in the Web service, the parameters those procedures expect, and the type of return information the client Web application will receive.

Configuring a Web Service Scan

Use the New Scan page to configure a web service scan.

> **Note:** This feature does not appear in the Actions group in the navigation pane unless **Enable "Scan Web Service" action** is selected in the toolbar options. To enable or disable this feature, click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar. (It is enabled by default.) See "Using the Interface" on page 116 and "Configuring Toolbar Options" on page 120 if necessary.

Accessing the New Scan Page

To access the New Scan page in the Fortify WebInspect Enterprise Web Console, do one of the following:

- In the Actions group on the navigation pane, click **SCAN WEB SERVICE**.
- In the Filtered Views group on the navigation pane, click **SCANS**, and then click **Add > Create a Web Service Scan**.

Specifying the Application Version

To specify the application version:

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

Configuring General Settings

To configure the general settings for the scan:

1. Click **GENERAL** in the navigation pane.
2. In the **Scan Name** field, type a name or brief description of the scan.
3. Optionally, select a template from the **Template** list to use an existing scan template with configured settings.
4. Click **Import** under Scan Type to open a standard file-selection dialog box and choose a Web Service Test Design (WSD) file that you previously created using the Web Service Test Designer. This file contains values for each operation in the service. For more information, see the *OpenText™ Fortify WebInspect Tools Guide*.

Configuring Authentication

To configure authentication for the scan:

1. Click **AUTHENTICATION** in the navigation pane.
2. If you need to access the target site through a proxy server, select **Network Proxy** and then choose an option from the **Proxy Profile** list.

   > **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the browser connection settings are not configured for proxy, then a proxy server will not be used.

   - **Auto Detect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use the file to configure the browser's Web proxy settings.
   - **Use System proxy settings on the sensor machine**: Import proxy server information from the sensor machine, to use it for the user account running the sensor that attempts to run a scan. Note that the sensor should run on a user account that has proxy settings configured,

not on the local system.

- **Use PAC file**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. If you select this option, click **EDIT** to enter the location (URL) of the PAC.
- **Use Explicit Proxy Settings**: Specify proxy server settings. If you select this option, click **EDIT** to enter proxy information.
- **Use Firefox proxy settings on the sensor machine**: Import your proxy server information from Firefox, to use it for the user account running the sensor that attempts to run a scan.

  Note: The sensor should run on a user account that has proxy settings configured, not on the local system.

3. Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.

Configuring Coverage

To configure coverage for the scan:

1. Click **COVERAGE** in the navigation pane.

   Note: You cannot select a policy. Fortify WebInspect uses the Simple Object Access Protocol (SOAP) policy by default.

2. If you want to capture traffic session data to view in the Traffic Viewer tool, select **Enable Traffic Monitor**.
3. If your site is case-sensitive, select the **Case-Sensitive URL** option to ensure the URL is treated as case-sensitive during the scan.

   Example: Some servers (such as IIS) do not differentiate between www.mycompany.com/samplepage and www.mycompany.com/SamplePage.

Configuring Priority

Configuring priority for the scan determines the order of the scan in the scan queue. To configure priority for the scan:

1. Click **PRIORITY** in the navigation pane.
2. If you want to create a template containing the settings you configured for this scan, select **Create Scan Template** and type a name for the new template in the **Template Name** field.
3. Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.
4. Select the sensor to run the scan. You can choose a specific sensor or select **Any Available** from the list.

Starting or Canceling the Scan

To start the scan:

- Click **SCAN**.

> **Note:** Even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

To cancel the scan:

- Click **CANCEL**.

> **Note:** If you selected **Create Scan Template**, but cancel the scan, the template will not be created.

Configuring a Scheduled Scan

Use the Configure Scheduled Scan page to create a scan schedule using the scan settings from an XML file, a scan template, or an existing scan, or the default settings and a start URL. Using this page does not drop or modify any scan settings.

To access the Configure Scheduled Scan page:

1. Click **Scan Schedules** in the navigation pane.
2. Do one of the following:
    - To create a new scan schedule, click **Add**.
    - To create a new scan based on an existing scan schedule, click **Copy** from the drop-down menu for the existing schedule.
    - To edit an existing scan schedule, click **Edit** from the drop-down menu for the schedule.

    The Configure Scheduled Scan page appears.

Specifying the Application Version

To specify the application version:

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

Configuring General Settings

To configure the schedule and settings to use:

1. Click **GENERAL** in the navigation pane.
2. In the **Schedule** group, configure the items described in the following table.

Item	Description
Schedule Name	Enter a name that identifies this scheduled scan.
Start Time	Enter the date and time you want the scan to begin. You can select the date from a calendar popup and the time from a clock popup.
Time Zone	The time zone for the location of the target server specified for the scheduled scan. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the target server is in a different time zone, you should usually select the server's time zone and specify the **Start Time** using local time. For example, if you are in New York City, USA (UTC-05:00) and the target server is in Rome, Italy (UTC+01:00), and you want to schedule a scan to begin at 8 a.m. Rome time, you could do either of the following: • Select the UTC+01:00 time zone (Rome) and specify a Start Time of 8 a.m. • Select the UTC-05:00 time zone (New York City) and specify a Start Time of 2 a.m.

   For a scan that is scheduled to recur, the following read-only fields provide recurrence information:

   - **Next Scheduled Time** - This field displays the time and date of the next scheduled scan.
   - **Last Occurred On** - This field displays the time and date when a scan last occurred.

3. In the Settings Source group, select one of the following options:
   - To use an existing settings file, select **Settings XML File** and click **Upload** to locate the file to use.
   - To use a scan template, select **Scan Template** and choose a template from the **Template** drop-down list.
   - To use settings from an existing scan, select **Scan Settings** and choose a scan from the **Scan** drop-down list.

- To use the default scan settings, do the following:
    i. Select **Default Settings** and type the start URL in the **URL** field.
    ii. Optionally, if you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:
        - **Directory only (self)** - OpenText Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.
        - **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
        - **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

Configuring Recurrence Settings

To schedule a scan on a recurring basis:

1. Click **Recurrence** in the SCHEDULE navigation pane.
2. Select the **Recurring** check box.

   Do NOT select this option if you want to schedule a one-time-only event.
3. Use the **Pattern** group to select the frequency of the event (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.
4. Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Configuring Behavior Settings

To set a priority, select a sensor, and define a blackout action:

1. Click **Behavior** in the SCHEDULE navigation pane.
2. In the Priority group, select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

   > **Note:** Scans that are manually initiated have priority over any scheduled scan.
3. In the Sensor group, select a sensor to conduct the scan from the **Selected Sensor** drop-down list. You can choose a specific sensor or select the **Any Available** option.

   > **Important!** A sensor can perform only one scan at a time. If it is conducting a scan when another scan is scheduled to occur, then:
   >
   > If the currently running scan has a higher priority, the OpenText Fortify WebInspect Enterprise Manager will place the second scan in a queue until the first scan finishes or until another sensor becomes available.

> If the currently running scan has a lower priority, the Fortify WebInspect Enterprise Manager will suspend that scan, assign the second scan to that sensor, and then reassign the suspended scan to the sensor when the higher priority scan is complete.

4. In the Blackout Action group, select one of the following options:
   - **Suspend the scan** - The sensor will suspend the scan during the blackout period and resume it when the blackout period ends.
   - **Stop the scan** - The sensor will stop the scan.

Configuring Overrides

To select a login macro from the macro repository and specify a policy:

1. Click **OVERRIDES** in the navigation pane.
2. To use a login macro, select a macro from the **Login Macro** drop-down list.

   > **Note:** The Login Macro drop-down list is available only if the application version specified has login macros in the macro repository.

3. To specify a different policy, select a policy from the **Policy** list. For more information, see "Policies List" on page 155.

Finishing Up

To finish and close the Configure Scheduled Scan page, do one of the following:

- To save the scheduled scan, click **Finish**.
- To close the Configure Scheduled Scan page without saving the scheduled scan, click **Cancel**.

Scan Schedules

The Scan Schedules form displays information about each scheduled scan.

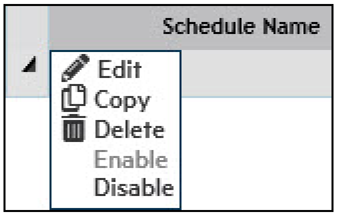
> **Note:** This feature does not appear in the Actions group in the navigation pane unless **Enable "New Scan Schedule" action** is selected in the toolbar options. To enable or disable this feature, click the **Options** link on the OpenText Fortify WebInspect Enterprise toolbar. (It is disabled by default.) See "Using the Interface" on page 116 and "Configuring Toolbar Options" on page 120 if necessary.

Reviewing Scheduled Scan Settings

Click a schedule name to review the settings for the scheduled scan.

Using the Context Menu

You can perform additional functions by clicking the drop-down arrow next to a schedule name and selecting an option from the context menu.



The available functions are:

- **Edit** - Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan window, allowing you to edit the settings for this scheduled scan.
- **Copy** - Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan window, allowing you to edit the settings and create an additional scheduled scan.
- **Delete** - Deletes the schedule.
- **Enable** - Activates a disabled scheduled scan. Requests are enabled, by default, when created.
- **Disable** - Deactivates a scheduled scan. The request remains in the grid, but the scan will not be executed unless the request is enabled prior to the scheduled time and date.

You can also delete a scheduled scan by selecting the check box next to the schedule name and clicking **Delete** above the form grid.

Using the Icons Above the Form Grid

You can perform additional functions using the icons at the top of the form.

Icon	Function
+ Add	Schedule a scan. For more information, see "Configuring a Scheduled Scan" on page 133.
🗑 Delete	Remove the scheduled event.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which

Icon	Function
	columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:
d.hh.mm
where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

   The table displays all records.

Scheduled Scan Dependencies

Certain objects in OpenText Fortify WebInspect Enterprise are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object.

A scheduled scan may be linked to a scan template. You cannot delete the template until you either delete all scheduled scans that use the template or modify those scan settings to use a different template. If the scan is currently running, you must cancel it.

Using Scan Requests from Fortify Software Security Center

> **Note:** This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

To process a scan request, you must create a web site scan or web service scan in Fortify WebInspect Enterprise. The Scan Requests form lists all requests issued by Fortify Software Security Center to Fortify WebInspect Enterprise to conduct a scan. The possible values for the Status column are Pending, In Progress, Canceled, and Complete.

For information about checking the scan request status, editing the scan request, and canceling the scan request in Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*.

Processing a Pending Request

To process a pending request for a web site or web service scan:

1. In the Filtered Views section of the navigation pane, click **Scan Requests**.
2. On the Scan Requests window, select a pending request. The information entered by the original requester is displayed on the Details tab in the lower pane.

   > **Tip:** You can restrict the display of scan requests to those that match criteria you specify. Click ▽ in the header of one or more columns and enter the appropriate filter information.

3. Mark the scan request as In Progress:
   a. On the Details tab in the lower pane, click the **Status** drop-down list and select **In Progress**.
   b. Click **Change Status**.
4. Click **Create a Web Site Scan** or **Create a Web Service Scan**.

   > **Note:** Fortify WebInspect Enterprise determines the start URL from the data in the scan request that was sent from Fortify Software Security Center. The New Scan page opens and the Start URL field is auto-filled with the URL from the scan request. If the URL is not properly formatted in the scan request, the Start URL cannot be determined and default information is used in the New Scan page. When this occurs, you can copy the URL Value from the Details tab on the Scan Requests page and paste it into the Start URL field of the New Scan page. For more information about using the New Scan page, see "Configuring a Web Site Scan" on page 125 or "Configuring a Web Service Scan" on page 130 in the web console help or the *OpenText™ Fortify WebInspect Enterprise User Guide*.

5. Upon completion, the scan is automatically published to Fortify Software Security Center by default. If you have disabled automatic publishing, then manually publish the scan.
   a. Do one of the following:
      - From the Project Version Details form, select the scan and click **Publish**.
      - From the Scans form, select the scan and click **Publish**.
      - Open a scan in the Scan Visualization window and click **Publish**.

   b. When the Status Summary is displayed, select **Associate scan with an "In Progress" scan request for the current project version**. The scan will appear on the Associated Scans tab of the appropriate scan request in the Scan Request form.
6. Mark the scan request as Completed:
   a. On the Scan Requests form, select the request for the scan.
   b. On the Details tab in the lower pane, click the **Status** drop-down list and select **Completed**.
   c. Click **Change Status**.

Associating Scans Manually

Associating a scan with a scan request is simply a tracking tool that provides a historical record of the scan activity related to a specific request. You can associate scans automatically when publishing (as in Step 5 of "Processing a Pending Request" on the previous page), or you can associate scans manually, using the following procedure:

1. Select a scan request from the top pane.
2. In the bottom pane, click the **Associated Scans** tab.
3. Click **Associate Scans**.

   The program displays a list of all scans associated with the selected application version that have not been associated with a specific request.
4. Select a scan and click **OK**.

See Also

"Creating a Scan Request in Fortify Software Security Center" below

Creating a Scan Request in Fortify Software Security Center

> **Note:** This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

Use the following procedure in Fortify Software Security Center to create a request for Fortify WebInspect Enterprise to conduct a dynamic scan:

1. On the Dashboard, move your cursor to the application version that you want to have scanned, and then select **Artifacts** from the shortcut menu.
2. On the ARTIFACT HISTORY page, click **DYNAMIC SCAN.**

   The DYNAMIC SCAN - *<APPLICATION VERSION>* dialog box opens.
3. Provide the information described in the following table.

   > **Note:** The following table does not list custom dynamic scan attributes that you or another Fortify Software Security Center administrator may have added to the system.

Dynamic Scan Attribute *** (Required field)**	**Description**
*URL	URL of the site to scan
Site Login	Username required to log on to the site to scan
Site Passcode	Password to use to gain access to the site

Dynamic Scan Attribute ***** **(Required field)**	**Description**
Network Login	Username required for network authentication
Network Passcode	Password required for network authentication
Related Host Name(s)	Allowable hosts for the application to scan
Web Services Used	Comma-delimited list of web services used by the application to scan
Technologies Used	Comma-delimited list of technologies used by the site to scan
Compliance Implications	Information about any potential compliance implications
Allowable Scan Times	Dates and times during which the tester can perform the scan **Example:** From 17:00 h to 06:00 h, Monday through Friday, from 09/03/18 to 11/30/18 You can run the scan immediately instead of scheduling it to run later. For instructions, see "Using Scan Requests from Fortify Software Security Center" on page 139.
WSDL	Browse to and select your Web Services Description Language file (*.wsdl, *.webmacro, or *.xml)

Note: The dynamic tester who handles the scan request on Fortify WebInspect Enterprise may be interested in additional application version attributes, such as business risk and compliance implications. The tester can use existing web services methods to retrieve those attributes for an application version.

4. Click **SUBMIT**.

   The request is transmitted to Fortify WebInspect Enterprise and placed in the Scan Requests form. Fortify Software Security Center displays a message to verify that the request submission was successful.

   Next, the dynamic tester who monitors and responds to scan requests runs the scan during the hours you specified, and then uploads the results to Fortify Software Security Center.

5. If you are a Fortify Software Security Center Administrator or Application security tester, you can run the requested dynamic scan immediately from Fortify WebInspect Enterprise. For instructions, see "Using Scan Requests from Fortify Software Security Center" on page 139.

Using Scan Templates

A scan template is any convenient collection of scan settings, potentially including particular macros, that you can reuse when you run scans. This form lists all scan templates that you have permission to view.

For each template, this form displays (by default) the following information:

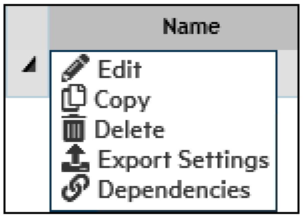
- **Name** - The name assigned to the template.
- **Application** - The specified application.

To view or modify details about a template, click the template name.

Depending on how the scan template was created, it is displayed with one of the following sets of fields:

- The **Global Template** check box (not selected), and the **Application** and **Version** fields that were selected when it was created
- The **Global Template** check box (selected), the organization and group combination that was selected when it was created, and the **Use Organization** check box. **Use Organization** is selected only if:
  - This OpenText Fortify WebInspect Enterprise instance was a migration from the Assessment Management Platform (AMP) product, and
  - This scan template was created in AMP and associated with an organization in AMP.

You can perform additional functions by clicking the drop-down arrow for a specific template.



The functions are:

- **Edit** - Displays the Configure Scan Template form, allowing you to modify the settings defined for the selected template.
- **Copy** - Opens the Configure Scan Template form, allowing you to modify (if necessary) and save the scan template settings.
- **Delete** - Delete the scan template.
- **Export Settings** - Export the template settings to an XML file for storage or transfer.
- **Dependencies** - Displays a list of objects (such as scans and scheduled scans) that are linked to this template. You cannot delete this template until you either delete the scheduled scan, assign a different template to the scheduled scan, or cancel the scan (if it is currently running). See "About Dependencies" on page 171 for more information.

You can also perform these functions using the icons at the top of the form.

Icon	Function
Add	Select **Create a Guided Template** to create a template using the Guided Scan user interface where all the scan settings can be reviewed and changed. Select **Create a Scan Template** to create a template using settings from an XML file, a scan template, or an existing scan. For more information, see "Configuring a Scan Template" on page 146.
Import	Select **Oracle Settings** to create a template that contains settings that are optimized for Oracle. Select **Websphere Settings** to create a template that contains settings that are optimized for WebSphere.
Delete	Delete the selected templates from the list.

You can also use the icons illustrated below.

Icon	Function
⟳	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:
d.hh.mm
where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

The table displays all records.

Configuring a Scan Template

Use the Configure Scan Template page to create a scan template using the scan settings from an XML file, an existing scan, or the default settings and a start URL. Using this page does not drop or modify any scan settings.

To access the page:

1. Click **Scan Templates** in the navigation pane.
2. Do one of the following:
   - To create a new scan template, click **Add > Create a Scan Template**.

     > **Note:** To create a new scan template using Guided Scan, click **Add > Create a Guided Template**.

   - To create a new scan based on an existing scan template, click **Copy** from the drop-down menu for the existing template.
   - To edit an existing scan template, click **Edit** from the drop-down menu for the template.

   The Configure Scheduled Template page appears.

Specifying the Application Version

To specify the application version:

1. To create a global template, select the **Global Template** check box. For more information about global templates, see "Using Scan Templates" on page 143.
2. Select an application from the **Application** list.
3. Select a version from the **Application Version** list.

Configuring General Settings

To specify a template name and the settings to use:

1. Click **GENERAL** in the navigation pane.
2. In the Template Name group, type a name in the **Scan Template Name** field.
3. In the Template Settings Source group, select one of the following options:
   - To use an existing settings file, select **Settings XML File** and click **Upload** to locate the file to use.
   - To use settings from an existing scan, select **Scan Settings** and choose a scan from the **Scan** drop-down list.
   - To use the default scan settings, do the following:

i. Select **Default Settings** and select the start URL in the **URL** drop-down list.

ii. Optionally, if you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:

- **Directory only (self)** - OpenText Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.
- **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

Configuring Overrides

To select a login macro from the macro repository and specify a policy:

1. Click **OVERRIDES** in the navigation pane.
2. To use a login macro, select a macro from the **Login Macro** drop-down list.

   > **Note:** The Login Macro drop-down list is available only if the application version specified has login macros in the macro repository.

3. To specify a different policy, select a policy from the **Policy** list. For more information, see "Policies List" on page 155.

Finishing Up

To finish and close the Configure Scan Template page, do one of the following:

- To change the scan settings, click **Finish with Guided Scan**.

  Guided Scan opens with the settings loaded. You can change the scan settings as usual. For more information, see the Guided Scan help or the *OpenText™ Fortify WebInspect Enterprise User Guide*. For more information, see "Editing a Scan Template in Guide Scan" below.
- To save the template, click **Finish**.
- To close the Configure Scan Template page without saving the template, click **Cancel**.

Editing a Scan Template in Guide Scan

You can edit an existing scan template using the Advanced Settings in Guided Scan. Editing a template in Guided Scan provides access to:

- Scan settings, such as scan mode, HTTP parsing options, policy, and more
- Crawl settings, such as link parsing, link sources, and session exclusions
- Audit settings, such as attack exclusions, attack expressions, vulnerability filtering, and more

Process Overview

The following table describes the process to edit an existing template in Guided Scan.

Stage	Description
1.	Open the template in the Fortify WebInspect Enterprise Web Console. 1. Click **Scan Templates** in the navigation pane. 2. Click **Edit** from the drop-down menu for the template or click the template name. The Update Scan Template page appears.
2.	Click **Finish with Guided Scan**. Guided Scan opens with the settings loaded.
3.	In Guided Scan, click **Advanced**.
4.	Change the settings as needed. For information about specific settings, see the Guided Scan help or "Advanced Guided Scan Settings" on page 361.
5.	Click **OK** in the Settings window.
6.	Click **Save** in the Templates section of the Guided Scan toolbar.
7.	In the Save Template dialog box, do one of the following: • To update the template you edited, click **Save** • To save the edits as a new template, change the name and click **Save**.
8.	Close Guided Scan.

See Also

"Configuring a Scan Template" on page 146

Scan Template Dependencies

Certain objects in Fortify WebInspect Enterprise are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object.

A scan template may be linked to the following objects:

- Scheduled scan
- Scan (only if scan has not completed)
- Site

You cannot delete this template until you either delete the associated scheduled scan, assign a different template to the scheduled scan, delete the site, or cancel the scan (if it is currently running).

Blackouts Overview

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

OpenText Fortify WebInspect Enterprise will not prevent you from scheduling a scan or attempting to start a scan manually during a blackout period. It will, however, display a message notifying you of the restriction. If you opt to override the warning, the Fortify WebInspect Enterprise manager will place the job in the pending job queue and will start the scan when the blackout period ends.

Similarly, if a scan is running when a blackout period begins, the Fortify WebInspect Enterprise manager will suspend the scan, place it in the pending job queue, and finish the scan when the blackout period ends. In cases where a blackout is defined for multiple IP addresses, the Fortify WebInspect Enterprise manager will suspend the scan only if the scan begins at one of the specified IP addresses. If the scan begins at a non-excluded IP address, but subsequently pursues a link to a host whose IP address is specified in the blackout setting, the scan will not be suspended.

A configuration file on the server allows you to disable this automatic suspension feature, allowing a running job to run to completion even if a blackout period begins during the scan.

To change this setting, contact Fortify Customer Support.

Using Blackouts

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

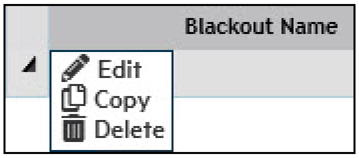
You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

For each blackout defined in the system, the Blackouts form displays (by default) the information described in the following table.

Item	Description
Blackout Name	The identifier for this blackout period.
Type	Allow or deny scans during this period.
IP Range	IP address (or range of IP addresses) that are affected by this blackout period. Use an asterisk (*) to specify all possible IP addresses.
Status	Future, or Scans Disallowed, or Scans Allowed.
Recurrence	One time only, or the defined recurrence pattern.
Next Occurrence	The date and time when the blackout is next scheduled to start, using the Web Console time zone specified in the Web Console options.
Next Occurrence (Target)	The date and time when the blackout is next scheduled to start, using the time zone for the location of the target server that is affected by the blackout. This is significant only when the Web Console user and the target server are in different time zones.
Security Group	Name of the security group with which this blackout is associated.
Organization Name	Name of the organization with which this blackout is associated.

To view or modify details about a blackout, click the blackout name.

You can perform additional functions by clicking the drop-down arrow next to a blackout name.



The function unique to this menu is:

Copy: Opens the Configure Blackout form containing blackout settings. You can modify the settings (if desired) and rename the blackout.

You can also perform additional functions using the commands at the top of the form:

Icon	Function
Add	Display the Configure Blackout window, allowing you to specify parameters

Icon	Function
	associated with a blackout period.
Delete	Delete the selected blackout period.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:
d.hh.mm
where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

   The table displays all records.

Creating a Blackout Period

To create a blackout period:

1. Do one of the following:
   - In the Actions group on the navigation pane, click **New Blackout**.

     Note: This action does not appear unless it is enabled from the toolbar **Options**.

   - In the Resources group on the navigation pane, click **Blackouts** and then click **Add**.
2. On the BLACKOUT: General window, enter the information described in the following table.

Field	Description
Business Unit	Select an organization and group. To associate the blackout with all groups in an organization, select **Use Organization**.
Name	Name for the blackout period.
Address	The URL or IP address (or range of IP addresses) that are affected by this blackout period. The value can be a single URL or IP address, or a range of IP addresses. If you need to exclude multiple ranges, you must create additional (overlapping) blackout periods. To specify a range, separate the beginning address and ending address with a hyphen. You can use the asterisk (*) as a wild card. The default setting (an asterisk) means all addresses. Wildcards in IP addresses must be at the end of the address as shown, but wildcards for host names must be at the beginning. Examples: • 192.16.12.1-192.16.12.210 • 192.16.12.* • *.domain.com
Schedule	In the **Schedule** group, enter the **Start Time** (the date and time at which the blackout period begins) and the **End Time** (the date and time at which the blackout period expires). You can enter the data manually or select the date from a calendar popup and the time from a clock popup.

Field	Description
	Time Zone is the time zone for the location of the target server that is affected by the blackout. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the target server is in a different time zone, you should usually select the server's time zone and specify the blackout period using local time. For example, if you are in New York City, USA (UTC-05:00) and the OpenText Fortify WebInspect Enterprise manager is in Rome, Italy (UTC+01:00), and you want to schedule a blackout to begin at 8 a.m. Rome time, you could do either of the following: • Select the UTC+01:00 time zone (Rome) and specify a Start Time of 8 a.m. • Select the UTC-05:00 time zone (New York City) and specify a Start Time of 2 a.m. **Duration** is the length of time during which the blackout is in effect. This value is calculated automatically after you specify the **Start Time** and **End Time**. Alternatively, if you specify the **Start Time** and the **Duration**, the **End Time** is calculated. If you edit the **Duration**, the **End Time** is recalculated. The format of **Duration** is d.hh.mm where d = the number of days hh = the number of hours mm = the number of minutes
Blackout Type	Select one of the following: • **Allow scans during this period**: Scans of the specified targets are allowed only during the specified time period. • **Deny scans during this period**: Scans of the specified targets are prohibited during the specified time period. Allowing or denying scans works very much like allowing or denying permissions. Deny always takes precedence over allow, so a scan can occur only at a particular time if there are no blackout periods that deny that time. An allow blackout period means that you will deny scans unless you are in the allowed range, not that you will allow scans only if you are in the allowed range. If you configure two separate

Field	Description
	“allow” blackout periods, a scan will be allowed only during the union of those periods. For example, if blackout period A allows scans from 1 p.m. to 3 p.m. and period B allows scans from 2 p.m. to 6 p.m., then scans will be allowed only from 2 p.m. to 3 p.m.

3. To schedule a blackout on a recurring basis, on the BLACKOUT: Recurring window:
   a. Select the **Recurring** check box to impose recurring blackouts. Do *not* select this option if you want to schedule a one-time-only event.
   b. Use the **Pattern** group to select the frequency of the blackout (daily or every x days, weekly, monthly, or yearly) and then provide the appropriate information.
   c. Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the blackout should occur.

Policies List

Fortify WebInspect provides various policies that you can use with your scans and crawls to determine the vulnerability of your Web application. Each policy is kept current using the SmartUpdate function, ensuring that assessments are accurate and capable of detecting the most recently discovered threats. The policies described here are listed by group.

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.

About OAST-related Checks

For networks that have Internet access, the Fortify WebInspect sensor uses a public DNS service when running OAST-related checks. Ensure that your firewall does not block access to **fortify-oast.net**. For networks lacking Internet access, the Fortify OAST on Docker image is available. For more information, see the *OpenText™ Fortify WebInspect and OAST on Docker User Guide*.

Best Practices

The Best Practices group contains policies designed to test applications for the most pervasive and problematic web application security vulnerabilities.

- **API**: This policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.

- **CWE Top 25 *<version>***: The Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25) is a list created by MITRE. The list demonstrates the most widespread and critical software weaknesses that can lead to vulnerabilities in software.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **Best Practices** group.
- **General Data Protection Regulation (GDPR)**: The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and provides a framework for organizations on how to handle personal data. The GDPR articles that pertain to application security and require businesses to protect personal data during design and development of their products and services are as follows:
  - Article 25, data protection by design and by default, which requires businesses to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.
  - Article 32, security of processing, which requires businesses to protect their systems and applications from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

  This policy contains a selection of checks to help identify and protect personal data specifically related to application security for the GDPR.
- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 - (NIST SP 800-53 Rev.5) provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. This policy contains a selection of checks that must be audited to meet the guidelines and standards of NIST SP 800-53 Rev.5.
- **OWASP Application Security Verification Standard (ASVS)**: The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test, and verify secure applications.

  This policy uses OWASP ASVS suggested CWE mapping for each category of SecureBase checks to include. Because CWE is a hierarchical taxonomy, this policy also includes checks that map to additional CWEs that are implied from OWASP ASVS suggested CWE using a "ParentOf" relationship.
- **OWASP Top 10 *<year>***: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about the most critical web application security flaws. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. Multiple releases of the OWASP Top Ten policy may be available. For more information, consult the OWASP Top Ten Project.
- **SANS Top 25*<year>***: The SANS Top 25 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software. These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to take over the software completely, steal data, or prevent the software from working

altogether.

- **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers.

By Type

The By Type group contains policies designed with a specific application layer, type of vulnerability, or generic function as its focus. For instance, the Application policy contains all checks designed to test an application, as opposed to the operating system.

- **Aggressive Log4Shell**: This policy performs a comprehensive security assessment of your web application for JNDI Reference injections in vulnerable versions of Apache Log4j libraries. In vulnerable versions, Log4j does not restrict JNDI features. This allows an attacker who can control log messages to inject JNDI references that point to an attacker-controlled server. This can lead to remote code execution on the vulnerable target. Compared with other policies that include Log4Shell agent, this policy performs a more accurate and decisive job, but produces a significant number of requests and has a longer scan time.
- **Aggressive SQL Injection**: This policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs a more accurate and decisive job, but has a longer scan time.
- **Apache Struts**: This policy detects supported known advisories against the Apache Struts framework.
- **Blank**: This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Client-side**: This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.
- **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.
- **Cross-Site Scripting**: This policy performs a security scan of your web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a website to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application

development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **By Type** group.

- **Mobile**: A mobile scan detects security flaws based on the communication observed between a mobile application and the supporting backend services.
- **NoSQL and Node.js**: This policy includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL, such as MongoDB, and server side infrastructures based on JavaScript, such as Node.js.
- **OAST**: This policy includes all checks that use Out-of-band Application Security Testing (OAST) technology in scanning logic.
- **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **PCI DSS 4.0**: The Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0) provides a baseline of technical and operational requirements designed to protect account data. This policy contains a selection of checks that need to be audited to meet the secure coding requirements of PCI DSS 4.0.
- **PCI Software Security Framework *<version>* (PCI SSF *<version>*)**: The PCI SSF provides a baseline of requirements and guidance for building secure payment systems and software that handle payment transactions. This policy contains a selection of checks that must be audited to meet the secure coding requirements of PCI SSF.
- **Privilege Escalation**: The Privilege Escalation policy scans your web application for programming errors or design flaws that allow an attacker to gain elevated access to data and applications. The policy uses checks that compare responses of identical requests with different privilege levels.
- **Server-side**: This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQL Injection**: The SQL Injection policy performs a security scan of your web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database.
- **Transport Layer Security**: This policy performs a security assessment of your web application for insecure SSL/TLS configurations and critical transport layer security vulnerabilities, such as Heartbleed, Poodle, and SSL Renegotiation attacks.
- **WebSocket**: This policy detects vulnerabilities related to WebSocket implementation in your application.

Custom

The Custom group contains all user-created policies and any custom policies modified by a user.

Hazardous

The Hazardous group contains a policy with potentially dangerous checks, such as a denial-of-service attack, that could cause production servers to fail. Use this policy against non-production servers and systems only.

- **All Checks**: An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the database. This scan includes all checks that are listed in the compliance reports that are available in Fortify web application and web services vulnerability scan products. This includes checks for known and unknown vulnerabilities at the web server, web application server, and web application layers.

  > **Caution!** An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. We strongly recommend 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.

Working with Applications

The following pages describe how to create and view application versions, and view application version details, deleted applications, and vulnerabilities. It also describes how to work with an alias and the macro repository.

Creating New Application Versions

OpenText Fortify WebInspect Enterprise users with the "Can Create Application Version" permission can create a new Application Version directly in Fortify WebInspect Enterprise. If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, these new Application Versions are automatically added to Fortify Software Security Center. Fortify Software Security Center users who can view the new Application Version in Fortify WebInspect Enterprise at the time of creation are automatically assigned to the new application version in Fortify Software Security Center. For additional users to be able to use the Application Version in Fortify Software Security Center, the WIE Administrator for Fortify Software Security Center must assign new users to the new Application Version.

Creating an Application Version

To create an Application Version:

1. Under Actions, select **New Application**.
2. On the General page, do the following:
   a. Select an organization and security group from the **Business Unit** drop-down list.

      > **Note:** This list includes only those organizations and security groups to which you have access.

   b. Select an existing **Application Name** from the drop-down list or click **Add** to create a new Application Name.
   c. Type a **Version Name**.
   d. Optionally, type the **URL** for the new Application Version.
   e. Optionally, add or remove **IP Addresses** in the Host section.
   f. Optionally, select the **Virtual Host** option to indicate the hosts reside on a single server.
3. On the Information page, it is optional to do the following:
   a. Type the **Operating System** and **Web Platform** information.
   b. Type the contact **Name** and **Email** address.
   c. Type any **Notes** that may be pertinent for the new Application Version.
4. Click **Finish**.

   The new Application Version is created in **WebInspect Enterprise** and, if applicable, is ported to Fortify Software Security Center during a subsequent sync.

See Also

"Viewing Application Versions" below

"Reviewing Application Version Details" on page 164

Viewing Application Versions

The Application Versions form displays, in the left column, a list of all defined applications and their component versions.

> **Note:** If OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center (SSC) and an application version is created in Fortify Software Security Center, it automatically appears in the Application Versions here in Fortify WebInspect Enterprise.

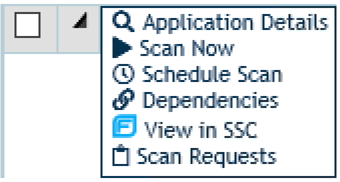
Click an application name to display information about all associated versions, or click a single version name.

For each version selected, this form displays:

- The application version name
- The number of issues detected in each of six categories
- The name of the security group with which this version is associated
- The name of the organization with which this version is associated
- The name of the application with which this version is associated

Click a version name to view application version details. See "Reviewing Application Version Details" on page 164.

You can perform additional functions by clicking the drop-down arrow for a specific application version.



Note: The functions listed will vary based on whether Fortify WebInspect Enterprise is installed as standalone or integrated with Fortify Software Security Center.

The functions are:

- **Application Details** - View application version details.
- **Scan Now** - Open the New Scan form, allowing you to enter scan settings and initiate a scan.
- **Schedule Scan** - Open the Configure Scheduled Scan form, allowing you enter scan settings and schedule a scan.
- **Delete** - Move the application version to the Deleted Applications page, where it can then be purged from the system. This function is available in standalone Fortify WebInspect Enterprise only. See "Managing Deleted Applications" on page 170 for more information.
- **Dependencies** - Displays a list of scans that are associated with this application version. You cannot purge a deleted application version until you delete the associated scans or move them to a different application version. You can export the list of dependencies to a comma-separated values (.csv) file. See "About Dependencies" on page 171 for more information.
- If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the following functions are also available:
  - **View in SSC** - Launch Fortify Software Security Center and navigate to the **Issues** tab of the Application Version window.
  - **Scan Requests** - View all Fortify Software Security Center scan requests associated with this application version.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:

d.hh.mm

where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

   The table displays all records.

See Also

"Creating New Application Versions" on page 160

"Reviewing Application Version Details" below

Reviewing Application Version Details

This form provides complete details about the selected application version, categorized on the tabs described in this topic.

All Scans

The **All Scans** tab lists all scans conducted for the application version and displays (by default) the following information:

- Scan name
- Scan status (failed or complete)
- Date and time the scan was conducted
- Date and time the scan was published
- If OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center (SSC), whether the scan was requested by Fortify Software Security Center
- Number of vulnerabilities detected, categorized by severity

- If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the published status (Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC)

Icons allow you to add scans, delete scans, move scans to a different application version, publish scans to SSC, and change the state of a scan. Click a scan name to open the Scan Visualization window for that scan.

Click the drop-down arrow for a specific scan and select an option to:

- View scan details in the Scan Visualization window.
- Move the scan to a different application version.
- Delete the scan.
- If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, publish scan data to SSC.
- Export the scan in Fortify WebInspect format, as XML, or as FPR, or export settings for the selected scan.

  Note: After exporting to the .fpr format, you must manually upload the .fpr file to Fortify Software Security Center (if applicable). OpenText does not support uploading both OpenText Fortify WebInspect FPR artifacts and Fortify WebInspect Enterprise FPR artifacts to the same application version in Fortify Software Security Center.

- Perform other functions.

Issues

This tab lists all vulnerabilities, sorted by severity, detected in this application version and displays (by default) the following information:

- Check ID - Identification number of the Fortify WebInspect probe that discovered the vulnerability.
- Check Name - Name of the check that discovered the vulnerability.
- Vulnerable URL - Location of the vulnerability.
- Severity - A relative assessment of the vulnerability, ranging from low to critical.
- Scan - Name of the scan.
- SSC Status - Indicates whether or not the issue has been uploaded to Fortify Software Security Center.

  Note: This information is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- Ignored - If a check mark appears in column, a user classified this vulnerability as Ignored (using the Review Vulnerability form).
- False Positive - If a check mark appears in column, a user classified this vulnerability as a false positive (using the Review Vulnerability form).

Click the drop-down arrow for a specific issue to view details or view the application version in Fortify Software Security Center (if applicable).

Click a check name to open the Issue Details form. This form has the following tabs:

- Vulnerability - Contains a complete description of the detected vulnerability, including instructions for verifying and fixing the problem.
- Request - Displays the HTTP request sent to the target site as a probe for the vulnerability.
- Response - Displays the HTTP response returned by the target site.
- Stack Trace - This feature is designed to support Fortify WebInspect Agent when it is installed and running on the target server. For certain checks (such as SQL injection, command execution, and cross-site scripting), Fortify WebInspect Agent intercepts Fortify WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, OpenText Fortify WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.
- Additional Info - For Flash files, displays decompiled code.

An icon enables you to show or hide ignored issues.

Scan Templates

This tab displays a list of scan templates associated with this application version and displays (by default) the following information for each template:

- Name - The name assigned to the template
- Application version - The application version associated with the specified application. Not applicable to global templates.

Click the drop-down arrow for a specific template and select options to edit, copy, or delete the template, or display dependencies associated with the template.

Click a template name to open the Configure Scan Template window to view or modify template settings.

Icons allow you to create or delete a template, or import a template that contains settings that are optimized for Oracle.

For more information about scan templates, see "Using Scan Templates" on page 143.

Schedules

This tab displays a list of all scans scheduled for the application version and displays (by default) the following information:

- Name of the scheduled scan
- URL of the scan target
- Recurrence
- Application version
- Sensor
- Policy

- Priority
- Scan type
- Last occurrence
- Last occurrence (target)
- Next occurrence
- Next occurrence (target)
- Security group
- Organization

Click a schedule name to open the Configure Scheduled Scan window to view or modify settings for the scan.

Click the drop-down menu next to each Check ID to edit, copy, delete, or enable/disable the scheduled scan.

Icons allow you to add or delete scheduled scans.

Properties

This tab lists information about the application version, including the application version name and URL, platform information, the contact's name and e-mail address, and host information.

Notes

This tab enables you to create or view notations associated with the application version.

Aliases

This tab displays all aliases created for the application version, and displays, for each alias, the following information:

- Primary URL for this application version
- Description of the alias
- Indication of whether or not the server differentiates between URLs based on case sensitivity

Click the drop-down menu for a specific alias to edit or delete the alias. See "Adding or Editing an Alias" on page 172 for detailed instructions.

Icons allow you to add or delete aliases, or recalculate all scans.

Login Macros

You can create login macros that are reusable at different locations and among different security groups across your enterprise. Login macros are added and maintained at the Application Version level, and are stored in a macro repository.

This tab displays a list of login macros that are available in the macro repository for the Application and Application Version being viewed. The list provides the Macro Name and the date and time of its last update.

You can add a new login macro to the repository on the Login Macros tab. You can also edit, download new versions, or delete individual login macros that are already in the list. See "Working with the Macro Repository" on page 173 for more information.

Additional Functions

You can also perform additional functions using the icons at the top of the form. These icons are available regardless of the tab being viewed.

Icon	Function
Scan Now	Display scan settings, as entered for the previous scan. You can modify the settings, if desired, before initiating the scan.
View in SSC	Launch the Fortify Software Security Center application and navigate to the **Issues** tab of the Application Version window. **Note:** This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.
Scan Requests	Navigate to the Scan Requests form, where you can process requests issued from Fortify Software Security Center. **Note:** This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:
d.hh.mm
where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

   The table displays all records.

See Also

"Creating New Application Versions" on page 160

"Reviewing Application Version Details" on page 164

Viewing Vulnerabilities

The Vulnerability Viewer can be invoked from the **Issues** tab on the Application Version Details window using either of two methods:

- If you click an entry in the Check Name column, the viewer appears at the bottom of the window.
- If you click the drop-down arrow next to the Check ID and select **View Details** from the menu, the viewer appears in a separate window.

The Vulnerability Viewer has the following tabs:

- **Vulnerability** - Contains a complete description of the detected vulnerability, including instructions for verifying and fixing the problem.
- **Request** - Displays the HTTP request sent to the target site as a probe for the vulnerability.
- **Response** - Displays the HTTP response returned by the target site.
- **Stack Trace** - This feature is designed to support OpenText Fortify WebInspect Agent when it is installed and running on the target server. For certain checks (such as SQL injection, command execution, and cross-site scripting), Fortify WebInspect Agent intercepts OpenText Fortify WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, Fortify WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.
- **Additional Info** - For Flash files, displays decompiled code.

Managing Deleted Applications

Note: This feature does not appear in the navigation pane until application versions are deleted and those application versions have scans, scan templates, or schedules associated with them.

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the Deleted Applications form displays a list of application versions that have been removed from Fortify Software Security Center.

For standalone Fortify WebInspect Enterprise installations, the form displays a list of application versions that have been removed using the Delete function on the Application Versions form.

For each version, this form displays:

- The application version name
- The number of issues detected in each of six severity categories
- The name of the security group
- The name of the organization
- The name of the application

Click a version name to view application version details; see "Reviewing Application Version Details" on page 164.

Recovering Deleted Applications (Standalone)

To recover a deleted application for standalone Fortify WebInspect Enterprise installations, click the drop-down arrow next to an application version name and select **Recover** (or select one or more application versions and click the **Recover** icon at the top of the form).

Recovering Deleted Applications (Integrated with Software Security Center)

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, you cannot recover a deleted application version. However, you can contact the system administrator and request that the associated scans, scan templates, and schedules be moved to another application version in the Admin Console.

Permanently Deleting Applications

To permanently delete an application version, click the drop-down arrow next to an application version name and select **Purge** (or select one or more application versions and click the **Purge** icon at the top of the form).

Caution! Purged versions cannot be recovered.

About Dependencies

Certain objects in OpenText Fortify WebInspect Enterprise are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object.

For example, if you have an application version that contains scans, you cannot delete that application version unless you first delete the associated scans or assign them to a different application version.

The dependencies are categorized in the following table. Dependent objects must be disassociated from the parent object before the parent object can be deleted.

