

# HP WebInspect Enterprise

for the Windows<sup>®</sup> operating system

Software Version: 10.20

---

## User Guide

Document Release Date: April 2014

Software Release Date: April 2014



## Legal Notices

### Copyright Notice

© Copyright 2014 Hewlett-Packard Development Company, L.P.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Disclaimer of Warranty

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

### Trademark Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

### Other Acknowledgements

This product contains the following Apache open source component: Log4Net (<http://logging.apache.org/log4net/>). This component was modified from its original form and incorporated into this software product. To learn more about the apache software license, please visit <http://www.apache.org/licenses/LICENSE-2.0>.

## Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- 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.

To check for recent updates, or to verify that you are using the most recent edition of a document, visit the following URL:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

For information or assistance regarding WebInspect Enterprise, contact customer support.

You can open a support case for WebInspect Enterprise via e-mail, online, or by telephone. These options are designed to provide easier access and improved customer satisfaction.

### E-Mail (Preferred Method)

Send an e-mail to [fortifytechsupport@hp.com](mailto:fortifytechsupport@hp.com) describing your issue. Please include the product name so we can help you faster.

### Online (Fortify Support Portal)

Access your account at the Fortify Support Portal at <https://support.fortify.com>

If you do not have an account, you forgot your username or password, or you need any assistance regarding your account, please contact us at [fortifytechsupport@hp.com](mailto:fortifytechsupport@hp.com) or (650) 735-2215.

### Telephone

Call our automated processing service at (650) 735-2215. Please clearly provide your name, telephone number, the name of the product, and a brief description of the issue.

# Contents

<b>1</b>	<b>Introduction</b>	<b>13</b>
	About WebInspect Enterprise	13
	About Scanning: Consequences and Considerations	14
<b>2</b>	<b>WebInspect Enterprise Administrative Console</b>	<b>17</b>
	Logging On	17
	Changing the Refresh Rate	18
	About the Administrative Console User Interface	18
	About SmartUpdates	21
	About the Scans Group and its Shortcuts	22
	Stopping, Suspending, Resuming, or Deleting Scans in the Scan Queue	22
	Managing System, Custom, and Master Scan Policies	23
	Creating Custom and Master Scan Policies	24
	About the Sensors Group and its Shortcut	25
	Managing Sensors and Their Scans	25
	About the Administration Group and its Shortcuts	27
	Managing the Activity Log	27
	Managing Connected Users	28
	Displaying License Information	29
	Displaying SmartUpdate History and Managing SmartUpdate Schedules	29
	Adding a SmartUpdate Schedule	31
	Approving and Declining SmartUpdates	31
	Managing Export Paths	32
	Managing E-mail Alerts	33
	Managing SNMP Alerts	34
	Managing Sensor Users	35
	About Roles and Permissions	36
	Managing Roles and Permissions	37
	Adding a User or Group to Multiple Roles Simultaneously	38
	Displaying the Roles of a User or Group or Removing a User or Group from Roles	38
	About WebInspect Enterprise System Administrators, Roles, and Permissions	39
	Managing Administrators for the WebInspect Enterprise System	39
	Adding a System Administrator	39
	Removing a System Administrator	40
	Managing Roles at the WebInspect Enterprise System Level	40
	Adding a WebInspect Enterprise System Role	40
	Adding Groups or Users to a WebInspect Enterprise System Role	40
	Copying a WebInspect Enterprise System Role	41
	Managing Global Roles	41

Creating a Global Role . . . . .	41
Removing a Global Role . . . . .	42
Distributing an Existing Global Role to All Organizations . . . . .	42
About Organization Administrators, Roles, and Permissions . . . . .	42
Managing Organizations . . . . .	43
Adding an Organization to the WebInspect Enterprise System . . . . .	43
Removing an Organization . . . . .	43
Renaming an Organization . . . . .	44
Managing Administrators for Organizations . . . . .	44
Adding an Organization Administrator . . . . .	44
Removing an Organization Administrator . . . . .	44
Configuring Organization Options . . . . .	44
Configuring Organization Maximum Scan Priority . . . . .	45
Configuring Organization Options: Disable Retest Browser Tab . . . . .	45
Managing Roles at the Organization Level . . . . .	45
Adding an Organization Role . . . . .	45
Adding Groups or Users to an Organization Role . . . . .	46
Copying or Moving an Organization Role . . . . .	46
Removing an Organization Role . . . . .	46
Renaming an Organization Role . . . . .	47
Managing Resources that are Available to Organizations . . . . .	47
Moving or Copying Objects to Other Organizations or Groups . . . . .	48
About Group Administrators, Roles, and Permissions . . . . .	48
Managing Groups . . . . .	49
Adding a Group . . . . .	49
Removing a Group . . . . .	50
Renaming a Group . . . . .	50
Managing Administrators for Groups . . . . .	51
Adding a Group Administrator . . . . .	51
Removing a Group Administrator . . . . .	51
Configuring Group Options . . . . .	51
Configuring Group Maximum Scan Priority . . . . .	51
Configuring Group IP and Host Permissions . . . . .	51
Managing Roles at the Group Level . . . . .	52
Adding a Group Role . . . . .	52
Adding Groups or Users to a Group Role . . . . .	52
Copying or Moving a Group Role . . . . .	53
Removing a Group Role . . . . .	53
Renaming a Group Role . . . . .	54
Managing Resources that are Available to Groups . . . . .	54
Moving or Copying Objects to Other Groups or Organizations . . . . .	55
Managing Proxy Server Settings . . . . .	55
Configuring Settings for SSC and Importing Projects into SSC from a .csv File . . . . .	56
Importing Projects into SSC from a .csv File Created by the Web Discovery Tool . . . . .	56
Managing Site Migration . . . . .	57
<b>3 WebInspect Enterprise Services Manager . . . . .</b>	<b>61</b>
About the Services Manager . . . . .	61

Configuring the Scan Uploader Service . . . . .	61
Service Status . . . . .	61
WebInspect Enterprise Configuration . . . . .	62
Dropbox Configuration . . . . .	62
Logging Configuration . . . . .	63
Start the Service . . . . .	63
Configuring the Task Service . . . . .	63
Service Status . . . . .	63
Database Configuration . . . . .	64
Logging Configuration . . . . .	64
SSC Poll Interval . . . . .	65
Start the Service . . . . .	65
Configuring the Scheduler Service . . . . .	65
Service Status . . . . .	65
WebInspect Enterprise Manager . . . . .	66
Logging Configuration . . . . .	66
Start the Service . . . . .	66
<b>4 WebInspect Enterprise Web Console . . . . .</b>	<b>67</b>
About the Web Console . . . . .	67
Logging Off, Configuring Options, and Viewing Information . . . . .	68
Configuring Default Group, Time Zone, and Available Scan and Blackout Actions . . . . .	69
About the Navigation Pane . . . . .	69
Configuring Scans, Scan Schedules, and Blackout Schedules (Actions Group) . . . . .	70
Configuring a Guided Scan . . . . .	70
Configuring a Web Site Scan . . . . .	70
Configuring a Web Service Scan . . . . .	70
Configuring a New Scan Schedule . . . . .	70
Configuring a New Blackout Schedule . . . . .	71
Displaying Project Versions, Scans, Scan Requests, and Scan Schedules (Filtered Views Group) . . . . .	71
Displaying Project Versions . . . . .	71
Displaying Scans . . . . .	75
Displaying Scan Requests . . . . .	78
Displaying Scan Schedules . . . . .	80
Adding a Scan Schedule . . . . .	80
General . . . . .	81
Recurrence . . . . .	81
Managing Scan Templates and Blackout Schedules (Resources Group) . . . . .	82
Managing Scan Templates . . . . .	82
Adding a Scan Template . . . . .	83
Managing Blackout Periods . . . . .	83
Adding a Blackout Period . . . . .	84
General . . . . .	84
Recurrence . . . . .	85
Displaying Deleted Project Versions (Administration Group) . . . . .	86
About Dependencies . . . . .	86
About Editing Form Layouts . . . . .	87

Configuring Which Columns to Display . . . . .	88
Configuring Grouping . . . . .	88
Configuring Sorting . . . . .	89
Configuring Paging . . . . .	89
About Scan Visualization. . . . .	89
About the Navigation Pane . . . . .	90
About the Site View . . . . .	90
About the Sequence View. . . . .	90
About the Excluded Hosts View. . . . .	91
About the Navigation Pane Icons. . . . .	91
About the Navigation Pane Shortcut Menu . . . . .	92
About the Information Pane . . . . .	93
About the Scan Info Panel . . . . .	93
About the Session Info Panel . . . . .	95
About the Summary Pane. . . . .	96
About the Vulnerabilities Tab. . . . .	96
About the Not Found Tab. . . . .	97
About the Information Tab . . . . .	97
About the Best Practices Tab . . . . .	98
About the Scan Log Tab. . . . .	98
About the Server Information Tab . . . . .	98
About the Reports Tab . . . . .	98
Reviewing and Retesting Vulnerabilities . . . . .	98
Editing and Adding Vulnerabilities . . . . .	100
About the Toolbar. . . . .	101
About Guided Scan . . . . .	102
About the Web Site Scan Wizard. . . . .	102
Specifying Scan Options in the Web Site Scan Step . . . . .	102
Specifying Authentication and Connectivity Options . . . . .	104
Specifying a Policy in the Coverage and Thoroughness Step . . . . .	105
Specifying a Template, Scan Priority, and Sensor in the Congratulations Step . . . . .	105
About the Web Service Scan Wizard . . . . .	106
Specifying Scan Options in the Web Service Scan Step . . . . .	106
Specifying Authentication and Connectivity Options . . . . .	106
Viewing the Coverage and Thoroughness Step . . . . .	107
Specifying a Template, Scan Priority, and Sensor in the Congratulations Step . . . . .	107
About Advanced Scan Settings . . . . .	107
SCAN . . . . .	108
General . . . . .	108
SCAN SETTINGS . . . . .	109
Method . . . . .	109
General . . . . .	110
Content Analyzers . . . . .	113
Requestor . . . . .	114
Session Storage. . . . .	115
Session Exclusions . . . . .	116
Allowed Hosts . . . . .	117