Parent Object	Dependent Objects
Scan Template	• Scheduled scan • Scan (only if scan has not completed) You cannot delete a scan template until you either delete the scheduled scan, assign a different template to the scheduled scan, or cancel the scan (if it is currently running or paused).
Application Version	Scan You cannot delete an application version until you delete the associated scans or move them to a different application version.
Custom Policy	• Scan • Scheduled scan You cannot delete a custom policy until you either delete the scan or the scheduled scan (or assign a different policy to the scheduled scan).

Adding or Editing an Alias

Sometimes, identical Web applications are deployed on different hosts. For example, during the development process, the same application may be deployed and tested on QA.testsite.com, Staging.testsite.com, and finally Production.testsite.com. This becomes problematic when performing a dynamic analysis scan because correlation uses the URL as a key component to match multiple vulnerabilities.

To overcome this problem, you can create an alias for those application versions by identifying all the equivalent URLs and hostnames for the Web application, which allows correlation to occur for all active and future scans.

When to Set Up Aliases

You should set up aliases before publishing. Otherwise, if conflicts occur, you may lose the vulnerability history because the correlation IDs may change. If you add or edit aliases after a scan has been published for that application version, you will be prompted to recalculate.

Note: Correlation is a mathematical calculation that uses a variety of values to determine if the vulnerability is really a duplicate of another vulnerability. You should recalculate whenever you change an alias.

Creating an Alias

To create an alias:

1. Select **Applications** from the navigation pane.
2. In the Application Version column, click the name of the application version for which you want to create an alias.
3. On the Application Version Details form, click the **Aliases** tab.
4. Click **Add**.
5. On the Add New Alias dialog box, in the **Primary URL** field, enter the alias URL (the umbrella under which other scans will be associated). Using the previous example, you might enter http://Production.testsite.com. Be sure to include the protocol (for example, http://).
6. If the server differentiates between URLs based on case sensitivity, select **Case Sensitive URL**.
7. Enter a description of the URL.
8. Click **Add**.
9. In the **Equivalent URLs** field, enter the URL of a host that will be covered by this alias. Using the previous example, you might enter http://QA.testsite.com.
10. To add other URLs, repeat steps 8-9.
11. When finished, click **Save**.
12. When notified that the alias was saved successfully, click **OK**.

The primary URL is listed on the form.

Working with the Macro Repository

You can create login macros that are reusable at different locations and among different security groups across your enterprise. Login macros are added and maintained at the Application Version level, and are stored in a macro repository.

Adding a New Macro

You add a login macro to the repository by uploading it.

> **Important!** The macro repository is intended for login macros only. You cannot upload a workflow macro to the macro repository.

To add a new login macro:

1. On the Application Version Details page, select the **Login Macros** tab.
2. Click **Add**.

   The Add New Macro window appears.
3. Type a **Macro Name** for the login macro.
4. Click **Browse** and select the login macro to be added.

5. Click **Open**.

   The new macro is added to the list of available login macros.

6. Click **OK**.

Downloading a Macro

To update an existing login macro in the repository, you can download the macro to your desktop, open it in the Web Macro Recorder, and record the changes. Afterward, use the Edit button to browse and upload the modified version.

To download an existing login macro:

1. On the Application Version Details page, select the **Login Macros** tab.

   A list of available login macros appears.

2. Click the drop-down menu next to the **Macro Name** and select **Download**.

   The Opening macro window appears.

3. Click **Save File** and **OK**.
4. Navigate to your desktop and save the file there.

After recording changes in the Web Macro Recorder, follow the procedure to update the login macro with the new version described in "Updating a Macro" below.

Updating a Macro

After revising a login macro, you can update the macro in the repository with the new version. The revised login macro will be updated in Scheduled Scans and Scan Templates where the macro is used.

> **Caution!** The macro repository does not maintain multiple versions of a login macro. Updating a login macro will overwrite and replace the existing macro.

To update the login macro:

1. On the Application Version Details page, select the **Login Macros** tab.

   A list of available login macros appears.

2. Click the drop-down menu next to the **Macro Name** and select **Edit**.

   The Edit Macro window appears.

3. Click **Update**.
4. Click **Browse** and select the revised login macro to be uploaded.
5. Click **Save**.

Deleting a Macro

To delete a login macro from the repository:

1. On the Application Version Details page, select the **Login Macros** tab.
   A list of available login macros appears.
2. Do one of the following:
   - Select one or more macros in the list and click **Delete**.
   - Click the drop-down menu next to the **Macro Name** and select **Delete**.

Using Repository Macros in Scans

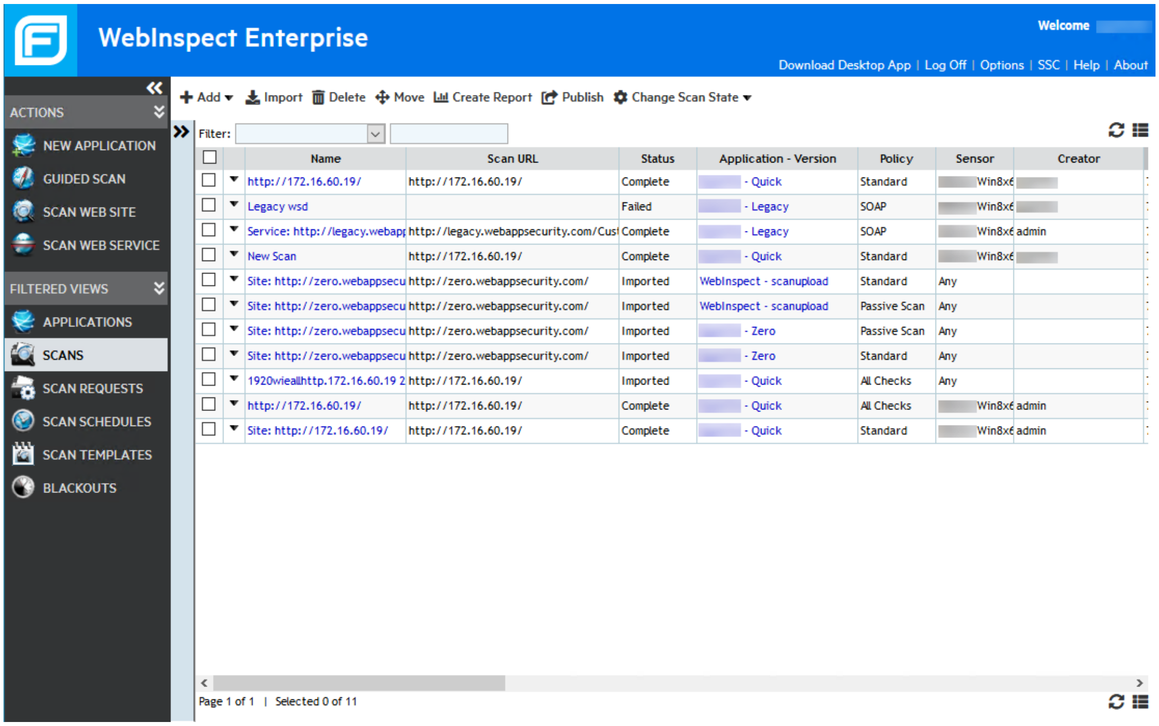
Login macros are added and maintained at the Application Version level and are available for use only within the Application Version for which it was added. Repository login macros are not available when using a global template.

Working with Scans

This section describes how to review the scan list, scan results, and scan dashboard, and how to add pages, directories, and variations. It also describes how to compare scans and publish to Fortify Software Security Center.

Reviewing the Scan List

The following is an example of the Scans form. In the Web Console, the user has selected **Filtered Views > Scans** in the left pane.



□		Name	Scan URL	Status	Application - Version	Policy	Sensor	Creator
□	▼	http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	[redacted]
□	▼	Legacy wsd		Failed	[redacted] - Legacy	SOAP	[redacted] Win8x6	[redacted]
□	▼	Service: http://legacy.webapp	http://legacy.webappsecurity.com/Cust	Complete	[redacted] - Legacy	SOAP	[redacted] Win8x6	admin
□	▼	New Scan	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	[redacted]
□	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	WebInspect - scanupload	Standard	Any	
□	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	WebInspect - scanupload	Passive Scan	Any	
□	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	[redacted] - Zero	Passive Scan	Any	
□	▼	Site: http://zero.webappsecu	http://zero.webappsecurity.com/	Imported	[redacted] - Zero	Standard	Any	
□	▼	1920wieallhttp.172.16.60.19 2	http://172.16.60.19/	Imported	[redacted] - Quick	All Checks	Any	
□	▼	http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	All Checks	[redacted] Win8x6	admin
□	▼	Site: http://172.16.60.19/	http://172.16.60.19/	Complete	[redacted] - Quick	Standard	[redacted] Win8x6	admin

Page 1 of 1 | Selected 0 of 11

Scans Form Columns

Each scan in the OpenText Fortify WebInspect Enterprise database is listed in the Scans form. The table displays (by default) the following columns:

- **Name** - The name assigned to the scan.
- **Scan URL** - Target Web site URL or IP address.
- **Status** - Current state of the scan (imported, complete, etc.).
- **Application Version** - Application version to which this scan is assigned. Click this field to open the associated Application Version Details form.
- **Policy** - The policy used for the scan.
- **Sensor** - The sensor that conducted the scan.
- **Creator** - User name of the person who initiated the scan.
- **Created** - Date and time the scan object was created or imported.
- **Started** - Date and time the scan started.
- **Completed** - Date and time the scan finished.
- **App Type** - Application type.
- **App Version** - Application version number.
- **Scan Request?** - If a check mark appears in this column, the scan was requested by OpenText Fortify Software Security Center (SSC).

> **Note:** This column is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **Results?** - If a check mark appears in this column, the number of vulnerabilities detected appears in columns sorted by severity.
- **Priority** - A relative value assigned to the scan; it is used to determine precedence if a sensor scheduling conflict occurs.
- **Vulnerabilities** (in columns sorted by severity) - Number of vulnerabilities detected.
- **WebInspect Agent Detected** - Indicator (Yes/No) whether OpenText Fortify WebInspect Agent was detected during the scan. For certain checks (such as SQL injection, command execution, and cross-site scripting), Fortify WebInspect Agent intercepts Fortify WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, Fortify WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.
- **Publish Status** - Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC.

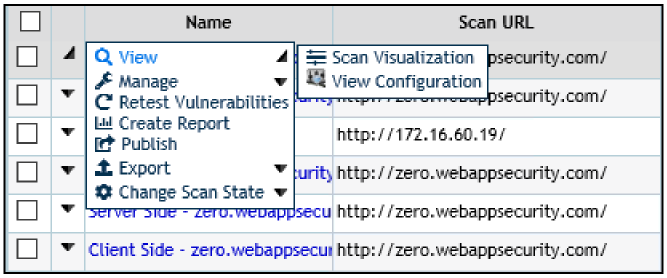
  > **Note:** This column is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **Publish Date** - The date on which the scan data was published to Fortify Software Security Center.

  > **Note:** This column is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

Available Functions

You can perform additional functions by clicking the drop-down arrow next to a scan name. In the following example, the user clicked the arrow for the second scan in the list, and slid the cursor to the right to see the suboptions for **View**.



□		Name	Scan URL
□	▲		psecurity.com/
□	▼		psecurity.com/
□	▼		http://172.16.60.19/
□	▼	urity	http://zero.webappsecurity.com/
□	▼	Server Side - zero.webappsecu	http://zero.webappsecurity.com/
□	▼	Client Side - zero.webappsecu	http://zero.webappsecurity.com/

The options are:

- **View**
  - **Scan Visualization** - Open the Scan Visualization window, allowing you to examine the scan results. You can also click a scan name to open the Scan Visualization window. See "Reviewing Scan Results" on page 182.
  - **View Configuration** - View (but not edit) the settings used for the selected scan.

- **Manage**
  - **Repeat Scan** - Rescan the target site using the same settings as the original scan.
  - **Copy** - Copy all settings that were used for this scan and pastes them into the Configure Scan window, allowing you to edit the settings before initiating the scan.
  - **Copy to Schedule** - Copy all settings that were used for this scan and pastes them into the Configure Scheduled Scan window, allowing you to edit the settings before scheduling the scan.
  - **Create Template from the Scan** - Create a scan template containing the settings that were used to produce this scan.
  - **Rename** - Assign a different name to the scan.
  - **Move** - Assign the scan to a different application version.
  - **Delete** - Delete the scan.
- **Retest Vulnerabilities** - Conduct a scan that examines only those portions of the target site in which vulnerabilities were detected during the original scan. Fortify WebInspect Enterprise does not conduct a new crawl of the site, but simply retraces the path of vulnerable sessions (as recorded in the original scan) and attacks the resources using the same checks previously employed. The default name of the scan is "Site Retest - <original scan name>"; for example, the retest of a site that originally resulted in a scan named MySite would produce a scan named Site Retest - MySite. However, you can specify a different name when launching the scan. For more information, see "Reviewing Vulnerabilities" on page 209.
- **Create Report** - Create a report for the scan. For more information, see the description of the **Create Report** icon below.
- **Publish** - Send scan data to Fortify Software Security Center. See "Publishing Scans to Fortify Software Security Center" on page 207.

  Note: This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **Export** - Export the selected scan as one of the following:
  - WebInspect Format (`.scan` file)
  - FPR (`.fpr` file)

    Note: After exporting to the .fpr format, you must manually upload the .fpr file to Fortify Software Security Center (if applicable). OpenText does not support uploading both Fortify WebInspect FPR artifacts and Fortify WebInspect Enterprise FPR artifacts to the same application version in Fortify Software Security Center.

  - XML
  - WAF (`.xml` file that can be imported as Web Application Firewall protection rules)
  - Scan settings file (`.xml` file)

> **Note:** When attempting to export scans using Internet Explorer, errors will result if the Internet option "Do not save encrypted pages to disk" is selected.

- **Change Scan State** - Start, stop, resume, or suspend the scan.

You can also perform additional functions using the icons at the top of the form, as described in the following table.

Icon	Function
Add	Start a new Guided Scan, Web site scan, or Web service scan. You can use this as an alternative to selecting **Guided Scan**, **Scan Web Site**, or **Scan Web Service** in the Actions section of the navigation pane.
Import	Import a scan. This feature opens the Upload Scan utility of the WebInspect Enterprise Desktop Application, which enables you to consolidate scans from Fortify WebInspect and Fortify WebInspect Enterprise and upload them to an application version. Scans can also be uploaded through the Scan Uploader service provided by the Fortify WebInspect Enterprise Services Manager. If you scan a Web site with Fortify WebInspect, you can copy the results to a location called a “dropbox.” The Scan Uploader service (which is separate from the Upload Scan utility) can access each dropbox periodically and, if files exist, it uploads those files to the Fortify WebInspect Enterprise Manager. You can configure this feature through the Fortify WebInspect Enterprise Services Configuration utility. Initial configuration is performed as part of product installation; for more information, see the *OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide*.
Delete	Delete selected scans or delete multiple scans by date range. To delete selected scans: 1. Select the check box for one or more scans in the scans list. 2. Click **Delete > Delete Selected Scans**. To delete scans by date range. 1. Click **Delete > Delete Scans**. The Delete Scans dialog box opens. 2. In the **Select scans** list, select the type of date range to use. Options are: • **Creation Date** – use the date and time the scan was created

Icon	Function
	- **Start Date** – use the date and time the scan started - **End Date** – use the date and time the scan ended 3. In the **From Date** box, type the beginning date and time of the range. **Tip:** Click the calendar and clock icons (📅🕒) to select dates and times. 4. In the **To Date** box, type the ending date and time of the range. **Tip:** Click the calendar and clock icons (📅🕒) to select dates and times. 5. Click **OK**.
Move	Use the check boxes to select scans and assign those scans to a different application version.
Create Report	Select a check box for one scan and create a report for that scan. The WebInspect Enterprise Desktop Application provides support for reporting. For more information, see "About the WebInspect Enterprise Desktop Application" on page 119. For detailed information about creating a report, see the Guided Scan and Reporting Help.
Publish	Use the check boxes to select scans and send their scan data to Fortify Software Security Center. See "Publishing Scans to Fortify Software Security Center" on page 207. **Note:** This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.
Change Scan State	Use the check boxes to select scans and select one of the following: - Start the scans. - Stop the scans (if running). - Resume the scans (if suspended). - Suspend the scans (if running). - Repeat the scans.

You can also use the icons illustrated below.

Icon	Function
🔄	Repopulate the form.
☰	Change the number of rows on the page, modify column widths, specify which columns are displayed, sort grid data, and arrange listed items into groups. See "Configuring Form Layouts" on page 121.

Searching On This Page

You can use global search to search on any column that is available on this page. For example, you can type in a portion of a URL, application name, or application version to find the specific application you are searching for.

Data Types

The column data types are:

- Text
- Date
- Number

Searching Text

If you are searching on a column that contains text, you can type in the exact name you are searching for. If what you are searching for includes embedded spaces, such as "Offshore QA Org", you can include those spaces in your search string. If you do not know the exact name, you can perform a wildcard search. Wildcard searches are entered as follows:

- *searchstring = ends with the text you are searching for
- searchstring* = begins with the text you are searching for
- *searchstring* = contains the text you are searching for

Searching Numbers and Dates

If you are searching on a number or a date, global search will attempt to parse the input into the value type. If global search can successfully parse the value, it will search on the value. You can also use "greater than" or "less than" searches. These searches are entered as follows:

- > 5 (search for values greater than 5)
- < 5 (search for values less than 5)

If you search on a date (i.e. 12/14/2015), global search will search for anything that occurred that day. If you search on an hour (i.e. 12/14/2015 11:00 PM), global search will search everything in that hour.

Searching for Time Spans

When searching for time spans, such as in the Duration column for Blackouts, the format is:
d.hh.mm
where
d = the number of days
hh = the number of hours
mm = the number of minutes

So for a 4 hour duration, the span is displayed as “0.04:00”. Use a similar format to search for time spans.

Searching Boolean Data and Check Boxes

If you search on a boolean data column or a check box column, enter “True” or “False” into the search box to filter on them. For a check box, "True" means that the check box is selected.

To perform a global search:

1. In the **Filter** list, select the column of data to search on.
2. In the text box next to the Filter list, type the search criteria.
3. Press **Enter** or click the refresh button.

   The table displays all records that meet the search criteria.

To clear the filter:

1. Clear the **Filter** list or the search criteria.
2. Press **Enter** or click the refresh button.

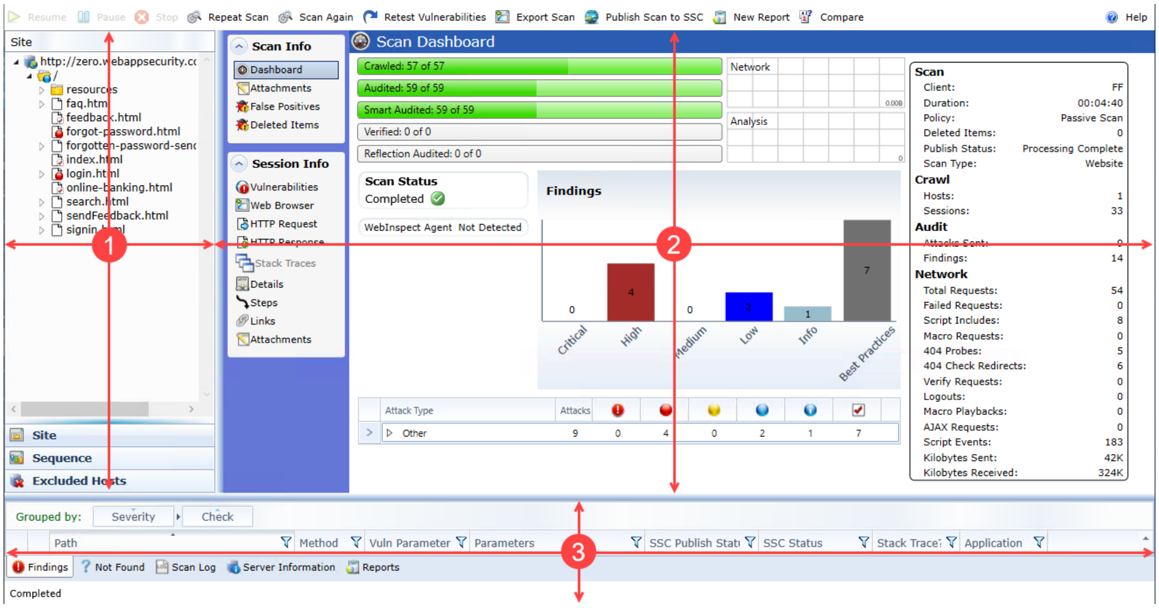
   The table displays all records.

Reviewing Scan Results

The Scan Visualization window emulates the OpenText Fortify WebInspect graphical presentation of scan results. To open this window:

- In the OpenText Fortify WebInspect Enterprise Web Console, select the **Scans** shortcut from the **Filtered Views** group and click the name of a scan (or click the drop-down arrow for the scan and select **View > Scan Visualization**).

The work area of the scan visualization is shown in the following screen capture:



Crawled: 57 of 57
Audited: 59 of 59
Smart Audited: 59 of 59
Verified: 0 of 0
Reflection Audited: 0 of 0

Scan Status
Completed

WebInspect Agent Not Detected

Attack Type	Attacks	!	●	●	●	i	✓
Other	9	0	4	0	2	1	7

Scan	
Client:	FF
Duration:	00:04:40
Policy:	Passive Scan
Deleted Items:	0
Publish Status:	Processing Complete
Scan Type:	Website
Crawl	
Hosts:	1
Sessions:	33
Audit	
Attacks Sent:	0
Findings:	14
Network	
Total Requests:	54
Failed Requests:	0
Script Includes:	8
Macro Requests:	0
404 Probes:	5
404 Check Redirects:	6
Verify Requests:	0
Logouts:	0
Macro Playbacks:	0
AJAX Requests:	0
Script Events:	183
Kilobytes Sent:	42K
Kilobytes Received:	324K

The scan visualization is divided into the following three regions:

1 Navigation Pane

2 Information Pane

3 Summary Pane

Navigation Pane

The navigation pane on the left side of the scan visualization includes the **Site**, **Sequence**, and **Excluded Hosts** buttons, which determine the contents (or "view") presented in the navigation pane.

- **Site view** - Fortify WebInspect Enterprise displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site, plus those sessions in which a vulnerability was discovered. During the crawl of the site, Fortify WebInspect selects the check box next to each session (by default) to indicate that the session will also be audited. When conducting a sequential crawl and audit (where the site is completely crawled before being audited), you can exclude a session from the audit by clearing its associated check box before the audit begins.
- **Sequence view** - Fortify WebInspect Enterprise displays server resources in the order they were encountered during a scan. You can specify a filter to limit which resources are displayed.
- **Excluded Hosts view** - Fortify WebInspect Enterprise displays a list of all disallowed hosts. These are hosts that may be referenced anywhere within the target site, but cannot be scanned because they are not specified in the Allowed Hosts setting (see "Legacy Scan Settings: Allowed Hosts" on page 231). To the right of the **Host** heading, you can click the filter icon to open a filter that enables you to choose a variety of conditions that must be met in order for an excluded host listed after filtering. The available conditions include the full set of current values, and you can also specify logical expressions regarding the values.

Note: In both Site view and Sequence view, blue text denotes a directory or file that was identified by Fortify WebInspect, rather than a resource that was discovered through a link. For example, Fortify WebInspect always submits the request “GET /backup/ HTTP/1.1” in an attempt to discover if the target Web site contains a directory named “backup.”

Navigation Pane Icons

Use the following table to identify resources displayed in the Sequence and Site views.

Icon	Definition
🌐	Server/host: Represents the top level of your site's tree structure.
📁	Blue folder: A private folder discovered not by crawling, but by attacks that often reveal vulnerabilities.
📁	Yellow folder: A folder whose contents are available over your Web site.
📁	Gray folder: A folder indicating the discovery of an item via path truncation. Once the parent is found, the folder will display in either blue or yellow, depending on its properties.
📄	File.
📃	Query or post.
📜	Document Object Model (DOM) event.

Vulnerability Icons

Icons superimposed on a folder or file indicate a discovered vulnerability.

Icon	Definition
📁❗	A red dot with an exclamation point indicates the object contains a critical vulnerability. An attacker might have the ability to execute commands on the server or retrieve and modify private information.
📁🔴	A red dot indicates the object contains a high vulnerability—generally, the ability to view source code, files out of the Web root, and sensitive error messages.
📄🟡	A gold dot indicates the object contains a medium vulnerability. These are generally non-HTML errors or issues that could be sensitive.

Icon	Definition
●	A blue dot indicates the object contains a low vulnerability. These are generally interesting issues, or issues that could potentially become higher ones.
i	An "i" in a blue circle indicates an informational item. These are interesting points in the site, or certain applications or Web servers.
✓	A red check mark indicates a "best practice" violation.

Each object represents a session, which is a matched set comprising the HTTP request sent by Fortify WebInspect to test for vulnerabilities and the HTTP response from the server.

Navigation Pane Shortcut Menu

If you right-click an item in the navigation pane while using the Site view or Sequence view (except as stated below), a shortcut menu presents the following options:

- **Expand Children** - (Site view only) Expands branching nodes in the site tree.
- **Collapse Children** - (Site view only) Contracts branching nodes into the superior node.
- **Copy URL** - Copies the URL of the selected session to the Windows clipboard (the same as selecting **Edit > Copy URL**).
- **View in Browser** - Displays the server's HTTP response in a browser.
- **Add** - Enables you to add a page, directory, or vulnerability discovered by means other than a scan (manual inspection, other tools, etc) for information purposes. You can then add any discovered vulnerabilities to those locations so that a more complete picture of the site is archived for analysis.

  - **Page** - A distinct URL (resource).
  - **Directory** - A folder containing a collection of pages.

    Choosing either **Page** or **Directory** opens a dialog box that enables you to name the page or directory and edit the HTTP request and response.

  - **Variation** - A subnode of a location that lists particular attributes for that location. For example, the login.asp location might have the variation:

    “(Query) Username=12345&Password=12345&Action=Login”

    Variations, like any other location, can have vulnerabilities attached to them, as well as subnodes.

    Choosing **Variation** opens the Add Variation dialog box, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.

  - **Vulnerability** - A specific security threat. Choosing **Vulnerability** invokes the Edit Vulnerabilities dialog box, allowing you to edit the various attributes, specify Post or Query, and edit the HTTP request and response.

- **Remove Location** - Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities.

  Note: You can recover removed locations (sessions) and their associated vulnerabilities. See "Recovering Deleted Items" on page 213 for details.
- **Edit Vulnerability** - Enables you to add an existing or custom vulnerability to the session, or change the Summary, Implication, Execution, Fix, and Reference Info descriptions associated with the vulnerability.
- **Review Vulnerability** - Enables you to retest the vulnerability or mark it as "ignored" or "false positive." See "Reviewing Vulnerabilities" on page 209.
- **Mark as False Positive** - Flags the vulnerability as a false positive and enables you to add a note.
- **Attachments** - Enables you to create a note or screenshot associated with the selected vulnerability.

  > **Note:** If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, notes longer than 2000 characters will be truncated when sent to Fortify Software Security Center.

Information Pane

When conducting or viewing a scan, the information pane contains one or two collapsible information panels (Scan Info and Session Info) and an information display area.

Scan Info Panel

This panel contains the following selections:

- **Dashboard** - The Dashboard displays a real-time summary of the scan results and a graphic representation of the scan progress. See "Reviewing the Scan Dashboard" on page 194 for additional information.
- **Attachments** - This feature lists all the notes and screenshots that are associated with all the objects in the scan. Attachments are added in the Session Info panel for individual objects, as described in the Session Info Panel section below.

  You can click the filter icon at the right of any column heading to open a filter that enables you to choose a variety of conditions regarding that column that must be met in order for an attachment (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column.
- **Traffic Monitor** - This feature enables you to display and review every HTTP request sent by Fortify WebInspect and the associated HTTP response received from the web server. This information comes from the traffic session file, which is stored in the database on the Fortify WebInspect Enterprise server along with the accompanying scan file. When you click the **Traffic Monitor** button, the traffic session file is downloaded to the program data folder on your local machine. The Traffic Viewer tool opens with the traffic session file in view.

  This feature is available only if:

  - Traffic Monitor Logging was enabled prior to conducting the scan
  - The scan Status is "Aborted" or "Complete"

For scans that were conducted in a standalone Fortify WebInspect and include a traffic session file, you can view the traffic sessions after the scan is uploaded to Fortify WebInspect Enterprise. When such a scan is opened in Fortify WebInspect Enterprise, the **Traffic Monitor** button appears automatically in the Scan Info panel.

For more information about enabling Traffic Monitor Logging, see "Configuring a Web Site Scan" on page 125 in this document and the Guided Scan and Reporting Help.

> **Note:** Traffic Monitor Logging cannot be enabled for Scheduled Scans.

For more information about the Traffic Viewer tool, refer to the Traffic Viewer tool online help or the *OpenText™ Fortify WebInspect Tools Guide*.

- **False Positives** - This feature lists all URLs that Fortify WebInspect Enterprise originally flagged as containing a vulnerability, but which a user later determined were false positives.

  You can click the filter icon at the right of any column heading to open a filter that enables you to choose a variety of conditions regarding that column that must be met in order for a false positive (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column.

  You can mark a selected false positive as a vulnerability, thereby removing it from the list of false positives, or you can edit its description.

  You can select one or more column headers and drag them above the table to organize the entries in the desired hierarchy.

- **Deleted Items** - Lists either deleted sessions or deleted vulnerabilities, depending on your selection. To recover a deleted item, select a session or vulnerability and click **Recover**.

  You can click the filter icon at the right of any column heading to open a filter that enables you to choose a variety of conditions regarding that column that must be met in order for a session or vulnerability (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column.

  You can select one or more column headers and drag them above the table to organize the entries in the desired hierarchy.

Note: To delete a session, right-click a session in the navigation pane or an item in the summary pane and select **Remove Location** from the shortcut menu.

To delete a vulnerability, do one of the following:

- Right-click an item on the **Findings** tab in the summary pane and select **Mark As Ignored** from the shortcut menu.
- Right-click a vulnerable session in the navigation pane, select **Edit Vulnerabilities** from the shortcut menu, and (on the Edit Vulnerabilities dialog box) click **Delete**.
- Right-click an item on any tab in the summary pane except **Scan Log** or **Reports**, select **Edit Vulnerability** from the shortcut menu, and (on the Edit Vulnerabilities dialog box) click **Delete**.

Session Info Panel

Fortify WebInspect Enterprise lists each session created during a scan in the navigation pane using either the Site view or Sequence view. Select a session and then click one of the options in the Session Info panel to display related information about that session. Some options appear only for specific types of scans as noted. Also, options are enabled only if they are relevant to the selected session. The available options are:

- **Vulnerabilities** - Displays the vulnerability information for the session selected in the navigation pane.
- **Web Browser** - (Web Site Scan or Guided Scan only; not available for Web Service Scan.) Displays the server's response as rendered by a Web browser for the session selected in the navigation pane. For Web Site scans only; not available for Web Service scans.
- **HTTP Request** - Displays the raw HTTP request sent by Fortify WebInspect to the server hosting the site you are scanning.
- **HTTP Response** - Displays the server's raw HTTP response to Fortify WebInspect's request. If you select a Flash (.swf) file, Fortify WebInspect displays HTML instead of binary data. This allows Fortify WebInspect Enterprise to display links in a readable format.
- **Stack Traces** - Displays stack traces provided for certain checks by OpenText Fortify WebInspect Agent, if Fortify WebInspect Agent is detected to be available. For certain checks (such as SQL injection, command execution, and cross-site scripting), Fortify WebInspect Agent intercepts Fortify WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, Fortify WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.
- **Details** - (Web Site Scan or Guided Scan only; not available for Web Service Scan.) Displays request and response details, such as the size of the response and the request method, for the session selected in the navigation pane. Note that the Response section contains two entries for content type: returned and detected. The **Returned Content Type** indicates the media type specified in the Content-Type entity-header field of the HTTP response. The **Detected Content Type** indicates the actual content-type as determined by Fortify WebInspect.
- **Steps** - (Web Site Scan or Guided Scan only; not available for Web Service Scan.) Displays the route taken by Fortify WebInspect to arrive at the session selected in the navigation pane or the URL selected in the summary pane. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.
- **Links** - (Web Site Scan or Guided Scan only; not available for Web Service Scan.) Displays (under Linked From) all resources at the target site that contain links to the selected resource. The links may be rendered by HTML tags, scripts, or HTML forms. It also lists (under Linked To) all resources that are referenced by links within the HTTP response for the selected session.
- **Attachments** - Displays all notes and screenshots associated with the selected session in the navigation pane (Site or Sequence view). If the selected session includes rolled up vulnerabilities, a note in the Comments area details the URLs that were rolled up and affected by the same vulnerability. For more information, see "About Vulnerability Rollup" on page 214.

  You can click the filter icon at the right of any column heading to open a filter that enables you to choose a variety of conditions regarding that column that must be met in order for an attachment (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column.

Icons allow you to add a note or screenshot as an attachment to the selected vulnerability, or to edit, view, or delete the selected attachment.

> **Note:** If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, notes longer than 2000 characters will be truncated when sent to Fortify Software Security Center.

To add an attachment to a session, do one of the following:

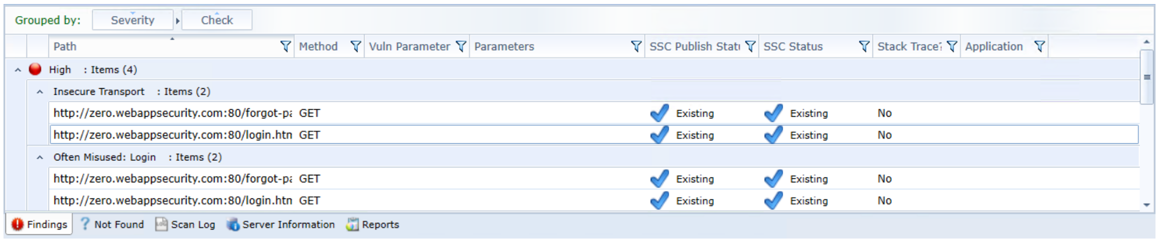
- Right-click a session (Web Site Scan or Guided Scan) or an operation or vulnerability (Web Service Scan) in the navigation pane and select **Attachments** from the shortcut menu.
- Right-click an item on the **Findings** tab of the summary pane and select **Attachments** from the shortcut menu.
- Select a session (Web Site Scan or Guided Scan) or an operation or vulnerability (Web Service Scan) in the navigation pane, then select **Attachments** from the Session Info panel and click the **Add** icon (in the information pane).

Scan Dashboard

For information about the contents of the Scan Dashboard, see "Reviewing the Scan Dashboard" on page 194.

Summary Pane

When conducting or viewing a scan, the horizontal Summary pane at the bottom of the window provides a centralized table of vulnerable resources and enables you to quickly access vulnerability information. You can click and drag the horizontal divider above the table to show or hide more of the Summary pane.



Grouped by: Severity ▸ Check

Path	Method	Vuln Parameter	Parameters	SSC Publish Stati	SSC Status	Stack Trace:	Application
● High : Items (4)							
Insecure Transport : Items (2)							
http://zero.webappsecurity.com:80/forgot-pa	GET			✓ Existing	✓ Existing	No	
http://zero.webappsecurity.com:80/login.htn	GET			✓ Existing	✓ Existing	No	
Often Misused: Login : Items (2)							
http://zero.webappsecurity.com:80/forgot-pa	GET			✓ Existing	✓ Existing	No	
http://zero.webappsecurity.com:80/login.htn	GET			✓ Existing	✓ Existing	No	

The table in the Summary pane has a set of default columns. To add or delete columns, right-click the column header bar and select or deselect the desired columns. Except as noted, the available columns are:

- **Link**: Whether the information applies to Scan A, to Scan B, or to both Scans A and B.
- **Severity**: (Available for **Findings** and **Not Found** tabs) A relative assessment of the vulnerability, ranging from low to critical. A table of associated severity icons is shown earlier in this topic.
- **Check**: A Fortify WebInspect probe for a specific vulnerability, such as cross-site scripting, unencrypted log-in form, etc.
- **Path**: The hierarchical path to the resource.

- **Method**: HTTP method, such as GET, PUT, etc.
- **Vuln Parameter**: The name of the vulnerable parameter.
- **Parameters**: Names of parameters and values assigned to them.
- **Reproducible**: Valid values are Reproduced, Not Found/Fixed, or New. Column is available for Site Retests only (Retest Vulnerabilities).
- **SSC Publish Status**: The status as it exists in Fortify Software Security Center (SSC), if previously published.

  Note: This column is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **SSC Status**: Expected status of the vulnerability when the scan is published to Fortify Software Security Center.

  Note: This column is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **Stack Trace?**: Stack trace information obtained from Fortify WebInspect Agent.
- **CWE IDs**: The Common Weakness Enumeration identifier(s) associated with the vulnerability.
- **Kingdom**: The category in which this vulnerability is classified, using a taxonomy of software security errors developed by the OpenText Fortify Software Security Research Group.
- **Application**: The application or framework in which the vulnerability is found, such as ASP.NET or Microsoft IIS server.
- **Response Length**: The response size in bytes for the vulnerable session.

You can click any column heading to sort the entries by that column.

You can group the data in a hierarchy by selecting column headings and dragging them to the area immediately above the column headings. For example, you can click and drag the **Severity** column heading and then click and drag the **Check** column heading to group by Severity, then by type of Check. Then, the table is organized by those hierarchical groupings, which no longer appear as columns in the table. By default, the **Findings** and **Not Found** tabs are organized by Severity and then by Check.

You can click the filter icon at the right of any column heading to open a filter that enables you to choose a variety of conditions regarding that column that must be met in order for an item (row) to remain listed in the table after filtering. The available conditions include the full set of current values in the column, and you can also specify logical expressions regarding the content of that column. For example, in the filter for the **Vuln Parameter** column, suppose you:

1. Leave the top set of check boxes as is.
2. Below the **Show rows with value that** text, select **Contains** from the drop-down menu.
3. Type **Id** in the text box below the drop-down menu.
4. Click **Filter**.

Then the table will show only rows that contain the text "Id" in the **Vuln Parameter** column. This would include rows for which the value of **Vuln Parameter** is **accountId** or **payeeId** or any other entry that includes "Id."

You can specify filters for multiple columns, one column at a time, and all the filters will be applied.

If a filter for a column has been specified, its icon becomes a darker blue than the icons for unused filters.

To quickly clear a filter, click **Clear Filter** while the filter is open to be specified.

Summary Pane Tabs

The summary pane has the following tabs:

- Findings
- Not Found
- Scan Log
- Server Information
- Reports

More information about each of these tabs follows.

Findings Tab

The **Findings** tab lists information about each vulnerability discovered during an audit of your Web presence. The severity of vulnerabilities is indicated by the following icons.

Critical	High	Medium	Low
❗	🔴	🟡	🔵

With a session selected, you can also view associated information by selecting an option from the Session Info panel.

Right-clicking an item in the Summary pane displays a shortcut menu containing the following commands:

- **Copy URL** - Copies the URL to the Windows clipboard.
- **Copy Selected Item(s)** - Copies the text of selected items to the Windows clipboard.
- **Copy All Items** - Copies the text of all items to the Windows clipboard.
- **Export** - Creates a comma-separated values (`.csv`) file containing either all items or selected items and displays it in Microsoft Excel.
- **View in Browser** - Renders the HTTP response in a browser.
- **Change Severity** - Change the severity level.
- **Edit Vulnerability** - Display the Edit Vulnerabilities dialog box, allowing you to modify various vulnerability characteristics.

- **Rollup Vulnerabilities** - Available if multiple vulnerabilities are selected; enables you to roll up the selected vulnerabilities into a single instance that is prefixed with the tag “[Rollup]” in Fortify WebInspect Enterprise and reports. See "About Vulnerability Rollup" on page 214 for more information.

  Note: If you have selected a rolled up vulnerability, this menu option is **Unroll Vulnerabilities**.

- **Review Vulnerability** - Available if one vulnerability is selected; enables you to retest the vulnerability. If the vulnerability was detected in only one scan, the Retest Vulnerabilities window opens; if the vulnerability was detected in both scans, you are first prompted to select a scan. See "Reviewing Vulnerabilities" on page 209 for more information.

  Note: The **Mark As** and **Send To** buttons are not enabled on the Retest Vulnerabilities window.

- **Mark as** - Flag the vulnerability as a false positive or as ignored. In both cases, the vulnerability is removed from the list. To view a list of all false positives, click **False Positives** in the Scan Info panel. To view (and optionally recover) deleted sessions and vulnerabilities, click **Deleted Items** in the Scan Info panel.
- **Remove Location** - Delete from the navigation pane the session associated with the selected vulnerability and also delete any associated vulnerabilities. To view (and optionally recover) deleted sessions, click **Deleted Items** in the Scan Info panel.
- **Attachments** - Create a note or associate an image with the selected vulnerability.

  Note: If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, notes longer than 2000 characters will be truncated when sent to Fortify Software Security Center.

- **Update SSC Status** - Change the status of an issue to be submitted to Fortify Software Security Center. Statuses are: New, Existing, Reintroduced, Resolved, Still an Issue, and Not Found. The availability of a specific status is determined by the current status.

  Note: This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

Note: For Post and Query parameters, click an entry in the **Parameters** column to display a more readable synopsis of the parameters.

Not Found Tab

The **Not Found** tab lists vulnerabilities that were detected by a previous scan in this application version, but were not detected by the current scan. These vulnerabilities are not included in counts on the Dashboard and are not represented in the Site view or the Sequence view of the navigation pane.

Right-clicking an item in the list presents the same options described above for the shortcut menu for a vulnerability .

Scan Log Tab

Use the **Scan Log** tab to view information about activities that occurred during the scan. For instance, the time at which certain audit methodologies are applied against your Web presence are listed here.

Server Information Tab

The **Server Information** tab lists items of interest pertaining to the server. Only one occurrence of an item or event is listed per server.

Reports Tab

The **Reports** tab displays a list of reports that have been run or are running for the scan.

Buttons above the list of reports allow you to:

- Abort report generation for a report that has not been completed (that is, the **State** of the report is **Pending** or **Running**).
- Save a completed report to a location you specify.
- Delete a completed report.

One way to create a report is to click **New Report** in the toolbar, as described below.

Toolbar

Actions available from the toolbar at the top of the Scan Visualization window include the following:

- **Resume** - Continue a scan after you paused the process.
- **Pause** - Halt a scan. Click **Resume** to continue.
- **Stop** - Terminate the scan; it cannot be resumed.
- **Repeat Scan** - Rescan the target site using the same settings as the original scan.
- **Scan Again** - Display settings used for this scan, allowing you to modify them before initiating another scan.
- **Retest Vulnerabilities** - This type of scan examines only those portions of the target site in which vulnerabilities were detected during the original scan. Fortify WebInspect Enterprise does not conduct a new crawl of the site, but simply retraces the path of vulnerable sessions (as recorded in the original scan) and attacks the resources using the same checks previously employed. The default name of the scan is "Site Retest - <original scan name>"; for example, the retest of a site that originally resulted in a scan named MySite would produce a scan named Site Retest - MySite. However, you can specify a different name when launching the scan.

  > **Important!** Fortify does not recommend retesting vulnerabilities in scans created using earlier versions of Fortify WebInspect. While retesting scans from earlier versions may work in many instances, it is not always reliable because individual checks may not flag the same vulnerability during a retest. Failure of a check to flag the same vulnerability while retesting a scan from an earlier version of Fortify WebInspect may not mean the vulnerability has been remediated.

- **Export Scan** - Export the selected scan (or settings for the selected scan) to a destination you select.

  > **Important!** When exporting a scan in XML format to import as an artifact to Fortify Software Security Center, fewer findings than were in the original scan may be present in the imported file.

- **Publish Scan to SSC** - Send scan data to Fortify Software Security Center. For more information, see "Publishing Scans to Fortify Software Security Center" on page 207.

  > **Note:** This option is available only if Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.

- **New Report** - Create a new report from a scan you select and open. The reports available in Fortify WebInspect Enterprise are a subset of the reports available in Fortify WebInspect.

  The WebInspect Enterprise Desktop Application provides support for reporting. For more information, see "About the WebInspect Enterprise Desktop Application" on page 119.

  For detailed information about creating a report, see the Guided Scan and Reporting Help.

- **Compare** - Compare two scans. See "Comparing Scans" on page 200.

See Also

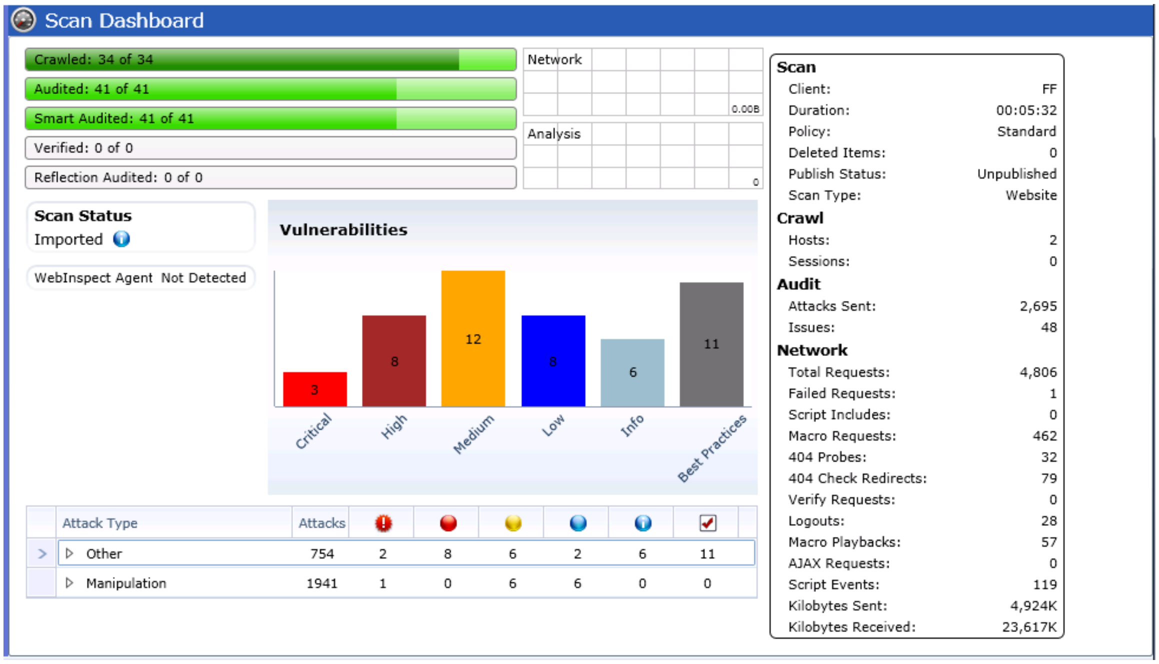
"Reviewing the Scan Dashboard" below

"Reviewing the Scan List" on page 175

Reviewing the Scan Dashboard

The Scan Dashboard is part of the scan visualization (see "Reviewing Scan Results" on page 182). It displays a real-time summary of the scan results and a graphic representation of the scan progress if the scan is under way. It can also display the results of a scan comparison (see "Comparing Scans" on page 200).

In the following example, the scan has been completed and imported.



Scan Dashboard

Crawled: 34 of 34
Audited: 41 of 41
Smart Audited: 41 of 41
Verified: 0 of 0
Reflection Audited: 0 of 0

Scan Status
Imported

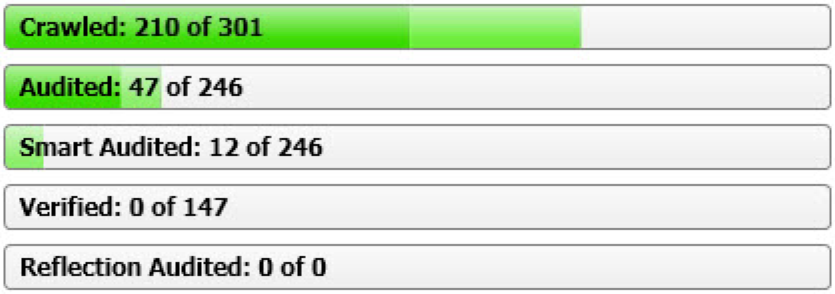
WebInspect Agent Not Detected

	Attack Type	Attacks	❗	●	●	●	ⓘ	☑
>	▷ Other	754	2	8	6	2	6	11
	▷ Manipulation	1941	1	0	6	6	0	0

Scan	
Client:	FF
Duration:	00:05:32
Policy:	Standard
Deleted Items:	0
Publish Status:	Unpublished
Scan Type:	Website
Crawl	
Hosts:	2
Sessions:	0
Audit	
Attacks Sent:	2,695
Issues:	48
Network	
Total Requests:	4,806
Failed Requests:	1
Script Includes:	0
Macro Requests:	462
404 Probes:	32
404 Check Redirects:	79
Verify Requests:	0
Logouts:	28
Macro Playbacks:	57
AJAX Requests:	0
Script Events:	119
Kilobytes Sent:	4,924K
Kilobytes Received:	23,617K

Progress Bars

Each bar represents the progress being made through that scanning phase. In the following example, the scan that includes these progress bars is under way:



Crawled: 210 of 301

Audited: 47 of 246

Smart Audited: 12 of 246

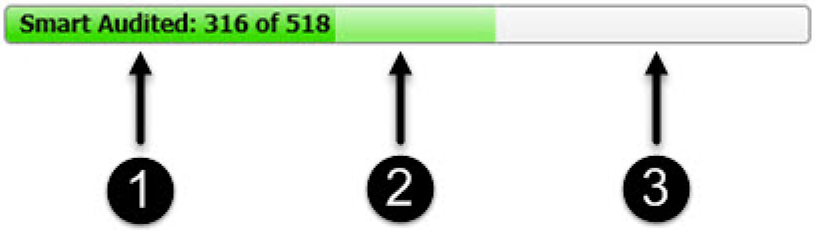
Verified: 0 of 147

Reflection Audited: 0 of 0

The following table describes the progress bars.

Progress Bar	Description
Crawled	Number of sessions crawled / total number of sessions to crawl.
Audited	Number of sessions audited / total number of sessions to audit. The total number includes all checks except those pertaining to server type, which are handled by smart audit.
Smart Audited	Number of sessions audited using smart audit / total number of sessions for smart audit. For smart audit, OpenText Fortify WebInspect detects the type of server on which the Web application is hosted. Fortify WebInspect runs checks that are specific to the server type and avoids checks that are not valid for the server type.
Verified	Number of persistent XSS vulnerable sessions verified / total number of persistent XSS vulnerable sessions to verify. When persistent XSS auditing is enabled, Fortify WebInspect sends a second request to all vulnerable sessions and examines all responses for probes that Fortify WebInspect previously made. When probes are located, Fortify WebInspect will record links between those pages internally.
Reflection Audited	Number of persistent XSS vulnerable linked sessions audited / total number of persistent XSS vulnerable linked sessions to audit. When persistent XSS auditing is enabled, this represents the work required for auditing the linked sessions found in the verification step for persistent XSS.

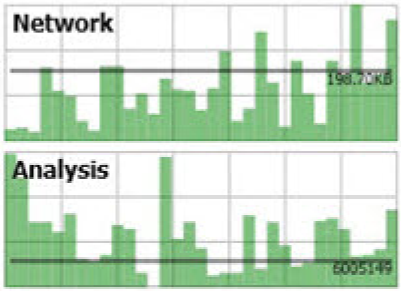
Progress Bar Colors



1. Dark green indicates sessions that have been processed.
2. Light green indicates excluded, aborted, or rejected sessions (sessions that were considered for processing, but were skipped due to settings or other reasons).
3. Light gray indicates the unprocessed sessions.

Activity Meters

Fortify WebInspect polls information about the activity occurring in the scan and displays the data in Activity Meters. The data presents a real-time snapshot of the scan activity. This information can help you to determine whether the scan is stalled or actively running.



The following table describes the Activity Meters.

Meter	Description
Network	The amount of data being sent and received by Fortify WebInspect. The chart shows this data as B, KB, or MB sent/received over the last one second.
Analysis	The amount of work being done per second by Fortify WebInspect in processing all threads.

Scan Status

The **Scan Status** field under the progress bars describes the status of the scan. The status is **Imported** in the example Scan Dashboard screenshot at the beginning of this topic.

Fortify WebInspect Agent Detected or Not Detected

Below the **Scan Status** field, the Scan Dashboard states either **WebInspect Agent Detected** or **WebInspect Agent Not Detected**. For certain checks (such as SQL injection, command execution, and cross-site scripting), OpenText Fortify WebInspect Agent intercepts Fortify WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, Fortify WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack trace to investigate areas that require remediation.

Vulnerabilities Graphics

The following table describes the vulnerabilities graphics.

Graphic	Description
Vulnerability Graph	A bar chart showing the total number of issues identified for the scan per severity level.
Attack Stats Grid	Number of attacks made and issues found, categorized by attack type and audit engine.

Statistics Panel - Scan Section

The following table describes the Scan Section of the Statistics Panel.

Item	Description
Client	The rendering engine or user agent specified for the scan. Options are: • IE (Internet Explorer) • FF (Firefox) • iPhone • iPad • Android • Windows Phone • Windows RT
Duration	Length of time scan has been running (can be incorrect if the scan terminates abnormally).
Policy	Name of the policy used for the scan. For a retest, the field contains a dash ("-"), because the retest does not use the entire policy; see "Reviewing Vulnerabilities" on page 209.

Item	Description
Deleted Items	The number of sessions and vulnerabilities removed by the user from the scan. To remove a session, right-click a session in the Navigation pane and select **Remove Location** from the shortcut menu. To remove a vulnerability, right-click a vulnerability in the Summary pane and select **Remove Location** from the shortcut menu. To restore a session or vulnerability that has been deleted, click **Deleted Items** in the Scan Info panel and select the session or vulnerability and click **Recover**. For more information, see "Reviewing Scan Results" on page 182.
Publish Status	The status of the scan in regard to the scan being published to OpenText Fortify Software Security Center. **Note:** This information is available only if OpenText Fortify WebInspect Enterprise is integrated with Fortify Software Security Center.
Scan Type	Type of scan: Website, Service, or Site Retest.

Statistics Panel - Crawl Section

The following table describes the Crawl Section of the Statistics Panel.

Item	Description
Hosts	Number of hosts included in the scan.
Sessions	Total number of sessions (excluding AJAX requests, script and script frame includes, and WSDL includes).

Statistics Panel - Audit Section

The following table describes the Audit Section of the Statistics Panel.

Item	Description
Attacks Sent	Total number of attacks sent.
Issues	Total number of issues found (all vulnerabilities, as well as best practices).

Statistics Panel - Network Section

The following table describes the Network Section of the Statistics Panel.

Item	Description
Total Requests	Total number of requests made.
Failed Requests	Total number of failed requests.
Script Includes	Total number of script includes.
Macro Requests	Total number of requests made as part of macro execution.
404 Probes	Number of file not found probes made to determine file not found status.
404 Check Redirects	Number of times a 404 probe resulted in a redirect.
Verify Requests	Requests made for detection of stored parameters.
Logouts	Number of times logout was detected and login macro executed.
Macro Playbacks	Number of times macros have been executed.
AJAX Requests	Total number of AJAX requests made.
Script Events	Total number of script events processed.
Kilobytes Sent	Total number of kilobytes sent.
Kilobytes Received	Total number of kilobytes received.

See Also

"Reviewing Scan Results" on page 182

Adding a Page or Directory

If you use manual inspection or other security analysis tools to detect resources that OpenText Fortify WebInspect did not discover, you can add these locations manually and assign a vulnerability to them. Incorporating the data into a Fortify WebInspect scan enables you to track vulnerabilities using Fortify WebInspect features.

Note: When creating additions to the data hierarchy, you must manually add resources in a logical sequence. For example, to create a subdirectory and page, you must create the subdirectory before creating the page.

To add a page of directory:

1. While reviewing the scan results, right-click an icon in the **Site View** in the **Navigation Pane** where you want to add the resource.
2. Select the type of resource you want to add from the context menu.

3. Replace the default **Name** of the page or directory with the name of the resource to be added.
4. If necessary, edit the HTTP **Request** and **Response**. Do not change the request path.
5. When finished, click **OK**.

Adding a Variation

If you use manual inspection or other security analysis tools to detect resources that OpenText Fortify WebInspect did not discover, you can add these locations manually and assign a vulnerability to them. Incorporating the data into a Fortify WebInspect scan enables you to track vulnerabilities using Fortify WebInspect features.

What is a Variation?

A variation is a subnode of a location that lists particular attributes for that location. For example, the login.asp location might have the variation:

```
(Post) uid=12345&Password=foo&Submit=Login
```

Variations, like any other location, can have vulnerabilities attached to them, as well as subnodes.

Procedure

To add a variation:

1. While reviewing the scan results, right-click an icon in the **Site View** in the **Navigation Pane** where you want to add the resource.
2. Select **Variation** from the context menu.
3. In the **Name** field, replace the default "attribute=value" with the actual parameters to be sent (for example, `uid=9999&Password=kungfoo&Submit=Login`).
4. Select either **Post** or **Query**.
5. If necessary, edit the HTTP **Request** and **Response**. Do not change the request path.
6. When finished, click **OK**.

Comparing Scans

You can compare the vulnerabilities revealed by two different scans of the same target and use this information to:

- Verify fixes: Compare vulnerabilities detected in the initial scan with those in a subsequent scan of a site in which the vulnerabilities were supposedly fixed.
- Check on scan health: Change scan settings and verify that those changes expand the attack surface.
- Find new vulnerabilities: Determine if new vulnerabilities have been introduced in an updated version of the site.

- Investigate Issues: Pursue anomalies such as false positives or missed vulnerabilities.
- Compare authorization access: Conduct scans using two different user accounts to discover vulnerabilities that are unique or common to both accounts.

Guidelines for Scan Comparison

Keep the following guidelines in mind when picking scans for comparison:

- Both of the scans to be compared (Scan A and Scan B) must be in the same application version. When you select the first scan, only other scans in the same application version are displayed for you to select as the second scan.
- You cannot conduct a comparison if either of the scans is currently running.
- Data from both scans must be stored in the same database type (SQL Server Express Edition or SQL Server Standard/Enterprise Edition).

Effect of Scheme, Host, and Port Differences on Scan Comparison

OpenText Fortify WebInspect does not ignore the scheme, host, and port when comparing scans from two duplicate sites that are hosted on different servers.

For example, the following site pairs would not be correlated in a scan comparison because of differences in scheme, host, or port:

Scheme

- Site A - http://zero.webappsecurity.com/
- Site B - https://zero.webappsecurity.com

Host

- Site A - http://dev.foo.com/index.html?par1=123&amp;par2=123
- Site B - http://qa.foo.com/index.html?par1=123&amp;par2=123

Port

- Site A - http://zero.webappsecurity.com:80/
- Site B - http://zero.webappsecurity.com:8080/

Selecting Scans to Compare

To compare two scans:

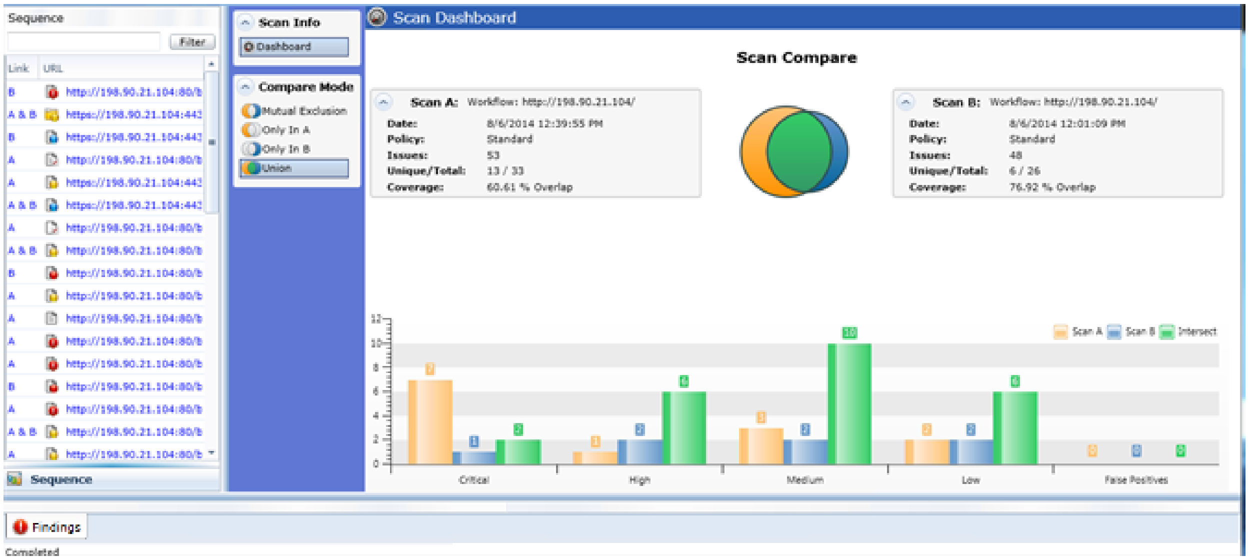
1. Select and open a scan from the Scans page. This scan will be Scan A in the comparison.
2. In the toolbar at the top of the Scan Visualization window, click **Compare**.
3. In the list of scans that appears, select a scan and click **OK**. This scan will be Scan B in the comparison.

   Both of the scans to be compared (Scan A and Scan B) must be in the same application version. When you select the first scan, only other scans in the same application version are displayed for you to select as the second scan.

A warning message appears if the selected scans have different start URLs, used different scan policies, or are of a different type (such as a Web Site Scan and a Web Service Scan). You can choose to continue, or you can terminate the comparison.

The scan comparison is generated and displayed.

Following is an example scan comparison.



Link	URL
B	http://198.90.21.104:80/b
A & B	https://198.90.21.104:443
B	https://198.90.21.104:443
A	http://198.90.21.104:80/b
A	https://198.90.21.104:443
A & B	https://198.90.21.104:443
A	http://198.90.21.104:80/b
A & B	http://198.90.21.104:80/b
B	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b
B	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b
A & B	http://198.90.21.104:80/b
A	http://198.90.21.104:80/b

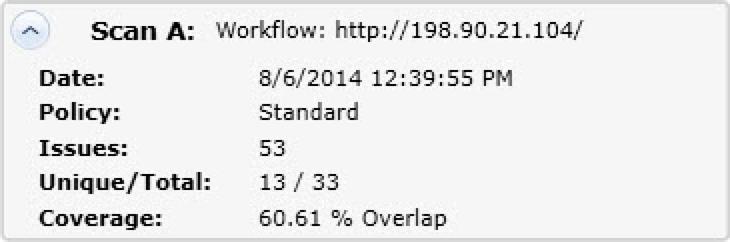
Scan A: Workflow: http://198.90.21.104/
Date: 8/6/2014 12:39:55 PM
Policy: Standard
Issues: 53
Unique/Total: 13 / 33
Coverage: 60.61 % Overlap

Scan B: Workflow: http://198.90.21.104/
Date: 8/6/2014 12:01:09 PM
Policy: Standard
Issues: 48
Unique/Total: 6 / 26
Coverage: 76.92 % Overlap

Reviewing the Scan Dashboard

The Scan Dashboard displays the scan comparison results.

Scan Descriptions



Scan A: Workflow: http://198.90.21.104/

Date:	8/6/2014 12:39:55 PM
Policy:	Standard
Issues:	53
Unique/Total:	13 / 33
Coverage:	60.61 % Overlap

The following information appears in boxes for Scan A and Scan B:

- **Scan A** or **Scan B**: Name of the scan.
- **Date**: Date and time the scan was conducted.
- **Policy**: Policy used for the scan; see "Policies List" on page 155 for more information.
- **Issues**: Total number of issues identified on the **Findings** tab.
- **Unique/Total**: Number of unique sessions created for this scan (that is, the number of sessions that appear in this scan and not the other scan), compared to the total number of sessions for this

scan .

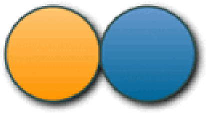
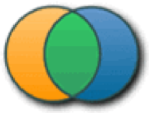
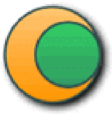
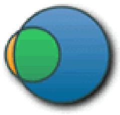
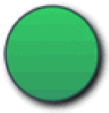
- **Coverage**: Percentage of sessions that are common to both scans.

Venn Diagram

The Venn diagram between the scan description boxes depicts the *session coverage* of Scan A (represented by a yellow circle) and the *session coverage* of Scan B (represented by a blue circle). The intersection of the two sets is represented by the green overlap. (In prior releases, the Venn diagram represented the overlap of vulnerabilities.)

The Venn diagram is scaled to reflect the actual relationship between the sets.

Several examples of session coverage overlap are illustrated below.

				
No Intersection	50% Intersection	A Encompasses B	Most of A Intersects B	Complete Intersection

Vulnerabilities Bar Chart

In separate groupings for each vulnerability severity and for False Positives, the bottom of the Scan Dashboard displays a set of bar charts that show the number of vulnerabilities found in Scan A, in Scan B, and in their intersection (**Intersect**). The same color coding is used as in the Venn diagram. These bar charts do not change based on the selected **Compare Mode**.

> **Note:** When comparing scans, Fortify WebInspect ignores the host and port. Consider two duplicate sites that are hosted on different servers. One site that is under development might be hosted at `http://dev.mysite.com` while that same site might be undergoing testing at `http://QA.mysite.com`. The host URL and port are *not* considered when comparing sessions and vulnerabilities between scans. For example:
>
> - Scan A: Session 1 is an http request to `http://qa.mysite.com/stuff/page/info.asp`. It has a vulnerability.
> - Scan B: Session 1 is an http request to `http://dev.mysite.com:8080/stuff/page/info.asp`. It has the same vulnerability as Scan A, session 1.
>
> When comparing scans, session 1 will appear as "Intersect" (intersection of A and B).

Compare Modes

You can select one of the following options in the **Compare Mode** section to the left of the Scan Dashboard to display different data in the **Sequence** area in the left pane (the data in the Scan Dashboard is *not* affected):

- **Mutual Exclusion**: Lists sessions that appear in Scan A or Scan B, but not in both scans
- **Only In A**: Lists sessions that appear in only Scan A
- **Only in B**: Lists sessions that appear in only Scan B
- **Union** (the default): Lists sessions that appear in Scan A, Scan B, or both Scans A & B

Session Filtering

The **Sequence** pane lists each session that matches the selected **Compare Mode**. An icon to the left of the URL indicates the severity of the vulnerability, if any, for that session. The severity icons are:

Critical	High	Medium	Low
❗	🔴	🟡	🔵

At the top of the **Sequence** pane, you can specify a filter and click **Filter** to limit the set of displayed sessions in the following ways:

- You can enter the URL with only its starting characters, as a "starts with" match. Your entry must begin with the protocol (http:// or https://).
- You can search for an exact match by specifying the URL in quotes. Your entry must begin with the quotes and protocol ("http:// or "https://)
- You can use an asterisk (*) as a wildcard character at the beginning or end of the string you enter.
- You can use asterisks (*) at both the beginning and end of the string you enter, which requires matches to contain the string between the asterisks.
- You can enter a question mark (?) followed by a full query parameter string to find matches to that query parameter.

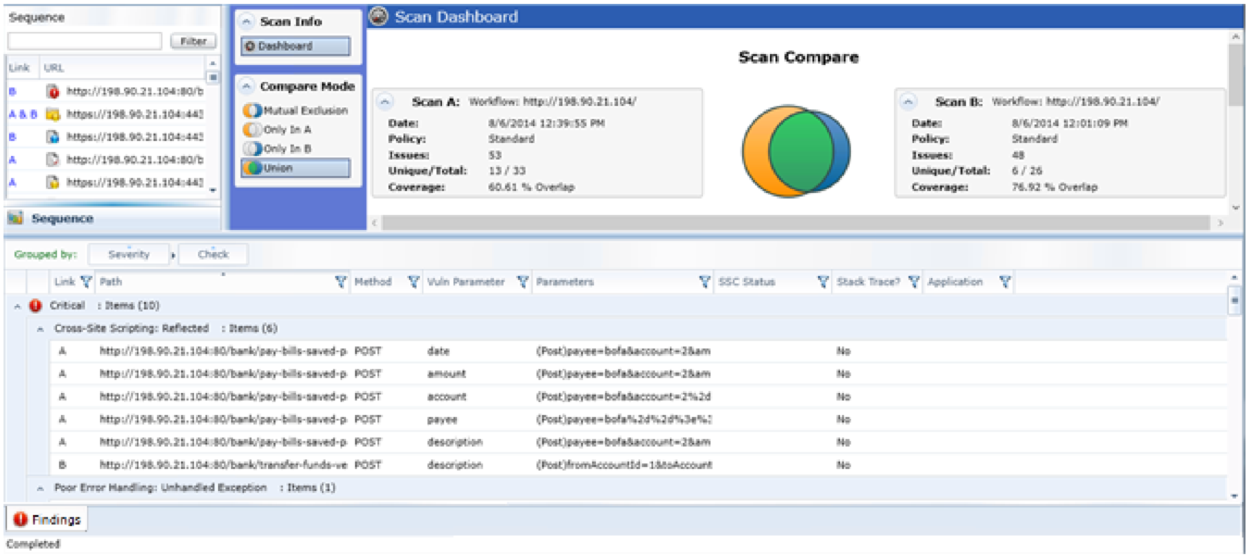
Using the Session Info Panel

When you select a session in the **Sequence** pane, the **Session Info** panel opens below the **Compare Mode** options. With a session selected, you can select an option in the **Session Info** panel to display more details about that session, to the right of the **Session Info** panel. If the session contains data for both scans, the data for some functions such as **Web Browser**, **HTTP Request**, and **Steps** are shown in a split view with Scan A on the left side and Scan B on the right side. The **Session Info** panel has the same options as a scan visualization except that the scan comparison does not include **Attachments**. For more information about the **Session Info** panel, see "Reviewing Scan Results" on page 182.

> **Note:** The **Steps** option displays the path taken by Fortify WebInspect to arrive at the session selected in the **Sequence** pane or the URL selected in the Summary pane. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology. In a scan comparison, if any of the steps for the session are different between the scans, the **In Both** column is added to the **Steps** table (as the first column). A value of **Yes** in the column for a particular step indicates that the step is the same for that session for both scans A and B. A value of **No** in the column for a particular step indicates that the step is different for that session between scans A and B.

Using the Summary Pane to Review Findings

When comparing scans, the horizontal Summary pane at the bottom of the window provides a centralized table of findings and enables you to quickly access vulnerability information. You can drag the horizontal divider above the table to show or hide more of the Summary pane.



Link	URL
B	http://198.90.21.104:80/b
A & B	https://198.90.21.104:443
B	https://198.90.21.104:443
A	http://198.90.21.104:80/b
A	https://198.90.21.104:443

Scan A: Workflow: http://198.90.21.104/
Date: 8/6/2014 12:39:55 PM
Policy: Standard
Issues: 53
Unique/Total: 13 / 33
Coverage: 60.61 % Overlap

Scan B: Workflow: http://198.90.21.104/
Date: 8/6/2014 12:01:09 PM
Policy: Standard
Issues: 48
Unique/Total: 6 / 26
Coverage: 76.92 % Overlap

Grouped by: Severity ▸ Check

Link	Path	Method	Vuln Parameter	Parameters	SSC Status	Stack Trace?	Application
Critical : Items (10)							
Cross-Site Scripting: Reflected : Items (6)							
A	http://198.90.21.104:80/bank/pay-bills-saved-p	POST	date	(Post)payee=bofa&account=2&am		No	
A	http://198.90.21.104:80/bank/pay-bills-saved-p	POST	amount	(Post)payee=bofa&account=2&am		No	
A	http://198.90.21.104:80/bank/pay-bills-saved-p	POST	account	(Post)payee=bofa&account=2%2d		No	
A	http://198.90.21.104:80/bank/pay-bills-saved-p	POST	payee	(Post)payee=bofa%2d%2d%3e%3		No	
A	http://198.90.21.104:80/bank/pay-bills-saved-p	POST	description	(Post)payee=bofa&account=2&am		No	
B	http://198.90.21.104:80/bank/transfer-funds-ve	POST	description	(Post)fromAccountId=1&toAccount		No	
Poor Error Handling: Unhandled Exception : Items (1)							

The set of entries (rows) displayed in the **Findings** tab depends on the option selected for **Compare Mode**. Possible values in the **Link** column reflect the selected **Compare Mode**.

See "Reviewing Scan Results" on page 182 for information about:

- The meanings of the displayed columns, and changing which columns are displayed
- Grouping the data in a hierarchy by clicking and dragging one or more column headings
- Limiting which rows are displayed by creating filters for one or more of the columns
- The following menu commands, which you can access by right-clicking an item in the **Findings** tab:
  - Copy URL
  - Copy Selected Item(s)
  - Copy All Items
  - Export

- View in Browser
- Review Vulnerability

About Publishing Scans to Fortify Software Security Center

Note: This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

Fortify Software Security Center (SSC) is a suite of tightly integrated solutions for identifying, prioritizing, and fixing security vulnerabilities in software. It uses OpenText Fortify Static Code Analyzer to conduct static analysis and OpenText Fortify WebInspect to conduct dynamic application security testing.

Although Fortify WebInspect can export scan data directly to Fortify Software Security Center, Fortify WebInspect Enterprise provides a central location for managing multiple Fortify WebInspect sensors and correlating scan results that can be published to individual application versions within Fortify Software Security Center.

Fortify WebInspect Enterprise maintains a history of all vulnerabilities for a particular application version, allowing it to correlate information obtained from subsequent scans. For example, when a second scan is introduced into Fortify WebInspect Enterprise for a specific application version, the program compares vulnerabilities in the scan with those in the history and assigns a status to each Fortify Software Security Center "issue" as follows:

SSC Status	Description
New	A previously unreported issue.
Existing	A vulnerability in the scan that is already in the history.
Not Found	A vulnerability in the history that is not found in the scan. This can occur because (a) the vulnerability has been remediated and no longer exists, or (b) because the latest scan used different settings, or scanned a different portion of the site, or for some other reason did not discover the vulnerability. You must decide whether the vulnerability still exists or whether it has been fixed.
Reintroduced	A vulnerability that appears in a current scan but was previously reported as resolved.

To change the SSC status for an individual issue, open a scan in the Scan Visualization window, right-click an item on the **Findings** or **Not Found** tab and select **Update SSC Status**.

The following example demonstrates a hypothetical series of scans for integrating vulnerabilities into Fortify Software Security Center.

First Scan

1. Scan the target site. In this example, assume that only one vulnerability (Vuln A) is discovered.
2. Examine the results. You can add screenshots and comments to vulnerabilities or mark vulnerabilities as false positive or ignored. You can also review, retest, and delete vulnerabilities.
3. Publish the scan.

Second Scan

1. The second scan again reveals Vuln A, but also discovers four more vulnerabilities (Vulns B, C, D, and E).
2. Examine the results. If you added audit data (such as comments and screenshots) to Vuln A when publishing the first scan, the data will be imported into the new scan.
3. Publish the scan to Fortify Software Security Center. Vuln A will be marked "Existing," Vulns B-E will be marked "New," and five items will exist in the Fortify Software Security Center system.

Third Scan

1. The third scan discovers Vulns B, C, and D, but not Vuln A or Vuln E.
2. After retesting Vuln A, you determine that it does, in fact, exist. You change its pending status to "Still an Issue."
3. After retesting Vuln E, you determine that it does not exist. You change its pending status to "Resolved."
4. Publish the scan to Fortify Software Security Center. Vulns B, C, and D will be marked "Existing." Five items will exist in the Fortify Software Security Center system.

Fourth Scan

1. The fourth scan does not find Vuln A or Vuln B. The scan does find Vulns C, D, E, and F.
2. Vuln E was previously declared to be resolved and so its status is set to “Reintroduced.”
3. You examine the vulnerabilities that were not found (A and B, in this example). If you determine that the vulnerability still exists, update the pending status to “Still an Issue.” If a retest verifies that the vulnerability does not exist, update the pending status to “Resolved.”
4. Publish the scan to Fortify Software Security Center. Vulns C and D will be marked "Existing."

See Also

"Publishing Scans to Fortify Software Security Center" below

Publishing Scans to Fortify Software Security Center

> **Note:** This topic applies only if OpenText Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center.

When a scan completes, it is automatically published to the associated application version in Fortify Software Security Center (SSC) if that application version is in the Finished state. If the application version is not finished, the scan is not published and an entry is written to the ManagerWS_trace log indicating that the scan could not be published because the associated application version is not finished.

> **Note:** Imported scans and scans that are uploaded from OpenText Fortify WebInspect are not automatically published.

You can manually publish a scan to Fortify Software Security Center from the following locations:

- Application Version Details form, **All Scans** tab with a scan selected, **Publish** button
- Scans form with a scan selected, **Publish** button
- Scan Visualization, **Publish Scan to SSC** button

When you publish a scan, Fortify WebInspect Enterprise displays a dialog box listing the number of vulnerabilities to be published, categorized by status and severity. To determine the status, Fortify WebInspect Enterprise compares previously submitted vulnerabilities (obtained by synchronizing with Fortify Software Security Center) with those reported in the current scan. If this is the first scan submitted to an application version, all vulnerabilities will be “New.”

If a vulnerability was previously reported, but is not in the current scan, it is marked as “Not Found.” You must determine if it was not found because it has been fixed or because the scan was configured differently (for example, you may have used a different scan policy, or you scanned a different portion of the site, or you terminated the scan prematurely). When examining the results, you can change the “pending status” of individual vulnerabilities detected by all but the first scan (by right-clicking an item in the summary pane). However, when publishing, you must specify how Fortify WebInspect should handle any remaining “Not Found” vulnerabilities.

1. Under **Default Status of “Not Found” Vulnerabilities**, do one of the following:
   - To retain these "Not Found" vulnerabilities in Fortify Software Security Center (indicating that they still exist), select **Retain: Assume all vulnerabilities still marked "Not Found" in the scan are still present**.
   - To change the status from "Not Found" to "Resolved" (implying that they have been fixed), select **Resolve: Assume all vulnerabilities still marked "Not Found" in the scan are fixed**.

   Note: This section may not appear if there are no "Not Found" vulnerabilities.
2. If this scan satisfies a scan request issued from Fortify Software Security Center, select **Associate scan with an "In Progress" scan request for the current application version**. See "Using Scan Requests from Fortify Software Security Center" on page 139 for more information.
3. Click **Publish**.

See Also

"About Publishing Scans to Fortify Software Security Center" on page 206

Working with Vulnerabilities

The following pages describe how to review, edit, and add vulnerabilities, add notes and screenshots to vulnerabilities, mark vulnerabilities as false positive, roll up vulnerabilities that share the same root cause, and recover deleted items.

Reviewing Vulnerabilities

After you conduct a scan and report discovered vulnerabilities, developers may correct their code and update the site. You can then open the original scan, select the once-vulnerable session (now supposedly remediated), and select **Review Vulnerability** from the shortcut menu. Assuming that the fundamental architecture of the site has not changed, you can verify that the threat no longer exists without rescanning the entire site (which, in some cases, could require several hours or even days).

You can use this feature simply to double-check a reported vulnerability, even while the scan is still running.

1. Do one of the following:
   - Right-click a vulnerable session in the navigation pane and select **Review Vulnerability**.
   - In the summary pane, select either the **Findings** or **Not Found** tab, right-click an item in the list, and select **Review Vulnerability**.
2. If multiple vulnerabilities are displayed, select one from the **Vulnerability to Review** list.
3. Use the tabs to display information about the original session (as selected in the **Steps to Reproduce** pane under the URL column):
   - **Browser** - The server’s response, as rendered in a browser.

     > **Note: Note:** This tab may or may not be visible. Retesting a cross-site scripting vulnerability may cause the script to loop infinitely on the **Browser** tab when using Microsoft Internet Explorer. Using the OpenText Fortify WebInspect Enterprise Administrative Console, the organization administrator can disable this tab.

   - **Request** - The raw HTTP request message.
   - **Response** - The raw HTTP response message.
   - **Vulnerability** - A description of the vulnerability, its implications, and suggestions on how to fix it.
   - **Attachments** - Notes and screenshots associated with the vulnerability, which you may add, view, edit, or delete.

Retesting the Session

To retest the session for the selected vulnerability:

1. Click **Retest**.
2. Select a sensor and click **OK**.

Results of the retest appear on the Status bar and in the lower pane in the **Response Match Status** column. The remaining client area is split into two panes: the original session is represented in the left pane, and the retested session appears in the right pane.

The status is reported as either "Vulnerability Detected" or "Vulnerability Not Detected."

Important! Fortify does not recommend retesting vulnerabilities in scans created using earlier versions of Fortify WebInspect. While retesting scans from earlier versions may work in many instances, it is not always reliable because individual checks may not flag the same vulnerability during a retest. Failure of a check to flag the same vulnerability while retesting a scan from an earlier version of Fortify WebInspect may not mean the vulnerability has been remediated.

The reliability of the reported findings is mitigated by the Response Match Status, which may have the following values:

- Match - The resource has not changed significantly; Fortify WebInspect Enterprise was able to access the session via the same path used by the original scan.
- Inconclusive - Based on the HTTP response, the resource has changed in a manner that may or may not substantiate the finding that a vulnerability has or has not been detected during the retest.
- Different - The HTTP response is radically different from the response received during the original scan, suggesting major changes to the resource.

If you think that Fortify WebInspect Enterprise has erroneously determined that the vulnerability exists, you can remove the vulnerability by clicking **Mark as** and selecting **False Positive** from the drop-down list. Alternatively, you can ignore the vulnerability by selecting **Ignored**.

Editing and Adding Vulnerabilities

After OpenText Fortify WebInspect Enterprise assesses your application’s vulnerabilities, you may want to edit and save the results for a variety of reasons, including:

- Security - If an HTTP request or response contains passwords, account numbers, or other sensitive data, you may want to delete or modify this information before making the scan results available to other persons in your organization.
- Correction - Fortify WebInspect Enterprise occasionally reports a “false positive.” This occurs when Fortify WebInspect Enterprise detects indications of a possible vulnerability, but further investigation by a developer determines that the problem does not actually exist. You can delete the vulnerability from the session or delete the entire session. Alternatively, you can designate it as a false positive; to do so, right-click the session in either the Site or Sequence view and select Mark As False Positive.
- Severity Modification - If you disagree with Fortify WebInspect Enterprise’s ranking of a vulnerability, you can assign a different level.
- Record Keeping - You can modify any of the text fields associated with an individual vulnerability (Summary, Implication, Execution, Fix, and Reference Info). For example, you could add a paragraph to the Fix section describing how you actually fixed the problem.
- Enhancement - If you discover a new vulnerability, you could define it and add it to a session as a custom vulnerability

To Edit or Add a Vulnerability

To edit or add a vulnerability:

1. Do one of the following:
   - In the summary pane, right-click an item on any tab except **Scan Log** or **Server Information**, and select **Edit Vulnerability**.
   - In the navigation pane, right-click a session and select **Edit Vulnerability** or **Add > Vulnerability**.
2. Select a vulnerability (if the session includes multiple vulnerabilities).
3. To add an existing vulnerability to the session (that is, one that exists in the database), click **Add Existing**.
   a. On the Add Existing Vulnerability window, enter part of a vulnerability name, or a complete vulnerability ID number or type.

      > **Note:** The * and % characters can be used interchangeably as wildcards. However, a wildcard is allowed only at the beginning, at the end, or at the beginning and end of a string. If placed within a string (such as "mic*soft,"), these characters will not function as wildcards.

   b. Click **Search**.
   c. Select one or more of the vulnerabilities returned by the search.
   d. Click **OK**.
4. To add a custom vulnerability, click **Add Custom**. You can then edit the vulnerability as described in Step 6.
5. To delete the vulnerability from the selected session, click **Delete**.
6. To edit the vulnerability, you can modify the check name, check type, severity, or probability. You can also change the descriptions that appear on the **Summary**, **Implication**, **Execution**, **Fix**, and **Reference Info** tabs.
7. Click **OK** to save the changes.

To Remove Edits

To remove any modifications you made to existing vulnerability descriptions, select a check name and click **Restore Defaults**.

Adding a Vulnerability Note

To add a vulnerability note:

1. Open a scan in the Scan Visualization window. See "Reviewing Scan Results" on page 182.
2. Do one of the following to select a vulnerability:
   - On the **Findings** tab in the Summary pane, right-click a vulnerable URL.
   - On the Navigation pane, right-click a vulnerable session or URL.
3. On the shortcut menu, click **Attachments > Add Vulnerability Note**.
4. If you selected a session with multiple vulnerabilities, select the check box next to one or more vulnerabilities.
5. In the Comments section, enter a note related to the vulnerability (or vulnerabilities) you selected.
6. Click **OK**.

You can view notes and screenshots for a selected session by clicking **Attachments** on the Session Info panel.

Adding a Vulnerability Screenshot

To add a vulnerability screenshot:

1. Open a scan in the Scan Visualization window. See "Reviewing Scan Results" on page 182.
2. Do one of the following to select a vulnerability:
   - On the **Findings** tab in the Summary pane, right-click a vulnerable URL.
   - On the Navigation pane, right-click a vulnerable session or URL.
3. On the shortcut menu, click **Attachments > Add Vulnerability Screenshot**.
4. If you selected a session with multiple vulnerabilities, select the check box next to one or more vulnerabilities.
5. Enter a name (40 characters max.) for the screenshot in the **Name** field.
6. Click the browse button ... and choose a file using the standard file-selection window. You can specify only one image file even if you have selected multiple vulnerabilities.
7. (Optional) In the Comments section, enter a note related to the vulnerability screenshot you selected.
8. Click **OK**.

You can view notes and screenshots for a selected session by clicking **Attachments** on the Session Info panel.

Marking a Vulnerability as a False Positive

If you think that OpenText Fortify WebInspect has erroneously determined that a session contains a vulnerability, you can remove the vulnerability from the session.

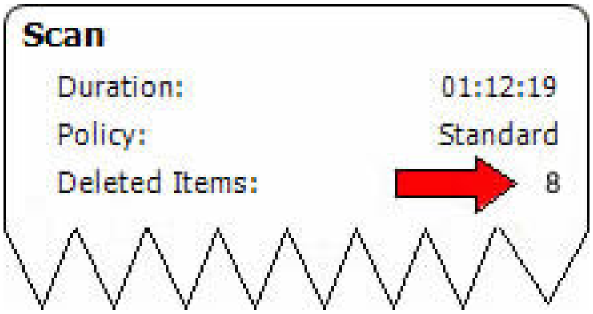
1. In the Site view of the Scan Visualization window, right-click an item in the navigation pane and select **Mark as False Positive**.
2. (Optional) Enter a comment.
3. Click **OK**.

> **Tip:** To view a list of all sessions that have been marked as false positives, select **False Positives** from the Scan Info panel.

Recovering Deleted Items

When you remove a session or when you ignore or delete a vulnerability, OpenText Fortify WebInspect Enterprise deletes the item from the Navigation pane (in both the Site and Sequence views) and from the **Findings** tab in the Summary pane.

The number of deleted items is displayed on the Dashboard (under the Scan category).



Scan

Duration:	01:12:19
Policy:	Standard
Deleted Items:	8

To recover removed sessions and ignored vulnerabilities:

1. On the Scan Info panel, click **Deleted Items**.
2. Click the drop-down list to toggle between **Vulnerabilities** and **Sessions**.
3. Select one or more items you want to recover.
4. Click **Recover**.

Recovered vulnerabilities reappear in the Navigation pane in both the Site and Sequence views (along with their parent sessions) and also reappear in the **Findings** tab in the summary pane. Recovered sessions also reappear in the navigation pane along with any child sessions and their vulnerabilities.