HTTP Parsing .....	118
Filters .....	119
Cookies/Headers .....	119
Proxy .....	120
Authentication .....	121
File Not Found .....	122
Policy .....	122
CRAWL SETTINGS .....	123
Link Parsing .....	123
Session Exclusions .....	123
AUDIT SETTINGS .....	124
Session Exclusions .....	124
Attack Exclusions .....	125
Attack Expressions .....	126
Vulnerability Filters .....	126
Smart Scan .....	126
SCAN BEHAVIOR .....	127
Blackout Action .....	127
EXPORT .....	127
General .....	127
<b>5 Guided Scan for Web Sites, Using Predefined Templates .....</b>	<b>129</b>
About Guided Scan .....	129
Guided Scan Templates .....	130
Predefined Templates .....	130
Mobile Templates .....	130
About the Toolbar Buttons .....	131
About the Guided Scan Steps .....	132
Configuring the Guided Scan .....	133
Site .....	133
Start Parameters .....	133
Login .....	135
Network Authentication .....	135
Application Authentication .....	136
Workflows .....	137
Workflows .....	137
Active Learning .....	138
Optimization Tasks .....	138
Settings .....	140
Final Review .....	140
Importing HP Unified Functional Testing (UFT) Files in a Guided Scan .....	140
Specifying Advanced Scan Settings for Guided Scan .....	141
Method .....	142
Scan Mode .....	142
Crawl and Audit Mode .....	142
Crawl and Audit Details .....	142
Navigation .....	143

General	143
Scan Details	143
Crawl Details	146
Audit Details	148
Content Analyzers	148
Silverlight	148
Flash	148
JavaScript/VBScript	148
Recommendations	149
Run Recommendation Modules when the scan is paused or completed	149
Network Authentication	150
Web Macro	150
File Not Found	150
Web Service	150
Form Values	150
Custom Parameters	150
Mobile Site	151
Requestor	151
Requestor Performance	151
Requestor Settings	152
Stop Scan If Loss Of Connectivity Detected	152
Session Storage	153
Log Rejected Session to Database	153
Session Storage	154
Session Exclusions	154
Excluded or Rejected File Extensions	154
Excluded MIME Types	154
Other Exclusion/Rejection Criteria	155
Allowed Hosts	157
HTTP Parsing	157
HTTP Parameters Used for State	157
Determine State from URL Path	158
HTTP Parameters Used for Navigation	158
Advanced HTTP Parsing	158
Custom Parameters	159
URL Rewriting	159
RESTful Services	159
Enable automatic seeding of rules which were not used during a scan	160
Double Encode URL Parameters	160
Creating Rules for Matrix and Path Parameters	161
Filters	164
Filter HTTP Request Content	164
Filter HTTP Response Content	164
Cookies/Headers	165
Standard Header Parameters	165
Append Custom Headers	165
Append Custom Cookies	165

Proxy .....	166
Proxy Settings.....	166
Authentication .....	168
Scan requires network authentication.....	168
Client Certificates.....	168
Specifying Client Certificates When Tools Should Require Them .....	168
Site Authentication.....	169
File Not Found .....	169
Determine ‘File Not Found’ (FNF) using HTTP response codes .....	169
Determine ‘FNF’ from custom supplied signature.....	170
Auto detect ‘FNF’ page .....	170
Policy .....	170
Creating a Policy .....	170
Importing a Policy .....	171
Deleting a Policy .....	171
Editing a Policy .....	171
Specifying Advanced Crawl Settings for Guided Scan.....	171
Link Parsing.....	172
Session Exclusions.....	172
Excluded or Rejected File Extensions .....	172
Excluded MIME Types.....	172
Other Exclusion/Rejection Criteria .....	173
Specifying Advanced Audit Settings for Guided Scan .....	175
Session Exclusions.....	175
Excluded or Rejected File Extensions .....	175
Excluded MIME Types.....	175
Other Exclusion/Rejection Criteria .....	176
Attack Exclusions.....	177
Excluded Parameters .....	177
Excluded Cookies.....	178
Excluded Headers.....	179
Audit Inputs Editor and Import Audit Inputs Buttons .....	179
Attack Expressions.....	180
Vulnerability Filtering .....	180
Select Vulnerability Filters to Enable.....	180
Smart Scan .....	181
Enable Smart Scan .....	181
Use regular expressions on HTTP responses to identify server/application types.....	181
Use server analyzer fingerprinting and request sampling to identify server/application types .....	181
Custom server/application type definitions (more accurate detection) .....	181
<b>6 Guided Scan Using Mobile Templates .....</b>	<b>183</b>
About Guided Scans Using Mobile Templates .....	183
About Mobile Scans.....	183
Creating a Mobile Scan .....	184
Creating a Custom User Agent Header .....	185
About the Site Stage.....	186

Verifying the Web Site .....	186
Choosing the Scan Type .....	187
About the Login Stage .....	188
Network Authentication Step .....	188
Application Authentication Step .....	189
About the Workflows Stage .....	190
Importing Burp Proxy Results .....	190
About the Active Learning Stage .....	190
Profiling the site for optimal settings .....	191
Enhancing coverage of your web site .....	192
Web Form Values .....	192
About the Settings Stage .....	193
Final Review Step .....	193
About Native Scans .....	194
Supported Devices .....	195
Supported Development Emulators .....	195
Creating a Native Scan .....	195
About the Native Mobile Stage .....	196
Choosing the Device/Emulator Type .....	197
Choosing the Scan Type .....	200
About the Login Stage .....	200
Network Authentication Step .....	201
Application Authentication Step .....	201
About the Application Stage .....	202
Run Application Step .....	202
About the Settings Stage .....	203
Final Review Step .....	203
Post Scan Steps .....	203
<b>A Policies .....</b>	<b>205</b>
About Policies .....	205
List of Policies .....	205

# 1 Introduction

This chapter introduces the functionality and interfaces of WebInspect Enterprise, and describes considerations and consequences of scanning.

## About WebInspect Enterprise

WebInspect Enterprise is a distributed network of HP scanners controlled by a system manager with a centralized database. WebInspect Enterprise must be integrated with HP Fortify Software Security Center (SSC) and it provides SSC with information detected through dynamic scans of Web sites and Web services.

This innovative architecture allows 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 HP scanners across your organization controlling product updates, scan policies, scan permissions, tools usage and scan results, all centrally from the 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 HP scanners or the 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 through a centralized database of scan results.
- Facilitate integration with third-party products and deployment of customized Web-based front ends using the WebServices application programming interface (API).

WebInspect Enterprise comprises the following:

- The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console or the Administrative Console. The Administrative Console is used for administrative and security functions. It is described in [Chapter 2, WebInspect Enterprise Administrative Console](#).
- The WebInspect Enterprise Services Manager, also known as the WebInspect Enterprise Services Configuration Utility. This interface is used to configure or modify services associated with WebInspect Enterprise.
- The 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. It is described in [Chapter 4, WebInspect Enterprise Web Console](#).
- The WebInspect Enterprise Thin Client download, which contains the following:
  - Guided Scan. This function directs you through the best steps to configure a scan that is tailored to your application, and is the preferred alternative to the standard Web Site scan. It is described in [Chapter 5, Guided Scan for Web Sites, Using Predefined Templates](#).

- Report generation. This function creates a new report from a scan the user selects. The reports available in WebInspect Enterprise are a subset of the reports available in WebInspect. For more information, see [About the Reports Tab](#) on page 98 and [About the Toolbar](#) on page 101.

The first time a user launches Guided Scan or creates a report in WebInspect Enterprise or Software Security Center (SSC), the WebInspect Enterprise Thin Client application, including and installation wizard and its own Help system, is automatically downloaded and installed on the user's local computer. Then the interface for the function the user selected opens, and Help becomes available for either function any time you use it. You can also refer to this guide.

- Scanners. Two types of scanners are supported:
  - Sensor - This is the WebInspect application when connected to WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans with no direct user interaction through its graphical user interface. It receives its instructions exclusively from the configurable connection to a WebInspect Enterprise Manager.
  - Client - A client is any HP scanner that connects to WebInspect Enterprise to receive license, permissions, updates or scan data, and which also presents a user interface through which scans may be conducted. WebInspect Enterprise controls permissions for a client and also provides the policies used by clients. A client can be configured to upload scan results to WebInspect Enterprise automatically at the completion of the scan or only when specifically instructed by the user.
- Microsoft SQL Server.

For information about system requirements, see the *HP Fortify Software Security Center System Requirements* for version 4.10. For information about installing or upgrading WebInspect Enterprise, see the *HP WebInspect Enterprise Installation Guide*.

## About Scanning: Consequences and Considerations

HP scanners are aggressive Web application analyzers that rigorously inspect your entire Web site for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which scanning policy you apply and the options you select, it 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.

Consider the following:

- If your system generates e-mail messages in response to user-submitted forms, you might want to consider disabling your mail server. Alternatively, you could redirect all e-mail messages to a queue and then, following the audit, manually review and delete those messages that were generated in response to forms submitted by HP scanners.
- If for any reason you do not want to audit certain directories, you must specify those directories using the Excluded URLs settings of HP scanners.
- During an audit of any type, HP scanners submit 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.
- HP scanners test for certain vulnerabilities by attempting to upload files to your server. If your server allows this, HP scanners will record this susceptibility and attempt to delete the uploaded file. Sometimes, however, the server will not allow a file to be deleted. For this reason, part of your post-scan maintenance should include searching for and deleting files having names that begin with “CreatedByHP.”

- 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.

If HP scanners are to navigate through all possible links in the application, they must be able to submit appropriate data for each form. They do so by using a file containing the names of input controls and the associated values that need to be submitted during a scan of your Web site. Each HP scanner includes a default Web form file containing sample name/value pairs. You can use the Web Form Editor (accessible through the **Tools** menu on the WebInspect Enterprise Administrative Console) to create your own file containing Web form values.