See Also

"Reviewing Scan Results" on page 182

About Vulnerability Rollup

Some sites contain a vulnerability class that is endemic throughout the site. For example, a cross-site scripting vulnerability may exist in every POST and GET method for every parameter on an entire site due to lack of input validation. This means that numerous cross-site scripting vulnerabilities will be listed on the Findings tab in the summary pane. To prevent overwhelming your development team, you can roll up such vulnerabilities into a single instance that is prefixed with the tag “[Rollup]” in OpenText Fortify WebInspect, OpenText Fortify WebInspect Enterprise, and reports.

What Happens to Rolled Up Vulnerabilities

When you select multiple vulnerabilities and use the rollup feature, all vulnerabilities except the first selected vulnerability are marked as ignored. The first selected vulnerability remains visible and represents the rollup. Although the rest of the selected vulnerabilities are marked as ignored, they do not appear as ignored vulnerabilities in the Recover Deleted Items window.

Caution! Rolling up vulnerabilities indicates that they share the same root cause, and that fixing the root cause will fix all rolled up vulnerabilities. Future scans will automatically ignore rolled up vulnerabilities if found. If any of the rolled up vulnerabilities do not share the same root cause, they will still be ignored.

Rollup Guidelines

The following guidelines apply to vulnerability rollup:

- Scans that include vulnerability rollups can be rescanned and bulk retested.
- Only the visible vulnerability is retested during bulk retest. The rest of the vulnerabilities are ignored and will not show up as rolled up on the retest.
- Rollup is local to a scan and is not propagated between scans.
- Rollup works only when you select multiple vulnerabilities that have not been rolled up. Inadvertently selecting a currently rolled up vulnerability will prevent the Rollup Vulnerability option from appearing in the shortcut menu.
- You can only undo a rollup if you single select a vulnerability that is currently rolled up.

Rolling Up Vulnerabilities

To rollup vulnerabilities:

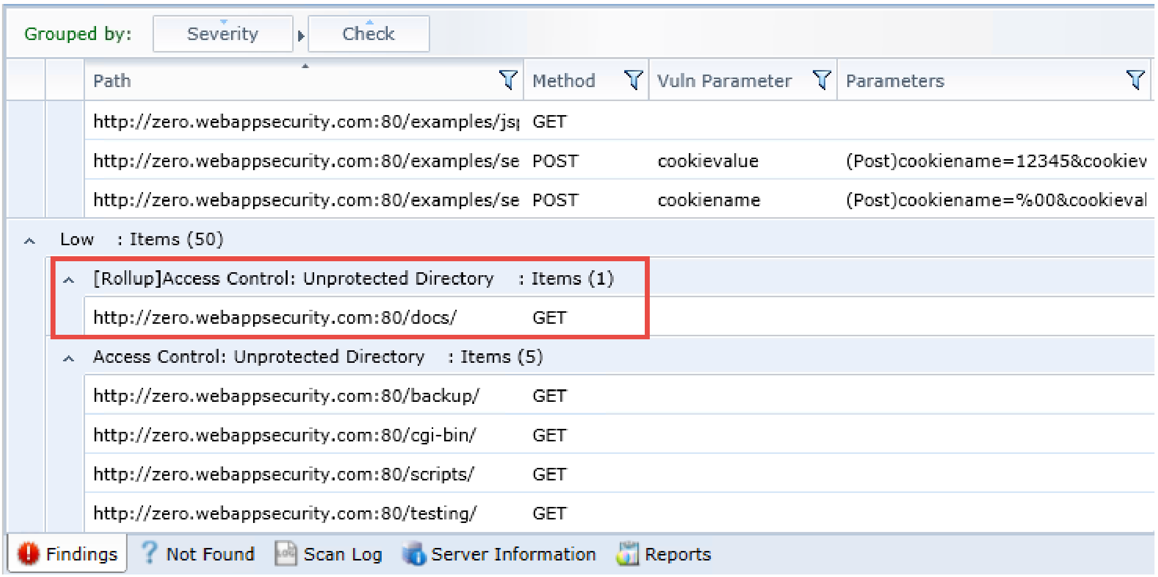
1. On the **Findings** tab in the summary pane, select several vulnerabilities to rollup.
2. Right click and select **Rollup Vulnerabilities** from the shortcut menu.

   The following warning appears:

   Rolling up these vulnerabilities indicates that they share the same root cause, and that fixing the root cause will fix all rolled up vulnerabilities. Future scans will automatically ignore rolled up vulnerabilities if found. If any of these vulnerabilities do not share the same root cause, they will still be ignored. Do you wish to continue?

3. Do one of the following:
   - Click **OK** to rollup the vulnerabilities.
   - Click **Cancel** to leave the vulnerabilities as they are.

   If you click **OK**, the selected vulnerabilities are rolled into a single instance and the check name is prefixed with the tag “[Rollup]”, as shown in the following image. Additionally, a note is added to the Attachments on the Session Info panel detailing the URLs that were rolled up and affected by the same vulnerability. For more information, see "Session Info Panel" on page 187.



Path	Method	Vuln Parameter	Parameters
http://zero.webappsecurity.com:80/examples/jsı	GET		
http://zero.webappsecurity.com:80/examples/se	POST	cookievalue	(Post)cookiename=12345&cookiev
http://zero.webappsecurity.com:80/examples/se	POST	cookiename	(Post)cookiename=%00&cookieval
Low : Items (50)			
[Rollup]Access Control: Unprotected Directory : Items (1)			
http://zero.webappsecurity.com:80/docs/	GET		
Access Control: Unprotected Directory : Items (5)			
http://zero.webappsecurity.com:80/backup/	GET		
http://zero.webappsecurity.com:80/cgi-bin/	GET		
http://zero.webappsecurity.com:80/scripts/	GET		
http://zero.webappsecurity.com:80/testing/	GET		

Undoing Rollup

The rollup feature is reversible. To undo a rollup:

1. On the **Findings** tab in the summary pane, right-click any vulnerability that has been rolled up.
2. Select **Unroll Vulnerabilities**.

   The rollup is reversed, and the vulnerabilities appear on the Findings tab. Additionally, the note detailing the rolled up vulnerabilities is removed from the Attachments on the Session Info panel.

   Note: If Fortify WebInspect Enterprise is integrated with OpenText Fortify Software Security Center, and you undo a rollup in a scan that has been published to Fortify Software Security Center, the note that was added about the rollup will not be deleted from Fortify WebInspect Enterprise or Fortify Software Security Center.

See Also

"Findings Tab" on page 191

Advanced Settings

The following pages describe the advanced scan settings, including crawl and audit settings.

Legacy Scan: General

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan

Enter a name for the scan.

Scan URL

Select one of the following scan types.

Standard Scan

OpenText Fortify WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

1. In the **URL** field, type or select the complete URL or IP address of the site you want to examine.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, you will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

   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 pursue links that use fully qualified URLs (as opposed to relative paths).

   Fortify WebInspect supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets.
2. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:

   - **Directory only (self)** - Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.

   - **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.

   - **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

List-Driven Scan

Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility.

- Click **Browse** to select a text file or XML file containing the list of URLs you want to scan.
- Click **View** to view the contents of the selected file.

Workflow-Driven Scan

Fortify WebInspect audits only those URLs included in the macro that you previously recorded and 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, they will all be included in the same scan.

- Click **Browse** and select a macro containing the URLs you want to scan.

Web Service Scan

When performing a Web Service scan, Fortify WebInspect crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

- Click **Browse** to select a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Priority

Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

Sensor

Select which sensor should conduct the scan. You can choose a specific sensor or select the **Run on Any Available Sensor** option.

A sensor can perform only one scan at a time. If it is conducting a scan when another scan is scheduled to occur, then:

- If the currently running scan has a higher priority, the Fortify WebInspect Enterprise Manager will place the pending scan in a queue until the first scan finishes or until another sensor becomes available.
- If the currently running scan has a lower priority, the Fortify WebInspect Enterprise Manager will suspend that scan, assign the second scan to that sensor, and then reassign the suspended scan to the sensor when the higher priority scan is complete.

Scans that are manually initiated have priority over any scheduled scan.

Legacy Scan Settings: Method

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Mode

Select one of the following modes:

- **Crawl Only** - This option completely maps a site's tree structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
- **Crawl and Audit** - As OpenText Fortify WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed. This is described in the Crawl and Audit Mode section as the option to crawl and audit Simultaneously.
- **Audit Only** - Fortify WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

If the selected scan mode is Crawl and Audit, choose one of the following:

- **Simultaneously** - As Fortify WebInspect maps the site’s hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed.
- **Sequentially** - In this mode, Fortify WebInspect crawls the entire site, mapping the site’s hierarchical data structure, and then conducts a sequential audit, beginning at the site’s root. If you select this option, you can specify the order in which the crawl and audit should be conducted.
    - **Test each engine type per session (engine driven)**: Fortify WebInspect audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.
    - **Test each session per engine type (session driven)**: Fortify WebInspect runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Scan Behavior

You can select any of the following optional behaviors:

- **Use a login macro for forms authentication** - This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent Fortify WebInspect from terminating prematurely if it inadvertently logs out of your application. The drop-down list contains the names of all macros that have been uploaded to OpenText Fortify WebInspect Enterprise. Macros that are available in the repository for the selected Application and Application Version are listed with “(Repository)” prepended to the macro name. You can select one of these, or you can click **Browse** to locate a macro and upload it. See "Working with the Macro Repository" on page 173 for more information.

  If you specified login parameters when recording the macro, Fortify WebInspect will substitute these credentials for those used in the macro when it scans a page containing the input control associated with this entry.
- **Use a startup macro** - This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that Fortify WebInspect will use to navigate to that area. It may also include login information, but does not contain logic that will prevent Fortify WebInspect from logging out of your application. Fortify WebInspect visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). The drop-down list contains the names of all macros that have been uploaded to Fortify WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro and upload it.

  > **Important!** Do not use a login macro and a startup macro with the same name. The scan may yield undesirable results.
- **Auto-fill Web forms during crawl** - If you select this option, Fortify WebInspect submits values for input controls found on all HTML forms it encounters while scanning the target site. Fortify WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. Use the **Browse** button to specify the file containing the values you want to use. Alternatively, you can select **Edit** (to modify the currently selected file) or **Create** (to record new Web form values).

Legacy Scan Settings: General

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Details

You may choose the following options:

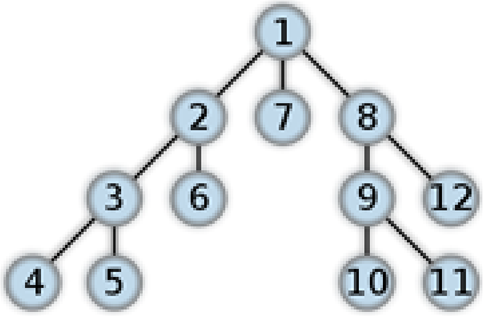
- **Enable Path Truncation** - Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. OpenText Fortify WebInspect truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ will cause the server to reveal directory contents or will cause unhandled exceptions.
- **Attach debug information in request header** - If you select this option, Fortify WebInspect includes a "Memo:" header in the request containing information that can be used by support personnel to diagnose problems.
- **Case-sensitive request and response handling** - Select this option if the server at the target site is case-sensitive to URLs.
- **Compress response data** - If you select this option, Fortify WebInspect saves disk space by storing each HTTP response in a compressed format in the database.
- **Maximum crawl-audit recursion depth** - When an attack reveals a vulnerability, Fortify WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The maximum value is 1,000.

Crawl Details

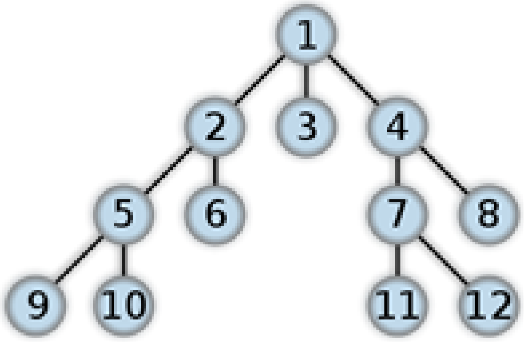
You may choose the following options:

- **Crawler** - Select either **Depth First** or **Breadth First**.

  Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.



By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



When performing a depth-first crawl, Fortify WebInspect pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a “shopping cart” page before accessing the “check-out” page).

- **Enable keyword search audit** - A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
- **Perform redundant page detection** - Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, Fortify WebInspect would never be able to finish the scan. This option, however, allows Fortify WebInspect to identify and exclude processing of redundant resources.
- **Limit maximum single URL hits to** - Use this field to limit the number of times a single link will be followed during a crawl. Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL.
- **Include parameters in hit count** - If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.

  For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice).

- **Limit maximum link traversal sequence to** - This option restricts the number of hyperlinks that can be sequentially accessed as Fortify WebInspect crawls the site. For example, if five resources are linked as follows:
  - Page A contains a hyperlink to Page B
  - Page B contains a hyperlink to Page C
  - Page C contains a hyperlink to Page D
  - Page D contains a hyperlink to Page E

  And if this option is set to "3," then Page E will not be crawled.

  The default value is 15.
- **Limit maximum crawl folder depth to** - The Crawl Depth value determines how deeply Fortify WebInspect traverses the hierarchical levels of your Web site. If set to 1, Fortify WebInspect drills down one level; if set to 2, Fortify WebInspect drills down two levels; and so on. The maximum value is 1000.
- **Limit maximum crawl count to** - This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.

  Note: The limit set here does not directly correlate to the Crawled progress bar that is displayed during a scan. The maximum crawl count set here applies to links found by the Crawler during a crawl of the application. The Crawled progress bar includes all sessions (requests and responses) that are parsed for links during a crawl and audit, not just the links found by the Crawler during a crawl.
- **Limit maximum Web form submissions to** - Normally, when Fortify WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed. There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form. Use this setting to limit the total number of submissions that Fortify WebInspect will perform.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

Legacy Scan Settings: Content Analyzers

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Flash

If you enable the Flash analyzer, OpenText Fortify WebInspect analyzes Flash files, Adobe's vector graphics-based resizable animation format.

JavaScript/VBScript

The JavaScript/VBScript analyzer is always enabled. It allows Fortify WebInspect to crawl links defined by JavaScript or Visual Basic script, and to create and audit any documents rendered by JavaScript.

Tip: To increase the speed at which Fortify WebInspect conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Configure the settings in the lower pane of the window, as described below.

Option	Description
Crawl links found from script execution	If you select this option, the crawler will follow dynamic links (i.e., links generated during JavaScript execution).
Reject script include file requests to offsite hosts	Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is: `<script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>` Fortify WebInspect will download and parse such files, regardless of their origin or file type, unless you select the Reject Script option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).
Create script event sessions	Fortify WebInspect creates and saves a session for each change to the Document Object Model (DOM).
Verbose script parser debug logging	If you select this setting *and* if the Application setting for logging level is set to Debug, Fortify WebInspect logs every method called on the DOM object. This can easily create

Option	Description
	several gigabytes of data for medium and large sites.
Log JavaScript errors	Fortify WebInspect logs JavaScript parsing errors from the script parsing engine.
Enable JS Framework UI Exclusions	If you select this option, the Fortify WebInspect JavaScript parser ignores common jQuery and Ext JS user interface components, such as a calendar control or a ribbon bar. These items are then excluded from JavaScript execution during the scan.
Max script events per page	Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999. The default value is 1000.
Enable classic script engine	The current script engine operates more like a browser and supports more web applications than did the script engine used in previous Fortify WebInspect versions. You can select this option to use the previous script engine instead.
Enable Advanced JS Framework Support	When this option is selected, Fortify WebInspect can recognize certain JavaScript frameworks and more intelligently execute script by recognizing patterns that these frameworks use. This option is available only for the current script engine and is disabled if you select the **Enable classic script engine** option.
Enable Site-Wide Event Reduction	When this option is selected, the crawler and JavaScript engine recognize common functional areas that appear among different parts of the website, such as common menus or page footers. This eliminates the need to find within HTML content the dynamic links and forms that have already been crawled, resulting in quicker scans. This option is enabled by default and should not normally be disabled.
Enable SPA support	When this option is selected for single-page applications, 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.

Option	Description
	Caution! SPA support should be enabled for single-page applications only. Enabling SPA support to scan a non-SPA website will result in a slow scan.

Silverlight

If you enable the Silverlight analyzer, Fortify WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment.

Legacy Scan Settings: Requestor

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Requestor Performance

Select one of the following options:

- **Use a shared requestor** - If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of OpenText Fortify WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
- **Use separate requestors** - If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

  When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl requestor thread count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5. The **Audit requestor thread count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

Note: Depending on the capacity of the application being scanned, increasing thread counts may increase request failures due to increased load on the server, causing some responses to exceed

the **Request timeout** setting. Request failures may reduce scan coverage because the responses that failed may have exposed additional attack surface or revealed vulnerabilities. If you notice increased request failures, you might reduce them by either increasing the **Request timeout** or reducing the **Crawl requestor thread count** and **Audit requestor thread count**.
Also, depending on the nature of the application being scanned, increased crawl thread counts may reduce consistency between subsequent scans of the same site due to differences in crawl request ordering. By reducing the default **Crawl requestor thread count** setting to 1, consistency may be increased.

Requestor Settings

You may select the following options:

- **Limit maximum response size to** - Select this option to limit the size of accepted server responses and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
- **Request retry count** - Specify how many times Fortify WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
- **Request timeout** - Specify how long Fortify WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, Fortify WebInspect resubmits the request until reaching the retry count. If Fortify WebInspect then receives no response, it logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct Fortify WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

Note: If these options are selected and the **Request timeout** setting (above) is reached, the scan may stop when the server does not respond within the period set for the Request timeout. If the server responds with the extended Request timeout period, then the extended period becomes the new Request timeout for the current scan.

The following options are available:

- **Consecutive "single host" retry failures to stop scan** - Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.
- **Consecutive "any host" retry failures to stop scan** - Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.
- **Nonconsecutive "single host" retry failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
- **Nonconsecutive "any host" request failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.

- **If first request fails, stop scan** - Selecting this option will force Fortify WebInspect to terminate the scan if the target server does not respond to Fortify WebInspect's first request.
- **Response codes to stop scan if received** - Enter the HTTP status codes that, if received, will force Fortify WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Legacy Scan Settings: Session Storage

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the database. This saved information can be used for two purposes, as follows:

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, OpenText Fortify WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Fortify Customer Support personnel can extract the generated (but not sent) HTTP requests for analysis. Sessions may be rejected for the reasons cited in the following table:

Reject Reason	Explanation
Invalid Host	Any host that is not specified as an Allowed Host.
Excluded File Extension	Files having an extension that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected File Extensions.
Excluded URL	URLs or hosts that are excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected URLs

Reject Reason	Explanation
	and Hosts.
Outside Root URL	If the **Restrict to Folder** option is selected when starting a scan, any resource not qualified by the available options (**Directory only (self)** , **Directory and subdirectories**, or **Directory and parent directories**).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the **Limit maximum crawl folder depth to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the **Limit Maximum Single URL hits to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
404 Response Code	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine File Not Found (FNF) using HTTP response codes** is selected and the response contains a code that matches the requirements.
Solicited File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Auto detect FNF page** is selected and Fortify WebInspect determined that the response constituted a "file not found" condition.
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine FNF from custom supplied signature** is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

Session Storage

Fortify WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

Legacy Scan Settings: Session Exclusions

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

> **Note:** The following settings apply to both the crawl and audit phases of a scan. To specify exclusions for only the crawl or only the audit, use the Crawl Settings - Session Exclusions or the Audit Settings - Sessions Exclusions.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not request files of the type you specify.
- **Exclude** - Fortify WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

Excluded MIME Types

Fortify WebInspect will not process files associated with the MIME type you specify. For more information, see "MIME Types" on the next page.

Excluded or Rejected URLs and Hosts

You can identify a URL or host (using a regular expression) and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

You must use a regular expression to designate a host or URL.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following regular expression and select **Reject**.

Microsoft\.com

Note that the period (or dot) is preceded by a backslash, indicating that the next character is special (that is, it is not the character used in regular expressions to match any single character except a newline character).

Example 2

Enter a string such as logout. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the logout example, Fortify WebInspect will exclude or reject URLs such as logout.asp or applogout.jsp.

Example 3

If you enter /myApp /

then Fortify WebInspect will exclude or reject all resources in the myApp directory, such as:

http://www.test.me /myApp /filename.htm

If you enter /W3SVC[0-9]*/

then Fortify WebInspect will exclude or reject the following directories:

- http://www.test.me /W3SVC55/
- http://www.test.me /W3SVC5/
- http://www.test.me/W3SVC550/

Adding a URL or Host

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either **Host** or **URL**.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one of the following:
    - Reject - Do not send request to targeted URL or host.
    - Exclude - Send request, but do not process response.
5. Click **Update**.

MIME Types

Multipurpose Internet Mail Extensions (MIME) is a specification for formatting non-ASCII messages so they can be sent over the Internet. The Content-Type header indicates the type and subtype of the message content, for example Content-Type: text/plain. The combination of type and subtype is generally called a MIME type (also known as Internet media type). Examples include:

- text/html
- image/jpeg
- image/gif
- audio/x-wave
- audio/mpeg

- video/mpeg
- application/zip

Legacy Scan Settings: Allowed Hosts

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Allowable Hosts for Crawl and Audit

Use the Allowed Host settings to add domains that may be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl or audit.

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 OpenText Fortify WebInspect 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, Fortify WebInspect 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

Note: If you specify a port number, then the allowed host must be an exact match.

If you use a regular expression to specify a host, select **Regex**.

Legacy Scan Settings: HTTP Parsing

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then OpenText Fortify WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, "userid" is the parameter you would identify.

> **Note:** You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

Fortify WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "1234567" is the session information:

http://www.onlinestore.com/bikes/(1234567)/index.html

The regular expression for identifying the parameter would be: /\([\w\d]+\)/

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. Two default regular expressions identify two ASP.NET cookieless session IDs. The third regular expression matches jsessionid cookie.

HTTP Parameters Used for Navigation

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

- http://www.anysite.com?Master.asp?Page=1
- http://www.anysite.com?Master.asp?Page=2;
- http://www.anysite.com?Master.asp?Page=13;Subpage=4

Ordinarily, Fortify WebInspect would assume that these three requests refer to identical resources and would scan only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

The first and second examples contain one resource parameter: "Page." The third example contains two parameters: "Page" and "Subpage."

To identify resource parameters:

1. Click **Add**.
2. Enter the parameter name and click **Update**.

   The string you entered appears in the **Parameter** list.
3. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) Fortify WebInspect should use.

Legacy Scan Settings: Filters

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Using the Filter Settings

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use OpenText Fortify WebInspect or those who have access to the raw data.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

Adding a Regular Expression Rule

To add a regular expression rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.
2. From the **Section** list, select an area to search.
3. In the **Find Condition** field, type (or paste) the string you want to locate (or enter a regular expression that describes the string). You can also click the list button to insert regular expression elements.
4. Type (or paste) the replacement string in the **Replace** field.
5. For case-sensitive searches, select the **Case-Sensitive** check box.
6. Click **Update**.

Legacy Scan Settings: Cookies/Headers

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Standard Header Parameters

You can elect to include referer and/or host headers in requests sent by OpenText Fortify WebInspect.

- **Include 'referer' in HTTP request headers** - Select this check box to include referer headers in HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
- **Include 'host' in HTTP request headers** - Select this check box to include host headers with HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit Fortify WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when Fortify WebInspect is auditing that site. You can add multiple custom headers.

To add a custom header:

1. In the top box, enter the header using the format <name>: <value>.
2. Click **Add**.

The new header appears in the list of custom headers.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by Fortify WebInspect to the server when conducting a scan.

To add a custom cookie:

1. In the top box, enter the header using the format <name>=<value>. For example, if you enter

   CustomCookie=ScanEngine

   then each HTTP-Request will contain the following header:

   Cookie: CustomCookie=ScanEngine
2. Click **Add**.

The new cookie appears in the list of custom cookies.

Legacy Scan Settings: Proxy

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Proxy Settings

Select one of the following options:

- **Direct Connection (proxy disabled)** - Select this option if you are not using a proxy server.
- **Automatically detect proxy settings** - If you select this option, OpenText Fortify WebInspect will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file

and use this to configure the browser's web proxy settings.

- **Use System proxy settings** - Select this option to use the proxy server settings on the machine that will conduct the scan.
- **Use Firefox proxy settings** - Select this option to use the proxy server settings configured for the Firefox browser on the machine that will conduct the scan.

  Note: Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the browser connection settings are not configured for proxy, then a proxy server will not be used.

- **Configure a proxy using a PAC file URL** - Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** field.
- **Explicitly configure proxy** - Select this option to access the Internet through a proxy server, and then enter the requested information:
  a. In the **Server** field, type the URL or IP address of your proxy server.
  b. In the **Port** field, enter the port number (for example, 8080).
  c. Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.
  d. If your proxy server requires authentication, enter the qualifying user name and password.
  e. 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 Proxy For** field. Use commas to separate entries.

  For proxy servers accepting https connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information.

Legacy Scan Settings: Authentication

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Requires Network Authentication

Select this option if users must log on to your Web site or application. Then select an authentication method and specify a user name and password.

Caution! OpenText Fortify WebInspect will crawl 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 a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact Fortify Customer Support.

The authentication methods are:

Basic

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a dialog box for a user to enter a previously assigned user name and password and then attempts to establish a connection to a server using the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.

NTLM

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 Fortify WebInspect has to pass through a proxy server to submit its requests to the Web server, Fortify WebInspect may not be able to crawl or audit that Web site. Use caution when configuring Fortify WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

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. This authentication method will be successful only if the Web server has been configured to return a response header of “WWW-Authenticate: Kerberos” instead of “WWW-Authenticate: Negotiate.”

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.

Automatic

Allow Fortify WebInspect 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 is noticeably improved.

Client Certificates

Client certificate authentication allows users to present client certificates rather than entering a user name and password.

To use client certificates:

1. Select **Use Client Certificate**.
2. Click **Browse** to choose a certificate.

Legacy Scan Settings: File Not Found

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Determine File Not Found (FNF) Using HTTP Response Codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.

- **Forced valid response codes (never an FNF)**: You can specify HTTP response codes that should never be treated as a file-not-found response.
- **Forced FNF response codes (always an FNF)**: Specify those HTTP response codes that will always be treated as a file-not-found response. OpenText Fortify WebInspect will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a semicolon.

Determine File Not Found from Custom Supplied Signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result from 404 pages that are unique to your site.

You can specify a signature using plain text, a regular expression, or, using the **SPI Regex** option. For information about the Regular Expression Editor tool, see the *OpenText™ Fortify WebInspect Tools Guide*.

Auto-Detect File Not Found Page

Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found. Select this check box if you want Fortify WebInspect to detect these "custom" file-not-found pages.

Fortify WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you select the **Auto-Detect File Not Found Page** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

Legacy Scan Settings: Policy

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Policy

Select a policy. A policy is a collection of audit engines and attack agents that OpenText Fortify WebInspect uses when auditing or crawling your Web application. Each component has a specific task, such as testing for cross-site scripting susceptibility, building the site tree, probing for known server vulnerabilities, etc. For policy descriptions, see "Policies List" on page 155.

Note: You cannot select a policy for a Web Service scan.

Legacy Crawl Settings: Link Parsing

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Link Parsing

OpenText Fortify WebInspect follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature to identify (using regular expressions) links that you want Fortify WebInspect to follow.

To add a specialized link identifier:

1. Click **Add**.
2. In the **Custom Links** field, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comments** field.
4. Click **Update**.

Legacy Crawl Settings: Session Exclusions

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

> **Note:** All items specified in the **Scan Settings - Session Exclusions** are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the **Scan Settings - Session Exclusions** panel. This panel (Crawl Settings - Session Exclusions) enables you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited.

To add a MIME Type:

1. Click **Add**.
2. In **the Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the Web site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host
   - **Exclude** - Send request, but do not process response
5. Click **Update**.

Legacy Audit Settings: Session Exclusions

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Audit Settings - Session Exclusions) enables you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.

3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. For more information, see "MIME Types" on page 230.

To add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host.
   - **Exclude** - Send request, but do not process response.
5. Click **Update**.

Legacy Audit Settings: Attack Exclusions

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Excluded Parameters

Use this feature to prevent OpenText Fortify WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

1. In the Excluded Parameters group, click **Add**.
2. In the **Parameter** field, enter the name of the parameter you want to exclude.
3. Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.
4. Click **Update**.

Excluded Cookies

Use this feature to prevent Fortify WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values. This setting requires you to enter the name of a cookie.

In the following example HTTP response, the name of the cookie is "FirstCookie."

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

To exclude certain cookies:

1. In the Excluded Cookies group, click **Add**.
2. In the **Parameter** field, type a cookie name or enter a regular expression that you believe will match the cookies you want to exclude.
3. Click **Update**.

Excluded Headers

Use this feature to prevent Fortify WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression as follows:

1. In the Excluded Headers group, click **Add**.
2. In the **Parameter** field, type a header name or enter a regular expression that you believe will match the headers you want to exclude.
3. Click **Update**.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs.

To load inputs that you previously created using the editor, click the **Browse** button next to the **Import Audit Inputs** button.

Legacy Audit Settings: Attack Expressions

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- ja-jp: Japanese - Japan
- ko-Kr: Korean - Korea
- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan
- es-mx: Spanish - Mexico

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Legacy Audit Settings: Vulnerability Filters

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Select Vulnerability Filters to Enable

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition** - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection Dom Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

To add a filter to your default settings, select a filter in the **Available** area and click **>**. The filter is removed from the **Available** list and added to the **Selected** list.

To disable a filter, select a filter in the **Selected** list and click **<**. The filter is removed from the **Selected** list and added to the **Available** list.

To add all available filters, click **>>**.

To remove all selected filters, click **<<**.

Audit Settings: Smart Scan

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, OpenText Fortify WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select **Enable Smart Scan**, you can choose one or both of the identification methods described below.

- **Use regular expressions on HTTP responses** - This method searches the server response for strings that match predefined regular expressions designed to identify specific servers.
- **Use server analyzer fingerprinting and request sampling** - This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server type.

Custom Server/Application Type Definitions (more accurate detection)

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions (more accurate detection)** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.
2. In the **Host** field, enter the domain name or host, or the server's IP address.
3. Select one or more entries from the **Server/Application** list.
4. Click **OK**.

Legacy Scan Behavior: Blackout Action

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Blackout Action

A blackout period is a block of time during which scans are not permitted.

If a blackout period begins while a scan is running, you may either stop the scan or suspend it. The sensor will resume a suspended scan when the blackout period ends.

Legacy Export: General

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list.

You are not required to use a template.

Export Scan Results

Select this option to export the scan results. Then provide the requested information.

- **Export Path** - Enter or select a destination for the exported scan. Because the OpenText Fortify WebInspect Enterprise Manager service writes the output, the specified path must be writable by the Manager service user. You should use a UNC pathname so that it will be accessible to both the Fortify WebInspect Enterprise Manager and end users. You may alternatively specify a drive letter and path (for example, C:\WIE\Output\), but the path will apply to the Fortify WebInspect Enterprise Manager and may not be accessible to end users.
- **Export Format** - Select how you want the exported file to be formatted. Your choices are WebInspect Scan File (.scan) or Extensible Markup Language (.xml).
- **Automatically generate file name** - If you select this option, the name of the file will be formatted as <scan name> <date/time>.[xml or scan]. For example, if the scan name is "mysite" and the scan is generated at 6:30 on April 5, the file name would be "mysite 04_05_2007 06_30.scan [or .xml]." This is useful for recurring scans.

  If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **File Name** field.

Blackout Settings

The following pages describe blackout settings, including general settings and settings for recurring blackouts.

Blackout: General

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

Creating a Blackout Period

To create a blackout period, provide the information described in the following table.

Item	Description
Business Unit	Select an organization and group. To associate the blackout with all groups in an organization, select **Use Organization**.

Item	Description
Name	Enter a unique identifier for this blackout period.
Address	The URL or IP address (or range of IP addresses) that are affected by this blackout period. The value can be a single URL or IP address, or a range of IP addresses. If you need to exclude multiple ranges, you must create additional (overlapping) blackout periods. To specify a range, separate the beginning address and ending address with a hyphen. You can use the asterisk (*) as a wild card. The default setting (an asterisk) means all addresses. Wildcards in IP addresses must be at the end of the address as shown, but wildcards for host names must be at the beginning. Examples: • 192.16.12.1-192.16.12.210 • 192.16.12.* • *.domain.com
Start Time	The date and time at which the blackout period begins.
End Time	The date and time at which the blackout period expires.
Time Zone	Select the time zone for the location of the target server that is affected by the blackout. The time zone defaults to the zone in which you are working (see "Configuring Toolbar Options" on page 120). If the target server is in a different time zone, you should usually select the server's time zone and specify the blackout period using local time. For example, if you are in New York City, USA (UTC-05) and the OpenText Fortify WebInspect Enterprise server is in Rome, Italy (UTC+01), and you want to schedule a blackout to begin at 8 a.m. Rome time, you could do either of the following: • Select the UTC+01 time zone (Rome) and specify a Start time of 8 a.m. • Select the UTC-05 time zone (New York City) and specify a Start time of 2 a.m.
Duration	The length of time during which the blackout is in effect. This value is calculated automatically after you specify the Start Time and End Time. Alternatively, if you specify the Start Time and the Duration, the End Time is calculated. If you edit the Duration, the End Time is recalculated. The format is:

Item	Description
	d.hh.mm where d = the number of days hh = the number of hours mm = the number of minutes
Blackout Type	Select one of the following: • **Allow scans during this period**: Scans of the specified targets are allowed only during the specified time period. • **Deny scans during this period**: Scans of the specified targets are prohibited during the specified time period. Allow and deny work very much like allow and deny for permissions. Deny always takes precedence over allow, so a scan can occur only at a particular time if there are no blackout periods that deny that time. An allow blackout period means deny scans UNLESS you are in the allowed range, as opposed to allow scans ONLY if you are in the allowed range. If you configure two separate "allow" blackout periods, a scan will be allowed only during the union of those periods. For example, if period A allows scans from 1 p.m. to 3 p.m. and period B allows scans from 2 p.m. to 6 p.m., then scans will be allowed only from 2 p.m. to 3 p.m.

Blackout: Recurrence

Application Version

Select an application from the **Applications** list and then select a version from the **Application Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Recurring

To schedule a blackout on a recurring basis:

1. Select the **Recurring** check box.
   Do NOT select this option if you want to schedule a one-time-only event.

2. Use the **Pattern** group to select the frequency of the event (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.
3. Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Legacy Scheduled Scan Settings

The following pages describe the Legacy Scheduled Scan settings, including crawl and audit settings.

Legacy Scheduled Scan - Schedule: General

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Enter or select the following settings. Then enter additional settings (as required) using the panels in the left column. To schedule the scan, click **Finish**.

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Schedule Name

Enter a name that identifies this scheduled scan.

Start Time

Enter the date and time you want the scan to begin. You can select the date from a calendar popup and the time from a clock popup.

Time Zone

The time zone for the location of the target server specified for the scheduled scan. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the target server is in a different time zone, you should usually select the server's time zone and specify the **Start Time** using local time. For example, if you are in New York City, USA (UTC-05:00) and the target server is in Rome, Italy (UTC+01:00), and you want to schedule a scan to begin at 8 a.m. Rome time, you could do either of the following:

- Select the UTC+01:00 time zone (Rome) and specify a Start Time of 8 a.m.
- Select the UTC-05:00 time zone (New York City) and specify a Start Time of 2 a.m.

Next Scheduled Time

For a scan that is scheduled to recur, this read-only field displays the time and date of the next scheduled scan.

Last Occurred On

For a scan that is scheduled to recur, this read-only field displays the time and date when a scan last occurred.

Enter other settings as required using the panels in the left column.

> **Note:** Even while the scan is under way, you can change the status of vulnerabilities that have already been identified, add attachments to them, mark them as false positives, or mark them to be ignored.

Legacy Scheduled Scan - Schedule: Recurrence

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Recurring

To schedule a scan on a recurring basis:

1. Select the **Recurring** check box.

   Do NOT select this option if you want to schedule a one-time-only event.

2. Use the **Pattern** group to select the frequency of the event (daily or every *x* days, weekly, monthly, or yearly) and then provide the appropriate information.
3. Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Legacy Scheduled Scan - Scan: General

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan URL

Select one of the following scan types.

Standard Scan

OpenText Fortify WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

1. In the **URL** field, type or select the complete URL or IP address of the site you want to examine.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, you will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

   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 pursue links that use fully qualified URLs (as opposed to relative paths).

   Fortify WebInspect supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets.
2. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:
   - **Directory only (self)** - Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.

- **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

List-Driven Scan

Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility.

- Click **Browse** to select a text file or XML file containing the list of URLs you want to scan.
- Click **View** to view the contents of the selected file.

Workflow-Driven Scan

Fortify WebInspect audits only those URLs included in the macro that you previously recorded and 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, they will all be included in the same scan.

- Click **Browse** and select a macro containing the URLs you want to scan.

Web Service Scan

When performing a Web Service scan, Fortify WebInspect crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

- Click **Browse** to select a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Priority

Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

Sensor

Select which sensor should conduct the scan. You can choose a specific sensor or select the **Any Available** option.

> **Important!** A sensor can perform only one scan at a time. If it is conducting a scan when another scan is scheduled to occur, then:
>
> - If the currently running scan has a higher priority, the Fortify WebInspect Enterprise Manager will place the second scan in a queue until the first scan finishes or until another sensor becomes available.

- If the currently running scan has a lower priority, the Fortify WebInspect Enterprise Manager will suspend that scan, assign the second scan to that sensor, and then reassign the suspended scan to the sensor when the higher priority scan is complete.

Scans that are manually initiated have priority over any scheduled scan.

Legacy Scheduled Scan - Scan Settings: Method

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://*<Fully Qualified Domain Name (FQDN) or HostName>*/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Mode

Select one of the following modes:

- **Crawl Only** - This option completely maps a site's tree structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
- **Crawl and Audit** - As OpenText Fortify WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed. This is described in the Crawl and Audit Mode section as the option to crawl and audit Simultaneously.
- **Audit Only** - Fortify WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

If the selected scan mode is Crawl and Audit, choose one of the following:

- **Simultaneously** - As Fortify WebInspect maps the site’s hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed.

- **Sequentially** - In this mode, Fortify WebInspect crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root. If you select this option, you can specify the order in which the crawl and audit should be conducted.
  - **Test each engine type per session (engine driven)**: Fortify WebInspect audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.
  - **Test each session per engine type (session driven)**: Fortify WebInspect runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Scan Behavior

You can select any of the following optional behaviors:

- **Use a login macro for forms authentication** - This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent Fortify WebInspect from terminating prematurely if it inadvertently logs out of your application. The drop-down list contains the names of all macros that have been uploaded to OpenText Fortify WebInspect Enterprise. Macros that are available in the repository for the selected Application and Application Version are listed with "(Repository)" prepended to the macro name. You can select one of these, or you can click **Browse** to locate a macro and upload it. See "Working with the Macro Repository" on page 173 for more information.

  If you specified login parameters when recording the macro, Fortify WebInspect will substitute these credentials for those used in the macro when it scans a page containing the input control associated with this entry.
- **Use a startup macro** - This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that Fortify WebInspect will use to navigate to that area. It may also include login information, but does not contain logic that will prevent Fortify WebInspect from logging out of your application. Fortify WebInspect visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). The drop-down list contains the names of all macros that have been uploaded to Fortify WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro and upload it.

  > **Important!** Do not use a login macro and a startup macro with the same name. The scan may yield undesirable results.
- **Auto-fill Web forms during crawl** - If you select this option, Fortify WebInspect submits values for input controls found on all HTML forms it encounters while scanning the target site. Fortify WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. Use the **Browse** button to specify the file containing the values you want to use. Alternatively, you can select **Edit** (to modify the currently selected file) or **Create** (to record new Web form values).

Legacy Scheduled Scan - Scan Settings: General

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Details

You may choose the following options:

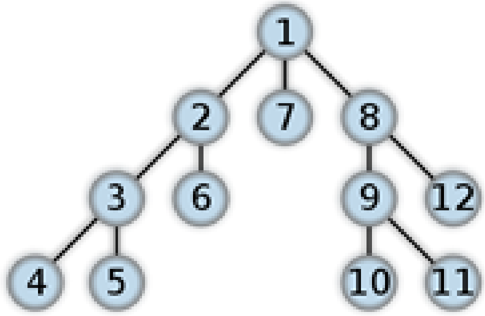
- **Enable Path Truncation** - Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. OpenText Fortify WebInspect truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ will cause the server to reveal directory contents or will cause unhandled exceptions.
- **Attach debug information in request header** - If you select this option, Fortify WebInspect includes a "Memo:" header in the request containing information that can be used by support personnel to diagnose problems.
- **Case-sensitive request and response handling** - Select this option if the server at the target site is case-sensitive to URLs.
- **Compress response data** - If you select this option, Fortify WebInspect saves disk space by storing each HTTP response in a compressed format in the database.
- **Maximum crawl-audit recursion depth** - When an attack reveals a vulnerability, Fortify WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The maximum value is 1,000.

Crawl Details

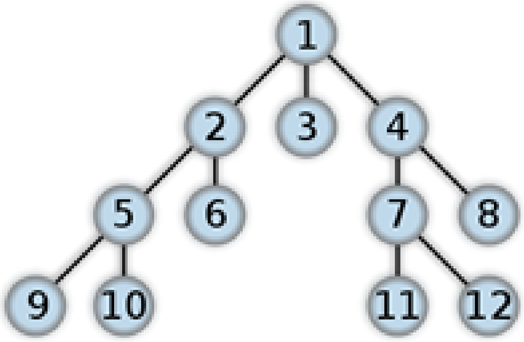
You may choose the following options:

- **Crawler** - Select either **Depth First** or **Breadth First**.

  Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.

  By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.

  When performing a depth-first crawl, Fortify WebInspect pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a “shopping cart” page before accessing the “check-out” page).

- **Enable keyword search audit** - A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.

- **Perform redundant page detection** - Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, Fortify WebInspect would never be able to finish the scan. This option, however, allows Fortify WebInspect to identify and exclude processing of redundant resources.
- **Limit maximum single URL hits to** - Use this field to limit the number of times a single link will be followed during a crawl. Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL.
- **Include parameters in hit count** - If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.

  For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice).
- **Limit maximum link traversal sequence to** - This option restricts the number of hyperlinks that can be sequentially accessed as Fortify WebInspect crawls the site. For example, if five resources are linked as follows:
  - Page A contains a hyperlink to Page B
  - Page B contains a hyperlink to Page C
  - Page C contains a hyperlink to Page D
  - Page D contains a hyperlink to Page E

  And if this option is set to "3," then Page E will not be crawled.

  The default value is 15.
- **Limit maximum crawl folder depth to** - The Crawl Depth value determines how deeply Fortify WebInspect traverses the hierarchical levels of your Web site. If set to 1, Fortify WebInspect drills down one level; if set to 2, Fortify WebInspect drills down two levels; and so on. The maximum value is 1000.
- **Limit maximum crawl count to** - This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.

  Note: The limit set here does not directly correlate to the Crawled progress bar that is displayed during a scan. The maximum crawl count set here applies to links found by the Crawler during a crawl of the application. The Crawled progress bar includes all sessions (requests and responses) that are parsed for links during a crawl and audit, not just the links found by the Crawler during a crawl.
- **Limit maximum Web form submissions to** - Normally, when Fortify WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed. There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one

value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form. Use this setting to limit the total number of submissions that Fortify WebInspect will perform.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

Legacy Scheduled Scan - Scan Settings: Content Analyzers

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Content Analyzers

JavaScript/VBScript - The JavaScript/VBScript analyzer is always enabled. It allows OpenText Fortify WebInspect to crawl links defined by JavaScript or Visual Basic script, and to create and audit any documents rendered by JavaScript. There are settings associated with the JavaScript/VBScript content analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described in "Parser Settings" on the next page.

Flash - If you enable the Flash analyzer, OpenText Fortify WebInspect analyzes Flash files, Adobe's vector graphics-based resizable animation format. There are no associated settings.

Silverlight - If you enable the Silverlight analyzer, Fortify WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment. There are no associated settings.

Parser Settings

There are settings associated with the JavaScript/VBScript analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described below.

- **Crawl links found from script execution** - If you select this option, the crawler will follow dynamic links (that is, links generated during JavaScript or Visual Basic script).
- **Reject script includes to offsite hosts** - Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is <script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>. Fortify WebInspect will download and parse such files, regardless of their origin or file type, unless you select the **Reject Script** option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).
- **Isolate script analysis (out-of-process execution)** - Fortify WebInspect analyzes and executes JavaScript and VBScript to discover links to other resources. Applications or Web sites containing an inordinate number of links can sometimes exhaust the amount of memory allocated to this process. If this occurs, you can assign this function to a separate (remote) process, which will accommodate an infinite number of links. You may, however, notice a slight increase in the amount of time required to scan the site.
- **Create DOM sessions** - Fortify WebInspect creates and saves a session for each change to the Document Object Model (DOM).
- **Verbose script parser debug logging** - If you select this setting and if the Application setting for logging level is set to Debug, Fortify WebInspect logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
- **Log JavaScript errors** - Fortify WebInspect logs JavaScript parsing errors from the script parsing engine.
- **Maximum script events per page** - Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999.

Legacy Scheduled Scan - Scan Settings: Requestor

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://*<Fully Qualified Domain Name (FQDN) or HostName>*/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Requestor Performance

Select one of the following options:

- **Use a shared requestor** - If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of OpenText Fortify WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
- **Use separate requestors** - If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

  When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl requestor thread count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5. The **Audit requestor thread count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

Note: Depending on the capacity of the application being scanned, increasing thread counts may increase request failures due to increased load on the server, causing some responses to exceed the **Request timeout** setting. Request failures may reduce scan coverage because the responses that failed may have exposed additional attack surface or revealed vulnerabilities. If you notice increased request failures, you might reduce them by either increasing the **Request timeout** or reducing the **Crawl requestor thread count** and **Audit requestor thread count**.
Also, depending on the nature of the application being scanned, increased crawl thread counts may reduce consistency between subsequent scans of the same site due to differences in crawl request ordering. By reducing the default **Crawl requestor thread count** setting to 1, consistency may be increased.

Requestor Settings

You may select the following options:

- **Limit maximum response size to** - Select this option to limit the size of accepted server responses and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
- **Request retry count** - Specify how many times Fortify WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
- **Request timeout** - Specify how long Fortify WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, Fortify WebInspect resubmits the request until reaching the retry count. If Fortify WebInspect then receives no response, it logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct Fortify WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

> **Note:** If these options are selected and the **Request timeout** setting (above) is reached, the scan may stop when the server does not respond within the period set for the Request timeout. If the server responds with the extended Request timeout period, then the extended period becomes the new Request timeout for the current scan.

The following options are available:

- **Consecutive "single host" retry failures to stop scan** - Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.
- **Consecutive "any host" retry failures to stop scan** - Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.
- **Nonconsecutive "single host" retry failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
- **Nonconsecutive "any host" request failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.
- **If first request fails, stop scan** - Selecting this option will force Fortify WebInspect to terminate the scan if the target server does not respond to Fortify WebInspect's first request.
- **Response codes to stop scan if received** - Enter the HTTP status codes that, if received, will force Fortify WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Legacy Scheduled Scan - Scan Settings: Session Storage

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the database. This saved information can be used for two purposes.

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, OpenText Fortify WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Fortify Customer Support personnel can extract the generated (but not sent) HTTP requests for analysis. Sessions may be rejected for the reasons cited in the following table.

Reject Reason	Explanation
Invalid Host	Any host that is not specified as an Allowed Host.
Excluded File Extension	Files having an extension that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected File Extensions.
Excluded URL	URLs or hosts that are excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected URLs and Hosts.
Outside Root URL	If the **Restrict to Folder** option is selected when starting a scan, any resource not qualified by the available options (Directory Only, Directory and Subdirectories, or Directory and Parent Directories).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the **Limit maximum crawl folder depth to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the **Limit Maximum Single URL hits to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
404 Response Code	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine File Not Found (FNF) using HTTP response**

Reject Reason	Explanation
	codes is selected and the response contains a code that matches the requirements.
Solicited File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Auto detect FNF page** is selected and Fortify WebInspect determined that the response constituted a "file not found" condition.
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine FNF from custom supplied signature** is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

Session Storage

Fortify WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

Legacy Scheduled Scan - Scan Settings: Session Exclusions

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Note: The following settings apply to both the crawl and audit phases of a scan. To specify exclusions for only the crawl or only the audit, use the Crawl Settings - Session Exclusions or the Audit Settings - Sessions Exclusions.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not request files of the type you specify.
- **Exclude** - Fortify WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

Excluded MIME Types

Fortify WebInspect will not process files associated with the MIME type you specify. For more information, see "MIME Types" on page 230.

Excluded or Rejected URLs and Hosts

You can identify a URL or host (using a regular expression) and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

You must use a regular expression to designate a host or URL.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following regular expression and select **Reject**.

Microsoft\.com

Note that the period (or dot) is preceded by a backslash, indicating that the next character is special (that is, it is not the character used in regular expressions to match any single character except a newline character).

Example 2

Enter a string such as logout. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the logout example, Fortify WebInspect will exclude or reject URLs such as logout.asp or applogout.jsp.

Example 3

If you enter /myApp /

then Fortify WebInspect will exclude or reject all resources in the myApp directory, such as:

http://www.test.me /myApp /filename.htm

If you enter /W3SVC[0-9]*/

then Fortify WebInspect will exclude or reject the following directories:

- http://www.test.me /W3SVC55/
- http://www.test.me /W3SVC5/
- http://www.test.me/W3SVC550/

Adding a URL or Host

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either **Host** or **URL**.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one of the following:
   - Reject - Do not send request to targeted URL or host.
   - Exclude - Send request, but do not process response.
5. Click **Update**.

Legacy Scheduled Scan - Scan Settings: Allowed Hosts

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Allowable Hosts for Crawl and Audit

Use the Allowed Host settings to add domains that may be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl or audit.

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 OpenText Fortify WebInspect 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, Fortify WebInspect 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

Note: If you specify a port number, then the allowed host must be an exact match.

If you use a regular expression to specify a host, select **Regex**.

Legacy Scheduled Scan - Scan Settings: HTTP Parsing

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then OpenText Fortify WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, "userid" is the parameter you would identify.

> **Note:** You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

Fortify WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "1234567" is the session information:

http://www.onlinestore.com/bikes/(1234567)/index.html

The regular expression for identifying the parameter would be: /\([\w\d]+\)/

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. Two default regular expressions identify two ASP.NET cookieless session IDs. The third regular expression matches jsessionid cookie.

HTTP Parameters Used for Navigation

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

- http://www.anysite.com?Master.asp?Page=1
- http://www.anysite.com?Master.asp?Page=2;
- http://www.anysite.com?Master.asp?Page=13;Subpage=4

Ordinarily, Fortify WebInspect would assume that these three requests refer to identical resources and would scan only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

The first and second examples contain one resource parameter: "Page." The third example contains two parameters: "Page" and "Subpage."

To identify resource parameters:

1. Click **Add**.
2. Enter the parameter name and click **Update**.

   The string you entered appears in the **Parameter** list.
3. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) Fortify WebInspect should use.

Legacy Scheduled Scan - Scan Settings: Filters

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Using Filters

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use Fortify WebInspect or those who have access to the raw data.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

Adding a Regular Expression Rule

To add a regular expression rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.
2. From the **Section** list, select an area to search.
3. In the **Find Condition** field, type (or paste) the string you want to locate (or enter a regular expression that describes the string). You can also click the list button to insert regular expression elements.
4. Type (or paste) the replacement string in the **Replace** field.

5. For case-sensitive searches, select the **Case-Sensitive** check box.
6. Click **Update**.

Legacy Scheduled Scan - Scan Settings: Cookies/Headers

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Standard Header Parameters

You can elect to include referer and/or host headers in requests sent by OpenText Fortify WebInspect.

- **Include 'referer' in HTTP request headers** - Select this check box to include referer headers in HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
- **Include 'host' in HTTP request headers** - Select this check box to include host headers with HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit Fortify WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when Fortify WebInspect is auditing that site. You can add multiple custom headers.

To add a custom header:

1. In the top box, enter the header using the format <name>: <value>.
2. Click **Add**.

The new header appears in the list of custom headers.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by Fortify WebInspect to the server when conducting a scan.

To add a custom cookie:

1. In the top box, enter the header using the format <name>=<value>. For example, if you enter
   CustomCookie=ScanEngine
   then each HTTP-Request will contain the following header:
   Cookie: CustomCookie=ScanEngine
2. Click **Add**.

The new cookie appears in the list of custom cookies.

Legacy Scheduled Scan - Scan Settings: Proxy

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://*<Fully Qualified Domain Name (FQDN) or HostName>*/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Proxy Settings

Select one of the following options:

- **Direct Connection (proxy disabled)** - Select this option if you are not using a proxy server.
- **Automatically detect proxy settings** - If you select this option, OpenText Fortify WebInspect will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's web proxy settings.
- **Use System proxy settings** - Select this option to use the proxy server settings on the machine that will conduct the scan.
- **Use Firefox proxy settings** - Select this option to use the proxy server settings configured for the Firefox browser on the machine that will conduct the scan.

> **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the browser connection settings are not configured for proxy, then a proxy server will not be used.

- **Configure a proxy using a PAC file URL** - Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** field.
- **Explicitly configure proxy** - Select this option to access the Internet through a proxy server, and then enter the requested information:
  a. In the **Server** field, type the URL or IP address of your proxy server.
  b. In the **Port** field, enter the port number (for example, 8080).
  c. Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.
  d. If your proxy server requires authentication, enter the qualifying user name and password.
  e. 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 Proxy For** field. Use commas to separate entries.

  For proxy servers accepting https connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information.

Legacy Scheduled Scan - Scan Settings: Authentication

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Requires Network Authentication

Select this option if users must log on to your Web site or application. Then select an authentication method and specify a user name and password.

> **Caution!** OpenText Fortify WebInspect will crawl 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 a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact Fortify Customer Support.

The authentication methods are:

Basic

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a dialog box for a user to enter a previously assigned user name and password and then attempts to establish a connection to a server using the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.

NTLM

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 Fortify WebInspect has to pass through a proxy server to submit its requests to the Web server, Fortify WebInspect may not be able to crawl or audit that Web site. Use caution when configuring Fortify WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

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. This authentication method will be successful only if the Web server has been configured to return a response header of “WWW-Authenticate: Kerberos” instead of “WWW-Authenticate: Negotiate.”

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.

Automatic

Allow Fortify WebInspect 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 is noticeably improved.

Client Certificates

Client certificate authentication allows users to present client certificates rather than entering a user name and password.

To use client certificates:

1. Select **Use Client Certificate**.
2. Click **Browse** to choose a certificate.

Legacy Scheduled Scan - Scan Settings: File Not Found

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Determine File Not Found (FNF) Using HTTP Response Codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.

- **Forced valid response codes (never an FNF)**: You can specify HTTP response codes that should never be treated as a file-not-found response.
- **Forced FNF response codes (always an FNF)**: Specify those HTTP response codes that will always be treated as a file-not-found response. OpenText Fortify WebInspect will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a semicolon.

Determine File Not Found from Custom Supplied Signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result from 404 pages that are unique to your site.

You can specify a signature using plain text, a regular expression, or, using the **SPI Regex** option. For information about the Regular Expression Editor tool, see the *OpenText™ Fortify WebInspect Tools Guide*.

Auto-Detect File Not Found Page

Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found. Select this check box if you want Fortify WebInspect to detect these "custom" file-not-found pages.

Fortify WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you select the **Auto-Detect File Not Found Page** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

Legacy Scheduled Scan - Scan Settings: Policy

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Scan Policy

Select a policy. A policy is a collection of audit engines and attack agents that Fortify WebInspect uses when auditing or crawling your Web application. Each component has a specific task, such as testing for cross-site scripting susceptibility, building the site tree, probing for known server vulnerabilities, etc. For policy descriptions, see "Policies List" on page 155.

Legacy Scheduled Scan - Crawl Settings: Link Parsing

Note: The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Link Parsing

OpenText Fortify WebInspect follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature to identify (using regular expressions) links that you want Fortify WebInspect to follow.

To add a specialized link identifier:

1. Click **Add**.
2. In the **Custom Links** field, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comments** field.
4. Click **Update**.

Legacy Scheduled Scan - Crawl Settings: Session Exclusions

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

> **Note:** All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Crawl Settings - Session Exclusions) enables you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

Follow the steps below to add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. For more information, see "MIME Types" on page 230.

Follow the steps below to add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

Follow the steps below to add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host
   - **Exclude** - Send request, but do not process response
5. Click **Update**.

Legacy Scheduled Scan - Audit Settings: Session Exclusions

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Audit Settings - Session Exclusions) enables you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. For more information, see "MIME Types" on page 230.

To add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.

3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host.
   - **Exclude** - Send request, but do not process response.
5. Click **Update**.

Legacy Scheduled Scan - Audit Settings: Attack Exclusions

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Excluded Parameters

Use this feature to prevent OpenText Fortify WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

1. In the Excluded Parameters group, click **Add**.
2. In the **Parameter** field, enter the name of the parameter you want to exclude.
3. Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.
4. Click **Update**.

Excluded Cookies

Use this feature to prevent Fortify WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values. This setting requires you to enter the name of a cookie.

In the following example HTTP response, the name of the cookie is "FirstCookie."

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

To exclude certain cookies:

1. In the Excluded Cookies group, click **Add**.
2. In the **Parameter** field, type a cookie name or enter a regular expression that you believe will match the cookies you want to exclude.
3. Click **Update**.

Excluded Headers

Use this feature to prevent Fortify WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression as follows:

1. In the Excluded Headers group, click **Add**.
2. In the **Parameter** field, type a header name or enter a regular expression that you believe will match the headers you want to exclude.
3. Click **Update**.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs.

To load inputs that you previously created using the editor, click the **Browse** button next to the **Import Audit Inputs** button.

Legacy Scheduled Scan - Audit Settings: Attack Expressions

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- ja-jp: Japanese - Japan
- ko-Kr: Korean - Korea
- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan
- es-mx: Spanish - Mexico

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Legacy Scheduled Scan - Audit Settings: Vulnerability Filters

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Select Vulnerability Filters to Enable

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition** - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.

- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection Dom Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

To add a filter to your default settings, select a filter in the **Available** area and click **>**. The filter is removed from the **Available** list and added to the **Selected** list.

To disable a filter, select a filter in the **Selected** list and click **<**. The filter is removed from the **Selected** list and added to the **Available** list.

To add all available filters, click **>>**.

To remove all selected filters, click **<<**.

Legacy Scheduled Scan - Audit Settings: Smart Scan

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, OpenText Fortify WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select **Enable Smart Scan**, you can choose one or both of the identification methods described below.

- **Use regular expressions on HTTP responses** - This method searches the server response for strings that match predefined regular expressions designed to identify specific servers.
- **Use server analyzer fingerprinting and request sampling** - This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server type.

Custom Server/Application Type Definitions (more accurate detection)

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions (more accurate detection)** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.
2. In the **Host** field, enter the domain name or host, or the server's IP address.
3. Select one or more entries from the **Server/Application** list.
4. Click **OK**.

Legacy Scheduled Scan - Scan Behavior: Blackout Action

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Blackout Action

A blackout period is a block of time during which scans are not permitted.

If a blackout period begins while a scan is running, you may either stop the scan or suspend it. The sensor will resume a suspended scan when the blackout period ends.

Legacy Scheduled Scan - Export: General

> **Note:** The Legacy Scheduled Scan page is not available in the OpenText Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanSchedule.aspx

Project Version

Select a project from the **Projects** list and then select a version from the **Project Versions** list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template.

Export Scan Results

Select this option to export the scan results. Then provide the requested information.

- **Export Path** - Select a destination for the exported scan. Export paths are designated using the Fortify WebInspect Enterprise console. Contact your Fortify WebInspect Enterprise administrator if no paths are available.
- **Export Format** - Select how you want the exported file to be formatted. Your choices are WebInspect Scan File (.scan) or Extensible Markup Language (.xml).
- **Automatically generate file name** - If you select this option, the name of the file will be formatted as <scan name> <date/time>.[xml or scan]. For example, if the scan name is "mysite" and the scan is generated at 6:30 on April 5, the file name would be "mysite 04_05_2007 06_30.scan [or .xml]." This is useful for recurring scans.

  If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **File Name** field.

Legacy Scan Template Settings

The following pages describe the Legacy Scan Template settings, including crawl and audit settings.

Legacy Scan Template - Scan: General

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://*<Fully Qualified Domain Name (FQDN) or HostName>*/WIE/WebConsole/LegacyScanTemplate.aspx

When you click the **Add** button to add a scan template, the Configure Scan Template page opens with the SCAN: General category selected and its form displayed. When you click the template name to view or edit an existing scan template, the fields described below have already been specified (except where noted).

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Because the global scan template can be associated with any project version, you do not have to specify the **URL** if you choose a Standard Scan in the Scan URL section of the form. You can subsequently select this global template as the scan template for any Web Site Scan.

Automatically Update Related Scheduled Scans

This option is available only while editing an existing scan template. Select the **Update Scheduled Scans** check box to propagate the revised template to all scheduled scans that use the template. The revised settings are propagated to the scheduled scans upon saving the template.

If you do not select the check box, the changes are saved only in the template.

Scan Template Created From

This is a read-only field indicating the source of the settings. If you started to create the template by clicking **Add**, you are using default settings. If you started to create the template by clicking **Import**, you are using settings optimized for the **Import** submenu option you selected—**Oracle Settings** or **Websphere Settings**.

Scan Template Name

Enter a name for this template.

Scan URL

Select one of the following scan types.

Standard Scan

OpenText Fortify WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.

1. In the **URL** field, type or select the complete URL or IP address of the site you want to examine.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, you will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

   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 pursue links that use fully qualified URLs (as opposed to relative paths).

   Fortify WebInspect supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). IPV6 addresses must be enclosed in brackets.
2. If you select **Restrict to folder**, you can limit the scope of the scan to the area you choose from the drop-down list. The choices are:
   - **Directory only (self)** - Fortify WebInspect will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify

WebInspect will assess only the "two" directory.

- **Directory and subdirectories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories** - Fortify WebInspect will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

List-Driven Scan

Perform a scan using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). You can use a text file, formatted as comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility.

- Click **Browse** to select a text file or XML file containing the list of URLs you want to scan.
- Click **View** to view the contents of the selected file.

Workflow-Driven Scan

Fortify WebInspect audits only those URLs included in the macro that you previously recorded and 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, they will all be included in the same scan.

- Click **Browse** and select a macro containing the URLs you want to scan.

Web Service Scan

When performing a Web Service scan, Fortify WebInspect crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

- Click **Browse** to select a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Legacy Scan Template - Scan Settings: Method

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Scan Mode

Select one of the following modes:

- **Crawl Only** - This option completely maps a site's tree structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
- **Crawl and Audit** - As OpenText Fortify WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed. This is described in the Crawl and Audit Mode section as the option to crawl and audit Simultaneously.
- **Audit Only** - Fortify WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

If the selected scan mode is Crawl and Audit, choose one of the following:

- **Simultaneously** - As Fortify WebInspect maps the site’s hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed.
- **Sequentially** - In this mode, Fortify WebInspect crawls the entire site, mapping the site’s hierarchical data structure, and then conducts a sequential audit, beginning at the site’s root. If you select this option, you can specify the order in which the crawl and audit should be conducted.
  - **Test each engine type per session (engine driven)**: Fortify WebInspect audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.
  - **Test each session per engine type (session driven)**: Fortify WebInspect runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Scan Behavior

You can select any of the following optional behaviors:

- **Use a login macro for forms authentication** - This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent Fortify WebInspect from terminating prematurely if it inadvertently logs out of your application. The drop-down list contains the names of all macros that have been uploaded to OpenText Fortify WebInspect Enterprise. Macros that are available in the repository for the selected Application and Application Version are listed with “(Repository)” prepended to the macro name. You can select one of these, or you can click **Browse** to locate a macro and upload it. See "Working with the Macro Repository" on page 173 for more information.

If you specified login parameters when recording the macro, Fortify WebInspect will substitute these credentials for those used in the macro when it scans a page containing the input control associated with this entry.

- **Use a startup macro** - This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that Fortify WebInspect will use to navigate to that area. It may also include login information, but does not contain logic that will prevent Fortify WebInspect from logging out of your application. Fortify WebInspect visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). The drop-down list contains the names of all macros that have been uploaded to Fortify WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro and upload it.

  > **Important!** Do not use a login macro and a startup macro with the same name. The scan may yield undesirable results.

- **Auto-fill Web forms during crawl** - If you select this option, Fortify WebInspect submits values for input controls found on all HTML forms it encounters while scanning the target site. Fortify WebInspect will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. Use the **Browse** button to specify the file containing the values you want to use. Alternatively, you can select **Edit** (to modify the currently selected file) or **Create** (to record new Web form values).

Legacy Scan Template - Scan Settings: General

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Scan Details

You may choose the following options:

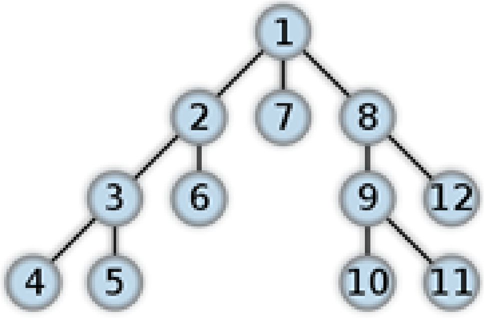
- **Enable Path Truncation** - Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. OpenText Fortify WebInspect truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ will cause the server to reveal directory contents or will cause unhandled exceptions.
- **Attach debug information in request header** - If you select this option, Fortify WebInspect includes a "Memo:" header in the request containing information that can be used by support personnel to diagnose problems.
- **Case-sensitive request and response handling** - Select this option if the server at the target site is case-sensitive to URLs.
- **Compress response data** - If you select this option, Fortify WebInspect saves disk space by storing each HTTP response in a compressed format in the database.
- **Maximum crawl-audit recursion depth** - When an attack reveals a vulnerability, Fortify WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The maximum value is 1,000.

Crawl Details

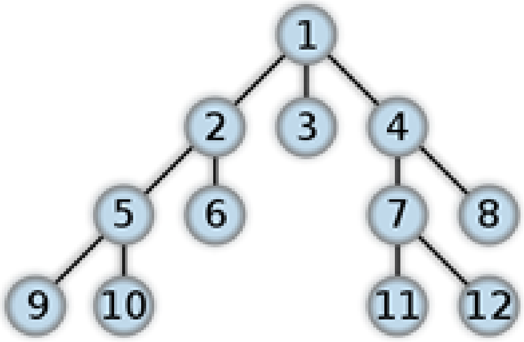
You may choose the following options:

- **Crawler** - Select either **Depth First** or **Breadth First**.

  Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn't finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6.



By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



When performing a depth-first crawl, Fortify WebInspect pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a “shopping cart” page before accessing the “check-out” page).

- **Enable keyword search audit** - A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
- **Perform redundant page detection** - Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, Fortify WebInspect would never be able to finish the scan. This option, however, allows Fortify WebInspect to identify and exclude processing of redundant resources.
- **Limit maximum single URL hits to** - Use this field to limit the number of times a single link will be followed during a crawl. Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL.
- **Include parameters in hit count** - If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count.

  For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice).

- **Limit maximum link traversal sequence to** - This option restricts the number of hyperlinks that can be sequentially accessed as Fortify WebInspect crawls the site. For example, if five resources are linked as follows:
  - Page A contains a hyperlink to Page B
  - Page B contains a hyperlink to Page C
  - Page C contains a hyperlink to Page D
  - Page D contains a hyperlink to Page E

  And if this option is set to "3," then Page E will not be crawled.

  The default value is 15.
- **Limit maximum crawl folder depth to** - The Crawl Depth value determines how deeply Fortify WebInspect traverses the hierarchical levels of your Web site. If set to 1, Fortify WebInspect drills down one level; if set to 2, Fortify WebInspect drills down two levels; and so on. The maximum value is 1000.
- **Limit maximum crawl count to** - This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.

  Note: The limit set here does not directly correlate to the Crawled progress bar that is displayed during a scan. The maximum crawl count set here applies to links found by the Crawler during a crawl of the application. The Crawled progress bar includes all sessions (requests and responses) that are parsed for links during a crawl and audit, not just the links found by the Crawler during a crawl.
- **Limit maximum Web form submissions to** - Normally, when Fortify WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed. There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form. Use this setting to limit the total number of submissions that Fortify WebInspect will perform.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

Legacy Scan Template - Scan Settings: Content Analyzers

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

```
https://<Fully Qualified Domain Name (FQDN) or
HostName>/WIE/WebConsole/LegacyScanTemplate.aspx
```

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Content Analyzers

JavaScript/VBScript - The JavaScript/VBScript analyzer is always enabled. It allows OpenText Fortify WebInspect to crawl links defined by JavaScript or Visual Basic script, and to create and audit any documents rendered by JavaScript. There are settings associated with the JavaScript/VBScript content analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described in "Parser Settings" below.

Flash - If you enable the Flash analyzer, OpenText Fortify WebInspect analyzes Flash files, Adobe's vector graphics-based resizable animation format. There are no associated settings.

Silverlight - If you enable the Silverlight analyzer, Fortify WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment. There are no associated settings.

Parser Settings

There are settings associated with the JavaScript/VBScript analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described below.

- **Crawl links found from script execution** - If you select this option, the crawler will follow dynamic links (that is, links generated during JavaScript or Visual Basic script).
- **Reject script includes to offsite hosts** - Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript "include file" request is <script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>. Fortify WebInspect will download and parse such files, regardless of their origin or file type, unless you select the **Reject Script** option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).
- **Isolate script analysis (out-of-process execution)** - Fortify WebInspect analyzes and executes JavaScript and VBScript to discover links to other resources. Applications or Web sites containing an inordinate number of links can sometimes exhaust the amount of memory allocated to this process. If this occurs, you can assign this function to a separate (remote) process, which will accommodate an infinite number of links. You may, however, notice a slight increase in the amount

of time required to scan the site.

- **Create DOM sessions** - Fortify WebInspect creates and saves a session for each change to the Document Object Model (DOM).
- **Verbose script parser debug logging** - If you select this setting and if the Application setting for logging level is set to Debug, Fortify WebInspect logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
- **Log JavaScript errors** - Fortify WebInspect logs JavaScript parsing errors from the script parsing engine.
- **Maximum script events per page** - Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999.

Legacy Scan Template - Scan Settings: Requestor

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://*<Fully Qualified Domain Name (FQDN) or HostName>*/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Requestor Performance

Select one of the following options:

- **Use a shared requestor** - If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of OpenText Fortify WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
- **Use separate requestors** - If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

  When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl requestor thread count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5. The **Audit requestor thread count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

Note: Depending on the capacity of the application being scanned, increasing thread counts may increase request failures due to increased load on the server, causing some responses to exceed the **Request timeout** setting. Request failures may reduce scan coverage because the responses that failed may have exposed additional attack surface or revealed vulnerabilities. If you notice increased request failures, you might reduce them by either increasing the **Request timeout** or reducing the **Crawl requestor thread count** and **Audit requestor thread count**.
Also, depending on the nature of the application being scanned, increased crawl thread counts may reduce consistency between subsequent scans of the same site due to differences in crawl request ordering. By reducing the default **Crawl requestor thread count** setting to 1, consistency may be increased.

Requestor Settings

You may select the following options:

- **Limit maximum response size to** - Select this option to limit the size of accepted server responses and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
- **Request retry count** - Specify how many times Fortify WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
- **Request timeout** - Specify how long Fortify WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, Fortify WebInspect resubmits the request until reaching the retry count. If Fortify WebInspect then receives no response, it logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct Fortify WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

Note: If these options are selected and the **Request timeout** setting (above) is reached, the scan may stop when the server does not respond within the period set for the Request timeout. If the server responds with the extended Request timeout period, then the extended period becomes the new Request timeout for the current scan.

The following options are available:

- **Consecutive "single host" retry failures to stop scan** - Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.
- **Consecutive "any host" retry failures to stop scan** - Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.

- **Nonconsecutive "single host" retry failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
- **Nonconsecutive "any host" request failures to stop scan** - Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.
- **If first request fails, stop scan** - Selecting this option will force Fortify WebInspect to terminate the scan if the target server does not respond to Fortify WebInspect's first request.
- **Response codes to stop scan if received** - Enter the HTTP status codes that, if received, will force Fortify WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Legacy Scan Template - Scan Settings: Session Storage

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the database. This saved information can be used for two purposes, as follows:

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, OpenText Fortify WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Fortify Customer Support personnel can extract the generated (but not sent) HTTP requests for analysis. Sessions may be rejected for the reasons cited in the following table:

Reject Reason	Explanation
Invalid Host	Any host that is not specified as an Allowed Host.
Excluded File Extension	Files having an extension that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected

Reject Reason	Explanation
	File Extensions; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected File Extensions; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected File Extensions.
Excluded URL	URLs or hosts that are excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded or Rejected URLs and Hosts; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded or Rejected URLs and Hosts.
Outside Root URL	If the **Restrict to Folder** option is selected when starting a scan, any resource not qualified by the available options (Directory Only, Directory and Subdirectories, or Directory and Parent Directories).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the **Limit maximum crawl folder depth to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the **Limit Maximum Single URL hits to** option in Default (or Current) Scan Settings/Scan Settings/General has been exceeded.
404 Response Code	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine File Not Found (FNF) using HTTP response codes** is selected and the response contains a code that matches the requirements.
Solicited File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Auto detect FNF page** is selected and Fortify WebInspect determined that the response constituted a "file not found" condition.
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine FNF from custom supplied signature** is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

Reject Reason	Explanation
Custom File Not Found	In the Default (or Current) Scan Settings/Scan Settings/File Not Found group, the option **Determine FNF from custom supplied signature** is selected and the response contains one of the specified phrases.
Rejected Response	Files having a MIME type that is excluded by settings specified in Default (or Current) Scan Settings/Scan Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Crawl Settings/Session Exclusions/Excluded MIME Types; also Default (or Current) Scan Settings/Audit Settings/Session Exclusions/Excluded MIME Types.

Session Storage

Fortify WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

Legacy Scan Template - Scan Settings: Session Exclusions

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Note: The following settings apply to both the crawl and audit phases of a scan. To specify exclusions for only the crawl or only the audit, use the Crawl Settings - Session Exclusions or the Audit Settings - Sessions Exclusions.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not request files of the type you specify.
- **Exclude** - Fortify WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

Excluded MIME Types

Fortify WebInspect will not process files associated with the MIME type you specify. For more information, see "MIME Types" on page 230.

Excluded or Rejected URLs and Hosts

You can identify a URL or host (using a regular expression) and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

You must use a regular expression to designate a host or URL.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following regular expression and select **Reject**.

Microsoft\.com

Note that the period (or dot) is preceded by a backslash, indicating that the next character is special (that is, it is not the character used in regular expressions to match any single character except a newline character).

Example 2

Enter a string such as logout. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the logout example, Fortify WebInspect will exclude or reject URLs such as logout.asp or applogout.jsp.

Example 3

If you enter /myApp /

then Fortify WebInspect will exclude or reject all resources in the myApp directory, such as:

http://www.test.me /myApp /filename.htm

If you enter /W3SVC[0-9]*/

then Fortify WebInspect will exclude or reject the following directories:

- http://www.test.me /W3SVC55/
- http://www.test.me /W3SVC5/
- http://www.test.me/W3SVC550/

Adding a URL or Host

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either **Host** or **URL**.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one of the following:
   - Reject - Do not send request to targeted URL or host.
   - Exclude - Send request, but do not process response.
5. Click **Update**.

Legacy Scan Template - Scan Settings: Allowed Hosts

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Allowable Hosts for Crawl and Audit

Use the Allowed Host settings to add domains that may be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl or audit.

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 OpenText Fortify WebInspect 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, Fortify WebInspect 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

Note: If you specify a port number, then the allowed host must be an exact match.

If you use a regular expression to specify a host, select **Regex**.

Legacy Scan Template - Scan Settings: HTTP Parsing

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then OpenText Fortify WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, "userid" is the parameter you would identify.

Note: You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

Fortify WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "1234567" is the session information:

http://www.onlinestore.com/bikes/(1234567)/index.html

The regular expression for identifying the parameter would be: /\([\w\d]+\)/

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. Two default regular expressions identify two ASP.NET cookieless session IDs. The third regular expression matches jsessionid cookie.

HTTP Parameters Used for Navigation

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

- http://www.anysite.com?Master.asp?Page=1
- http://www.anysite.com?Master.asp?Page=2;
- http://www.anysite.com?Master.asp?Page=13;Subpage=4

Ordinarily, Fortify WebInspect would assume that these three requests refer to identical resources and would scan only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

The first and second examples contain one resource parameter: "Page." The third example contains two parameters: "Page" and "Subpage."

To identify resource parameters:

1. Click **Add**.
2. Enter the parameter name and click **Update**.

   The string you entered appears in the **Parameter** list.
3. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) Fortify WebInspect should use.

Legacy Scan Template - Scan Settings: Filters

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

Adding a Regular Expression Rule

To add a regular expression rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.
2. From the **Section** list, select an area to search.
3. In the **Find Condition** field, type (or paste) the string you want to locate (or enter a regular expression that describes the string). You can also click the list button to insert regular expression elements.
4. Type (or paste) the replacement string in the **Replace** field.
5. For case-sensitive searches, select the **Case-Sensitive** check box.
6. Click **Update**.

Legacy Scan Template - Scan Settings: Cookies/Headers

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Standard Header Parameters

You can elect to include referer and/or host headers in requests sent by OpenText Fortify WebInspect.

- **Include 'referer' in HTTP request headers** - Select this check box to include referer headers in HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
- **Include 'host' in HTTP request headers** - Select this check box to include host headers with HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit Fortify WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when Fortify WebInspect is auditing that site. You can add multiple custom headers.

To add a custom header:

1. In the top box, enter the header using the format <name>: <value>.
2. Click **Add**.

The new header appears in the list of custom headers.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by Fortify WebInspect to the server when conducting a scan.

To add a custom cookie:

1. In the top box, enter the header using the format <name>=<value>. For example, if you enter

   CustomCookie=ScanEngine

   then each HTTP-Request will contain the following header:

   Cookie: CustomCookie=ScanEngine
2. Click **Add**.

The new cookie appears in the list of custom cookies.

Legacy Scan Template - Scan Settings: Proxy

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Proxy Settings

Select one of the following options:

- **Direct Connection (proxy disabled)** - Select this option if you are not using a proxy server.
- **Automatically detect proxy settings** - If you select this option, OpenText Fortify WebInspect will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's web proxy settings.
- **Use System proxy settings** - Select this option to use the proxy server settings on the machine that will conduct the scan.
- **Use Firefox proxy settings** - Select this option to use the proxy server settings configured for the Firefox browser on the machine that will conduct the scan.

> **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the browser connection settings are not configured for proxy, then a proxy server will not be used.

- **Configure a proxy using a PAC file URL** - Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** field.
- **Explicitly configure proxy** - Select this option to access the Internet through a proxy server, and then enter the requested information:
  a. In the **Server** field, type the URL or IP address of your proxy server.
  b. In the **Port** field, enter the port number (for example, 8080).
  c. Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.
  d. If your proxy server requires authentication, enter the qualifying user name and password.
  e. 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 Proxy For** field. Use commas to separate entries.

  For proxy servers accepting https connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information.

Legacy Scan Template - Scan Settings: Authentication

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Scan Requires Network Authentication

Select this option if users must log on to your Web site or application. Then select an authentication method and specify a user name and password.

> **Caution!** OpenText Fortify WebInspect will crawl 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 a user name and password that has administrative rights. If

you are unsure about your access rights, contact your System Administrator or internal security professional, or contact Fortify Customer Support.

The authentication methods are:

Basic

A widely used, industry-standard method for collecting user name and password information. The Web browser displays a dialog box for a user to enter a previously assigned user name and password and then attempts to establish a connection to a server using the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.

NTLM

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 Fortify WebInspect has to pass through a proxy server to submit its requests to the Web server, Fortify WebInspect may not be able to crawl or audit that Web site. Use caution when configuring Fortify WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

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. This authentication method will be successful only if the Web server has been configured to return a response header of “WWW-Authenticate: Kerberos” instead of “WWW-Authenticate: Negotiate.”

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.

Automatic

Allow Fortify WebInspect 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 is noticeably improved.

Client Certificates

Client certificate authentication allows users to present client certificates rather than entering a user name and password.

To use client certificates:

1. Select **Use Client Certificate**.
2. Click **Browse** to choose a certificate.

Legacy Scan Template - Scan Settings: File Not Found

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Determine File Not Found (FNF) Using HTTP Response Codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.

- **Forced valid response codes (never an FNF)**: You can specify HTTP response codes that should never be treated as a file-not-found response.
- **Forced FNF response codes (always an FNF)**: Specify those HTTP response codes that will always be treated as a file-not-found response. OpenText Fortify WebInspect will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a semicolon.

Determine File Not Found from Custom Supplied Signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result from 404 pages that are unique to your site.

You can specify a signature using plain text, a regular expression, or, using the **SPI Regex** option. For information about the Regular Expression Editor tool, see the *OpenText™ Fortify WebInspect Tools Guide*.

Auto-Detect File Not Found Page

Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found. Select this check box if you want Fortify WebInspect to detect these "custom" file-not-found pages.

Fortify WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you select the **Auto-Detect File Not Found Page** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

Legacy Scan Template - Scan Settings: Policy

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Scan Policy

Select which policy will be used by this template. A policy is a collection of audit engines and attack agents that Fortify WebInspect uses when auditing or crawling your Web application. Each component has a specific task, such as testing for cross-site scripting susceptibility, building the site tree, probing for known server vulnerabilities, etc. For policy descriptions, see "Policies List" on page 155.

Legacy Scan Template - Crawl Settings: Link Parsing

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Link Parsing

OpenText Fortify WebInspect follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature to identify (using regular expressions) links that you want Fortify WebInspect to follow.

To add a specialized link identifier:

1. Click **Add**.
2. In the **Custom Links** field, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comments** field.
4. Click **Update**.

Legacy Scan Template - Crawl Settings: Session Exclusions

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Session Exclusions Note: All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Crawl Settings - Session Exclusions) enables you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. For more information, see "MIME Types" on page 230.

To add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host
   - **Exclude** - Send request, but do not process response
5. Click **Update**.

Legacy Scan Template - Audit Settings: Session Exclusions

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Audit Settings - Session Exclusions) enables you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

To add a file extension:

1. Click **Add**.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. For more information, see "MIME Types" on page 230.

To add a MIME Type:

1. Click **Add**.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option.

To add a URL or host:

1. Click **Add**.
2. From the **Type** list, select either Host or URL.
3. In the **URLs and Hosts** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select one or both of the following:
   - **Reject** - Do not send request to targeted URL or host.
   - **Exclude** - Send request, but do not process response.
5. Click **Update**.

Legacy Scan Template - Audit Settings: Attack Exclusions

> **Note:** The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:
>
> https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Excluded Parameters

Use this feature to prevent OpenText Fortify WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

1. In the Excluded Parameters group, click **Add**.
2. In the **Parameter** field, enter the name of the parameter you want to exclude.
3. Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.
4. Click **Update**.

Excluded Cookies

Use this feature to prevent Fortify WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values. This setting requires you to enter the name of a cookie.

In the following example HTTP response, the name of the cookie is "FirstCookie."

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

To exclude certain cookies:

1. In the Excluded Cookies group, click **Add**.
2. In the **Parameter** field, type a cookie name or enter a regular expression that you believe will match the cookies you want to exclude.
3. Click **Update**.

Excluded Headers

Use this feature to prevent Fortify WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression as follows:

1. In the Excluded Headers group, click **Add**.
2. In the **Parameter** field, type a header name or enter a regular expression that you believe will match the headers you want to exclude.
3. Click **Update**.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs.

To load inputs that you previously created using the editor, click the **Browse** button next to the **Import Audit Inputs** button.

Legacy Scan Template - Audit Settings: Attack Expressions

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- ja-jp: Japanese - Japan
- ko-Kr: Korean - Korea
- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan
- es-mx: Spanish - Mexico

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Legacy Scan Template - Audit Settings: Vulnerability Filters

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Select Vulnerability Filters to Enable

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition** - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection Dom Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

To add a filter to your default settings, select a filter in the **Available** area and click **>**. The filter is removed from the **Available** list and added to the **Selected** list.

To disable a filter, select a filter in the **Selected** list and click **<**. The filter is removed from the **Selected** list and added to the **Available** list.

To add all available filters, click **>>**.

To remove all selected filters, click **<<**.

Legacy Scan Template - Audit Settings: Smart Scan

Note: The Legacy Scan Template page is not available in the Fortify WebInspect Enterprise user interface. It is only available at the following URL:

https://<*Fully Qualified Domain Name (FQDN) or HostName*>/WIE/WebConsole/LegacyScanTemplate.aspx

Project Version

From the drop-down lists, you can select a **Project** and **Version** with which this template will be associated.

Alternatively, if you select the **Global Template** check box, then instead of specifying a project and project version, you must select an organization and group from a drop-down list.

If you select **Global Template**, all the other forms you can select in the left column also display the **Global Template** option as selected as well as the organization and group you selected, rather than the project and project version.

Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, OpenText Fortify WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select **Enable Smart Scan**, you can choose one or both of the identification methods described below.

- **Use regular expressions on HTTP responses** - This method searches the server response for strings that match predefined regular expressions designed to identify specific servers.
- **Use server analyzer fingerprinting and request sampling** - This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server type.

Custom Server/Application Type Definitions (more accurate detection)

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions (more accurate detection)** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.
2. In the **Host** field, enter the domain name or host, or the server's IP address.
3. Select one or more entries from the **Server/Application** list.
4. Click **OK**.

Chapter 5: WebInspect Enterprise Guided Scan and Reporting

This chapter describes Guided Scan functionality and report generation.

About Guided Scan and Reporting

Guided Scan directs you through the best steps to configure a scan that is tailored to your application, and it is the preferred method for performing a scan. Reporting enables you to create a new report from a scan you select and open.

The WebInspect Enterprise Desktop Application provides support for Guided Scan and reporting. Before you can use these features, you must download and install the application. For more information, see the WebInspect Enterprise Web Console chapter in the *OpenText™ Fortify WebInspect Enterprise User Guide*.

Launching a Guided Scan

To launch Guided Scan in Internet Explorer:

1. In the WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A message appears asking if you want to allow the program to open.
2. Click **Allow**.

To launch Guided Scan in Chrome:

1. In the WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A message appears asking if you want to open the program.
2. Click **Open WIE.Desktop**.

To launch Guided Scan in Firefox:

1. In the WebInspect Enterprise Web Console, click **Actions > Guided Scan**.

   A Launch Application window appears.
2. Select **WIE.Desktop**, and then click **Open Link**.

Selecting the Type of Guided Scan to Run

The first step in Guided Scan is to select the type of scan you want to run, from three types of web site scans using predefined templates and two types of scans using mobile templates. The following paragraphs provide more information to help you select the type of scan to run and cross-references to related topics.

Predefined Templates for Scanning Web Sites

For a **Standard Scan**, a **Quick Scan**, or a **Thorough Scan**, see "Configuring Web Site Scans Using a Predefined Template" on page 320. The only difference among these web site scans created using the predefined templates is the default extent of crawl coverage, which you can change:

- Click **Standard Scan** to use scan settings that (by default) focus on coverage rather than performance. Large sites could take days to crawl with these settings.
- Click **Quick Scan** to use scan settings that (by default) focus on breadth and performance rather than digging deep. It is especially good for very large sites.
- Click **Thorough Scan** to use scan settings that (by default) perform an exhaustive crawl of your site. We recommend that you split your site into parts and only scan smaller chunks of your site with these settings. It is not recommended for large sites.