If you select the option to submit forms during a crawl of your site, HP scanners will complete and submit all forms encountered. Although this enables HP scanners to navigate seamlessly through your application, it may also produce the following consequences:

- If, when a user normally submits a form, the application creates and sends e-mail messages or bulletin board postings (to a product support or sales group, for example), HP scanners will also generate these messages as part of their probe.
- If your system writes records to a back-end server (database, LDAP, etc.) based on forms submitted by clients, then forms submitted by HP scanners will create spurious records. Some users, before auditing their production system, create a copy of their 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 form values used by HP scanners. You can determine these values by opening the Web Form Editor.

During the audit phase of a scan, HP scanners resubmit forms numerous times, manipulating every possible parameter to reveal problems in the applications. This will greatly increase the number of messages and database records created.





## 2 WebInspect Enterprise Administrative Console

The WebInspect Enterprise Administrative Console, also known as the WebInspect Enterprise Console or the Administrative Console, is used for administrative and security functions. This chapter has the following sections:

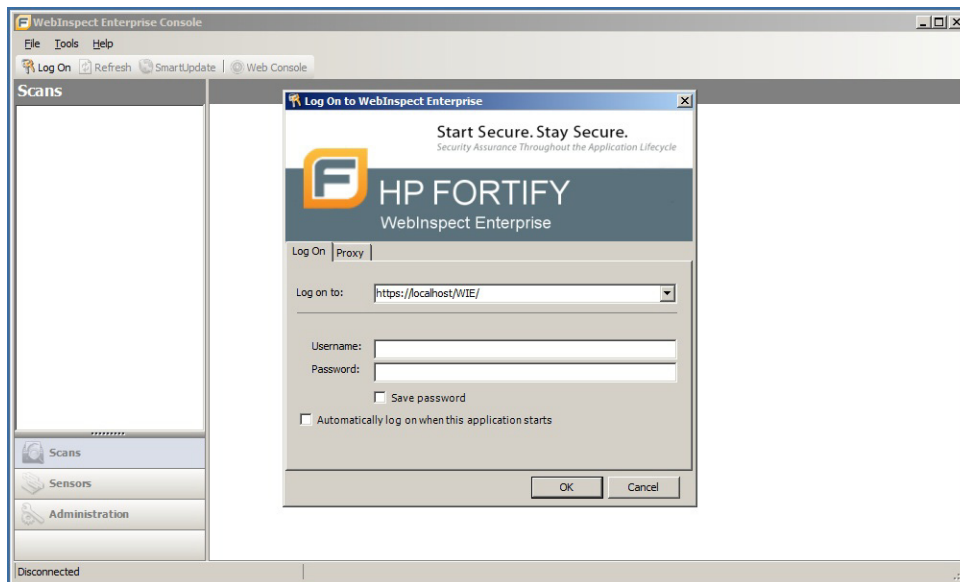
- [Logging On](#)
- [Changing the Refresh Rate](#) on page 18
- [About the Administrative Console User Interface](#) on page 18
- [About SmartUpdates](#) on page 21
- [About the Scans Group and its Shortcuts](#) on page 22
- [About the Sensors Group and its Shortcut](#) on page 25
- [About the Administration Group and its Shortcuts](#) on page 27

### Logging On

To log on to the Administrative Console:

- 1 Click **Start** → **HP WebInspect Enterprise 10.20 Console**.

The *Log On to WebInspect Enterprise* window appears.





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 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 WebInspect Enterprise manager:
  - a Click the **Proxy** tab.
  - b Select one of the following:
    - **Use the Internet Explorer proxy** (to use the proxy server specified in **Tools** → **Internet Options** → **Connections** → **LAN Settings**).
    - **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**.



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.

## Changing the Refresh Rate

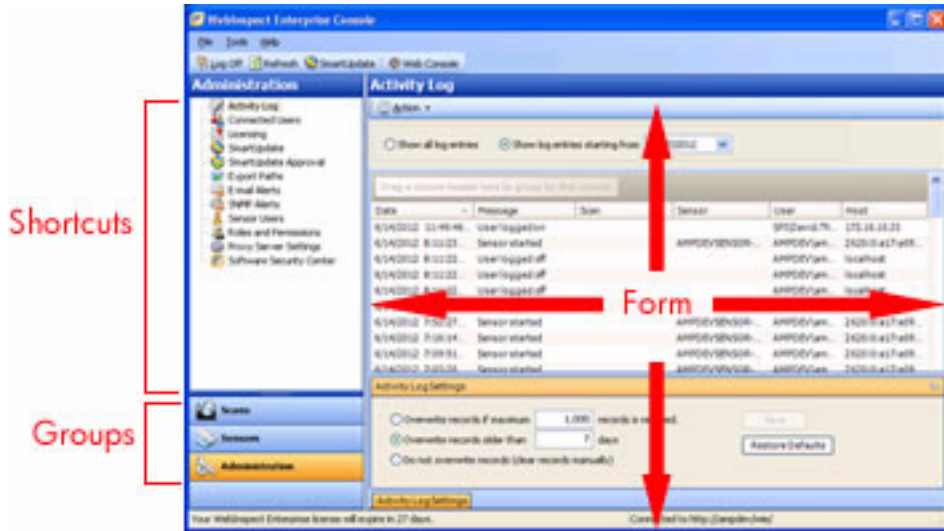
To specify a refresh rate for the WebInspect Enterprise Administrative Console:

- 1 After you log on, from the **Tools** menu, select **Options**.  
The *WebInspect Enterprise Options* window opens.
- 2 To refresh the Administrative Console information periodically, select the **Automatically refresh display every** check box and specify how often (in seconds) the display should be updated.
- 3 Click **OK**.

## About the Administrative Console User Interface

The Administrative Console user interface comprises the following main areas:

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



The buttons in the Groups pane on the left represent groups of 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 **Activity Log** shortcut to display a form containing a time-stamped history of WebInspect Enterprise Manager activities.

The Groups pane contains the following buttons and associated shortcuts:

Group Button	Associated Shortcuts
Scans	Scan Queue Scan Policies
Sensors	Sensors
Administration	Activity Log Connected Users Licensing SmartUpdate SmartUpdate Approval Export Paths E-Mail Alerts SNMP Alerts Sensor Users Roles and Permissions Proxy Server Settings Software Security Center Site Migration. This shortcut is available only if WebInspect Enterprise was installed as a migration from Assessment Management Platform (AMP) and there are still AMP sites that can be migrated to WebInspect Enterprise project versions, and only if the logged-in user is a WebInspect Enterprise system administrator and a group administrator for the AMP site.

For forms containing lists (grids), you can initiate commands related to a list or to the individual objects on a list. Simply select an object and then click a command in the **Action** menu (or in the shortcut menu that appears when you right-click an object). The availability of particular commands depends on the status of the selected object and the permissions granted to you by your assigned role (although system administrators have no restrictions on the functions they can perform). For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The following table describes the menus and toolbar buttons.

Menu / Button	Description
File	Allows you to: <ul style="list-style-type: none"> <li>• Log off the application.</li> <li>• Refresh the display.</li> <li>• Import to SSC a set of projects that were sites discovered by the Web Discovery tool. (This option is also available under the <b>Action</b> menu when the Software Security Center shortcut is selected for the Administration group; see <a href="#">Importing Projects into SSC from a .csv File Created by the Web Discovery Tool</a> on page 56).</li> <li>• Exit the application.</li> </ul>
Tools	Allows you to: <ul style="list-style-type: none"> <li>• Manually initiate a SmartUpdate. See <a href="#">About SmartUpdates</a>.</li> <li>• Change the refresh rate for the console. See <a href="#">Changing the Refresh Rate</a> on page 18.</li> <li>• Launch various tools described in the <i>Tools Guide for WebInspect Products</i>.</li> </ul>
Help	Allows you to: <ul style="list-style-type: none"> <li>• Open the Help file for the Administrative Console.</li> <li>• Open your e-mail application to send an e-mail to HP Support.</li> <li>• Open the <i>About WebInspect Enterprise Console</i> dialog for version information.</li> </ul>
Log On/Off	Log on to or log off from the Administrative Console application.
Refresh	Refresh the display.
SmartUpdate	Manually initiate a SmartUpdate call to the HP server. See <a href="#">About SmartUpdates</a> .
Web Console	Log on to the WebInspect Enterprise Web Console.

## About SmartUpdates

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

The SmartUpdate feature downloads HP's latest adaptive agents and programs, as well as vulnerability and policy information. Each time you log in to the WebInspect Enterprise Administrative Console, it contacts the WebInspect Enterprise manager and downloads any available console binary updates.



If your WebInspect Enterprise manager cannot connect to the Internet, contact HP Support to obtain an offline SmartUpdate utility.

To initiate a SmartUpdate, do either of the following:

- Click the **SmartUpdate** icon on the toolbar.
- Click the **Tools** menu and click **SmartUpdate**.

Note that scans cannot start while sensors are receiving a SmartUpdate. Scheduled scans stay in “pending” state until the SmartUpdate completes to prevent sensors from retrieving partial SmartUpdates when they update their local SecureBase from WebInspect Enterprise.

For information about displaying the history of SmartUpdates and managing SmartUpdate schedules, see [Displaying SmartUpdate History and Managing SmartUpdate Schedules](#) on page 29.

For information about approving or declining installation of downloaded SmartUpdates, see [Approving and Declining SmartUpdates](#) on page 31.

## About the Scans Group and its Shortcuts

The **Scans** group in the left pane contains the following shortcuts with associated forms in the right pane:

- **Scan Queue.** Allows you to stop, suspend, resume, or delete scans in the queue that are running or waiting to run. See [Stopping, Suspending, Resuming, or Deleting Scans in the Scan Queue](#) on page 22.
- **Scan Policies.** Allows you to manage system, custom, and master policies. See [Managing System, Custom, and Master Scan Policies](#) on page 23.

### Stopping, Suspending, Resuming, or Deleting Scans in the Scan Queue

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, and the organization and group.

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 (unless you plan to change which columns are displayed in the form).
- 3 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the scan request. The availability of particular commands depends on the status of the selected scan and on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Stop	Terminate the scan. The scan request is removed from the scan queue. The results, although incomplete, are available for inspection.
Suspend	Halt the scanning process. The scan request displays a status message of “Suspended (Manual).” You can resume the scan at the point at which it was suspended.
Resume	Continue the scanning process at the point at which it was suspended. 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.
Delete	Remove the scan from the WebInspect Enterprise database.
Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns are displayed in the form.