Mobile Templates for Scanning Mobile Sites or Recording Back-End Traffic

- Click **Mobile Scan** to scan a mobile web site from the machine where your instance of Fortify WebInspect or Fortify WebInspect Enterprise is installed. Fortify WebInspect or Fortify WebInspect Enterprise emulates a mobile browser to access the mobile version of the site. See "Configuring Mobile Web Site Scans Using a Mobile Template" on page 332.
- Click **Native Scan** to manually crawl a native mobile application and capture the web traffic as a workflow macro. You generate the traffic on an Android, Windows, or iOS device or a software emulator running a mobile application. See "Configuring Native Scans Using a Mobile Template" on page 343.

Guided Scan Logging

When using Guided Scan, application logs are written to log files located at:

```
C:\ProgramData\HP\WIE\Guided Scan\Logs\
```

Application logs include all logs that are related to Guided Scan Wizard functionality, such as error, connectivity, proxy, and profiler logs. You can use this information for troubleshooting issues that arise while using Guided Scan.

Generating a Report

Create a new report from the scan you select and open. The reports available in Fortify WebInspect Enterprise are a subset of the reports available in OpenText Fortify WebInspect. You can generate a report in the following ways:

- Click **New Report** in the toolbar at the top of the Scan Visualization window for the selected scan.
- Click **Create Report** in the Scans form with a scan selected.

In the Generate a Report window, select the desired reports and complete the associated fields that appear for each one in the right pane. You can click the drop-down button for the **Favorites** field to select an existing favorite set of reports, organize existing favorites, or add the set of reports you selected as a new favorite.

Click the **Advanced** button to display the Advanced Report Options window and optionally specify the following for the report:

- A title for the cover page. This title appears below the report title.
- A company name for the cover page. This name appears above the report title.
- An image that appears at the top right of the cover page.
- An image that appears in the footer on each page after the cover page.

To start the report creation, click **Finish**. On the **Reports** tab in the Summary pane, you can see the report generation status (**Pending**, **Running**, or **Complete**) as it changes. You can save a completed report to a location you specify. If you selected multiple reports in the Generate a Report window, they are generated as one PDF file.

To control who can manage reports, in the Administrative Console, the **Administration** group, **Roles and Permissions** shortcut, **Roles** tab, **Organization** level includes a **Reports** category with the options **Can Create**, **Can View**, **Can Update**, and **Can Delete**. You must be allowed to view the scans for which you want to create reports.

Configuring a Guided Scan

The Guided Scan three types of web site scans using predefined templates and two types of scans using mobile templates.

Predefined Templates for Scanning Web Sites

For a **Standard Scan**, a **Quick Scan**, or a **Thorough Scan**, see "Configuring Web Site Scans Using a Predefined Template" on the next page. The only difference among these web site scans created using the predefined templates is the default extent of crawl coverage, which you can change:

- Click **Standard Scan** to use scan settings that (by default) focus on coverage rather than performance. Large sites could take days to crawl with these settings.
- Click **Quick Scan** to use scan settings that (by default) focus on breadth and performance rather than digging deep. It is especially good for very large sites.
- Click **Thorough Scan** to use scan settings that (by default) perform an exhaustive crawl of your site. We recommend that you split your site into parts and only scan smaller chunks of your site with these settings. It is not recommended for large sites.

Mobile Templates for Scanning Mobile Sites or Recording Back-End Traffic

- Click **Mobile Scan** to scan a mobile web site from the machine where your instance of OpenText Fortify WebInspect or OpenText Fortify WebInspect Enterprise is installed. Fortify WebInspect or

Fortify WebInspect Enterprise emulates a mobile browser to access the mobile version of the site. See "Configuring Mobile Web Site Scans Using a Mobile Template" on page 332.

- Click **Native Scan** to manually crawl a native mobile application and capture the Web traffic as a workflow macro. You generate the traffic on an Android, Windows, or iOS device or a software emulator running a mobile application. See "Configuring Native Scans Using a Mobile Template" on page 343.

Note: The Guided Scan wizard includes a tutorial that runs the first time you select a type of Guided Scan. You can close the tutorial at any time and return to it later by clicking the **Tutorial** button at the top right of the display.

Configuring Web Site Scans Using a Predefined Template

Guided Scan directs you through the best steps to configure a scan that is tailored to your application, and it is the preferred method for performing a scan. This topic describes use of the "predefined templates" for scanning websites. The only difference among the predefined templates—Standard Scan, Quick Scan, and Thorough Scan—is the default extent of crawl coverage, which you can change.

For general information about Guided Scan, including launching Guided Scan, see "About Guided Scan and Reporting" on page 317.

Setting the Rendering Engine

The rendering engine you select determines which Web Macro Recorder is opened when recording a new macro or editing an existing macro while configuring a Guided Scan.

To set the rendering engine:

1. Click the **Rendering Engine** drop-down list in the Guided Scan toolbar.
2. Select a rendering engine from the list. Options are:
   - **Session-based** – Selecting this option designates the Session-based Web Macro Recorder, which uses Internet Explorer browser technology.
   - **Event-based (preferred)** – Selecting this option designates the Event-based Web Macro Recorder, which uses TruClient and Firefox technology.

Overview of Guided Scan Stages and Steps

The tree in the left pane of the Guided Scan display enables you to see your progress as you specify settings in the right pane for the various pages of your scan. "Guided Scan -" and the current stage and steps comprise the name of the wizard page in the title bar. The initial page is Guided Scan - Site - Start Parameters - Verify Web Site, where **Site** is the stage and **Start Parameters** and the **1. Verify Web Site** step are highlighted in the left pane. Details for you to complete are displayed in the right pane of each page.

Following is an outline of the stage, steps, and substeps you will perform, as they appear in the tree in the left pane:

- **Site** - Specify the Web site to scan and verify you can access it.
  - **Start Parameters**
    - **1. Verify Web Site** - Specify the Web site to scan and verify you can access it.
    - **2. Choose Scan Type** - Select **Standard** scan or, if you are using pre-recorded macros, **Workflows** scan; select scan method (crawl, crawl and audit, or audit); and select scan policy.
- **Login** - Specify authentication settings for login.
  - **Network Authentication**
    - **Configure Network Authentication** - Specify the network authentication method and/or client certificate.
  - **Application Authentication**
    - **Use a Login Macro** - Specify whether to use one or more login macros for this site and whether to select, create, or edit a macro. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password.
- **Workflows**- Specify workflows (appears only when the selected **Scan Type** is **Workflows**).
  - **Workflows**
    - **1. Manage Workflows** - Specify whether to select, create, or edit a workflow macro.
    - **2. Record/Edit Workflow** - Record or edit a workflow macro.
- **Active Learning** - Allow Guided Scan to profile your site and recommend optimized scan settings accordingly.
  - **Optimization Tasks**
    - **Profile your site for optimal settings** - Run the Profiler and review what it recommends.
- **Settings** - Address configuration errors, optionally save scan settings, specify the application version to scan, and start the scan.
  - **Final Review**
    - **Validate Settings and Start Scan** - Address any errors detected by the wizard, optionally save scan settings for reuse later if desired, save or load a template, and begin the scan.

Use the procedure in the following sections to configure the Guided Scan. Headings in the following sections are named and listed in the same order as in the Guided Scan tree in the left pane.

Site

During the **Site** stage, you will:

- Verify the Web site you want to scan
- Choose a scan type

Start Parameters

1. Verify Web Site

1. In the **Start URL** field, type or select the complete URL or IP address of the site to scan.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, Fortify WebInspect will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting.

   An invalid URL or IP address results 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 do not pursue links that use fully qualified URLs (as opposed to relative paths).

   Fortify WebInspect and OpenText Fortify WebInspect Enterprise support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets. Examples:

   - http://[::1] — Fortify WebInspect scans "localhost."
   - http://[fe80::20c6:29ff:fe32:bae1]/subfolder/ — Fortify WebInspect scans the host at the specified address starting in the "subfolder" directory.
   - http://[fe80::20c6:29ff:fe32:bae1]:8080/subfolder/ — Fortify WebInspect scans a server running on port 8080 starting in "subfolder."

2. (Optional) To limit the scope of the scan to an area, select the **Restrict to Folder** check box, and then select one of the following options from the list:

   - **Directory only (self)** - Fortify WebInspect or Fortify WebInspect Enterprise will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect will assess only the "two" directory.
   - **Directory and subdirectories** - Fortify WebInspect or Fortify WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
   - **Directory and parent directories** - Fortify WebInspect or Fortify WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

3. If you must access the target site through a proxy server, click **Proxy** in the lower left of the right pane and then select one of the following options from the **Proxy Settings** list:

   - **Direct Connection (proxy disabled)**
   - **Auto detect proxy settings**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
   - **Use System proxy settings**: Import your proxy server information from the local machine.
   - **Use Firefox proxy settings**: Import your proxy server information from Firefox.

- **Configure proxy settings using a PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. Enter the location (URL) of the PAC.
- **Explicitly configure proxy settings**: Specify proxy server settings as indicated.

> **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server is not used.

4. Click **Verify** and follow the instructions in the yellow instruction bar.

   When a screenshot of the Web site or directory structure appears, you have successfully verified your connection to the Start URL.
5. Click the **Next** icon, which is always available at the top right of the left pane.

   The Guided Scan - Site - Start Parameters - Choose Scan Type page appears, and under the **Site** stage in the left pane, **Start Parameters** and the **2. Choose Scan Type** step are highlighted.

2. Choose Scan Type

To complete the scan type and other fields in the Choose Scan Type window:

1. (Optional) You can change the default scan name in the **Scan Name** text box.
2. Select one of the following scan types:
   - **Standard**: Fortify WebInspect performs an automated analysis, starting from the target URL. This is the normal way to start a scan.
   - **Workflows**: If you select this option, an additional **Workflows** stage appears in the left pane. Its use is described later in this procedure. You can continue through the Guided Scan wizard's default sequence and later complete the workflow scan settings when the **Workflows** stage becomes selected using the default sequence. This procedure assumes that you use the default sequence.
3. In the **Scan Method** area, select one of the following scan methods:
   - **Crawl Only**: This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
   - **Crawl and Audit**: Fortify WebInspect or Fortify WebInspect Enterprise maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see the Fortify WebInspect Enterprise Web Console Help system.
   - **Audit Only**: Fortify WebInspect or Fortify WebInspect Enterprise applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.
4. In the **Policy** area, select a policy from the drop-down list. For information about policies, see the Fortify WebInspect Enterprise Web Console Help system.

5. Adjust the slider to select a value for **Crawl Coverage** — **Quick, Moderate, Default,** or **Thorough**. Use the guidance provided on screen for each option.
   - If you initially clicked **Standard Scan** after you chose a Guided Scan, the **Default** option is selected by default.
   - If you initially clicked **Quick Scan** after you chose a Guided Scan, the **Quick** option is selected by default.
   - If you initially clicked **Thorough Scan** after you chose a Guided Scan, the **Thorough** option is selected by default.
6. In the **Single-Page Applications** area, select an option for crawling and auditing single-page applications (SPAs). When 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. Options for Single-Page Applications are:
   - **Automatic** - If Fortify WebInspect detects a SPA framework, it automatically switches to SPA-support mode.
   - **Enabled** - Indicates that SPA frameworks are used in the target application.

     > **Caution!** SPA support should be enabled for single-page applications only. Enabling SPA support to scan a non-SPA website will result in a slow scan.
   - **Disabled** - Indicates that SPA frameworks are not used in the target application.

   For more information, see "Single-page Application Scans" on page 358.
7. Click the **Next** icon at the top of the left pane.

   By default, the Guided Scan - Login - Application Authentication - Select Login Macro page appears, and under the **Login** stage in the left pane, **Application Authentication** and the **1. Select Login Macro** step are highlighted.

Login

During the **Login** stage, if the application you need to scan requires network authentication, a client certificate, and/or application-level authentication, you can configure them here. You can also create or assign a login macro.

- If you do *not* need to perform network authentication or use a client certificate, go to Application Authentication in this procedure.
- If you do *not* need to perform network authentication but you *do* need to use a client certificate, go to Configuring Client Authentication.
- If you *do* need to perform network authentication, click **Network Authentication** under the **Login** stage in the left pane. The Guided Scan - Login - Network Authentication - Configure Network Authentication page appears, and under the **Login** stage, **Network Authentication** and the **Configure Network Authentication** step are highlighted. In this case, proceed to Configuring Network Authentication.

Configuring Network Authentication

If your site requires network authentication:

1. Select the **Network Authentication** check box.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NTLM**
3. Complete the **User Name** and **Password** fields.

Configuring Client Authentication

If you need to use a client certificate for network authentication:

1. Select the **Client Certificate** check box.
2. In the **Certificate Store** area, select one of the following:
   - **Local Machine** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate on the local machine based on your selection in the **Certificate** area.
   - **Current User** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate for the current user based on your selection in the **Certificate** area.
3. Select either **My** or **Root** from the drop-down list.
4. To view certificate details in the **Certificate Information** area, select a certificate in the **Certificate** area.
5. Click the **Next** icon.

Application Authentication Step

If your site requires authentication, you can use this step to create, select, or edit a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and clicking a button such as Log In or Log On.

If the macro uses parameters for which values are masked in the Web Macro Recorder, then these values are also masked when configuring a Guided Scan in Fortify WebInspect Enterprise.

The following options are available for login macros:

- Using a Login Macro without Privilege Escalation
- Using Login Macros for Privilege Escalation

Using a Login Macro without Privilege Escalation

To use a login macro:

1. Select the **Use a login macro for this site** check box.
2. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     i. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.

     ii. Select the **Application** and **Application Version** from the drop-down lists.
     iii. Select a repository macro from the **Macro** drop-down list.
     iv. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
3. Click the **Next** button.

Using Login Macros for Privilege Escalation

If you selected the Privilege Escalation policy or another policy that includes enabled Privilege Escalation checks, at least one login macro for a high-privilege user account is required. For more information, see "Privilege Escalation Scans" on page 357.

To use login macros:

1. Select the **High-Privilege User Account Login Macro** check box. This login macro is for the higher-privilege user account, such as a Site Administrator or Moderator account.
2. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     i. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.

     ii. Select the **Application** and **Application Version** from the drop-down lists.
     iii. Select a repository macro from the **Macro** drop-down list.
     iv. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

After recording or selecting the first macro and clicking the next arrow, a "Configure Low Privilege Login Macro" prompt appears.

3. Do one of the following:
   - To perform the scan in authenticated mode, click **Yes**. For more information, see About Privilege Escalation Scans.

     Guided Scan returns to the Select Login Macro window for you to create or select a low-privilege login macro. Continue to Step 4.
   - To perform the scan in unauthenticated mode, click **No**. For more information, see About Privilege Escalation Scans.

     The Application Authentication Step is complete. Proceed to After Creating or Selecting the Login Macro(s).
4. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     1. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.
     2. Select the **Application** and **Application Version** from the drop-down lists.
     3. Select a repository macro from the **Macro** drop-down list.
     4. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
5. After recording or selecting the second macro, click the **Next** button.

After Creating or Selecting the Login Macro(s)

- If you selected a Standard scan, then the Optimization Tasks page appears. In this case, go to Active Learning.
- If you selected a Workflows scan, then the Manage Workflows page appears. In this case, proceed to Workflows.

Workflows

The **Workflows** stage appears only if you selected **Workflows** as the **Scan Type** in the **Site** stage; if you chose **Standard**, the **Workflows** stage does not appear.

You can create a workflow macro to ensure Fortify WebInspect Enterprise audits the pages you specify in the macro. Fortify WebInspect Enterprise audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit.

You can create multiple workflow macros, one for each use case on your site. You do not need to specify a logout condition. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan. In addition, you can import Burp Proxy captures and add them to your scan.

1. Manage Workflows

1. If you selected the **Workflows** scan option, optionally select a workflow in the Workflows table, if any, and click any of the following if available:
   - **Record** opens the Web Macro Recorder, allowing you to create a macro. The Record/Edit Workflow page appears, **Workflows** and the **2. Record/Edit Workflow** step are highlighted in the left pane, and the Web Macro Recorder opens. Go to step 2. Record/Edit Workflows.
   - **Edit** opens the Web Macro Recorder and loads the selected macro. The Record/Edit Workflow page appears, and **Workflows** and the **2. Record/Edit Workflow** step are highlighted in the left pane, and the Web Macro Recorder opens. Go to step 2. Record/Edit Workflows.
   - **Delete** removes the selected macro from the Workflows table (but does not delete it from your disk).
   - **Import** opens a standard file-selection window, allowing you to select a previously recorded .webmacro file or Burp Proxy captures. For more information about Burp Proxy captures, see Importing Burp Proxy Results.

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

   - **Export** opens a standard file-selection window, allowing you to save a recorded macro to a *.webmacro file.

   > **Note:** If you have installed OpenText Unified Functional Testing (UFT) on your computer, then Fortify WebInspect detects this automatically and displays an option to import a UFT (.usr) file. See "Importing OpenText UFT One Files" on page 359.
   >
   > For information about the Web Macro Recorder tool, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide.*

2. After you specify and play a workflow macro, it appears in the Workflows table and its Allowed Hosts are added to the Guided Scan - Workflows - Workflows - Manage Workflows page. You can enable or disable access to particular hosts.
3. When you have finished managing your workflows, click the **Next** icon. If you did not record or edit a macro, the Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings page appears, and under the **Active Learning** stage, **Optimization Tasks** and the **Profile site for optimal settings** step are highlighted in the left pane. In this case, go to Active Learning.

Importing Burp Proxy Results

If you have run Burp Proxy security tests, the traffic collected during those tests can be imported into a workflow macro, reducing the time it would otherwise take to retest the same areas.

To add Burp Proxy results to a workflow macro:

1. If you are not on the *Workflows* screen, click the **1. Manage Workflows** step under the **Workflows** stage in the Guided Scan tree.
2. Click the **Import** button.

   The *Import Macro* file selector appears.
3. Change the file type in the drop-down menu from **Web Macro (*.webmacro)** to **Burp Proxy (*.*)**.
4. Navigate to your Burp Proxy files and select the desired file.
5. Click **Open**.

2. Record/Edit Workflows

1. Follow the instructions in the yellow instruction bar of the Web Macro Recorder to create or edit a workflow macro. For information, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
2. When you complete this step, click the **Next** icon. The Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings page appears, and under the **Active Learning** stage, **Optimization Tasks** and the **Profile site for optimal settings** step are highlighted under the **Active Learning** stage in the left pane.

Active Learning

During the **Active Learning** stage:

- The Profiler runs and determines whether any settings need to be modified.
- You set the scan optimization option if necessary.
- You can navigate to key locations in your site that should be fully exercised.

Optimization Tasks – Profile site for optimal settings

In this step, the Profiler conducts a preliminary examination of your target Web site. Based on its findings, the Profiler returns a list of suggested changes to particular scan settings in the **Settings** section. You can accept or reject each recommendation.

For example, the Profiler might detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Profiler's suggestion to configure the required information before continuing.

Similarly, your settings might specify that Fortify WebInspect or Fortify WebInspect Enterprise should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it suggests that you modify the Fortify WebInspect or Fortify WebInspect Enterprise setting to accommodate this feature.

To run the Profiler:

1. Click **Profile**.

   Results appear in the **Settings** area.
2. Accept or reject the suggested settings. To reject, clear the associated check box.
3. If necessary, provide the requested information.
4. Click the **Next** icon.

Several options may be presented even if you do not run the Profiler, as follows:

- **Auto-fill Web forms during crawl**

  Select this option if you want Fortify WebInspect or Fortify WebInspect Enterprise to submit values for input controls on forms it encounters while scanning the target site. Fortify WebInspect or Fortify WebInspect Enterprise will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. See the Web Form Editor chapter in the *OpenText™ Fortify WebInspect Tools Guide* or the Web Form Editor Help for detailed information about using the Web Form Editor tool. You may:

  - Click the browse button to locate and load a file.
  - Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
  - Click **Create** to open the Web Form Editor and create a file.

- **Add allowed hosts**

  Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See the Fortify WebInspect Enterprise Web Console Help system for more information.

  To add allowed domains:

  a. Click **Add**.
  b. On the Specify Allowed Host page, enter a URL (or a regular expression representing a URL) and click **OK**.

- **Apply sample macro**

  Fortify WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the prepackaged macro containing the login script.

If the Profiler does not recommend changes, the Scan Wizard displays the message: "No settings changes are recommended; the profiler could not find any necessary optimizations for this site."

- Click the **Next** icon.

  In the **Settings** stage, **Final Review** and the **Validate Settings and Start Scan** step are highlighted.

Settings

During the *Settings* stage, you can set a number of options that affect how the collected traffic is audited. The available options vary, based on the selections you have made.

Final Review – Validate Settings and Start Scan

Options on this page allow you to save the current scan settings, save or load a template, and start the scan.

1. To save your current settings as an external XML file for future use, select **Click here to save settings**. Use the standard Save as window to name and save the file.
2. To save or load a template, continue according to the following table.

If you want to...	Then...
Save the current scan settings as a template in the Fortify WebInspect Enterprise database **Note:** When editing an existing template, the Save is actually an update. You can save any edits to settings and change the Template Name. However, you cannot change the Application, Application Version, or Global Template settings.	a. Do one of the following: ○ Click **Save** in the Template section of the toolbar. ○ Select **Click here to save template**. The Save Template window appears. b. Select an application from the **Application** drop-down list. c. Select an application version from the **Application Version** drop-down list. d. Type a name in the **Template** field.
Load scan settings from a template	a. Click **Load**. A confirmation message appears advising that your current scan settings will be lost. b. Click **Yes**. The Load Template window appears. c. Select an application from the **Application** drop-down list. d. Select an application version from the **Application Version** drop-down list. e. Select the template from the **Template** drop-down list. f. Click **Load**. Guided Scan returns to the Site Stage for you to verify the Web site and step through the settings from the template.

3. If you have loaded a template, some of the fields in the **WebInspect Enterprise** area are pre-populated. Otherwise, do the following:
   - Select an application from the **Application** drop-down list.
   - Select an application version from the **Application Version** drop-down list.
   - Select a sensor to conduct the scan from the **Sensor** drop-down list.
   - Select a **Priority** for the scan.
4. In the **Scan Now** area, review your scan settings, and then click **Start Scan** to begin the scan.

Configuring Mobile Web Site Scans Using a Mobile Template

Guided Scan directs you through the best steps to configure a scan that is tailored to your application, and it is the preferred method for performing a scan. This topic describes use of the Mobile Scan template to scan a mobile web site.

For general information about Guided Scan, including launching Guided Scan, see "About Guided Scan and Reporting" on page 317.

About Mobile Web Site Scans

Using the Mobile Scan template to create a mobile web site scan enables you to scan the mobile version of a web site using the desktop version of your browser from within OpenText Fortify WebInspect or OpenText Fortify WebInspect Enterprise.

A Mobile Scan for a mobile web site is nearly identical to a Web Site Scan and it mirrors the settings options you see when using one of the Predefined templates to perform a Standard scan, a Thorough scan, or a Quick scan. The only difference is that you need to select a user agent header to allow your browser to emulate a mobile browser.

Fortify WebInspect and Fortify WebInspect Enterprise come with several mobile user agent options, and you can create a custom option and create a user agent for another version of Android device, Windows device, or other mobile device. For information about creating a user agent header, see Creating a Custom User Agent Header.

The Guided Scan wizard will guide you through the stages and steps that are required to scan your application. The tree in the left pane tracks your progress. If you need to return to a previous step or stage, click the Back navigation button, or click the step in the Guided Scan tree to go there directly.

This Guided Scan consists of the following four or potentially five stages, each of which has one or more steps:

- **Site**: where you verify the site you want to scan and select the type of scan you want to run.
- **Login**: where you define the type of authorization your site requires.
- **Workflows**: appears only if the **Scan Type** selected in the **Site** stage is **Workflows**.
- **Active Learning**: where you run the Profiler to conduct a preliminary examination of the target Web site to determine if particular settings should be modified.

- **Settings**: where you review and validate your choices, save the current scan settings, save or load a template, and run the scan.

Creating a Mobile Web Site Scan

To create a mobile web site scan:

1. Log into Fortify WebInspect Enterprise.
2. From the Web Console, click **Guided Scan** under **Actions** to start a Guided Scan.
3. Click **Mobile Scan** in the **Mobile Templates** section.

   The Guided Scan wizard displays the first step in the **Site** stage: **Verify Web Site**.
4. To configure the rendering engine and user agent you want to use:
   a. Click the **Mobile Client** icon in the toolbar.
   b. Select the **Rendering engine** you want to use. The Rendering Engine you select determines which Web Macro Recorder is opened when recording a new macro or editing an existing macro while configuring a Guided Scan. The Rendering Engine options are:
      - **Session-based** – Selecting this option designates the Session-based Web Macro Recorder, which uses Internet Explorer browser technology.
      - **Event-based (preferred)** – Selecting this option designates the Event-based Web Macro Recorder, which uses TruClient and Firefox technology.

   c. Select the **User Agent** that represents the agent string you want your rendering engine to present to the site.

      If you created your own user agent header string, it will appear as **Custom**.

      If the user agent you need is not listed, you can create a custom user agent. See Creating a Custom User Agent Header.

   d. When you have selected the rendering engine and user agent as needed, go to About the Site Stage.

Creating a Custom User Agent Header

Fortify WebInspect and Fortify WebInspect Enterprise includes user agents for Android, Windows, and iOS devices. If you are using one of these options, you do not need to create a custom user agent header. If you want your Web browser to identify itself as a different mobile device or a specific OS version, create a custom user agent header as follows:

1. Click the **Advanced** icon in the Guided Scan toolbar.

   The Scan Settings window appears.
2. In the **Scan Settings** column, select **Cookies/Headers**.
3. In the **Append Custom Headers** section, double-click the User-Agent string.

   The Specify Custom Header window appears.
4. Type in `User-Agent:` followed by the user agent header string for the desired device.
5. Click **OK**.

   The new custom user agent will now be available to select as your **Mobile Client**.

About the Site Stage

During the **Site** stage, you will:

- Verify the web site you want to scan.
- Choose a scan type.

Verifying the Web Site

To verify your Web site:

1. In the **Start URL** field, type or select the complete URL or IP address of the site to scan.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, Fortify WebInspect or Fortify WebInspect Enterprise will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

   An invalid URL or IP address results 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 do not pursue links that use fully qualified URLs (as opposed to relative paths).

   Fortify WebInspect and Fortify WebInspect Enterprise support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets. Examples:

   - http://[::1] - Scans "localhost."
   - http://[fe80::20c6:29ff:fe32:bae1]/subfolder/ - Scans the host at the specified address starting in the "subfolder" directory.
   - http://[fe80::20c6:29ff:fe32:bae1]:8080/subfolder/ - Scans a server running on port 8080 starting in "subfolder."

2. (Optional) To limit the scope of the scan to an area, select the **Restrict to Folder** check box, and then select one of the following options from the list:

   - **Directory only (self)** - Fortify WebInspect or Fortify WebInspect Enterprise will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of www.mycompany/one/two/, Fortify WebInspect or Fortify WebInspect Enterprise will assess only the "two" directory.
   - **Directory and subdirectories** - Fortify WebInspect or Fortify WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
   - **Directory and parent directories** - Fortify WebInspect or Fortify WebInspect Enterprise will begin crawling and/or auditing at the URL you specify, but will not access any directory that is lower in the directory tree.

3. If you must access the target site through a proxy server, click **Proxy** in the lower left of the right pane to display the **Proxy Settings** area, and then select an option from the **Proxy Settings** list:
   - **Direct Connection (proxy disabled)**
   - **Auto detect proxy settings**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.
   - **Use System proxy settings**: Import your proxy server information from the local machine.
   - **Use Firefox proxy settings**: Import your proxy server information from Firefox.
   - **Configure proxy settings using a PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. Enter the location (URL) of the PAC.
   - **Explicitly configure proxy settings**: Specify proxy server settings as indicated.

   > **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," or if the Internet Explorer setting "Use a proxy server for your LAN" is not selected, then a proxy server is not used.

4. Click **Verify**.

   When a screenshot of the Web site or directory structure appears, you have successfully verified your connection to the Start URL.
5. Click the **Next** button.

   The Choose Scan Type window appears.

Choosing the Scan Type

To complete the scan type and other fields in the Choose Scan Type window:

1. Type a name for your scan in the **Scan Name** field.
2. Select one of the following scan types:
   - **Standard**: Fortify WebInspect or Fortify WebInspect Enterprise performs an automated analysis, starting from the target URL. This is the normal way to start a scan.
   - **Workflows**: If you select this option, an additional **Workflows** stage is added to the Guided Scan.
3. In the **Scan Method** area, select one of the following scan methods:
   - **Crawl Only**: This option completely maps a site's hierarchical data structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
   - **Crawl and Audit**: Fortify WebInspect or Fortify WebInspect Enterprise maps the site's hierarchical data structure and audits each resource (page). Depending on the default settings you select, the audit can be conducted as each resource is discovered or after the entire site is crawled. For information regarding simultaneous vs. sequential crawl and audit, see the Fortify WebInspect Enterprise Web Console Help system.
   - **Audit Only**: Fortify WebInspect or Fortify WebInspect Enterprise applies the methodologies

of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

4. In the **Policy** area, select a policy from the Policy list. For information about policies, see the Fortify WebInspect Enterprise Web Console Help system.
5. Adjust the slider to select a value for **Crawl Coverage** — **Quick, Moderate, Default,** or **Thorough**. Use the guidance provided on screen for each option.
6. In the **Single-Page Applications** area, select an option for crawling and auditing single-page applications (SPAs). When 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. Options for Single-Page Applications are:
   - **Automatic** - If Fortify WebInspect detects a SPA framework, it automatically switches to SPA-support mode.
   - **Enabled** - Indicates that SPA frameworks are used in the target application.

     > **Caution!** SPA support should be enabled for single-page applications only. Enabling SPA support to scan a non-SPA website will result in a slow scan.

   - **Disabled** - Indicates that SPA frameworks are not used in the target application.

   For more information, see "Single-page Application Scans" on page 358.
7. Click the **Next** button.

   The **Login** stage appears with **Application Authentication** highlighted in the left pane.

About the Login Stage

During the **Login** stage, if the application you need to scan requires network authentication, a client certificate, and/or application-level authentication, you can configure them here. You can also create or assign a login macro.

- If you do *not* need to perform network authentication or use a client certificate, go to Application Authentication Step in this procedure.
- If you do *not* need to perform network authentication but you *do* need to use a client certificate, go to Configuring Client Authentication in this procedure.
- If you *do* need to perform network authentication, click **Network Authentication** under the **Login** stage in the left pane. The Guided Scan - Login - Network Authentication - Configure Network Authentication page appears, and under the **Login** stage, **Network Authentication** and the **Configure Network Authentication** step are highlighted. In this case, proceed to Configuring Network Authentication.

Configuring Network Authentication

If your site requires network authentication:

1. Select the **Network Authentication** check box.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NTLM**
3. Complete the **User Name** and **Password** fields.

Configuring Client Authentication

If you need to use a client certificate for network authentication:

1. Select the **Client Certificate** check box.
2. In the **Certificate Store** area, select one of the following:
   - **Local Machine** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate on the local machine based on your selection in the **Certificate** area.
   - **Current User** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate for the current user based on your selection in the **Certificate** area.
3. Select either **My** or **Root** from the drop-down list.
4. To view certificate details in the **Certificate Information** area, select a certificate in the **Certificate** area.
5. Click the **Next** icon.

   The Application Authentication page appears.

Application Authentication Step

If your site requires authentication, you can use this step to create, select, or edit a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and clicking a button such as Log In or Log On.

If the macro uses parameters for which values are masked in the Web Macro Recorder, then these values are also masked when configuring a Guided Scan in Fortify WebInspect Enterprise.

The following options are available for login macros:

- Using a Login Macro without Privilege Escalation
- Using Login Macros for Privilege Escalation

Using a Login Macro without Privilege Escalation

To use a login macro:

1. Select the **Use a login macro for this site** check box.
2. Do one of the following:
    - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
    - To edit an existing login macro shown in the Login Macro field, click **Edit**.
    - To record a new macro, click **Create**.
    - To use a macro from the macro repository:
        i. Click **Download**.

           The Download a Macro from WebInspect Enterprise window appears.

        ii. Select the **Application** and **Application Version** from the drop-down lists.

        iii. Select a repository macro from the **Macro** drop-down list.

        iv. Click **OK**.

    For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
3. Click the **Next** button.

Using Login Macros for Privilege Escalation

If you selected the Privilege Escalation policy or another policy that includes enabled Privilege Escalation checks, at least one login macro for a high-privilege user account is required. For more information, see "Privilege Escalation Scans" on page 357.

To use login macros:

1. Select the **High-Privilege User Account Login Macro** check box. This login macro is for the higher-privilege user account, such as a Site Administrator or Moderator account.
2. Do one of the following:
    - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
    - To edit an existing login macro shown in the Login Macro field, click **Edit**.
    - To record a new macro, click **Create**.
    - To use a macro from the macro repository:
        i. Click **Download**.

           The Download a Macro from WebInspect Enterprise window appears.

        ii. Select the **Application** and **Application Version** from the drop-down lists.

        iii. Select a repository macro from the **Macro** drop-down list.

        iv. Click **OK**.

    For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

After recording or selecting the first macro and clicking the next arrow, a "Configure Low Privilege Login Macro" prompt appears.

3. Do one of the following:
   - To perform the scan in authenticated mode, click **Yes**. For more information, see About Privilege Escalation Scans.

     Guided Scan returns to the Select Login Macro window for you to create or select a low-privilege login macro. Continue to Step 4.

   - To perform the scan in unauthenticated mode, click **No**. For more information, see About Privilege Escalation Scans.

     The Application Authentication Step is complete. Proceed to After Creating or Selecting the Login Macro(s).

4. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     i. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.

     ii. Select the **Application** and **Application Version** from the drop-down lists.

     iii. Select a repository macro from the **Macro** drop-down list.

     iv. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

5. After recording or selecting the second macro, click the **Next** button.

After Creating or Selecting the Login Macro(s)

- If you selected a Standard scan, then the Optimization Tasks page appears. In this case, go to Active Learning.
- If you selected a Workflows scan, then the Manage Workflows page appears. In this case, proceed to Workflows.

About the Workflows Stage

The **Workflows** stage appears only if you selected **Workflows** as the **Scan Type** in the **Site** stage; if you chose **Standard**, the **Workflows** stage does not appear.

You can create a workflow macro to ensure Fortify WebInspect Enterprise audits the pages you specify in the macro. Fortify WebInspect Enterprise audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit.

You can create multiple workflow macros, one for each use case on your site. You do not need to specify a logout condition. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, they will all be included in the same scan. In addition, you can import Burp Proxy captures and add them to your scan.

To complete the Workflows settings, click any of the following in the Workflows table:

- **Record**. Opens the Web Macro Recorder, allowing you to create a macro.
- **Edit**. Opens the Web Macro Recorder and loads the selected macro.
- **Delete**. Removes the selected macro (but does not delete it from your disk).
- **Import**. Opens a standard file-selection window, allowing you to select a previously recorded .webmacro file or Burp Proxy captures. For more information about Burp Proxy captures, see Importing Burp Proxy Results at the end of this topic.

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

- **Export**. Opens a standard file-selection window, allowing you to save a recorded macro. After a macro is selected or recorded, you may optionally specify allowed hosts.

  Note: If you have installed OpenText Unified Functional Testing (UFT One) on your computer, then Fortify WebInspect or Fortify WebInspect Enterprise detects this automatically and displays an option to import a UFT .usr file. See "Importing OpenText UFT One Files" on page 359.

  For information about the Web Macro Recorder tool, see the *OpenText™ Fortify WebInspect Tools Guide*.

After you specify and play a workflow macro, it appears in the Workflows table and its Allowed Hosts are added to the Guided Scan - Workflows - Workflows - Manage Workflows page. You can enable or disable access to particular hosts.

Importing Burp Proxy Results

If you have run Burp Proxy security tests, the traffic collected during those tests can be imported into a workflow macro, reducing the time it would otherwise take to retest the same areas.

To add Burp Proxy results to a workflow macro:

1. If you are not on the Workflows page, click the **1. Manage Workflows** step under the **Workflows** stage in the Guided Scan tree.
2. Click the **Import** button.

   The Import Macro file selector appears.
3. Change the file type in the drop-down menu from **Web Macro (*.webmacro)** to **Burp Proxy (*.*)**.
4. Navigate to your Burp Proxy files and select the desired file.
5. Click **Open**.

About the Active Learning Stage

During the **Active Learning** stage:

- The Profiler runs and determines whether any settings need to be modified.
- You set the scan optimization option if necessary.

Optimization Tasks – Profiling site for optimal settings

In this step, the Profiler conducts a preliminary examination of your target Web site. Based on its findings, the Profiler returns a list of suggested changes to particular scan settings in the **Settings** section. You can accept or reject each recommendation.

For example, the Profiler might detect that authorization is required to enter the site, but you have not specified a valid user name and password. Rather than proceed with a scan that would return significantly diminished results, you could follow the Profiler's suggestion to configure the required information before continuing.

Similarly, your settings might specify that Fortify WebInspect or Fortify WebInspect Enterprise should not conduct "file-not-found" detection. This process is useful for Web sites that do not return a status "404 Not Found" when a client requests a resource that does not exist (they may instead return a status "200 OK," but the response contains a message that the file cannot be found). If the Profiler determines that such a scheme has been implemented in the target site, it would suggest that you modify the Fortify WebInspect or Fortify WebInspect Enterprise setting to accommodate this feature.

To run the Profiler:

1. Click **Profile**.

   Results appear in the **Settings** area.
2. Accept or reject the suggested settings. To reject, clear the associated check box.
3. If necessary, provide the requested information.
4. Click the **Next** icon.

Several options may be presented even if you do not run the Profiler, as follows:

- **Auto-fill Web forms during crawl**

  Select this option if you want Fortify WebInspect or Fortify WebInspect Enterprise to submit values for input controls on forms it encounters while scanning the target site. Fortify WebInspect or Fortify WebInspect Enterprise will extract the values from a prepackaged default file or from a file that you create using the Web Form Editor. See the Web Form Editor chapter in the *OpenText™ Fortify WebInspect Tools Guide* or the Web Form Editor Help for detailed information about using the Web Form Editor tool. You may:

  - Click the browse button to locate and load a file.
  - Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
  - Click **Create** to open the Web Form Editor and create a file.
- **Add allowed hosts**

Use the Allowed Host settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See the Fortify WebInspect Enterprise Web Console Help system for more information.

To add allowed domains:

a. Click **Add**.

b. On the Specify Allowed Host page, enter a URL (or a regular expression representing a URL) and click **OK**.

- **Apply sample macro**

  Fortify WebInspect's example banking application, zero.webappsecurity.com, uses a Web form login. If you scan this site, select **Apply sample macro** to run the prepackaged macro containing the login script.

If the Profiler does not recommend changes, the Scan Wizard displays the message: "No settings changes are recommended; the Profiler could not find any necessary optimizations for this site."

When you click the **Next** icon, the Guided Scan - Active Learning - Optimization Tasks page appears, and the **Optimization Tasks** step is highlighted in the left pane.

- Click the **Next** icon.

  In the **Settings** stage, **Final Review** and the **Validate Settings and Start Scan** step are highlighted.

About the Settings Stage

During the *Settings* stage, you can set a number of options that affect how the collected traffic is audited. The available options vary, based on the selections you have made.

Final Review – Validate Settings and Start Scan

Options on this page allow you to save the current scan settings, save or load a template, and start the scan.

1. To save your current settings as an external XML file for future use, select **Click here to save settings**. Use the standard Save as window to name and save the file.
2. To save or load a template, continue according to the following table.

If you want to...	**Then...**
Save the current scan settings as a template in the Fortify WebInspect Enterprise database **Note:** When editing an existing template, the Save is actually an update. You can save any edits to settings and change the Template Name. However, you cannot	a. Do one of the following: ○ Click **Save** in the Template section of the toolbar. ○ Select **Click here to save template**. The Save Template window appears. b. Select an application from the

If you want to...	Then...
change the Application, Application Version, or Global Template settings.	**Application** drop-down list. c. Select an application version from the **Application Version** drop-down list. d. Type a name in the **Template** field.
Load scan settings from a template	a. Click **Load**. A confirmation message appears advising that your current scan settings will be lost. b. Click **Yes**. The Load Template window appears. c. Select an application from the **Application** drop-down list. d. Select an application version from the **Application Version** drop-down list. e. Select the template from the **Template** drop-down list. f. Click **Load**. Guided Scan returns to the Site Stage for you to verify the Web site and step through the settings from the template.

3. If you have loaded a template, some of the fields in the **WebInspect Enterprise** area are pre-populated. Otherwise, do the following:
   - Select an application from the **Application** drop-down list.
   - Select an application version from the **Application Version** drop-down list.
   - Select a sensor to conduct the scan from the **Sensor** drop-down list.
   - Select a **Priority** for the scan.
4. In the **Scan Now** area, review your scan settings, and then click **Start Scan** to begin the scan.

Configuring Native Scans Using a Mobile Template

To skip to information in this topic about configuring the proxy for the selected profile, see "Setting the Mobile Device/Emulator Proxy Address" on page 346.

To skip to information in this topic about installing the client certificate for the selected profile, see "Adding a Trusted Certificate" on page 347.

Guided Scan directs you through the best steps to configure a scan that is tailored to your application, and it is the preferred method for performing a scan. This topic describes use of the Native Scan template.

For general information about Guided Scan, including launching Guided Scan, see "About Guided Scan and Reporting" on page 317.

> **Note:** Most of the information in this topic is iOS-specific, but it equally relates to Android and Windows devices and emulator usage. Please consult your OS documentation if you have questions on setting up proxies, installing certificates, or other OS-specific tasks.

About Native Scans

You use a Native Scan to manually crawl a native mobile application and capture the Web traffic as a workflow macro. You generate the traffic on an Android, Windows, or iOS device or a software emulator running a mobile application.

The Guided Scan wizard will guide you through the stages and steps that are required to record and scan your application traffic. The tree in the left pane tracks your progress. If you need to return to a previous step or stage, click the Back navigation button, or click the step in the Guided Scan tree to go there directly.

This Guided Scan consists of the following four stages, each of which has one or more steps:

- **Native Mobile**: where you choose a device or emulator, configure device/emulator proxy, and select the type of scan you want to run.
- **Login**: where you define the type of authentication if the back-end of your mobile application requires it.
- **Application**: where you run your application, record web traffic, and identify the hosts and RESTful endpoints to include in your scan.
- **Settings**: where you review and validate your choices, save the current scan settings, save or load a template, and run the scan.

Supported Devices

OpenText Fortify WebInspect and OpenText Fortify WebInspect Enterprise support scanning the back-end traffic on Android, Windows, and iOS devices.

Android Device Support

Any Android device, such as an Android-based phone or tablet.

Windows Device Support

Any Windows device, such as a Windows phone or Surface tablet.

iOS Device Support

Any iOS device, such as an iPhone or iPad, running the latest version of iOS.

Supported Development Emulators

In addition to support for Android and iOS devices, you can run your application through your Android or iOS emulator in your development environment. When scanning traffic generated via your device emulator, you must ensure that the development machine is on the same network as Fortify WebInspect Enterprise and that you have set up a proxy between Fortify WebInspect Enterprise and your development machine.

Creating a Native Scan

To create a Native Scan, you will need to make sure your device or emulator is on the same network as Fortify WebInspect Enterprise. In addition, you need to have authorization and access to the ports on the machine where you are running Fortify WebInspect Enterprise in order to successfully create a proxy connection.

To create a Native Scan:

1. Open Fortify WebInspect Enterprise.
2. From the Web Console, click **Guided Scan** under **Actions** to start a Guided Scan.
3. Click **Native Scan** in the **Mobile Templates** section.