## Managing System, Custom, and Master Scan Policies

The Scan Policies form lists all policies configured in your environment, the product to which the policy applies, whether or not it is a pre-packaged system policy, when it was last updated, and for custom policies the organization to which it is assigned.

See [Appendix A, Policies](#), for a description of each system (non-custom) policy and its components.

You can copy a system policy and modify it as needed, making it a custom policy. You can then specify the custom policy as a master policy that you make available to an organization you select.

To manage scan policies:

- 1 Select **Scans** in the left pane and then select the **Scan Policies** shortcut above.
- 2 Select a policy (unless you plan to use the Import command to import a policy).
- 3 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the policy. The availability of particular commands depends on the permissions granted to you by your assigned role and on whether the policy is a system policy or a custom policy. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Edit	(Available only for custom policies, not system policies.) Open the Policy Manager, allowing you to view and modify the selected policy. You must install Microsoft SQL Server Express before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager.
View	(Available only for system policies, not custom policies.) Open the Policy Manager, allowing you to view the selected policy. You must install Microsoft SQL Server Express before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager. The View command is available only for system policies.
Copy	Create a copy of the selected policy. After you rename the policy, the Policy Manager opens and loads the selected policy, allowing you to edit it. Once edited and saved, the policy is added to the list of scan policies.
Delete	(Available only for custom policies, not system policies.) Delete the selected policy from the repository.
Rename	(Available only for custom policies, not system policies.) Change the name of a custom policy.
*Import	Import a policy from a standalone HP scanner.
*Export	(Available only for custom policies, not system policies.) Export a policy to a standalone HP scanner.

\* All sensors in the WebInspect Enterprise system access common policies from the repository. The import and export of policies is useful only if you run the HP scanner independent of the WebInspect Enterprise system and want to incorporate the results of that scan into the WebInspect Enterprise system.

## Creating Custom and Master Scan Policies

System administrators can create custom scan policies at the WebInspect Enterprise system level and assign each one to an organization and groups. One custom policy can be designated as the master policy and it will automatically propagate to the organization and group level, eliminating the need to update each individual copy of that policy in each organization and group.

You must be a system administrator to create master policies.

To create a custom policy and optionally make it a master policy that you make 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.

WebInspect Enterprise checks for and downloads any updates to the policy.
  - d On the *Copy Policy* dialog, 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 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 your 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 Add the new custom policy to the list of allowed policies. Select the policy from the **Available** list and click .

## About the Sensors Group and its Shortcut

The **Sensors** group in the left pane has one shortcut: **Sensors**. It allows you to manage the sensors and to stop or suspend scans.

A sensor is defined as WebInspect (and only WebInspect) when it is connected to WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans and it provides no user interface.

## Managing Sensors and Their Scans

For each sensor in the system, the Sensors form displays the name, version, host name, and status, and a status message that indicates 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 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 Microsoft .NET Framework version 4.0.

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 a command in the **Action** menu or in the shortcut menu that appears when you right-click the sensor. The availability of particular commands depends on the permissions granted to you by your assigned role and on the status of the selected sensor. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Edit Sensor Details	Modify the name, location, and description of the sensor.
Stop Scan	Abort the scan. The job cannot be resumed.
Suspend Scan	Interrupt the scan. The scan can then be manually resumed later.
Pause Sensor	Temporarily halt the sensor. If a scan is running on that sensor, the scan will be suspended. Use this command 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	Turn the sensor 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 WebInspect Enterprise system.  Note: To enable this command, you must stop the WebInspect Sensor service ( <b>Start</b> → <b>Control Panel</b> → <b>Administrative Tools</b> → <b>Services</b> ), taking the sensor offline.

# About the Administration Group and its Shortcuts

The **Administration** group in the left pane contains the following shortcuts with associated forms in the right pane:

- **Activity Log.** Allows you to export the log, clear the log, or copy selected log entries to the clipboard. See [Managing the Activity Log](#) on page 27.
- **Connected Users.** Displays information about connected users and allows you to disassociate a user from a multi-user license. See [Managing Connected Users](#) on page 28.
- **Licensing.** Displays information about the WebInspect Enterprise license. See [Displaying License Information](#) on page 29.
- **SmartUpdate.** Displays the history of SmartUpdates and allows you to manage SmartUpdate schedules. See [Displaying SmartUpdate History and Managing SmartUpdate Schedules](#) on page 29.
- **SmartUpdate Approval.** Allows you to approve or decline installation of downloaded SmartUpdates. See [Approving and Declining SmartUpdates](#) on page 31.
- **Export Paths.** Allows you to add, edit, or delete paths to which Web Console users can export scan results. See [Managing Export Paths](#) on page 32.
- **E-Mail Alerts.** Allows you to send e-mail alerts to recipients you specify when selected type of events occur. See [Managing E-mail Alerts](#) on page 33.
- **SNMP Alerts.** Allows you to send Simple Network Management Protocol (SNMP) alerts when selected types of events occur. See [Managing SNMP Alerts](#) on page 34.
- **Sensor Users.** Allows you to add or remove sensor accounts, which exist to run scans on behalf of WebInspect Enterprise users. See [Managing Sensor Users](#) on page 35.
- **Roles and Permissions.** Allows you to assign administrators for three security levels (system, organization, and group). Administrators can then define roles, assign users to roles, and configure other security-related parameters. See [About Roles and Permissions](#) on page 36.
- **Proxy Server Settings.** Allows you to configure proxy server settings as may be required to communicate with HP for SmartUpdates and licensing. See [Managing Proxy Server Settings](#) on page 55.
- **Software Security Center.** Allows you to change the WebInspect Enterprise settings for Software Security Center (SSC) that must be configured in order to publish scans to SSC or to import projects into SSC from a .csv file that was created using the Web Discovery tool. Also includes the option to import such projects from a .csv file. See [Configuring Settings for SSC and Importing Projects into SSC from a .csv File](#) on page 56.
- **Site Migration.** Allows you to migrate scan information from the Assessment Management Platform (AMP) sites you select to WebInspect Enterprise project versions. This shortcut appears only if the WebInspect Enterprise instance was a migration from AMP version 9.20 and has any remaining AMP sites that have not yet been fully migrated to project versions. See [Managing Site Migration](#) on page 57.

## Managing the Activity Log

The Activity Log form lists significant 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 list 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).

To manage the activity log:

- 1 Select **Administration** in the left pane and then select the **Activity Log** shortcut above.
- 2 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click an item in the list. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Export Activity Log to [TSV / CSV / XML]	Save the activity log to a text file using either a tab-separated, comma-separated, or XML format.
Clear Activity Log	Delete all entries in the activity log.
Copy Message(s) to Clipboard	After you select the log entries of interest, copy all of their text to the clipboard.
Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns are displayed in the form.

## Managing Connected Users

The Connected Users form lists each user who is currently logged in to the WebInspect Enterprise system. Each item 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 date and time when the user connected to the system
- Status
- Message

A summary at the bottom of the panel 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).

To manage connected 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 are displayed in the form).

- 3 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected user. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
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	Open the <i>Column Setting</i> window, allowing you to specify which columns are displayed in the form.

## Displaying License Information

System administrators can display license information.

To display the Licensing form, select **Administration** in the left pane and then select the **Licensing** shortcut above. The Licensing form displays the following information about the activation ID and license issued by HP for the operation of WebInspect Enterprise:

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

**Important:** If the WebInspect Enterprise Administrative Console is installed on a machine that does not have Internet access, see the *WebInspect Enterprise Installation Guide* for instructions on activating the application.

## Displaying SmartUpdate History and Managing SmartUpdate Schedules

For an introduction to SmartUpdates, see [About SmartUpdates](#) on page 21.

The top section of the SmartUpdate form lists each update package that has been downloaded from HP. 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 update.

The bottom section of the SmartUpdate form lists SmartUpdates 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.

To manage the SmartUpdate history and schedules:

- 1 Select **Administration** in the left pane and then select the **SmartUpdate** shortcut above.
- 2 Click a command in the **Action** menu. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Clear Completed Updates	Delete from the list the SmartUpdates that have been completed.
Add Schedule	Open the <i>SmartUpdate Settings</i> window, allowing you to schedule a SmartUpdate. See <a href="#">Adding a SmartUpdate Schedule</a> .
Edit Schedule	After you select a scheduled SmartUpdate in the SmartUpdate Schedules list, open the <i>SmartUpdate Settings</i> window, allowing you to modify the settings for that scheduled SmartUpdate.
Delete Schedule	After you select a scheduled SmartUpdate in the SmartUpdate Schedules list, delete it.
History Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns are displayed in the SmartUpdate History section of the form.
Schedule Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns are displayed in the SmartUpdate Schedules section of the form.

If you need to use a proxy server to communicate with the HP SmartUpdate database, select the **Proxy Server Settings** shortcut in the **Administration** group. See [Managing Proxy Server Settings](#) on page 55.

Note that 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 WebInspect Enterprise.

## Adding a SmartUpdate Schedule

To add a SmartUpdate schedule:

- 1 After you click **Add Schedule** in the **Action** menu, on the *SmartUpdate Settings* window, select the **General** form in the left column:
  - 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 3](#).
- 2 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 details.
  - d 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 SmartUpdate should occur.
- 3 Click **OK** to schedule the update.

## Approving and Declining SmartUpdates

The SmartUpdate Approval form lists all binary updates that have been received for WebInspect Enterprise’s client products, such as WebInspect and sensors. None of these applications can be updated until an administrator specifically approves the update. Items in the list can be grouped according to product, importance, or approval status.

The possible approval statuses are:

- **Not Approved**—Update has not been approved 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.

Once administrative approval is obtained, the update becomes available to client applications. For 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 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 WebInspect (such as a special build developed for a specific customer) by selecting the specific sensor when configuring the scan in WebInspect Enterprise.

Ordinarily, sensors that are running a non-approved version of 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 version are then eligible to be selected.

To approve or disapprove (decline) the installation of a SmartUpdate:

- 1 Select **Administration** in the left pane and then select the **SmartUpdate Approval** shortcut above.
- 2 Select the SmartUpdate you want to approve or decline.
- 3 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected SmartUpdate. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Approve	Make the binary update available to clients.
Decline	Withhold distribution of the binary update.

Note that 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 WebInspect Enterprise.

## Managing Export Paths

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

To manage export paths:

- 1 Select **Administration** in the left pane and then select the **Export Paths** shortcut above.
- 2 Select an export path (unless you plan to add an export path).
- 3 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected export path. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Add	Open the <i>Export Path Settings</i> window, allowing you to add an export path.
Edit	After you select an export path in the list, open the <i>Export Path Settings</i> window, allowing you to modify the export path.
Delete	After you select an export path in the list, remove it from the form. You cannot remove an export path that is currently being used or is associated with a scheduled scan.

- 4 When you specify an export path for the Add or Edit command, use the Universal Naming Convention (or click the **Browse** button and select a folder).

If you browse for a folder and select a local folder rather than a network folder, the selection refers to the hard drive of the machine on which the WebInspect Enterprise manager is installed. Also note that the WebInspect Enterprise manager must have access to any location you designate as an export path.



## Managing E-mail Alerts

You can direct WebInspect Enterprise to send an e-mail message to recipients you specify whenever certain types of 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 triggered the alert
- The organization
- The group

To manage e-mail alerts:

- 1 Select **Administration** in the left pane and then select the **E-mail Alerts** shortcut above.
- 2 If necessary, click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings if you plan to send e-mail notifications for specific WebInspect Enterprise events. Specify the SMTP settings as follows:
  - **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 be 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 `text@text.text`, where `text` is any text you care to enter.
  - **Use SSL**—Select this check box 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 Select an e-mail alert (unless you plan to add an e-mail alert).
- 4 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected e-mail alert. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Add	Open the <i>E-Mail Alert Settings</i> window, allowing you to add an e-mail alert.
Edit	After you select an e-mail alert in the list, open the <i>E-Mail Alert Settings</i> window, allowing you to modify the e-mail alert.
Delete	After you select an e-mail alert in the list, remove it from the form.

- 5 If you are adding or editing an email alert, complete the settings as follows:
  - a Enter a name for the alert.
  - 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 specific IP address or range of IP addresses, enter the address or range. 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**.

## Managing SNMP Alerts

You can direct WebInspect Enterprise to send a Single Network Management Protocol (SNMP) alert whenever certain types of 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 event or action that triggered the alert
- The organization
- The group

To manage SNMP alerts:

- 1 Select **Administration** in the left pane and then select the **SNMP Alerts** shortcut above.
- 2 If necessary, click **SNMP Settings** (at the bottom of the form) to configure Simple Network Management Protocol (SNMP) settings if you plan to send SNMP alerts for specific WebInspect Enterprise events. Specify the SNMP settings as follows:
  - **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**—In 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 Select an SNMP alert (unless you plan to add an SNMP alert).
- 4 Click a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected SNMP alert. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Add	Open the <i>SNMP Alert Settings</i> window, allowing you to add an SNMP alert.
Edit	After you select an SNMP alert in the list, open the <i>SNMP Alert Settings</i> window, allowing you to modify the SNMP alert.
Delete	After you select an SNMP alert in the list, remove it from the form.

- 5 If you are adding or editing an SNMP alert, complete the settings as follows:
  - a Enter a name for the alert.
  - 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 Enter the 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**.

## Managing Sensor Users

The Sensor Users form lists all WebInspect Enterprise sensor accounts, which exist to run scans on behalf of WebInspect Enterprise users.

Prior to or during installation of WebInspect Enterprise, at least one Windows user account was created and made a WebInspect Enterprise sensor user.

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

- 1 Select **Administration** in the left pane and then select the **Sensor Users** shortcut above.
- 2 Click **Add**.
- 3 In the *Select Users or Groups* dialog, 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 you identify the localhost or domain.

Click **Advanced** on the *Select Users or Groups* dialog to search for users or groups.

- 4 Click **OK**.

To remove an account:

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

## About Roles and Permissions

A role is a named collection of permissions that administrators specify. The Roles and Permissions form allows you to assign administrators for three hierarchical security levels—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 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.

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:

- 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 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.



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

- 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 renaming or removing organizations or groups, adding a user or group to multiple roles simultaneously, displaying the roles of a user or group, or removing a user or group from roles, see [Managing Roles and Permissions](#) on page 37.

For information about managing roles and permissions at the WebInspect Enterprise System level, see [About WebInspect Enterprise System Administrators, Roles, and Permissions](#) on page 39.

For information about managing roles and permissions at the organization level, see [About Organization Administrators, Roles, and Permissions](#) on page 42.

For information about managing roles and permissions at the group level, see [About Group Administrators, Roles, and Permissions](#) on page 48.

Initial configuration of the roles and permissions is described in the *WebInspect Enterprise Installation Guide*.

## Managing Roles and Permissions

To manage roles and permissions:

- 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 a command in the **Action** menu or in the shortcut menu that appears when you right-click the selected item in the Security Group Hierarchy. The availability of particular commands depends on the type of item selected in the Security Group Hierarchy, and on the permissions granted to you by your assigned role.

The commands in the **Action** menu are:

Command	Definition
Add Organization	After you select WebInspect Enterprise System in the Security Group Hierarchy, create an organization. See <a href="#">Adding an Organization to the WebInspect Enterprise System</a> on page 43.
Rename Organization	After you select an organization in the Security Group Hierarchy, change its name. See <a href="#">Renaming an Organization</a> on page 44.
Remove Organization	After you select an organization in the Security Group Hierarchy, remove (delete) it. See <a href="#">Removing an Organization</a> on page 43.
Add Group	After you select an organization in the Security Group Hierarchy, add a new group to it. See <a href="#">Adding a Group</a> on page 49.
Rename Group	After you select a group in the Security Group Hierarchy, change its name. See <a href="#">Renaming a Group</a> on page 50.
Remove Group	After you select a group in the Security Group Hierarchy, remove (delete) it. See <a href="#">Removing a Group</a> on page 50.

Command	Definition
Add User(s) to Roles	After you select an item in the Security Group Hierarchy, add a user to multiple roles simultaneously. See <a href="#">Adding a User or Group to Multiple Roles Simultaneously</a> for more information.
Role Membership and Removal	After you select an item in the Security Group Hierarchy, click the command, specify a user name or group name, and display members in the role, optionally remove a user or group from a role. For more information, see <a href="#">Displaying the Roles of a User or Group or Removing a User or Group from Roles</a> on page 38.

## Adding a User or Group to Multiple Roles Simultaneously

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 command **Add User(s) to Roles** is a time-saving alternative.

To add a user or group to multiple roles:

- 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 opens.

- 3 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 and select a user or group.
- 4 Select a role from the **Roles** list.

For information about global roles, which include “(global)” as a suffix, see [Managing Global Roles](#) on page 41.

“All Custom Roles” are the roles that have been added at all levels—WebInspect Enterprise System, organizations, and groups.

- 5 If you selected a global role, under Project 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 Project Hierarchy select the roles to which the user or group you selected is to be assigned.

- 6 Click **Apply**.

## Displaying the Roles of a User or Group or Removing a User or Group from Roles

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

- 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 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, WebInspect Enterprise displays all the roles to which you are assigned.

If you enter a user name or group name other than your own, you must be an administrator to see their roles. 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 roles, select the check boxes for the roles from which they are to be removed and click **Remove**.

## About WebInspect Enterprise System Administrators, Roles, and Permissions

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

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

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** in the Security Group Hierarchy pane, the following tabs appear in the System Permissions section:

- Administrators
- Roles
- Global Roles

## Managing Administrators for the WebInspect Enterprise System

### Adding a System Administrator

To add a 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 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 6 Click **OK**.

## Removing a System Administrator

To remove a 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**.

## Managing Roles at the WebInspect Enterprise System Level

### Adding a WebInspect Enterprise System Role

To add a 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, 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.
- 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.

### Adding Groups or Users to a WebInspect Enterprise System Role

To assign groups or users to a 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 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 7 Click **OK**.



## Copying a WebInspect Enterprise System Role

You can copy a WebInspect Enterprise System role and keep it at the 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 WebInspect Enterprise System role to it.

To copy a 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, 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 WebInspect Enterprise System role to an organization or a group.
- 9 Select the organization or group to which the WebInspect Enterprise System role will be copied.
- 10 Click **OK**.

## Managing Global Roles

A global role is one that defines permissions for all three hierarchical levels (WebInspect Enterprise System, organization, and group). When it is created, WebInspect Enterprise automatically copies the role to all levels (that is, to the 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 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.

### Creating a Global Role

To create 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, 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**.



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

## About Organization Administrators, Roles, and Permissions

A 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 projects 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 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 projects.

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

Organization roles have the following categories of activities:

- Blackouts
- Policies
- E-mail Alerts

- SNMP Alerts
- Reports

Security within the WebInspect Enterprise system is arranged according to a hierarchy of organizations and groups. You may have one or more organizations, and each organization may 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 in the Security Group Hierarchy pane, the following tabs appear in the Organization Permissions section:

- Administrators
- Configuration
- Roles
- Resources
- Move/Copy Objects

Note: When a project version is created in HP Fortify Software Security Center (SSC), it is also created automatically in 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 project version in WebInspect Enterprise, use the Administrative Console to move that project version to that group. See [About Group Administrators, Roles, and Permissions](#) on page 48.

## Managing Organizations

The WebInspect Enterprise System must have at least one organization. Your system should initially have a Default Organization.

### Adding an Organization to the WebInspect Enterprise System

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 **Action** and select **Add Organization**.  
The *Create Organization* dialog appears.
- 4 Type a name for the organization.
- 5 Click **OK**.

### 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 appears.
- 4 Type a new name for the organization.
- 5 Click **OK**.

## Managing Administrators for Organizations

### 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 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 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**.

## 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 Organization Maximum Scan 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).

More severe restrictions can be assigned to a group within the organization. For example, if the maximum priority for an organization is 3, the administrator of a group within that organization may set the group maximum priority to either 3, 4, or 5. The group's maximum scan priority may not be set to 1 or 2, however.