   The Guided Scan wizard displays the first step in the **Native Mobile** stage: **Choose Device/Emulator Type**.

About the Native Mobile Stage

The first stage in the process is the **Native Mobile** stage. In this stage you will:

- Set up the device or emulator to use a proxy connection
- Log the device or emulator on to the same network as your instance of Fortify WebInspect Enterprise
- Install a client certificate on your device or emulator
- Name the scan for future reference
- Select a scan method
- Select a scan policy
- Select the crawl coverage amount

Choosing the Device/Emulator Type

Guided Scan provides you with the options described in the following table.

Option	Description
Profile	The type of device or emulator you want to scan. Select a type from the drop-down menu. For more information, see "Selecting a Profile" on the next page.

Option	Description
Mobile Device/Emulator Proxy	The IP address and port number for the proxy that Fortify WebInspect Enterprise creates for listening to the traffic between your device or emulator and the Web service or application being tested. Unless the IP address and/or port are reserved for the other activities, use the default strings. For more information, see "Setting the Mobile Device/Emulator Proxy Address" below.
Trusted Certificate	The port and URL to acquire a client certificate for your device or emulator. To download and install the certificate on your device or emulator, see "Adding a Trusted Certificate" on the next page.

Selecting a Profile

To set the device profile, select an option from the Profile drop-down list. The following table describes the options.

Option	Description
iOS Device	An iPad or iPhone running the latest version of iOS.
iOS Simulator	The iOS emulator that is part of the iOS SDK.
Android Device	A phone or tablet running the Android operating system.
Android Emulator	The Android emulator that is part of the Android SDK.
Windows Device	A Windows mobile device.

Setting the Mobile Device/Emulator Proxy Address

The **Mobile Device/Emulator Proxy** section lists the **Host** IP address and the **Port** number that will be used to establish a proxy connection between your device or emulator and Fortify WebInspect Enterprise. Use the suggested settings unless the IP address and/or port number are unavailable on your system.

> **Note:** If you are unable to connect to the server or access the Internet after setting your proxy, you may need to open up or change the port on your firewall specified in the **Native Mobile** stage. If it still does not work, you might need to select the IP address of the active network adapter. The IP address presented in the Fortify WebInspect Enterprise interface enables you to click the address and select an alternate from a drop-down list.

To set up a proxy on an iOS device or iOS emulator:

1. Run the **Settings** application.
2. Select **Wi-Fi**.
3. Select the Wi-Fi network you are using to connect to Fortify WebInspect Enterprise.

4. Scroll down to the **HTTP Proxy** section and select **Manual**.

   The screen displays the network configuration options for the network your device is connected to.

5. Scroll down further and type in the **Server** IP address and the **Port** number provided by Fortify WebInspect Enterprise. If you do not have this information, see "Choosing the Device/Emulator Type" on page 345.

6. In Fortify WebInspect Enterprise, click the **Verify** button in the **Trusted Certificate** section to verify the connection is working properly.

   The **Verify** activity progress bar appears.

7. Launch the default browser on your device and visit any site to verify that Fortify WebInspect Enterprise is able to see the back-end traffic.

   If everything is configured properly, after a few moments, the **Verify** activity progress bar will state that the traffic has been successfully verified.

8. Click **OK** to dismiss the verification progress bar and then click the Next button to select a scan type.

To set up a proxy on an Android device, a Windows device, or your PC, consult your operator’s instructions.

Adding a Trusted Certificate

If your site requires a secure connection (https), each time you configure a scan, Fortify WebInspect Enterprise generates a unique client certificate for your device. You will need to install the certificate into the device’s certificate repository.

There are three ways to add a certificate:

- Scan the QR code from the **Trusted Certificate** section of Guided Scan (requires QR reader software)
- Type the address into the built-in browser on your device or device emulator.
- Copy the certificate to your system clipboard for applying later (used when scanning with a device emulator).

Choose the option that best suits your needs.

> **Note:** After completing the scan, you should remove the certificate from the repository on your device. See Post Scan Steps.

To add a certificate to an iOS device:

1. After scanning the QR code or typing the provided URL into your browser, the Install Profile page appears.

   > **Note:** The WebInspect Root certificate status will display as Not Trusted until you add it to your root chain.

2. Tap the **Install** button.

A warning screen will appear stating that the certificate is not trusted. Once you add the certificate to the certificate repository on your device or emulator, the warning will go away.

3. Tap **Install** on the **Warning** screen.

   The display changes to that of the current network your device or emulator is connected to. Make sure it is connected to the same network as Fortify WebInspect Enterprise.

Choosing the Scan Type

After setting up your device or emulator to work with Fortify WebInspect Enterprise during the first part of the **Native Mobile** stage, you will need to select the type of scan you would like to run. The following table describes the options.

Option	Description
Scan Name	Type a name for the scan so that later you can identify the scan on the Manage Scans page.
Scan Method	Choose the type of scan you want from the following list: • **Crawl Only**: maps the attack surface of the specified workflow(s) • **Crawl and Audit**: maps the attack surface of the specified workflow(s) and scans for vulnerabilities • **Audit Only**: attack only the specified workflows
Policy	Select a policy for the scan from the drop-down menu. For information on creating and editing policies, see the Policy Manager chapter in the *OpenText™ Fortify WebInspect Tools Guide*.
Crawl Coverage	Adjust the slider to select a value — **Quick, Moderate, Default,** or **Thorough**. Use the guidance provided on screen for each option.

About the Login Stage

During the **Login** stage, if the application you need to scan requires network authentication, a client certificate, and/or application-level authentication, you can configure them here. You can also create or assign a login macro.

- If you do *not* need to perform network authentication or use a client certificate, go to Application Authentication Step in this procedure.
- If you do *not* need to perform network authentication but you *do* need to use a client certificate, go to Configuring Client Authentication in this procedure.
- If you *do* need to perform network authentication, click **Network Authentication** under the **Login** stage in the left pane. The Guided Scan - Login - Network Authentication - Configure Network Authentication page appears, and under the **Login** stage, **Network Authentication** and the **Configure Network Authentication** step are highlighted. In this case, proceed to Network Authentication Step.

Configuring Network Authentication

If your site requires network authentication:

1. Select the **Network Authentication** check box.
2. Select a **Method** from the drop-down list of authentication methods. The authentication methods are:
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NTLM**
3. Complete the **User Name** and **Password** fields.

Configuring Client Authentication

If you need to use a client certificate for network authentication:

1. Select the **Client Certificate** check box.
2. In the **Certificate Store** area, select one of the following:
   - **Local Machine** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate on the local machine based on your selection in the **Certificate** area.
   - **Current User** - Fortify WebInspect or Fortify WebInspect Enterprise uses a certificate for the current user based on your selection in the **Certificate** area.
3. Select either **My** or **Root** from the drop-down list.
4. To view certificate details in the **Certificate Information** area, select a certificate in the **Certificate** area.
5. Click the **Next** icon.

   The Application Authentication page appears.

Application Authentication Step

If your site requires authentication, you can use this step to create, select, or edit a login macro to automate the login process and increase the coverage of your site. A login macro is a recording of the activity that is required to access and log in to your application, typically by entering a user name and password and clicking a button such as Log In or Log On.

If the macro uses parameters for which values are masked in the Web Macro Recorder, then these values are also masked when configuring a Guided Scan in Fortify WebInspect Enterprise.

The following options are available for login macros:

- Using a Login Macro without Privilege Escalation
- Using Login Macros for Privilege Escalation

Using a Login Macro without Privilege Escalation

To use a login macro:

1. Select the **Use a login macro for this site** check box.
2. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     1. Click **Download**.

        The Download a Macro from OpenText Fortify WebInspect Enterprise window appears.
     2. Select the **Application** and **Application Version** from the drop-down lists.
     3. Select a repository macro from the **Macro** drop-down list.
     4. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
3. Click the **Next** button.

Using Login Macros for Privilege Escalation

If you selected the Privilege Escalation policy or another policy that includes enabled Privilege Escalation checks, at least one login macro for a high-privilege user account is required. For more information, see "Privilege Escalation Scans" on page 357.

To use login macros:

1. Select the **High-Privilege User Account Login Macro** check box. This login macro is for the higher-privilege user account, such as a Site Administrator or Moderator account.
2. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     1. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.
     2. Select the **Application** and **Application Version** from the drop-down lists.
     3. Select a repository macro from the **Macro** drop-down list.
     4. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

After recording or selecting the first macro and clicking the next arrow, a "Configure Low Privilege Login Macro" prompt appears.

3. Do one of the following:
   - To perform the scan in authenticated mode, click **Yes**. For more information, see "Privilege Escalation Scans" on page 357.

     Guided Scan returns to the Select Login Macro window for you to create or select a low-privilege login macro. Continue to Step 4.

   - To perform the scan in unauthenticated mode, click **No**. For more information, see "Privilege Escalation Scans" on page 357.

     The Application Authentication Step is complete. Proceed to the Application Stage to run your application.

4. Do one of the following:
   - To use a pre-recorded login macro, click the ellipsis button (**...**) to browse for a saved macro.
   - To edit an existing login macro shown in the Login Macro field, click **Edit**.
   - To record a new macro, click **Create**.
   - To use a macro from the macro repository:
     1. Click **Download**.

        The Download a Macro from WebInspect Enterprise window appears.
     2. Select the **Application** and **Application Version** from the drop-down lists.
     3. Select a repository macro from the **Macro** drop-down list.
     4. Click **OK**.

   For details about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

5. After recording or selecting the second macro, click the **Next** button.

About the Application Stage

The **Application** stage is where you run your application. During the **Application** stage:

- Run the mobile application to generate and collect Web traffic.
- Identify the hosts and RESTful endpoints you want to include.

Run Application Step

To run the application and generate and collect Web traffic:

1. Click the **Record** button.
2. Exercise the application, navigating through the interface as your customers will.
3. When you have generated enough traffic, click the **Stop** button.
4. Click **Play** to verify your workflow.

After running the application and collecting Web traffic, a list will be generated of the Allowed Hosts and potential RESTful Endpoints.

Finalize Allowed Hosts Step

To select the allowed hosts to include in your audit, click the check boxes in the **Enabled** column of the Allowed Hosts table.

The list of RESTful endpoints is generated by listing every possible combination that could be a RESTful endpoint. Select the actual RESTful endpoints from the list by selecting their **Enabled** check boxes. To reduce the list to a more likely subset, click the **Detect** button. Heuristics are applied, filtering out some of the less likely results. Select the **Enabled** check boxes from the resulting list.

If Fortify WebInspect Enterprise did not find all of the RESTful endpoints, you can add them manually.

To set up a new RESTful endpoint rule:

1. Click the **New Rule** button.

   A new rule input box appears in the RESTful Endpoints table.
2. Following the sample format in the input box, type in a RESTful endpoint.

To import a list of RESTful endpoints:

1. Click the **Import** button.

   A file selector appears.
2. Select a Web Application Description Language (.wadl) file.
3. Click **OK**.

About the Settings Stage

During the *Settings* stage, you can set a number of options that affect how the collected traffic is audited. The available options vary, based on the selections you have made.

Final Review – Validate Settings and Start Scan

Options on this page allow you to save the current scan settings, save or load a template, and start the scan.

1. To save your current settings as an external XML file for future use, select **Click here to save settings**. Use the standard Save as window to name and save the file.
2. To save or load a template, continue according to the following table.

If you want to...	Then...
Save the current scan settings as a template in the Fortify WebInspect Enterprise database **Note:** When editing an existing template,	a. Do one of the following: ○ Click **Save** in the Template section of the toolbar. ○ Select **Click here to save template**.

If you want to...	Then...
the Save is actually an update. You can save any edits to settings and change the Template Name. However, you cannot change the Application, Application Version, or Global Template settings.	The Save Template window appears. b. Select an application from the **Application** drop-down list. c. Select an application version from the **Application Version** drop-down list. d. Type a name in the **Template** field.
Load scan settings from a template	a. Click **Load**. A confirmation message appears advising that your current scan settings will be lost. b. Click **Yes**. The Load Template window appears. c. Select an application from the **Application** drop-down list. d. Select an application version from the **Application Version** drop-down list. e. Select the template from the **Template** drop-down list. f. Click **Load**. Guided Scan returns to the Site Stage for you to verify the Web site and step through the settings from the template.

3. If you have loaded a template, some of the fields in the **WebInspect Enterprise** area are pre-populated. Otherwise, do the following:
   - Select an application from the **Application** drop-down list.
   - Select an application version from the **Application Version** drop-down list.
   - Select a sensor to conduct the scan from the **Sensor** drop-down list.
   - Select a **Priority** for the scan.
4. In the **Scan Now** area, review your scan settings, and then click **Start Scan** to begin the scan.

Post Scan Steps

After you have completed your scan and run Fortify WebInspect Enterprise, you will need to reset your Android device, Windows device, iOS device, or emulator to its former state. The following steps show how to reset an iOS device to the way it was before you began. Steps for other devices and for emulators are similar, but they depend on the version of the OS you are running.

To remove the Fortify WebInspect Certificate on an iOS device:

1. Run the **Settings** application.
2. Select **General** from the **Settings** column.
3. Scroll down to the bottom of the list and select **Profile WebInspect Root**.
4. Tap the **Remove** button.

To remove the Proxy Settings on an iOS device:

1. Run the **Settings** application.
2. Select **Wi-Fi** from the **Settings** column.
3. Tap the **Network** name.
4. Delete the **Server** IP address and the **Port** number.

Multi-user Login Scans

Applications that allow only a single active login session per user prevent multi-threaded scanning. With multiple logins, the threads invalidate each other's state, resulting in slow scan times.

A solution to this problem is to convert the recorded credentials in a login macro to parameters and use multiple login accounts with the same application privileges. You can use the Multi-user Login option in the Scan Settings: Authentication window to parameterize the username and password in a login macro, and define multiple username and password pairs to use in a scan. This approach allows the scan to run across multiple threads. Each thread has a different login session, resulting in faster scan times.

Before You Begin

You must use a parameterized login macro to configure a multi-user login scan. For more information, see the Parameters Editor topic in the Web Macro Recorder chapters of the *OpenText™ Fortify WebInspect Tools Guide*.

Known Limitations

The following known limitations apply to the multi-user login feature:

- When using this feature, Fortify WebInspect does not detect several login-related SecureBase checks.

- This feature currently supports only shared requestor threads. Using default scan settings with separate crawl and audit threads is not supported. For more information, see "Scan Settings: Requestor" on page 372.
- The scan does not distribute the work equally among the multiple users logged in. For example, one configured user might use up to 75% of the scan activities while all other users are allocated to the remaining 25% of scan activities.

Process Overview

To configure a multi-user login scan, use the process described in the following table.

Stage	Description
1.	Set the shared requestor to the desired number of users. For more information, see "Scan Settings: Requestor" on page 372. **Important!** The number of shared requestor threads should not be more than the number of configured users. Requestor threads without valid users will cause the scan to run longer. Remember to count the original username and password in the parameterized macro as the first user when you configure multiple users.
2.	Ensure that you have a login macro with parameterized username and password. For more information, see the Parameters Editor topic in the Web Macro Recorder chapters of the *OpenText™ Fortify WebInspect Tools Guide*.
3.	In the Guided Scan wizard, enable the multi-user checkbox as described in "Configuring a Multi-user Login Scan" below.
4.	Add credentials for multiple users as described in "Adding Credentials" on the next page.
5.	Continue through the scan wizard as normal and conduct the scan.

Configuring a Multi-user Login Scan

To configure a multi-user login scan:

1. In the Guided Scan wizard, click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Authentication**.
3. Select the **Use a login macro for forms authentication** checkbox.

   Important! You must select this checkbox to enable the multi-user login option.
4. Click the ellipsis button … and select a saved macro that already has parameterized credentials.
5. Select the **Multi-user Login** checkbox.

> **Note:** If you clear the Multi-user Login checkbox prior to running the scan, the additional credentials will not be used during the scan. Fortify WebInspect will use only the original credentials recorded in the login macro.

6. Continue as follows:
   - To add a user’s credentials, go to "Adding Credentials" below.
   - To edit a user’s credentials, go to "Editing Credentials" below.
   - To delete a user’s credentials, go to "Deleting Credentials" below.

Adding Credentials

To add credentials:

1. Under Multi-user Login, click **Add**.

   The Multi-user Credential Input dialog box appears.
2. In the **Username** field, type a username
3. In the **Password** field, type the corresponding password.
4. Click **OK**.
5. Repeat Steps 1-4 for each user login to add.

> **Important!** The number of shared requestor threads should not be more than the number of configured users. Requestor threads without valid users will cause the scan to run longer. Remember to count the original username and password in the parameterized macro as the first user when you configure multiple users.

Editing Credentials

To edit credentials:

1. Under Multi-user Login, select a Username/Password pair and click **Edit**.

   The Multi-user Credential Input dialog box appears.
2. Edit the credentials as needed.
3. Click **OK**.

Deleting Credentials

To delete credentials:

1. Under Multi-user Login, select a Username/Password pair to be removed.
2. Click **Delete**.

Privilege Escalation Scans

Privilege escalation vulnerabilities result from programming errors or design flaws that grant an attacker elevated access to an application and its data. OpenText Fortify WebInspect can detect privilege escalation vulnerabilities by conducting either a low-privilege or unauthenticated crawl followed by a high-privilege crawl and audit in the same scan. Fortify WebInspect includes a Privilege Escalation policy as well as privilege escalation checks that can be enabled in other policies, including custom policies. In Guided Scan, Fortify WebInspect automatically detects when you have selected a policy with privilege escalation checks enabled, and prompts you for the required login macro(s).

Two Modes of Privilege Escalation Scans

Fortify WebInspect can perform privilege escalation scans in two modes, determined by the number of login macros you use:

- Authenticated Mode – This mode uses two login macros: one for low-privilege access and one for high-privilege access. In this mode, a low-privilege crawl is followed by a high-privilege crawl and audit. You can perform this type of scan using Guided Scan.
- Unauthenticated Mode – This mode uses only a high-privilege login macro. In this mode, the low-privilege crawl is actually an unauthenticated crawl. Any privilege escalation detected during this scan is moving from unauthenticated to high privilege. You can perform this type of scan using Guided Scan and providing only a high-privilege login macro.

> **Note:** OpenText Fortify WebInspect Enterprise does not support privilege escalation scans using the Scan Configuration wizard.

What to Expect During the Scan

When conducting a scan with privilege escalation checks enabled, Fortify WebInspect first performs a low-privilege crawl of the site. During this crawl, the Site view is not populated with the hierarchical structure of the Web site. Nor are vulnerabilities populated in the Summary pane. However, you can confirm that the scan is actively working by clicking the Scan Log tab in the Summary pane. You will see messages in the log indicating the "Scan Start" time and the "LowPrivilegeCrawlStart" time. When the low-privilege crawl of the site is complete, the high-privilege crawl and audit phase of the scan occurs. During this phase, the Site view will be populated and any vulnerabilities found will appear in the Summary pane.

See Also

"Configuring Web Site Scans Using a Predefined Template" on page 320

"Configuring Mobile Web Site Scans Using a Mobile Template" on page 332

"Configuring Native Scans Using a Mobile Template" on page 343

Single-page Application Scans

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. However, these features are provided as a courtesy and the primary objective is for the feature to gain wider exposure 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, WebInspect offers a solution to the challenge of vulnerability testing on SPAs.

Enabling SPA Support

When you enable SPA support, 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.

You can enable SPA support in the scan settings or in Guided Scan.

Caution! SPA support should be enabled for single-page applications only. Enabling SPA support to scan a non-SPA website will result in a slow scan.

See also

- "Scan Settings: JavaScript" on page 370
- "Configuring Web Site Scans Using a Predefined Template" on page 320

- "Configuring Mobile Web Site Scans Using a Mobile Template" on page 332
- "Configuring Native Scans Using a Mobile Template" on page 343

Importing OpenText UFT One Files

If you have the OpenText UFT One application installed, Fortify WebInspect detects it and allows you to import a UFT file (.usr) into your workflow scan to enhance the thoroughness and attack surface of your scan. For more information about OpenText UFT One, see UFT One software on the OpenText Web site.

To import a UFT (.usr) file into a Guided Scan:

1. Launch a Guided Scan, and then select **Workflows** as the **Scan Type**. The following additional text appears under the Workflows scan option:

   OpenText Unified Functional Testing (UFT One) has been detected. You can import scripts to improve the thoroughness of your security test.
2. Click **Next**.
3. In the **Login** section, the **Application Authentication** option is automatically selected. Complete the fields as indicated, and then click **Next**.
4. On the Manage Workflows window, the Workflow table appears. Click **Import** to display the Import Scripts window.
5. On the Import Scripts window, you may:
   - Type the file name.
   - Browse to your file to locate your file with a .usr extension. Select **OpenText UFT One** from the drop-down file type, and then navigate to the file.
   - Click **Edit** to launch the OpenText UFT One application.
6. (Optional) On the Import Scripts window, you may select either of the following options:
   - **Show OpenText UFT One UI during import**
   - **Open script result after import**
7. Select the .usr file to import, and then click **Import**. After your file is successfully imported, the file appears in the Workflows table.
8. Select one of the following from the Workflows table:
   - **Record** - launches the Web Macro Recorder. For more information, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
   - **Edit** - enables you to modify the file using the Web Macro Recorder. For more information, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.
   - **Delete** - deletes the script from the Workflows table.

- **Import** - imports another file.
- **Export** - saves a file in .webmacro format with the name and location you specify.

9. Click **Next**.

   When the first .usr script file is added to the list, its name (or default name) appears in the Workflows table and an Allowed Hosts table is added to the pane.

   Adding another .usr script file can add more allowed hosts. Any host that is enabled is available to all the listed workflow .usr script files, not just the workflow .usr file for which it was added. The Guided Scan will play all the listed workflow files and make requests to all the listed allowed hosts, whether or not their check boxes are selected. If a check box for an allowed host is selected, Fortify WebInspect will crawl or audit the responses from that host. If a check box is not selected, Fortify WebInspect will not crawl or audit the responses from that host.

   In addition, if a particular workflow .usr script uses parameters, a Macro Parameters table is displayed when that workflow macro is selected in the list. Edit the values of the parameters as needed.

10. After you have completed changes or additions to the Workflow table, proceed in the Guided Scan wizard to complete your settings and run the scan. For more information about recording a new login macro or using an existing login macro, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

Testing Login Macros

Fortify WebInspect performs tests on the login macro at the start of the scan if **Enable macro validation** is selected in Scan Settings: Authentication from Advanced Settings in Guided Scan. For more information, see "Scan Settings: Authentication" on page 393.

Validation Tests Performed

The following table describes the tests that Fortify WebInspect performs.

Test	Result of Failure
Determine if the validation step is missing.	The scan continues, but a warning is written to the scan log.
Verify that the auto-generated macro logs into the application.	The scan stops and an error is written to the scan log.
Verify that the replay of the macro logs into the application.	The scan stops and an error is written to the scan log.

If a scan stops after failing a test, it may be possible to examine the specific error message in the scan log to determine and resolve the issue. Use the error message and the troubleshooting tips in this topic to help resolve the issue.

Troubleshooting Tips

In all cases of macro failure, it is possible that an invalid macro was recorded. However, a previously good macro that fails is almost always due to site changes or credentials.

The following table provides possible causes and solutions for each error message.

Note: This table does not include all possible causes and solutions for each error message. Additional troubleshooting may be necessary.

Error Message	**Possible Cause**	**Possible Solution**
Automatic login generation failed	The login macro could not be created because the user credentials provided are not valid.	Try the Auto-gen Login Macro option again using credentials that are known to be valid.
Execution Failed	An HTML element, such as a verification element, username, or password, was not located.	Record a new macro in the Web Macro Recorder to identify the login input elements.
	The username has been deactivated (removed from the database) and/or the password has changed.	Record a new macro in the Web Macro Recorder using credentials that are known to be valid.
Logged in verification step not found	The login macro does not contain a verification step.	Edit the macro in the Web Macro Recorder to add a verification step to indicate a successful login.
Verification step did not fail after invalid login	The verification step succeeded after an invalid login attempt. A valid verification step should only succeed upon successful login. This indicates that an incorrect login verification object was selected.	Edit the macro in the Web Macro Recorder to select another object for the verification step.

Advanced Guided Scan Settings

The following pages describe the advanced Guided Scan settings, including crawl and audit settings.

Scan Settings: Method

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.
   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Method**.

Scan Mode

The following table describes the available options.

Option	Description
Crawl Only	This option completely maps a site's tree structure. After a crawl has been completed, you can click **Audit** to assess an application’s vulnerabilities.
Crawl & Audit	As OpenText Fortify WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed. This is described in the Crawl and Audit Mode section as the option to crawl and audit Simultaneously.
Audit Only	Fortify WebInspect applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

The following table describes the available options.

Option	Description
Simultaneously	As Fortify WebInspect maps the site's hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content could change before the crawl can be completed.
Sequentially	In this mode, Fortify WebInspect crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.

Crawl and Audit Details

The following table describes the available options.

Option	Description
Include search probes (send search attacks)	If you select this option, Fortify WebInspect will send requests for files and directories that might or might not exist on the server, even if those files are not found by crawling the site. This option is selected by default only when the Scan Mode is set to Crawl & Audit. The option is cleared(unchecked) by default when the Scan Mode is set to Crawl Only or Audit Only.
Crawl links on File Not Found responses	If you select this option, Fortify WebInspect will look for and crawl links on responses that are marked as “file not found.” This option is selected by default when the Scan Mode is set to Crawl Only or Crawl & Audit. The option is not available when the Scan Mode is set to Audit Only.

Navigation

The following table describes the available options.

Option	Description
Auto-fill Web forms during crawl	If you select this option, Fortify WebInspect submits values for input controls found on all forms. The values are extracted from a file you create using the Web form editor. Use the browse button to specify the file containing the values you want to use. Alternatively, you can select the **Edit** button (to modify the currently selected file) or the **Create** button (to create a Web form file). **Caution!** Do not rely on this feature for authentication. If the crawler and the auditor are configured to share state, and if Fortify WebInspect never inadvertently logs out of the site, then using values extracted by the Web Form Editor for a login form may work. However, if the audit or the crawl triggers a logout after the initial login, then Fortify WebInspect will not be able to log in again and the auditing will be unauthenticated. To prevent Fortify WebInspect from terminating prematurely if it inadvertently logs out of your

Option	Description
	application, go to "Scan Settings: Authentication" on page 393 and select **Use a login macro for forms authentication**.
Prompt for Web form values during scan (interactive mode)	If you select this option, Fortify WebInspect pauses the scan when it encounters an HTTP or JavaScript form and displays a window that enables you to enter values for input controls within the form. However, if you also select **Only prompt for tagged inputs**, Fortify WebInspect will not pause for user input unless a specific input control has been designated **Mark as Interactive Input** (using the Web Form Editor). This pausing for input is termed "interactive mode" and you can cancel it at any time during the scan.
Use Web Service Design	This option applies only to Web Service scans. When performing a Web service scan, Fortify WebInspect crawls the WSDL site and submits a value for each parameter in each operation. These values are contained in a file that you create using the Web Service Test Designer tool. Fortify WebInspect then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection. Use the browse button to specify the file containing the values you want to use. Alternatively, you can select the **Edit** button (to modify the currently selected file) or the **Create** button (to create a SOAP values file).

SSL/TLS Protocols

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols provide secure HTTP (HTTPS) connections for Internet transactions between Web browsers and Web servers. SSL/TLS protocols enable server authentication, client authentication, data encryption, and data integrity for Web applications.

Select the SSL/TLS protocol(s) used by your Web server. The following options are available:

- Use SSL 2.0
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2

If you do not configure the SSL/TLS protocol to match your Web server, Fortify WebInspect will still connect to the site, though there may be a performance impact.

For example, if the setting in Fortify WebInspect is configured to Use SSL 3.0 only, but the Web server is configured to accept TLS 1.2 connections only, Fortify WebInspect will first try to connect with SSL 3.0, but will fail. Fortify WebInspect will then implement each protocol until it discovers that TLS 1.2 is supported. The connection will then succeed, although more time will have been spent in the effort. The correct setting (Use TLS 1.2) in Fortify WebInspect would have succeeded on the first try.

Scan Settings: General

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.
   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **General**.

Scan Details

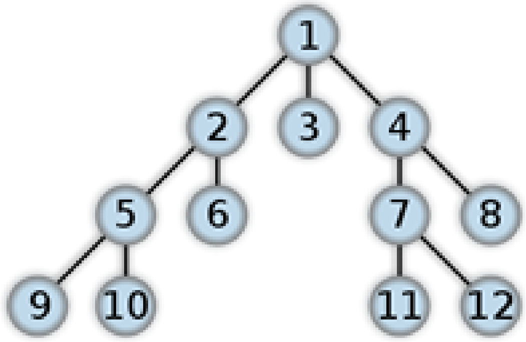
The following table describes the Scan Details options.

Option	**Description**
Enable Path Truncation	Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. OpenText Fortify WebInspect truncates paths, looking for directory listings or unusual errors within each truncation. **Example:** If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ may cause the server to reveal directory contents or may cause unhandled exceptions.
Case-sensitive request and response handling	Select this option if the server at the target site is case-sensitive to URLs.
Recalculate correlation data	This option is used only for comparing scans. The setting should be changed only upon the advice of Fortify Customer Support personnel. OpenText Fortify WebInspect Enterprise automatically generates its own correlation data using its own correlation provider.
Compress response data	If you select this option, Fortify WebInspect saves disk space by storing each HTTP response in a compressed format in the database.

Option	Description
Enable Traffic Monitor Logging	During a Web Site Scan, Fortify WebInspect Enterprise displays in the navigation pane only those sessions that reveal the hierarchical structure of the Web site plus those sessions in which a vulnerability was discovered. However, if you select the Traffic Monitor option, Fortify WebInspect adds the **Traffic Monitor** button to the Scan Info panel, allowing you to display and review every single HTTP request sent by Fortify WebInspect and the associated HTTP response received from the server.
Encrypt Traffic Monitor File	All sessions are normally recorded in the traffic monitor file as clear text. If you are concerned about storing sensitive information such as passwords on your computer, you can elect to encrypt the file. Encrypted files cannot be compressed. Selecting this option will significantly increase the size of exported scans containing log files. **Note:** The Traffic Viewer tool does not support the encryption of traffic files. The **Encrypt Traffic Monitor File** option is reserved for use under special circumstances with legacy traffic files only.
Maximum crawl-audit recursion depth	When an attack reveals a vulnerability, Fortify WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The default value is 2. The maximum recursion level is 1,000.

Crawl Details

By default, Fortify WebInspect uses breadth-first crawling, which begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



You cannot change the default crawling method in the user interface. However, the configurable Crawl Details options are described in the following table.

Option	Description
Enable keyword search audit (only available during a 'crawl only')	A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
Perform redundant page detection	Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, Fortify WebInspect would never be able to finish the scan. This option compares page structure to determine the level of similarity, allowing Fortify WebInspect to identify and exclude processing of redundant resources. **Important!** Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan. You can configure the following settings for redundant page detection: • **Page Similarity Threshold** – indicates how similar two pages must be to be considered redundant. Enter a percentage from 0 to 100, where 100 is an exact match. The default setting is 95 percent. • **Tag attributes to include** - identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes in this field in a comma-separated list adds those attributes and their values in the page structure. By default, "`id,class`" tag attributes are included. **Tip:** Certain sites may be primarily composed of one type of tag,

Option	Description
	such as `<div>`. Including these attributes creates a more rigid page match. Excluding these attributes creates a less strict match.
Limit maximum single URL hits to	Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL. Use this field to limit the number of times a single URL will be crawled. The default value is 5.
Include parameters in hit count	If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count. For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice). **Note:** This setting applies to both GET and POST parameters.
Limit maximum directory hit count to	This setting defines the maximum number of sub-directories to be traversed within each directory during the crawl. This setting reduces the scope of the crawl and might be useful in reducing scan times for some sites, such as those consisting of a content management system (CMS). The default setting is 200.
Minimum folder depth	If you select **Limit maximum directory hit count to** (above), this setting defines the folder depth at which the maximum directory hit count will begin to apply. The default setting is 1.
Limit maximum link traversal sequence to	This option restricts the number of hyperlinks that can be sequentially accessed as Fortify WebInspect crawls the site. For example, if five resources are linked as follows: • Page A contains a hyperlink to Page B • Page B contains a hyperlink to Page C • Page C contains a hyperlink to Page D

Option	Description
	• Page D contains a hyperlink to Page E and if this option is set to "3," then Page E will not be crawled. The default value is 15.
Limit maximum crawl folder depth to	This option limits the number of directories that may be included in a single request. The default value is 15. For example, if the URL is http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7 and this option is set to "4," then the contents of directories 5, 6, and 7 will not be crawled.
Limit maximum crawl count to	This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.
Limit maximum Web form submission to	Normally, when Fortify WebInspect encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed. There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form. Use this setting to limit the total number of submissions that Fortify WebInspect will perform. The default value is 3.
Suppress Repeated Path Segments	Many sites have text that resembles relative paths that become unusable URLs after Fortify WebInspect parses them and appends them to the URL being crawled. These occurrences can result in a runaway scan if paths are continuously appended, such as `/foo/bar/foo/bar/`. This setting helps reduce such occurrences and is enabled by default. With the setting **enabled**, the options are: **1** – Detect a single sub-folder repeated anywhere in the URL and reject the URL if there is a match. For example, `/foo/baz/bar/foo/` will match

Option	Description
	because "`/foo/`" is repeated. The repeat does not have to occur adjacently. **2** – Detect two (or more) pairs of adjacent sub-folders and reject the URL if there is a match. For example, `/foo/bar/baz/foo/bar/` will match because "`/foo/bar/`" is repeated. **3** – Detect two (or more) sets of three adjacent sub-folders and reject the URL if there is a match. **4** – Detect two (or more) sets of four adjacent sub-folders and reject the URL if there is a match. **5** – Detect two (or more) sets of five adjacent sub-folders and reject the URL if there is a match. If the setting is **disabled**, repeating sub-folders are not detected and no URLs are rejected due to matches.

Scan Settings: JavaScript

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **JavaScript**.

JavaScript Settings

The JavaScript analyzer enables Fortify WebInspect to crawl links defined by JavaScript, and to create and audit any documents rendered by JavaScript.

Tip: To increase the speed at which Fortify WebInspect conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Configure the settings as described in the following table.

Option	Description
Crawl links found from script execution	If you select this option, the crawler will follow dynamic links (i.e., links generated during JavaScript execution).

Option	**Description**
Verbose script parser debug logging	If you select this setting AND if the Application setting for logging level is set to Debug, Fortify WebInspect logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
Log JavaScript errors	Fortify WebInspect logs JavaScript parsing errors from the script parsing engine.
Enable JS Framework UI Exclusions	With this option selected, the Fortify WebInspect JavaScript parser ignores common jQuery and Ext JS user interface components, such as a calendar control or a ribbon bar. These items are then excluded from JavaScript execution during the scan.
Max script events per page	Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999. The default value is 1000.
Enable Site-Wide Event Reduction	When this option is selected, the crawler and JavaScript engine recognize common functional areas that appear among different parts of the website, such as common menus or page footers. This eliminates the need to find within HTML content the dynamic links and forms that have already been crawled, resulting in quicker scans. This option is enabled by default and should not normally be disabled.
SPA Support	SPA support applies to single-page applications. When 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. Options for SPA support are: • **Automatic** - If Fortify WebInspect detects a SPA framework, it automatically switches to SPA-support mode. • **Enabled** - Indicates that SPA frameworks are used in the target application. **Caution!** SPA support should be enabled for single-page applications only. Enabling SPA support to scan a non-SPA website will result in a slow scan. • **Disabled** - Indicates that SPA frameworks are not used in the target application.

Option	Description
	For more information, see "Single-page Application Scans" on page 358.

Scan Settings: Requestor

A requestor is the software module that handles HTTP requests and responses.

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Requestor**.

Requestor Performance

The following table describes the available options.

Option	Description
Use a shared requestor	If you select this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of OpenText Fortify WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
Use separate requestors	If you select this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans. When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl requestor thread count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5. The **Audit requestor thread count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

Option	Description
	Note: Depending on the capacity of the application being scanned, increasing thread counts may increase request failures due to increased load on the server, causing some responses to exceed the **Request timeout** setting. Request failures may reduce scan coverage because the responses that failed may have exposed additional attack surface or revealed vulnerabilities. If you notice increased request failures, you might reduce them by either increasing the **Request timeout** or reducing the **Crawl requestor thread count** and **Audit requestor thread count**. Also, depending on the nature of the application being scanned, increased crawl thread counts may reduce consistency between subsequent scans of the same site due to differences in crawl request ordering. By reducing the default **Crawl requestor thread count** setting to 1, consistency may be increased.

Requestor Settings

The following table describes the available options.

Option	Description
Limit maximum response size to	Select this option to limit the size of accepted server responses, and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
Request retry count	Specify how many times Fortify WebInspect will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
Request timeout	Specify how long Fortify WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, Fortify WebInspect resubmits the request until reaching the retry count. If it then receives no response, Fortify WebInspect logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds. **Note:** The first time a timeout occurs, Fortify WebInspect will extend the timeout period to confirm that the server is unresponsive. If the server responds within the extended Request timeout period, then

Option	Description
	the extended period becomes the new Request timeout for the current scan.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct Fortify WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

The following table describes the available options.

Option	Description
Consecutive 'single host' retry failures to stop scan	Enter the number of consecutive timeouts permitted from one specific server. The default value is 75.
Consecutive 'any host' retry failures to stop scan	Enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.
Nonconsecutive 'single host' retry failures to stop scan	Enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
Nonconsecutive 'any host' request failures to stop scan	Enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.
If first request fails, stop scan	Selecting this option will force Fortify WebInspect to terminate the scan if the target server does not respond to Fortify WebInspect's first request.
Response codes to stop scan if received	Enter the HTTP status codes that, if received, will force Fortify WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

Scan Settings: Session Exclusions

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.

2. In the Scan Settings group in the left pane, click **Session Exclusions**.

These settings apply to both the crawl and audit phases of a OpenText Fortify WebInspect vulnerability scan. To specify exclusions for only the crawl or only the audit, use "Crawl Settings: Session Exclusions" on page 406 or "Audit Settings: Session Exclusions" on page 409.

Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject** - Fortify WebInspect will not request files of the type you specify.
- **Exclude** - Fortify WebInspect will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

By default, most image, drawing, media, audio, video, and compressed file types are rejected.

To add a file extension:

1. Click **Add**.

   The Exclusion Extension window opens.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

Excluded MIME Types

Fortify WebInspect will not process files associated with the MIME type you specify. By default, image, audio, and video types are excluded.

To add a MIME Type:

1. Click **Add**.

   The Provide a Mime-type to Exclude window opens.
2. In the **Exclude Mime-Type** field, enter a MIME type.
3. Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component:

- **Reject** - Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP

response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

Editing Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Reject or Exclude a Host or URL window opens.
2. Select either **Host** or **URL**.
3. In the **Host** or **URL** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

Adding Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected Query Parameter or Post Parameter as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
   - **matches regex** - Matches the regular expression you specify in the **Match String** field.
   - **matches regex extension** - Matches a syntax available from OpenText's regular expression extensions you specify in the **Match String** field. For information about the Regular Expression Editor, see the Regular Expression Editor chapter in the *OpenText™ Fortify WebInspect Tools Guide*.
   - **matches** - Matches the text string you specify in the **Match String** field.
   - **contains** - Contains the text string you specify in the **Match String** field.
5. In the **Match String** field, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click + (or press Enter).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.

10. When the exclusion appears in the **Other Exclusion/Rejection Criteria** list, select either **Reject**, **Exclude**, or both.

    > **Note:** You cannot reject Response, Response Header, and Status Code Target types during a scan. You can only exclude these Target types.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, Fortify WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

Scan Settings: Allowed Hosts

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Allowed Hosts**.

Using the Allowed Host Setting

Use the Allowed Host setting to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the crawl and audit.

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 OpenText Fortify WebInspect 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, Fortify WebInspect 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 Domains

To add allowed domains:

1. Click **Add**.
2. On the Specify Allowed Host window, enter a URL (or a regular expression representing a URL) and click **OK**.

   > **Note:** When specifying the URL, do not include the protocol designator (such as http:// or https://).

Editing or Removing Domains

To edit or remove an allowed domain:

1. Select a domain from the **Allowed Hosts** list.
2. Click **Edit** or **Remove**.

Scan Settings: HTTP Parsing

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.
   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **HTTP Parsing**.

Options

The following table describes the HTTP Parsing options.

Option	**Description**
HTTP Parameters Used for State	If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following: .../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01 Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then OpenText Fortify WebInspect will replace its assigned value with the new session ID obtained from the server each time the connection is made. Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include userid=slbhkelvbkl73dhj. In this case, "userid" is the parameter you would identify. **Note:** You need to identify parameters only when the application

Option	Description
	uses URL rewriting or posted data to manage state. It is not necessary when using cookies. Fortify WebInspect can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "1234567" is the session information: http://www.onlinestore.com/bikes/(1234567)/index.html The regular expression for identifying the parameter would be: /\([\w\d]+\)/
Enable CSRF	The Enable CSRF option should only be selected if the site you are scanning includes Cross-Site Request Forgery (CSRF) tokens as it adds overhead to the process. For more information, see "CSRF" on page 382.
Determine State from URL Path	If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. Two default regular expressions identify two ASP.NET cookieless session IDs. The third regular expression matches jsessionid cookie.
HTTP Parameters Used for Navigation	Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples: • http://www.anysite.com?Master.asp?Page=1 • http://www.anysite.com?Master.asp?Page=2; • http://www.anysite.com?Master.asp?Page=13;Subpage=4 Ordinarily, Fortify WebInspect would assume that these three requests refer to identical resources and would conduct a vulnerability scan on only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used. The first two examples contain one resource parameter: "Page." The third example contains two parameters: "Page" and "Subpage." To identify resource parameters:

Option	Description
	1. Click **Add**. 2. On the HTTP Parameter window, enter the parameter name and click **OK**. The string you entered appears in the **Parameter** list. 3. Repeat this procedure for additional parameters.
Advanced HTTP Parsing	Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document. For pages that do not announce their character set, you can use the **Assumed 'charset' encoding** field to specify which language family (and implied character set) Fortify WebInspect should use. The **Treat query parameter value as parameter name when only value is present** check box determines how Fortify WebInspect interprets query parameters without values. For example: http://somehost?param If this check box is selected, Fortify WebInspect will interpret “param” to be a parameter named “param” with an empty value. If this check box is not selected, Fortify WebInspect will interpret “param” to be a nameless parameter with the value “param”. This setting can influence the way Fortify WebInspect calculates the hit count (see the **Limit maximum single URL hits to** setting under "Scan Settings: General" on page 365). This setting is useful for scenarios in which a URL contains an anti-caching parameter. These often take the form of a numeric counter or timestamp. For example, the following parameters are numeric counters: • http://somehost?1234567 • http://somehost?1234568 In such cases, the value is changing for each request. If the value is treated as the parameter name, and the “Include parameters in hit count” setting is selected, the crawl count may inflate artificially, thus increasing the scan time. In these cases, clearing the **Treat query parameter value as parameter name when only value is present** check box will prevent

Option	Description
	these counters from contributing to the hit count and produce a more reasonable scan time.

CSRF

The Enable CSRF option should only be selected if the site you are scanning includes Cross-Site Request Forgery (CSRF) tokens as it adds overhead to the process.

About CSRF

Cross-Site Request Forgery (CSRF) is a malicious exploit of a website where unauthorized commands are transmitted from a user’s browser that the website trusts. CSRF exploits piggyback on the trust that a site has in a user’s browser; using the fact that the user has already been authenticated by the site and the chain of trust is still open.

Example:

A user visits a bank, is authenticated, and a cookie is placed on the user’s machine. After the user completes the banking transaction, he or she switches to another browser tab and continues a conversation on an enthusiast Web site devoted to the user’s hobby. On the site, someone has posted a message that includes an HTML image element. The HTML image element includes a request to the user’s bank to extract all of the cash from the account and deposit it into another account. Because the user has a cookie on his or her device that has not expired yet, the transaction is honored and all of the money in the account is withdrawn.