## Configuring Organization Options: Disable Retest Browser Tab

The Retest feature allows 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.

## Managing Roles at the Organization Level

### 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, 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.
- 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

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 an organization 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 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 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 to copy or move an organization role to it.

To copy or move 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, 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 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**.

## Managing Resources that are Available to Organizations

You can specify which resources are available to an organization. For example, the WebInspect Enterprise system contains approximately 20 scanning policies. Your organization may choose to allow only particular ones.

Note: The group administrator may further restrict which resources are available to a group.

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 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 .

## Moving or Copying Objects to Other Organizations or Groups

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.

- 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
- Policies
- E-mail Alerts
- 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.

For example, 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.

For example, 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 appears informing you that all dependencies have been satisfied and prompting you to commit the move or copy, click **Yes**.

## 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 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:

- Project Versions
- Scans
- Scan Templates
- Scheduled Scans
- E-mail Alerts
- SNMP Alerts
- Blackouts
- HP Toolkit

Security within the WebInspect Enterprise system is arranged according to a hierarchy of organizations and groups. You may have one or more organizations, and each organization may 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 in the Security Group Hierarchy pane, the following tabs appear in the Group Permissions section:

- Administrators
- Configuration
- Roles
- Resources
- Move/Copy Objects

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

Note: When a project version is created in HP Fortify Software Security Center (SSC), it is also created automatically in 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 project version in WebInspect Enterprise, use the Administrative Console to move that project version to that group.

## Managing Groups

Each organization can have one or more groups.

### 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 **Action** and select **Add Group**.  
The *Create Group* dialog appears.
- 4 Type a name for the group in the **Name** field.
- 5 If you want the group to have unrestricted access to all resources that are available to the organization, select **Allow access to all of the Organization's current resources**.
- 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:
  - a Change the IP address or host name.
  - b Change permissions for running a Web Site scan and Web Service scan.
- 10 Click **OK** to close the *Create Group* dialog.

Note that users who create a group are automatically assigned as administrators 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 select **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 appears.
- 4 Type a new name for the group.
- 5 Click **OK**.

## Managing Administrators for Groups

### 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 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 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**.

## 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 Group Maximum Scan 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 a scan. Your choices may be restricted by your organization.

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).

### Configuring Group IP and Host Permissions

For each group, the ability to scan web sites is restricted to those IP addresses or hosts specified here.

- 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.

## Managing Roles at the Group Level

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

To assign 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 role from the **Role name** list.
- 5 Click **Add** (on the far right of the **User group or user names** pane).
- 6 On the *Select SSC Users or Groups* dialog, select users from the **Select Users** list.
- 7 Click **OK**.

If your domain server uses the Microsoft Windows 2000 or 2003 operating system, and you have more than 1000 users on your network, you must modify the Lightweight Directory Access Protocol (LDAP) policies used by the Microsoft Active Directory® service. Specifically, you must change the maximum page size that is supported for LDAP responses (which is set by default to 1,000 records). Alternatively, you can limit your search criteria so that fewer than 1000 records will be returned. For detailed information, refer to <http://support.microsoft.com/default.aspx?scid=kb;en-us;315071&sd=tech>.

## 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 to copy or move a group role to it.

To copy or move 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, 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 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 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**.

## Managing Resources that are Available to Groups

You can specify which resources are available to groups within an organization. For example, the WebInspect Enterprise system contains approximately 20 scanning policies. Your organization may choose to allow only particular ones. Of those, you might choose to 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 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 .

## Moving or Copying Objects to Other Groups or Organizations

You can assign a particular user-created object to a different group (and optionally to a 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.

- 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
  - SNMP Alerts
  - Project Versions
  - Deleted Project Versions
- 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 restoring deleted project 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 appears informing you that all dependencies have been satisfied and prompting you to commit the move or copy, click **Yes**.

## Managing Proxy Server Settings

If you must use a proxy server to communicate with HP for SmartUpdates and licensing issues, use the Proxy Server Settings form as follows:

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

SmartUpdate is not available if you use a SOCKS4 or SOCKS5 proxy server configuration. SmartUpdate is available through a proxy server only when using a standard proxy server.

## Configuring Settings for SSC and Importing Projects into SSC from a .csv File

The Software Security Center Settings in the Software Security Center form must be configured in order to do the following:

- Publish scans to HP Fortify Software Security Center (SSC).
- Import projects into SSC from a .csv file that was created by using the Web Discovery tool.

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

- 1 Select **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 WebInspect Enterprise server.
  - **Software Security Center URL.** The URL of the SSC server.
  - **Administrator: User Name** and **Password.** The user name and password of a general SSC administrator account created in SSC.  
Web Console users, when publishing scans to SSC, will be required to enter their own credentials.
  - **WebInspect Enterprise Service Account: User Name** and **Password.** The user name and password of an account in SSC with the role of WebInspect Enterprise System. This service controls the sharing of project versions with WebInspect Enterprise and obtains lists of completed and running scans from WebInspect Enterprise.
- 3 To verify the settings for connection to SSC, click **Test**.
- 4 To save the settings, click **Save**.

You can click a command in the **Action** menu. The availability of particular commands depends on the permissions granted to you by your assigned role. For information about roles and permissions, see [About Roles and Permissions](#) on page 36.

The commands in the **Action** menu are:

Command	Definition
Import Projects to SSC	Import projects into SSC from a .csv file created from IP addresses found using the Web Discovery tool. See <a href="#">Importing Projects into SSC from a .csv File Created by the Web Discovery Tool</a> .
Synchronize Projects	Synchronize projects between WebInspect Enterprise and SSC. This process generally occurs automatically.
Unregister WebInspect Enterprise	Disconnect WebInspect Enterprise from SSC. Use this command only if you are moving to another instance of SSC.

### Importing Projects into SSC from a .csv File Created by the Web Discovery Tool

You can use the Web Discovery tool to discover sites over a range of IP addresses and convert the discovered sites to projects in a .csv file. Then you can edit the data and import the projects into SSC. The procedure is as follows:

- 1 Run the Web Discovery tool against the desired range of IP addresses. See the “Web Discovery” chapter in the *Tools Guide for WebInspect Products*.

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 SSC project and project version names that are meaningful to you.
  - **SSC Project (required)**. This is the name to be given to the project to be imported into SSC. By default, the value is the IP address that was discovered.
  - **SSC Project Version (required)**. This is the name to be given to the project version to be imported into SSC. 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 project version properties in WebInspect Enterprise, but does not appear in SSC.
  - **Finish Using Project (optional)**. In conjunction with the following field, specify the project and project version having the project template attributes that will be used to finish the project version to be imported into SSC.
  - **Finish Using Project Version (optional)**. In conjunction with the preceding field, specify the project and project version having the project template attributes that will be used to finish the project version to be imported into SSC.
- 4 Save the edited file.
- 5 In the WebInspect Enterprise Administrative Console, click **File** → **Import Projects to SSC**. The *Create Project Versions from imported CSV files* dialog opens.
- 6 Browse to the `.csv` file location and click **OK**.  
The projects and project versions are created in SSC.

## Managing Site Migration

The **Site Migration** shortcut appears under the **Administration** group in the Administrative Console only if:

- A migration from Assessment Management Platform (AMP) version 9.20 to WebInspect Enterprise version 10.20 was performed, and
- The logged-in WebInspect Enterprise system administrator is also a group administrator for one or more AMP sites that have not been migrated to project versions yet. That administrator cannot migrate other AMP sites.

Site migration is optional—WebInspect Enterprise does not require anyone to migrate any sites at any particular time.

The form displayed for the **Site Migration** shortcut operates as follows:

- The form initially lists (in a table) every AMP site for which the logged-in WebInspect Enterprise system administrator is also a group administrator. Thus, different system administrators could see different AMP sites listed. (It does not matter whether any or all of the AMP site's scans have been published, or even whether any scans have been run.) All the listed AMP sites can have site-specific data that you might want to migrate to a project version. For each AMP site (table row), the form also provides a drop-down list of all the project versions to which the AMP site can be migrated.
- The form allows the WebInspect Enterprise system administrator to assign one or more particular currently unassigned AMP sites to a project version. The available project versions can already exist or can be created at the time of assignment. When the WebInspect Enterprise system administrator applies the assignments, all the remaining data that has not been previously migrated from those AMP sites is migrated to WebInspect Enterprise.

When the WebInspect Enterprise system administrator uses the option to create a new project version, the project version is not “finished” until its required fields are specified, but he can still create the project version and delay finishing it. Alternatively, to finish the project version immediately, he can copy the required fields of an existing finished project version that he selects from a list. A scan cannot be published to SSC until its associated project version is finished.

- At any point in time, the form lists every remaining unmigrated AMP site for which the logged-in WebInspect Enterprise system administrator is also a group administrator. When the last AMP site has been assigned to a project version and migrated, no AMP sites are listed in the **Site Migration** form; the **Site Migration** shortcut will no longer appear the next time that administrator logs in to the Administrative Console.

This design allows users to start running WebInspect Enterprise as soon as it was installed, regardless of the migration status of any AMP sites.

Each scan that was published from AMP to SSC was associated with a project version when it was published. During WebInspect Enterprise installation, the Initialization Wizard associated the scan with the same project version in WebInspect Enterprise, and the scan can be viewed in WebInspect Enterprise. When you use the **Site Migration** shortcut to migrate an AMP site to a WebInspect Enterprise project version, all of the scan data associated with that site’s unpublished scans is migrated to that project version. This data includes:

- **Scans.**
- **Scheduled scans.**
- **Scan templates.** In AMP, a scan template can be associated with either a project or an organization. In WebInspect Enterprise, a scan template can be associated with one or more selected project versions, or it can be created as a “global” scan template that is associated with all the project versions of one or more selected projects. (Global scan templates are introduced in WebInspect Enterprise version 10.20.)
  - If a scan template created in AMP was associated with a project, site migration makes it a global scan template associated with that project.
  - If a scan template created in AMP was associated with an organization, site migration makes it a global scan template associated with that organization, and the read-only **Use Organization** check box in the global scan template is selected. Users cannot edit (or create) global scan templates associated with organizations in WebInspect Enterprise, but system administrators and organization administrators can change permissions at the organization level.