CSRF exploits often involve sites that rely on trust in a user’s identity, often maintained through the use of a cookie. The user’s browser is then tricked into sending HTTP requests to the target site in hopes that a trust between the user’s browser and the target site still exists.

Using CSRF Tokens

To stop Cross-site request forgeries from occurring, common practice is to set up the server to generate requests that include a randomly generated parameter with a common name such as "CSRFToken". The token may be generated once per session or a new one generated for each request. If you have used CSRF tokens in your code and enabled CSRF in OpenText Fortify WebInspect, we will take this into consideration when crawling your site. Each time Fortify WebInspect launches an attack, it will request the form again to acquire a new CSRF token. This adds significantly to the time it takes for Fortify WebInspect to complete a scan, so do not enable CSRF if you are not using CSRF tokens on your site.

Scan Settings: Custom Parameters

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.

2. In the Scan Settings group in the left pane, click **Custom Parameters**.

Custom Parameters are used to accommodate sites that use URL rewriting techniques and/or Representation State Transfer (REST) web services technologies. You can write rules for these custom parameters, or you can import rules from a common configuration file written in Web Application Description Language (WADL). In addition to applying these rules that you discretely define or import, OpenText Fortify WebInspect will attempt (during a scan) to identify custom parameters and create rules to accommodate them.

URL Rewriting

Many dynamic sites use URL rewriting because static URLs are easier for users to remember and are easier for search engines to index the site. For example, an HTTP request such as

http://www.pets.com/ShowProduct/7

is sent to the server's rewrite module, which converts the URL to the following:

http://www.pets.com/ShowProduct.php?product_id=7

In this example, the URL causes the server to execute the PHP script "ShowProduct" and display the information for product number 7.

When Fortify WebInspect scans a page, it must be able to determine which elements are variables so that its attack agents can thoroughly check for vulnerabilities. To enable this, you must define rules that identify these elements. You can do so using a proprietary Fortify WebInspect syntax.

Examples

- HTML: <a href="someDetails/user1/">User 1 details</a>

  Rule: /someDetails/{username}/
- HTML: <a href="TwoParameters/Details/user1/Value2">User 1 details</a>

  Rule: /TwoParameters/Details/{username}/{parameter2}
- HTML: <a href="/Value2/PreFixParameter/Details/user1">User 1 details</a>

  Rule: /{parameter2}/PreFixParameter/Details/{username}

RESTful Services

A RESTful web service (also called a RESTful web API) is a simple Web service implemented using HTTP and the principles of REST. It has gained widespread acceptance across the Web as a simpler alternative to web services based on SOAP and Web Services Description Language (WSDL).

The following request adds a name to a file using an HTTP query string:

```
GET /adduser?name=Robert HTTP/1.1
```

This same function could be achieved by using the following method with a Web service. Note that the parameter names and values have been moved from the request URI and now appear as XML tags in the request body.

```
POST /users HTTP/1.1 Host: myserver
 Content-Type: application/xml
 <?xml version="1.0"?>
 <user>
 <name>Robert</name>
 </user>
```

In the case of both URL rewriting and RESTful web services, you must create rules that instruct Fortify WebInspect how to create the appropriate requests.

Creating a Rule

To create a rule:

1. Click **New Rule**.
2. In the Expression column, enter a rule. See "Path Matrix Parameters" on the next page for guidelines and examples.

The **Enabled** check box is selected by default. Fortify WebInspect examines the rule and, if it is valid, removes the red **X**.

Deleting a Rule

To delete a rule:

1. Select a rule from the **Custom Parameters Rules** list.
2. Click **Delete**.

Disabling a Rule

To disable a rule without deleting it:

1. Select a rule.
2. Clear the check mark in the **Enabled** column.

Importing Rules

To import a file containing rules:

1. Click Import....
2. Using a standard file-selection window, select the type of file (.wadl or .txt) containing the custom rules you want to apply.
3. Locate the file and click **Open**.

Enable automatic seeding of rules that were not used during scan

The most reliable rules for custom parameters are those deduced from a WADL file or created by developers of the Web site. If a rule is not invoked during a scan (because the rule doesn't match any

URL), then Fortify WebInspect can programmatically assume that a valid portion of the site has not been attacked. Therefore, if you select this option, Fortify WebInspect will create sessions to exercise these unused rules in an effort to expand the attack surface.

Double Encode URL Parameters

Double-encoding is an attack technique that encodes user request parameters twice in hexadecimal format in an attempt to bypass security controls or cause unexpected behavior from the application. For example, a cross-site scripting (XSS) attack might normally appear as:

```
<script>alert('FOO')</script>
```

This malicious code could be inserted into a vulnerable application, resulting in an alert window with the message “FOO.” However, the web application can have a filter that prohibits characters such as < (less than) > (greater than) and / (forward slash), since they are used to perform Web application attacks. The attacker could attempt to circumvent this safeguard by using a "double encoding" technique to exploit the client’s session. The encoding process for this JavaScript is:

Char	Hex encode	Encoded % Sign	Double encoded result
<	%3C	%25	%253C
/	%2F	%25	%252F
>	%3E	%25	%253E

Finally, the malicious code, double-encoded, is:

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
```

If you select this option, Fortify WebInspect will create double-encoded URL parameters (instead of single-encoded parameters) and submit them as part of the attack sequence. This is recommended when the Web server uses, for example, Apache mod-rewrite plus PHP or Java URL Rewrite Filter 3.2.0.

Path Matrix Parameters

There are three ways rules can be created in the system. Rules may be:

- Entered manually.
- Generated from a WADL file specified by the user or received through OpenText Fortify WebInspect Agent.
- Imported from a flat file containing a list of rules.

When entering rules manually, you specify the path segments of a URL that should be treated as parameters.

The rules use special characters to designate parts of the actual URL that contain parameters. If a URL matches a rule, OpenText Fortify WebInspect parses the parameters and attacks them. Notable components of a rule are:

- Path (gp/c/{book_name}/)
- Query (anything that follows "?")
- Fragment (anything that follows "#")

Definition of Path Segment

A path segment starts with ‘/’ characters and is terminated either by another ‘/’ character or by end of line. To illustrate, path "/a" has one segment whereas path "/a/" has two segments (the first containing the string “a” and the second being empty. Note that paths "/a" and "/a/" are not equal. When attempting to determine if a URL matches a rule, empty segments are considered.

Special Elements for Rules

A rule may contain the special elements described in the following table.

Element	Description
*	Asterisk. May appear in production defined below; presence in non-path productions means that this part of the URL will not participate in matching (or, in other words, will match anything).

{ }	Group; a named parameter that may appear within the path of the rule. The content has no special meaning and is used during reporting as the name of the attacked parameter. The character set allowed within the delimiting brackets that designate a group { } is defined in RFC 3986 as *pchar:
	pchar = unreserved / pct-encoded / sub-delims / ":" / "@"
	pct-encoded = "%" HEXDIG HEXDIG
	unreserved = ALPHA DIGIT - ._ ~
	reserved = gen-delims / sub-delims
	gen-delims = : / ; ? # [ ] @ "
	sub-delims = ! $ & ' ( ) * + , ; =
	A group’s content cannot include the "open bracket" and "close bracket" characters, unless escaped as pct-encoded element.

The rules for placing * out of path are described below. Within a path segment, any amount of * and {} groups can be placed, provided they're interleaved with plain text. For example:

Valid rule: /gp/c/*={param}

Invalid rule: /gp/c/*{}

Rules with segments having **, *{}, {}* or {}{} entries are invalid.

For a rule to match a URL, all components of the rule should match corresponding components of the crawled URL. Path comparison is done segment-wise, with * and {} groups matching any number of characters (including zero characters), plain text elements matching corresponding plain text elements of the path segment of the URL. So, for example:

/gp/c/{book_name} is a match for these URLs:

- http://www.amazon.com:8080/gp/c/Moby_Dick
- http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0
- https://www.amazon.com/gp/c/Hobbit

But it is not a match for any of these:

- http://www.amazon.com /gp/c/Moby_Dick/ (no match because of trailing slash)
- http://www.amazon.com/gp/c/Sex_and_the_City/Horror (no match because it has a different number of segments)

Fortify WebInspect will treat elements of path segments matched by {...} groups in the rule URL as parameters, similar to those found in a query. Moreover, query parameters of crawled URLs matched by rule will be attacked along with parameters within the URL's path. In the following example of a matched URL, Fortify WebInspect would conduct attacks on the format and price parameters and on the third segment of the path (Singularity_Sky):

http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&:price=0

Asterisk Placeholder

The "*" placeholder may appear in the following productions and subproductions of the URL:

- Path – cannot be matched as a whole, since * in path matches a single segment or less.
  - Path segments – as in /gp/*/{param}, which will match URLs with schema HTTP, hostname www.amazon.com, path containing three segments (first is exactly "gp", second is any segment, and the third segment will be treated as parameter and won't participate in matching).
  - Part of path segment – as in /gp/ref=*, which will match URLs with path containing two segments (first is exactly "gp", second containing any string with prefix "ref=").

- Query – as in /gp/c/{param}?*, which matches any URL with path of three segments (first segment is “gp”, second segment is “c” and third segment being a parameter, so it won’t participate in matching); this URL also MUST contain a query string of arbitrary structure. Note the difference between rules /gp/c/{param}and /gp/c/{param}?*. First rule will match URL http://www.amazon.com/gp/c/Three_Little_Blind_Mice, while second will not.
    - Key-value pair of query – as in /gp/c/{param}?format=* which will match URL only if query string has exactly one key-value pair, with key name being “format.”
    - Key-value pair of query – as in /gp/c/{param}?*=pdf which will match URL only if query string has exactly one key-value pair, with value being “pdf.”
- Fragment – as in case /gp/c/{param}#*which matches any URL with fragment part being present

Benefit of Using Placeholders

The main benefit of using placeholders is that it enables you to create rules that combine matrix parameters and URL path-based parameters within single rule. For relevant URL

http://www.amazon.com/gp/color;foreground=green;background=black/something?format=dvi

the following rule will allow attacks on all parameters

gp/*/{param}

with the matrix parameter segment being ignored by * placeholder within second segment of the path, but recognized by Fortify WebInspect and attacked properly.

Multiple Rules Matching a URL

In the case of multiple rules matching a given URL, there are two options:

- Stop iterating over the rules once a match is found and so use only the first rule.
- Iterate over all of the rules and collect all custom parameters that match.

For instance, for the following URL

http://mySite.com/store/books/Areopagitica/32/1

the following rules both match

- */books/{booktitle}/32/{paragraph}
- store/*/Areopagitica/{page}/{paragraph}

Fortify WebInspect will try to collect parameters from both rules to ensure the greatest attack coverage, so all three segments (“Areopagitica”, “32” and “1” in the example above) will be attacked.

Scan Settings: Filters

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.

2. In the Scan Settings group in the left pane, click **Filters**.

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use OpenText Fortify WebInspect or those who have access to the raw data or generated reports.

Options

The following table describes the Filter options.

Option	Description
Filter HTTP Request Content	Use this area to specify search-and-replace rules for HTTP requests.
Filter HTTP Response Content	Use this area to specify search-and-replace rules for HTTP responses.

Adding Rules for Finding and Replacing Keywords

To add a regular expression rule for finding or replacing keywords in requests or responses:

1. In either the **Request Content** or the **Response Content** group, click **Add**.

   The Add Request/Response Data Filter Criteria window opens.
2. In the **Search For Text** field, type (or paste) the string you want to locate (or enter a regular expression that describes the string).

   Click ▶ to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an expression).
3. In the **Search For Text In** field, select the section of the request or response you want to search for the filter pattern. The options are:
   - **All** – Search the entire request or response.
   - **Headers** – Search each header individually. Some headers, such as Set-Cookie and HTTP Version headers, are not searched.

     > **Note:** To ensure that all headers are searched, select Prefix.
   - **Post Data** – For requests only, search all of the HTTP message body data.
   - **Body** – Search all of the HTTP message body data.
   - **Prefix** – Simultaneously search everything that is in the request or status line, all headers, and the empty line prior to the body.
4. Type (or paste) the replacement string in the **Replacesearch text with** field.

> **Tip:** Click ▶ for assistance with regular expressions.

5. For case-sensitive searches, select the **Case-Sensitive Match** check box.
6. Click **OK**.

Scan Settings: Cookies/Headers

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.
   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Cookies/Headers**.

Standard Header Parameters

The following table describes the standard header parameters options.

Option	**Description**
Include 'referer' in HTTP request headers	Select this check box to include referer headers in OpenText Fortify WebInspect HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
Include 'host' in HTTP request headers	Select this check box to include host headers with Fortify WebInspect HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit Fortify WebInspect performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when Fortify WebInspect is auditing that site. You can add multiple custom headers.

The following table describes the default custom headers.

Header	**Description**
Accept: */*	Any encoding or file type is acceptable to the crawler.
Pragma: no-cache	This forces a fresh response; cached or proxied data is not acceptable.

Adding a Custom Header

To add a custom header:

1. Click **Add**.
   The Specify Custom Header window opens.
2. In the **Custom Header** field, enter the header using the format <name>: <value>.
3. Click **OK**.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by Fortify WebInspect to the server when conducting a vulnerability scan.

The default custom cookie is

CustomCookie=WebInspect;path=/

which is used simply to flag the scan traffic.

Adding a Custom Cookie

To add a custom cookie:

1. Click **Add**.
   The Specify Custom Cookie window opens.
2. In the **Custom Cookie** field, enter the cookie using the format <name>=<value>.
   For example, if you enter
   CustomCookie=ScanEngine
   then each HTTP-Request will contain the following header:
   Cookie: CustomCookie=ScanEngine
3. Click **OK**.

Scan Settings: Proxy

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.
   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Proxy**.

Options

The following table describes the Proxy options.

Option	**Description**
Direct Connection (proxy disabled)	Select this option if you are not using a proxy server.
Auto detect proxy settings	Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's Web proxy settings.
Use System proxy settings	Import your proxy server information from the local machine.
Use Firefox proxy settings	Import your proxy server information from Firefox. **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy server will not be used.
Configure proxy using a PAC file URL	Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the **URL** field.
Explicitly configure proxy	Configure a proxy by entering the requested information: 1. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080). 2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard. 3. If authentication is required, select a type from the **Authentication** list: • **Automatic** • **Basic** • **Digest** • **Kerberos** • **Negotiate** • **NT LAN Manager (NTLM)**

Option	Description
	4. If your proxy server requires authentication, enter the qualifying user name and password. 5. 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 Proxy For** field. Use commas to separate entries.
Specify Alternative Proxy for HTTPS	For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Scan Settings: Authentication

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **Authentication**.

Authentication is the verification of identity as a security measure. Passwords and digital signatures are forms of authentication. You can configure automatic authentication so that a user name and password will be entered whenever OpenText Fortify WebInspect encounters a server or form that requires authentication. Otherwise, a crawl might be prematurely halted for lack of logon information.

Network Authentication

Select the **Scan requires network authentication** check box if users must log on to your Web site or application.

Authentication Method

If authentication is required, select the authentication method as follows:

- **ADFS CBT**
- **Automatic**
- **Basic**
- **Digest**
- **Kerberos**
- **Negotiate**
- **NT LAN Manager (NTLM)**

Authentication Credentials

Type a user ID in the **User name** field and the user's password in the **Password** field. To guard against mistyping, repeat the password in the **Confirm Password** field.

> **Caution!** Fortify WebInspect will crawl 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 a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact Fortify Customer Support.

Client Certificate

Client certificate authentication enables users to present client certificates rather than entering a user name and password. You can select a certificate from the local machine or a certificate assigned to a current user.

To use client certificates:

1. Select **Enable** in the **Client Certificates** group.
2. Click **Select** to open the Client Certificates window.
3. Choose a certificate.
4. Click **OK**.

When using tools that incorporate a proxy (specifically Web Macro Recorder, Web Proxy, Web Brute, and Web Form Editor), you may encounter servers that do not ask for a client certificate even though a certificate is required. To accommodate this situation, you must edit the SPI.Net.Proxy.Config file using the following procedure.

Task 1: Find your certificate's serial number

1. Open Microsoft Internet Explorer.
2. From the **Tools** menu, click **Internet Options**.
3. On the Internet Options window, select the **Content** tab and click **Certificates**.
4. On the Certificates window, select a certificate and click **View**.
5. On the Certificate window, click the **Details** tab.
6. Click the **Serial Number** field and copy the serial number that appears in the lower pane (highlight the number and press **Ctrl** + **C**).
7. Close all windows.

Task 2: Create an entry in the SPI.Net.Proxy.Config file

1. Open the `SPI.Net.Proxy.Config` file for editing. The default location is `C:\Program Files\Fortify\Fortify WebInspect`.
2. In the ClientCertificateOverrides section, add the following entry:

```
<ClientCertificateOverride HostRegex="<RegularExpression>"
CertificateSerialNumber="Number" />
```

where:

<RegularExpression> is a regular expression matching the host URL (example: .*austin\.myco\.com).

Number is the serial number obtained in Task 1.

3. Save the edited file.

Enable Macro Validation

Most dynamic application scans require user authentication to expose the complete surface of the application. Failure of the login macro to log in to the application results in a poor quality scan. If the login macro quality is measured before the scan, then low quality scans can be avoided.

Select Enable macro validation to enable Fortify WebInspect to test for inconsistencies in macro behavior at the start of the scan. For more information about the specific tests performed, see "Testing Login Macros" on page 360.

Use a Login Macro for Forms Authentication

This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent Fortify WebInspect from terminating prematurely if it inadvertently logs out of your application. When recording this type of macro, be sure to specify the application's log-out signature. Click the ellipsis button ... to locate the macro.

Login Macro Parameters

This section appears only if you have selected **Use a login macro for forms authentication** and the macro you have chosen or created contains fields that are designated as username and password parameters (if you used the Web Macro Recorder).

If you start a scan using a macro that includes parameters for user name and password, then when you scan the page containing the input elements associated with these entries, Fortify WebInspect substitutes the user name and password specified here. This feature enables you to create the macro using your own user name and password, yet when other persons run the scan using this macro, they can substitute their own user name and password.

If the macro uses parameters for which values are masked in the Web Macro Recorder, then these values are also masked when configuring a Guided Scan in Fortify WebInspect Enterprise.

For information about creating parameters using the Web Macro Recorder, see the Web Macro Recorder chapters in the *OpenText™ Fortify WebInspect Tools Guide*.

Use a Startup Macro

This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that Fortify WebInspect will use to navigate to that area. It may also include login information, but does not contain logic that will prevent Fortify WebInspect from logging out of your application. Fortify WebInspect visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). Click the ellipsis button ... to locate the macro. Click **Record** to record a 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 or all Burp Proxy captures. You cannot use different types of macros in the same scan.

Multi-user Login

You can use the Multi-user Login option to parameterize the username and password in a login macro, and then define multiple username and password pairs to use in a scan. This approach allows the scan to run across multiple threads. Each thread has a different login session, resulting in faster scan times.

> **Important!** To use Multi-user Login, you must first select **Use a login macro for forms authentication** and do one of the following:
>
> - Record a new macro and parameterize the credentials.
> - Select an existing macro that already has parameterized credentials.
>
> For more information, see "Use a Login Macro for Forms Authentication" on the previous page.

To use multiple user logins to conduct the scan:

1. Select the **Multi-user Login** checkbox.

   > **Note:** If you clear the Multi-user Login checkbox prior to running the scan, the additional credentials will not be used during the scan. Fortify WebInspect will use only the original credentials recorded in the login macro.

2. Continue according to the following table.

To...	**Then...**
Add a user's credentials	a. Under Multi-user Login, click **Add**. The Multi-user Credential Input dialog box appears. b. In the **Username** field, type a username c. In the **Password** field, type the corresponding password. d. Click **OK**. e. Repeat Steps a-d for each user login to add. **Important!** The number of shared requestor threads should not be more than the number of configured users. Requestor threads without valid users will cause the scan to run longer. Remember to

To...	Then...
	count the original username and password in the parameterized macro as the first user when you configure multiple users. For more information, see "Scan Settings: Requestor" on page 372.
Edit a user's credentials	a. Under Multi-user Login, select a Username/Password pair and click **Edit**. The Multi-user Credential Input dialog box appears. b. Edit the credentials as needed. c. Click **OK**.
Delete a user's credentials	a. Under Multi-user Login, select a Username/Password pair to be removed. b. Click **Delete**.

For more information, see "Multi-user Login Scans" on page 354.

Scan Settings: File Not Found

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **File Not Found**.

Options

The following table describes the File Not Found options.

Option	Description
Determine File Not Found (FNF) using HTTP response codes	Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories. • **Forced valid response codes (never a FNF)**: You can specify HTTP response codes that should never be treated as a file-not-found response. • **Forced FNF response codes (always a FNF)**: Specify those HTTP

Option	Description
	response codes that will always be treated as a file-not-found response. OpenText Fortify WebInspect will not process the response contents. Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a comma.
Determine FNF from custom supplied signature	Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result in Fortify WebInspect from 404 pages that are unique to your site. You can specify a signature using plain text, a regular expression, or, using the **SPI Regex** option, regular expression extensions (see the Web Console Help for more information). For information about the Regular Expression Editor tool, see the *OpenText™ Fortify WebInspect Tools Guide*.
Auto detect FNF page	Some Web sites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains a message that the file cannot be found, or they might redirect to a home page or login page. Select this check box if you want Fortify WebInspect to detect these "custom" file-not-found pages. Fortify WebInspect attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you select the **Auto detect FNF page** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

Scan Settings: User Agent

You can configure user agent settings that will synchronize in both Fortify WebInspect and the Event-based Web Macro Recorder.

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Scan Settings group in the left pane, click **User Agent**.

Profile and User-Agent String

You can select a predefined Profile that specifies the user agent string for the browser. The following table describes the available profiles.

Profile	User-Agent String
Default	`Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0`
Internet Explorer 6	`Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)`
Internet Explorer 7	`Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)`
Internet Explorer 8	`Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB5; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)`
Googlebot 2.1	`Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)`
Bingbot	`Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)`
Yahoo! Slurp	`Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)`
iPhone, iOS 14.3	`Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.1`
Custom	User-specified.

Profile	User-Agent String
	Important! We recommend that the Custom profile be used by advanced users only.

Navigator Interface Settings

The Navigator Interface settings provide information that legacy web applications use to facilitate browser detection. You can customize these settings if you require browser-specific behavior. The settings are:

- **appName** - All browsers return "Netscape" as the value of this property.
- **appVersion** - The browser returns either "4.0" or a string representing version information about the browser.
- **platform** - The browser returns an empty string or a string representing the platform on which the browser is running.

> **Examples:**
>
> `MacIntel`, `Win32`, `Win64`, `iPhone`

Crawl Settings: Link Parsing

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Crawl Settings group in the left pane, click **Link Parsing**.

OpenText Fortify WebInspect follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the Custom Links feature and regular expressions to identify links that you want Fortify WebInspect to follow. These are called special link identifiers.

Adding a Specialized Link Identifier

To add a specialized link identifier:

1. Click **Add**.

   The Specialized Link Entry window opens.
2. In the **Specialized Link Pattern** field, enter a regular expression designed to identify the link.
3. (Optional) Enter a description of the link in the **Comment** field.
4. Click **OK**.

Crawl Settings: Link Sources

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Crawl Settings group in the left pane, click **Link Sources**.

What is Link Parsing?

The OpenText Fortify WebInspect crawler sends a request to a start URL and recursively parses links (URLs) from the response content. These links are added to a work queue and the crawler iterates through the queue until it is empty. The techniques used to extract the link information from the HTTP responses are collectively referred to as ‘link parsing.’ There are two choices for how the crawler performs link parsing: Pattern-based and DOM-based.

Pattern-based Parsing

Pattern-based link parsing uses a combination of text searching and pattern matching to find URLs. These URLs include the ordinary content that is rendered by a browser, such as <A> elements, as well as invisible text that may reveal additional site structure.

This option matches the default behavior used by earlier versions of Fortify WebInspect. This is a more aggressive approach to crawling the website and can increase the amount of time it takes to conduct a scan. The aggressive behavior can cause the crawler to create many extra links which are not representative of actual site content. For these situations, DOM-based parsing should expose the site’s URL content with fewer false positives.

Note: All of the DOM-based Parsing techniques for finding links are used when Pattern-based Parsing is selected.

DOM-based Parsing

The Document Object Model (DOM) is a programming concept that provides a logical structure for defining and building HTML and XML documents, navigating their structure, and editing their elements and content.

A graphical representation of an HTML page rendered as DOM would resemble an upside-down tree: starting with the HTML node, then branching out in a tree structure to include the tags, sub-tags, and content. This structure is called a DOM tree.

Using DOM-based parsing, Fortify WebInspect parses HTML pages into a DOM tree and uses the detailed parsed structure to identify the sources of hyperlinks with higher fidelity and greater confidence. DOM-based parsing can reduce false positives and may also reduce the degree of ‘aggressive link discovery.’

On some sites, the crawler iteratively requests bad links and the resulting responses echo those links back in the response content, sometimes adding extra text that compounds the problem. These repeated cycles of ‘bad links in and bad links out’ can cause scans to run for a long time or, in rare cases, forever. DOM-based parsing and careful selection of link sources provide a mechanism for limiting this runaway scan behavior. Web applications vary in structure and content, and some experimentation may be required to get optimal link source configurations.

To refine DOM-based Parsing, select the techniques you want to use for finding links. Clearing techniques that may not be a concern for your site may decrease the amount of time it takes to complete the scan. For a more thorough scan, however, select all techniques or use Pattern-based Parsing. The DOM-based Parsing techniques are described in the following table. For more information, see "Limitations of Link Source Settings" on page 406.

Technique	Description
Include Comment Links (Aggressive)	Programmers may leave notes to themselves that include links inside HTML comments that are not visible on the site, but may be discovered by an attacker. Use this option to find links inside HTML comments. Fortify WebInspect will find more links, but these may not always be valid URLs, causing the crawler to try to access content that does not exist. Also, the same link can be on every page and those links can be relative, which can exponentially increase the URL count and lengthen the scan time.

Include Conditional Comment Links	A conditional comment link occurs when the HTML on the page is conditionally included or excluded depending on the user agent (browser type and version) making the request.
	Regular comment example:
	`<!–hidden.txt -->`
	Conditional comment example:
	`<!--[if lt IE9]>`
	`<script src="//www.somesite.com/static/v/all/js/html5sh.js"></script>`
	`<link rel="stylesheet" type"text/css" href='//www.somesite.com/static/v/fn/css/IE8.css'>`
	`<![endif]-->`
	Fortify WebInspect emulates browser behaviors in evaluating HTML code and processes the DOM differently depending on the user agent. A link found in a comment by one user agent is a normal HTML link for other user agents.
	Use this option to find conditional links that are inside HTML commands, such as those commented out based on browser version. These conditional statements may also contain script includes that need to be executed when script parsing is enabled. Crawling these links will be more thorough, but can increase the scan time. Additionally, such comments may be out of date and pointless to crawl.

Include Plain Text Links	Plain text in a .txt file or a paragraph inside HTML code can be formatted as a URL, such as `http://www.something.com/mypage.html`. However, because this is only text and not a true link, the browser would not render it as a link, and the text would not be functionally part of the page. For example, the content may be part of a page that describes how to code in HTML using fake syntax that is not meant to be clicked by users. Use this option for Fortify WebInspect to parse these text links and queue them for a crawl. Also, using smart pattern matches, Fortify WebInspect can identify common file extensions, such as .css, .js, .bmp, .png, .jpg, .html, etc., and add these files to the crawl queue. Auditing these files that are referenced in plain text can produce false positives.

Include Links in Static Script blocks	Use this option for Fortify WebInspect to examine inside the opening and closing script tags for text that looks like links. Valid links may be found inside these script blocks, but developers may also leave comments that include text resembling links inside the opening and closing script tags. For example:
	`<script type="text/javascript">`
	`// go to http://www.foo.com/blah.html for help`
	`var url = "http:www.foo.com/xyz/" + path + "?help"`
	`</script>`
	Additionally, JavaScript code inside these tags can be handled by the JavaScript execution engine during the scan. However, searching for static links in a line of code that sets a variable, such as the “var url” in the example above, can create problems when those partial paths are added to the queue for crawling. If the variable includes a relative link with a common extension, such as “foo.html”, the crawler will append the extension to the end of every page that includes the line of code. This can produce unusable URLs and may create false positives.

Parse URLs Embedded in URLs	Use this option for Fortify WebInspect to parse any text that is inside an href attribute and add it to the crawl queue. The following is an example of a URL embedded in a URL:
	`<a href="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />`
	On some sites, however, file not found pages return the URL in a form action tag and append the URL to the original URL as follows:
	`<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah?`

	`http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />`
	Fortify WebInspect will then request the form action, and receive another file not found response, again with the URL appended in a form action, as shown below:
	`<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />`
	On such a site, these URLs will continue to produce file not found responses that add more URLs to the crawl queue, creating an infinite crawl loop. To avoid adding this type of URL to the crawl queue, do not use this option.

Allow Un-rooted URLs (for the above items)	This option modifies the behavior of the previous five options. Some links do not include the specific scheme, such as http, and are not fully qualified domain names. These links, which may resemble “xyz.html”, are considered unanchored or “un-rooted.” A relative link, such as “/xyz.html”, is not considered to be un-rooted because it is relative to the homepage and the link can be resolved. Use this option to treat un-rooted URLs as links when parsing. If this option is selected, the scan will be more thorough and more aggressive, but may take considerably longer to complete.

Form Actions, Script Includes, and Stylesheets

Some link types—such as form actions, script includes, and stylesheets—are special and are treated differently than other links. On some sites, it may not be necessary to crawl and parse these links. However, if you want an aggressive scan that attempts to crawl and parse everything, the following options will help accomplish this goal. For more information, see "Limitations of Link Source Settings" on page 406.

> **Note:** You can also allow un-rooted URLs for each of these options. See “Allow Un-rooted URLs” above.

Option	Description
Crawl Form Action Links	When Fortify WebInspect encounters HTML forms during the crawl, it creates variations on the inputs that a user can make and submits the forms as requests to solicit more site content. For example, for forms with

	a POST method, Fortify WebInspect can use a GET instead and possibly reveal information. In addition to this type of crawling, use this option for Fortify WebInspect to treat form targets as normal links.
Crawl Script Include Links	A script include imports JavaScript from a .js file and processes it on the current page. Use this option for Fortify WebInspect to crawl the .js file as a link.
Crawl Stylesheet Links	A stylesheet link imports the style definitions from a .css file and renders them on the current page. Use this option for Fortify WebInspect to crawl the .css file as a link.

Miscellaneous Options

The following additional options may help improve link parsing for your site. For more information, see "Limitations of Link Source Settings" on the next page.

Option	Description
Crawl Links on FNF Pages	If you select this option, Fortify WebInspect will look for and crawl links on responses that are marked as "file not found." This option is selected by default when the Scan Mode is set to Crawl Only or Crawl & Audit. The option is not available when the Scan Mode is set to Audit Only.
Suppress URLs with Repeated Path Segments	Many sites have text that resembles relative paths that become unusable URLs after Fortify WebInspect parses them and appends them to the URL being crawled. These occurrences can result in a runaway scan if paths are continuously appended, such as `/foo/bar/foo/bar/`. This setting helps reduce such occurrences and is enabled by default. With the setting **enabled**, the options are: **1** – Detect a single sub-folder repeated anywhere in the URL and reject the URL if there is a match. For example, `/foo/baz/bar/foo/` will match because "`/foo/`" is repeated. The repeat does not have to occur adjacently. **2** – Detect two (or more) pairs of adjacent sub-folders and reject the URL if there is a match. For example, `/foo/bar/baz/foo/bar/` will match because "`/foo/bar/`" is repeated. **3** – Detect two (or more) sets of three adjacent sub-folders and reject the

	URL if there is a match. **4** – Detect two (or more) sets of four adjacent sub-folders and reject the URL if there is a match. **5** – Detect two (or more) sets of five adjacent sub-folders and reject the URL if there is a match. If the setting is **disabled**, repeating sub-folders are not detected and no URLs are rejected due to matches.

Limitations of Link Source Settings

Clearing a link source check box prevents the crawler from processing that specific kind of link when it is found using static parsing. However, these links can be found in many other ways. For example, clearing the **Crawl Stylesheet Links** option does not control path truncation nor suppress .css file requests made by the script engine. Clearing this setting only prevents static link parsing of the .css response from the server. Similarly, clearing the **Crawl Script Include Links** option does not suppress .js, AJAX, frameIncludes, or any other file request made by the script engine. Therefore, clearing a link source check box is not a universal filter for that type of link source.

The goal for clearing a check box is to prevent potentially large volumes of bad links from cluttering the crawl and resulting in extremely long scan times.

Crawl Settings: Session Exclusions

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Crawl Settings group in the left pane, click **Session Exclusions**.

All items specified in the **Scan Settings - Session Exclusions** are automatically replicated in the **Session Exclusions** for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the **Scan Settings - Session Exclusions** panel.

This panel (**Crawl Settings - Session Exclusions**) enables you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested.

If you select **Exclude**, files having the specified extension will be requested, but will not be audited.

Adding a File Extension to Exclude/Reject

To add a file extension:

1. Click **Add**.

   The Exclusion Extension window opens.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited.

Adding a MIME Type to Exclude

To add a MIME Type:

1. Click **Add**.

   The Provide a Mime-type to Exclude window opens.
2. In the **Exclude Mime-type** field, enter a MIME type.
3. Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject** - OpenText Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

Editing the Default Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Reject or Exclude a Host or URL window opens.
2. Select either **Host** or **URL**.
3. In the **Host** or **URL** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.

4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

Adding Exclusion/Rejection Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected **Query parameter** or **Post parameter** as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
   - **matches regex** - Matches the regular expression you specify in the **Match String** field.
   - **matches regex extension** - Matches a syntax available from OpenText's regular expression extensions you specify in the **Match String** field. For information about the Regular Expression Editor, see the Regular Expression Editor chapter in the *OpenText™ Fortify WebInspect Tools Guide*.
   - **matches** - Matches the text string you specify in the **Match String** field.
   - **contains** - Contains the text string you specify in the **Match String** field.
5. In the **Match String** field, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click ➕ (or press **Enter**).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.
10. When the exclusion appears in the **Other Exclusion/Rejection Criteria** list, select either **Reject**, **Exclude**, or both.

    Note: You cannot reject Response, Response Header, and Status Code Target types during a scan. You can only exclude these Target types.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, Fortify WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

Audit Settings: Session Exclusions

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Audit Settings group in the left pane, click **Session Exclusions**.

All items specified in the **Scan Settings - Session Exclusions** are automatically replicated in the **Session Exclusions** for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the **Scan Settings - Session Exclusions** panel.

This panel (**Audit Settings - Session Exclusions**) enables you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, OpenText Fortify WebInspect will not request files having the specified extension.

If you select **Exclude**, Fortify WebInspect will request files having the specified extension, but will not audit them.

Adding a File Extension to Exclude/Reject

To add a file extension:

1. Click **Add**.

   The Exclusion Extension window opens.
2. In the **File Extension** field, enter a file extension.
3. Select either **Reject**, **Exclude**, or both.
4. Click **OK**.

Excluded MIME Types

Fortify WebInspect will not audit files associated with the MIME types you specify.

Adding a MIME Type to Exclude

To add a MIME type:

1. Click **Add**.

   The Provide a Mime-type to Exclude window opens.
2. In the **Exclude Mime-Type** field, enter a MIME type.
3. Click **OK**.

Other Exclusion/Rejection Criteria

You can identify various components of an HTTP message and then specify whether you want to exclude or reject a session that contains that component.

- **Reject** - Fortify WebInspect will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.
- **Exclude** - During a crawl, Fortify WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, Fortify WebInspect will not attack the

specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

Editing the Default Criteria

To edit the default criteria:

1. Select a criterion and click **Edit** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Reject or Exclude a Host or URL window opens.
2. Select either **Host** or **URL**.
3. In the **Host** or **URL** field, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
4. Select either **Reject**, **Exclude**, or both.
5. Click **OK**.

Adding Exclusion/Rejection Criteria

To add exclusion/rejection criteria:

1. Click **Add** (on the right side of the **Other Exclusion/Rejection Criteria** list).

   The Create Exclusion window opens.
2. Select an item from the **Target** list.
3. If you selected **Query parameter** or **Post parameter** as the target, enter the **Target Name**.
4. From the **Match Type** list, select the method to be used for matching text in the target:
   - **matches regex** - Matches the regular expression you specify in the **Match String** field.
   - **matches regex extension** - Matches a syntax available from OpenText's regular expression extensions you specify in the **Match String** field. For information about the Regular Expression Editor, see the Regular Expression Editor chapter in the *OpenText™ Fortify WebInspect Tools Guide*.
   - **matches** - Matches the text string you specify in the **Match String** field.
   - **contains** - Contains the text string you specify in the **Match String** field.
5. In the **Match String** field, enter the string or regular expression for which the target will be searched. Alternatively, if you selected a regular expression option in the **Match Type**, you can click the drop-down arrow and select **Create Regex** to launch the Regular Expression Editor.
6. Click ➕ (or press Enter).
7. (Optional) Repeat steps 2-6 to add more conditions. Multiple matches are ANDed.
8. If you are working in Current Settings, you can click **Test** to process the exclusions on the current scan. Any sessions from that scan that would have been filtered by the criteria will appear in the test screen, allowing you to modify your settings if required.
9. Click **OK**.

10. When the exclusion appears in the **Other Exclusion/Rejection Criteria** list, select either **Reject**, **Exclude**, or both.

    > **Note:** You cannot reject Response, Response Header, and Status Code Target types during a scan. You can only exclude these Target types.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following exclusion and select **Reject**.

Target	Target Name	Match Type	Match String
URL	N/A	contains	Microsoft.com

Example 2

Enter "logout" as the match string. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the "logout" example, Fortify WebInspect would exclude or reject URLs such as logout.asp or applogout.jsp.

Target	Target Name	Match Type	Match String
URL	N/A	contains	logout

Example 3

The following example rejects or excludes a session containing a query where the query parameter "username" equals "John."

Target	Target Name	Match Type	Match String
Query parameter	username	matches	John

Example 4

The following example excludes or rejects the following directories:

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

Target	Target Name	Match Type	Match String
URL	N/A	matches regex	/W3SVC[0-9]*/

Audit Settings: Attack Exclusions

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Audit Settings group in the left pane, click **Attack Exclusions**.

Excluded Parameters

Use this feature to prevent OpenText Fortify WebInspect from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

Adding Parameters to Exclude

To prevent certain parameters from being modified:

1. In the **Excluded Parameters** group, click **Add**.

   The Specify HTTP Exclusion window opens.
2. In the **HTTP Parameter** field, enter the name of the parameter you want to exclude.

   Click ▶ to insert regular expression notations.
3. Choose the area(s) in which the parameter may be found: **HTTP query data**, **HTTP post data**, and/or **HTTP custom data**.
4. Click **OK**.

Excluded Cookies

Use this feature to prevent Fortify WebInspect from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values.

This setting requires you to enter the name of a cookie. In the following example HTTP response ...

Set-Cookie: FirstCookie=Chocolate+Chip; path=/

... the name of the cookie is "FirstCookie."

Excluding Certain Cookies

To exclude certain cookies:

1. In the **Excluded Headers** group, click **Add**.

   The Regular Expression Editor appears.

   > **Note:** You can specify a cookie using either a text string or a regular expression.

2. To enter a text string:
   a. In the **Expression** field, type a cookie name.
   b. Click **OK**.
3. To enter a regular expression:
   a. In the **Expression** field, type or paste a regular expression that you believe will match the text for which you are searching.

      Click ▶ to insert regular expression notations.
   b. In the **Search Text** field, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** field).
   c. To find only those occurrences matching the case of the expression, select the **Match Case** check box.
   d. If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** field.
   e. Click **Test** to search the Search Text for strings that match the regular expression. Matches will be highlighted in red.
   f. Did your regular expression identify the string?
      - If *yes*, click **OK**.
      - If *no*, verify that the Search Text contains the string you want to identify or modify the regular expression.

Excluded Headers

Use this feature to prevent Fortify WebInspect from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

Excluding Certain Headers

To prevent certain headers from being modified, create a regular expression using the procedure described below.

1. In the **Excluded Headers** group, click **Add**.

   The Regular Expression Editor appears.

   > **Note:** You can specify a header using either a text string or a regular expression.
2. To enter a text string:
   a. In the **Expression** field, type a header name.
   b. Click **OK**.
3. To enter a regular expression:
   a. In the **Expression** field, type or paste a regular expression that you believe will match the text for which you are searching.

      Click ▶ to insert regular expression notations.

b. In the **Search Text** field, type or paste the text that is known to contain the string you want to find (as specified in the **Expression** field).

c. To find only those occurrences matching the case of the expression, select the **Match Case** check box.

d. If you want to replace the string identified by the regular expression, select the **Replace** check box and then type or select a string from the **Replace** field.

e. Click **Test** to search the Search Text for strings that match the regular expression. Matches will be highlighted in red.

f. Did your regular expression identify the string?

   - If *yes*, click **OK**.
   - If *no*, verify that the Search Text contains the string you want to identify or modify the regular expression.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create or modify parameters for audit engines and checks that require inputs.

- To launch the tool, click **Audit Inputs Editor**.
- To load inputs that you previously created using the editor, click **Import Audit Inputs**.

For detailed instructions on using the Audit Inputs Editor, see the Audit Inputs Editor chapter of the *OpenText™ Fortify WebInspect Tools Guide*.

Audit Settings: Attack Expressions

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Audit Settings group in the left pane, click **Attack Expressions**.

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan
- ja-jp: Japanese - Japan
- ko-kr: Korean - Korea
- pt-br: Portuguese - Brazil
- es-es: Spanish - Spain

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Audit Settings: Vulnerability Filtering

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Audit Settings group in the left pane, click **Vulnerability Filtering**.

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition** - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection Dom Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

Adding a Vulnerability Filter

All available filters are listed in either the **Disabled Filters** list or the **Enabled Filters** list.

To enable one or more filters:

1. Select the desired filters in the **Disabled Filters** list.
2. Click **Add**.

   The filters are moved to the **Enabled Filters** list.

To disable one or more filters:

1. Select the desired filters in the **Enabled Filters** list.
2. Click **Remove**.

   The filters are moved to the **Disabled Filters** list.

Audit Settings: Smart Scan

To access this feature from a Guided Scan:

1. Click the **Advanced** button in the toolbar Settings group.

   The Scan Settings window opens.
2. In the Audit Settings group in the left pane, click **Smart Scan**.

Enable Smart Scan

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, OpenText Fortify WebInspect will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select the **Enable Smart Scan** option, you can choose one or more of the identification methods described below.

Use regular expressions on HTTP responses to identify server/application types

This method, employed by previous releases of Fortify WebInspect, searches the server response for strings that match predefined regular expressions designed to identify specific servers.

Use server analyzer fingerprinting and request sampling to identify server/application types

This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server/application type.

Custom server/application type definitions (more accurate detection)

If you know the server type for a target domain, you can select it using the **Custom server/application type definitions (more accurate detection)** section. This identification method overrides any other selected method for the server you specify.

1. Click **Add**.

   The Server/Application Type Entry window opens.
2. In the **Host** field, enter the domain name or host, or the server's IP address.
3. (Optional) Click **Identify**.

   Fortify WebInspect contacts the server and uses the server analyzer fingerprinting method to determine the server type. If successful, it selects the corresponding check box in the **Server/Application Type** list.

   > **Note:** Alternatively, if you select the **Use Regular Expressions** option, enter a regular expression designed to identify a server. Click ▶ to insert regular expression notations or to launch the Regular Expression Editor (which facilitates the creation and testing of an

expression).

4. Select one or more entries from the **Server/Application Type** list.
5. Click **OK**.

Send Documentation Feedback

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

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

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

Feedback on User Guide (Fortify WebInspect Enterprise 23.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!