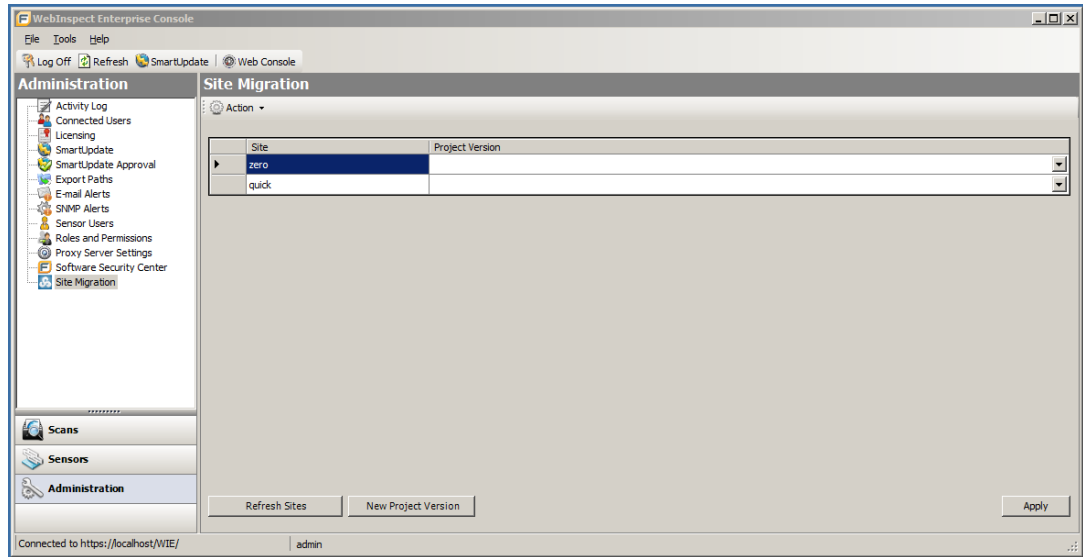
In addition to scan data, various types of data not associated with scans are also migrated from AMP, including blackout periods for sensors, custom policies, roles, proxy settings, configuration settings for email alerts and SNMP alerts, and SecureBase data.

Scans that were unpublished before performing site migration remain unpublished after site migration. (As a feature introduced in WebInspect Enterprise 10.20, when a new scan is completed by the sensor, it is *automatically* published to SSC.)

To migrate particular AMP sites to the desired WebInspect Enterprise project versions:

- 1 Start the Administrative Console if you have not already done so. Click **Start** → **HP WebInspect Enterprise 10.20 Console** and log on.
- 2 Select **Administration** in the left pane and then select the **Site Migration** shortcut above.

The *Site Migration* window appears in the right pane. The **Site** column lists the sites in AMP that remain unmigrated and can be assigned to new or existing project versions in WebInspect Enterprise. The drop-down list in the **Project Version** column displays existing project versions.



- 3 Select the site of interest in the **Site** column.

Note: You can assign multiple sites to the same project version. You can repeat [step 3](#) and [step 4](#) to assign various AMP sites to the same project versions or to various project versions, all at the same time when you later click **Apply**.

- 4 If you want to assign the site to an existing project version, select the desired project version from the **Project Version** drop-down list in the same row as the site you selected.

If you want to assign the site to a new project version that you create using this form:

- a Click **New Project Version** at the bottom of the form.
- b In the *Create SSC Project Version* dialog, do one of the following:
  - Select an existing project from the **Project** drop-down list.
  - Click **New Project** and then in the *Create SSC Project* dialog, enter a name for the new project and click **OK**. The new project appears in the **Project** field in the *Create SSC Project Version* dialog.
- c Enter a name for the new **Project Version**.
- d The optional **Finish Using** field provides a drop-down list of all the *finished* project versions in SSC. If you select one of these finished project versions, when you later click **Apply** the values of the attributes in the project template from the finished project version will be copied to the new project version, and the new project version will thereby be finished automatically.
 

If you do not select a value for this field, the project version you create will be unfinished. Until a project version is finished, you cannot publish scans to it (but finishing the project version will not automatically publish existing unpublished scans).
- e Click **OK**.
 

The new project version is added to the **Project Version** drop-down list so that you can select it (but the new project version is not actually created until you use it to perform the site migration in [step 6](#)).
- f Select the new **Project Version** from the drop-down list.

An icon in the column to the left of the **Site** column marks the site as ready for migration.

You can click **Refresh Project Versions** at any time to update the list of project versions, in case you or other users have updated the set of project versions in SSC.

- 5 Repeat [step 3](#) and [step 4](#) for other AMP sites, as needed.
- 6 Click **Apply**.

Any new project versions you specified and selected for site migration are created. The AMP sites that you assigned to project versions are migrated and removed from the list of sites in the **Site Migration** form. The unpublished scans that were created in AMP can now be viewed in scan visualizations in WebInspect Enterprise.

After site migration, a site's existing unpublished scans remain unpublished even if the project version to which the site has been migrated is finished. However, starting with WebInspect Enterprise 10.20, after a project version is finished, all *new* scans associated with it are *automatically* published to SSC.

You can click **Refresh Sites** at any time to update the list of sites to be migrated, in case other users are simultaneously migrating sites.

# 3 WebInspect Enterprise Services Manager

This chapter describes the WebInspect Enterprise Services Manager, also known as the WebInspect Enterprise Services Configuration Utility. It is used to configure or modify services associated with WebInspect Enterprise.

This chapter has the following sections:

- [About the Services Manager](#) on page 61
- [Configuring the Scan Uploader Service](#) on page 61
- [Configuring the Task Service](#) on page 63
- [Configuring the Scheduler Service](#) on page 65

## About the Services Manager

The WebInspect Enterprise Services Manager comprises the following services:

- **Scan Uploader Service.** This service handles the transfer of scans from WebInspect to WebInspect Enterprise.
- **Task Service.** This service monitors the queue for various tasks, including SSC project version updates and SSC issue synchronization.
- **Scheduler Service.** This service handles the scheduling of scans, discovery scans, and smart updates.

To start the utility, click **Start** → **All Programs** → **HP** → **HP WebInspect Enterprise 10.20** → **WebInspect Enterprise Services Manager**.

To access configuration information for a service, click its button in the left column.

## Configuring the Scan Uploader Service

If the WebInspect Enterprise Scan Uploader Service was installed, 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 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 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**.

## WebInspect Enterprise Configuration

This area of the interface reports the WebInspect Enterprise configuration.

To configure WebInspect Enterprise:

- 1 Click **Configure** in the WebInspect Enterprise Configuration section.  
The *WebInspect Enterprise Configuration* dialog appears.
- 2 Enter the URL of the WebInspect Enterprise Manager.
- 3 Provide the 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

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

Use the following procedure to create a dropbox.

- 1 Click **Add** in the Dropbox Configuration section.  
The *Configure Dropbox* dialog 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 project 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 settings:

- 1 Click **Configure** in the Logging Configuration section.  
The *Logging Configuration* dialog 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**  
On Windows Server 2003, the location is:  
`\Documents and Settings\All Users\Application Data\HP\WIE\UploaderService`  
On Windows Server 2008, the 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, 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, 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**.

## Start the Service

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

## Configuring the Task Service

### Service Status

This area of the interface reports the current status of the Task service, which handles background tasks such as SSC project version updates and SSC issue synchronization. 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 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 appears.
- 2 Enter a server name.
- 3 Specify the account under which WebInspect Enterprise will connect to the database.
  - **Windows Authentication** - The name and password specified in the WebInspect Enterprise Manager's user account is used to authenticate to the database. When working in a domain environment, the 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 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 settings:

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

The *Logging Configuration* dialog 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**

On Windows Server 2003, the location is:

```
\Documents and Settings\All Users\Application Data\HP\WIE\TaskService
```

On Windows Server 2008, the 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, 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, 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**.

## SSC Poll Interval

This area of the interface determines how often WebInspect Enterprise contacts Software Security Center (SSC) for updates.

To configure settings:

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

## Start 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, which handles background tasks such as SSC project version updates and SSC issue synchronization. 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 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**.

## WebInspect Enterprise Manager

If the 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 settings:

- 1 Click **Configure** in the Logging Configuration section.  
The *Logging Configuration* dialog appears.
- 2 The logging output is contained in `SchedulerService_trace.log`. To specify the location of the logs, choose one of the following:
  - **Default location**  
On Windows Server 2003, the location is:  
`\Documents and Settings\All Users\Application Data\HP\WIE\Scheduler`  
On Windows Server 2008, the 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, 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, 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**.

## Start the Service

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

---

# 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. This chapter has the following sections:

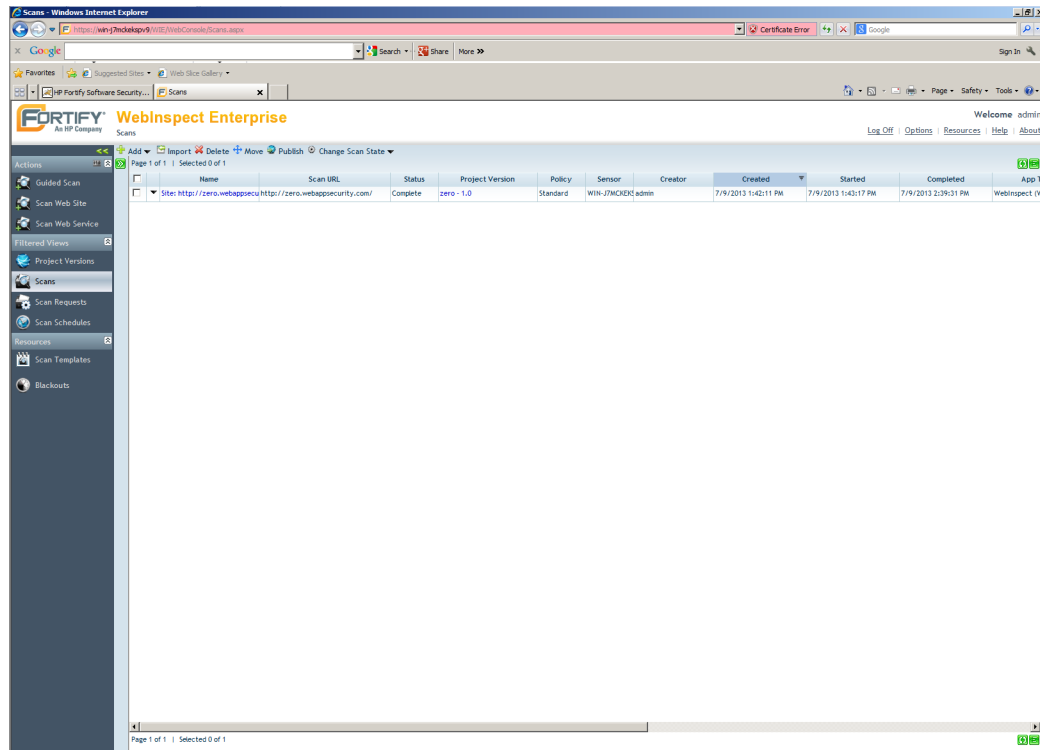
- [About the Web Console](#)
- [Logging Off, Configuring Options, and Viewing Information](#) on page 68
- [About the Navigation Pane](#) on page 69
- [About Dependencies](#) on page 86
- [About Editing Form Layouts](#) on page 87
- [About Scan Visualization](#) on page 89
- [About Guided Scan](#) on page 102
- [About the Web Site Scan Wizard](#) on page 102
- [About the Web Service Scan Wizard](#) on page 106
- [About Advanced Scan Settings](#) on page 107
- [Adding a Scan Schedule](#) on page 80
- [Adding a Blackout Period](#) on page 84

## About the Web Console

The 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 WebInspect Enterprise Web Console screens—logging off, configuring options, and viewing product information.
- **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** - Right pane to display the view or form selected in the navigation pane.

In the following screen capture, the user has selected the **Scans** button to display a form containing a list of all scans in the WebInspect Enterprise system.



## Logging Off, Configuring Options, and Viewing Information

The WebInspect Enterprise Web Console toolbar contains the following links:

- **Log Off** - Logs you off the WebInspect Enterprise Web Console application.
- **Options** - Opens the *Configure Options* window, allowing you to specify a default group and a Web console time zone, and enable or disable scanning and blackout options. See [Configuring Default Group, Time Zone, and Available Scan and Blackout Actions](#).
- **Resources** - Opens an HP WebInspect Enterprise page on the HP website.
- **Help** - Opens the Help file.
- **About** - Opens a window that displays the 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 WebInspect Enterprise application.

## Configuring Default Group, Time Zone, and Available Scan and Blackout Actions

Click **Options** on the toolbar to configure the following Web Console options.

Option	Description
Default Group	Select a group that will be used by client applications that cannot specify a group. A client application is WebInspect or any application that uses the WebInspect Enterprise application programming interface (API). Each user account is associated with a default group. If WebInspect Enterprise receives a call to create an object and the calling client application is not aware of the WebInspect Enterprise “group” category, 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 allows you to initiate a website scan from the Web Console, using the Scan Web Site function in the Actions group. If not selected, <b>Scan Web Site</b> does not appear on the navigation pane.
Enable “Scan Web Service” action	This option allows you to initiate a web service scan from the Web Console, using the Scan Web Service function in the Actions group. If not selected, <b>Scan Web Service</b> does not appear on the navigation pane.
Enable “New Scan Schedule” action	This option allows you to schedule a scan from the WebInspect Enterprise Web Console, using the New Scan Schedule function in the Actions group. If not selected, <b>New Scan Schedule</b> does not appear on the navigation pane.
Enable “New Blackout” action	This option allows you to create and modify blackout periods from the Web Console, using the New Blackout function in the Actions group. If not selected, <b>New Blackout</b> does not appear on the navigation pane.

After specifying an option, click **Save**.

## About the Navigation Pane

The navigation pane is divided into the following groups (headings):

- **Actions** - Options to initiate a Guided Scan, a Web Site Scan, or a Web Service Scan, or configure a scan schedule or a blackout schedule. See [Configuring Scans, Scan Schedules, and Blackout Schedules \(Actions Group\)](#).
- **Filtered Views** - Options to display project versions, scans, scan requests, or scan schedules. See [Displaying Project Versions, Scans, Scan Requests, and Scan Schedules \(Filtered Views Group\)](#) on page 71.
- **Resources** - Options to manage (display, add, import, or delete) scan templates, or manage (display, add, or delete) blackout schedules. See [Managing Scan Templates and Blackout Schedules \(Resources Group\)](#) on page 82.

- **Administration** - Display deleted project versions (present only if project versions have been deleted in SSC). See [Displaying Deleted Project Versions \(Administration Group\)](#) on page 86.

## Configuring Scans, Scan Schedules, and Blackout Schedules (Actions Group)

Click the options under **Actions** in the navigation pane to perform the Web Console tasks described in the following sections.

### Configuring a Guided Scan

Click **Guided Scan** to launch Guided Scan, the preferred method for performing a website scan. Guided Scan directs you through the best steps to configure a scan that is tailored to your application. For detailed information, see [Chapter 5, Guided Scan for Web Sites, Using Predefined Templates](#).

Guided Scan is also available for mobile device applications. See [Chapter 6, Guided Scan Using Mobile Templates](#).

### Configuring a Web Site Scan

Click **Scan Web Site** to launch the Scan Wizard, which leads you through a series of dialogs that allow you to specify settings (options) for the website scan.

Only the most often modified options are presented. To access the complete set of options, click **Advanced Settings** (at the bottom of the window).

This feature is available and the selection appears in the **Actions** group only if **Enable “Scan Web Site” action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

For detailed information, see [About the Web Site Scan Wizard](#) on page 102.

### Configuring a Web Service Scan

Click **Scan Web Service** to launch the Scan Wizard, which leads you through a series of dialogs that allow you to specify settings (options) for the web service scan.

When performing a Web service scan, WebInspect Enterprise crawls a WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a Web Service Test Design (WSD) 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.

This feature is available and the selection appears in the **Actions** group only if **Enable “Scan Web Service” action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

For detailed information, see [About the Web Service Scan Wizard](#) on page 106.

### Configuring a New Scan Schedule

Click **New Scan Schedule** (disabled by default) to specify settings (options) for a scan and designate the time when the scan should begin.

This feature is available and the selection appears in the **Actions** group only if **Enable “New Scan Schedule” action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

For detailed information, see [Adding a Scan Schedule](#) on page 80.

## Configuring a New Blackout Schedule

Click **New Blackout** (disabled by default) to specify time periods when scans are prohibited (or, conversely, time periods when scans are allowed).

This feature is available and the selection appears in the **Actions** group only if **Enable “New Blackout” action** is selected as an option. To enable or disable this feature, click the **Options** link on the WebInspect Enterprise toolbar.

For detailed information, see [Managing Blackout Periods](#) on page 83.

## Displaying Project Versions, Scans, Scan Requests, and Scan Schedules (Filtered Views Group)

### Displaying Project Versions

The Project Versions form displays, in the left column, a list of all defined projects and their component versions.

Note: When a new project version is created in SSC, it automatically appears in the Project Versions here in WebInspect Enterprise.

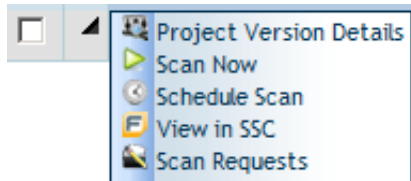
Click a project name to display information about all associated versions, or click a single version name.

For each version selected, the Project Versions form displays:

- The project 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 project with which this version is associated

To view project version details, click a project version name, or click the drop-down arrow to the left of the project version name and click **Project Version Details**. See [Displaying Project Version Details](#).

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



The functions unique to this menu are:

**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.

**View in SSC**—Launch HP Fortify Software Security Center (SSC) and navigate to the **Issues** tab of the Project Version window.

**Scan Requests**—View all SSC scan requests associated with this project version.

## Displaying Project Version Details

The Project Version Details form provides complete details about the selected project version, categorized on the following tabs:

- **All Scans**—Lists all scans conducted for the project 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
  - Whether the scan was requested by SSC
  - Number of vulnerabilities detected, categorized by severity
  - 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, import scans, delete scans, move scans to a different project 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. For more information, see [About Scan Visualization](#) on page 89.

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 project version, delete the scan, publish scan data to SSC, export the scan data in either XML or FPR format, or perform other functions.

- **Issues**—Displays a list of all vulnerabilities, sorted by severity, detected in this project version, and displays (by default) the following information:
  - Check ID - Identification number of the 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 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 project version in SSC.

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 WebInspect Agent target site.
- **Stack Trace** - This feature is designed to support HP 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), WebInspect Agent intercepts WebInspect HTTP requests and conducts runtime analysis on the target module. If this analysis confirms that a vulnerability exists, WebInspect Agent appends the stack trace to the HTTP response. Developers can analyze this stack



trace to investigate areas that require remediation. See [About the Dashboard](#) on page 93 and [About the Session Info Panel](#) on page 95.

— **Additional Info** - For Flash files, displays decompiled code.

An icon allows you to show or hide ignored issues.

- **Scan Templates**—Displays a list of scan templates associated with this project version and displays (by default) the following information:

— Template name

— Project version

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. See [About Dependencies](#) on page 86 for more information.

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 [Managing Scan Templates](#) on page 82 and [Adding a Scan Template](#) on page 83.

- **Schedules**—Lists all scans scheduled for the project version and displays (by default) the following information:

— Name of the scheduled scan

— URL of the scan target

— Recurrence

— Project 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**—Lists information about the project version, including the project version name and URL, platform information, the contact's name and e-mail address, and host information.
- **Notes**—Allows you to create or view notations associated with the project version.

- **Aliases**—Lists all aliases created for the project version, and displays for each alias the following information:
  - Primary URL for this project version
  - Description of the alias
  - Indication of whether or not the server differentiates between URLs based on case sensitivity.

Click the drop-down arrow for a specific alias to edit or delete the alias. See [Adding or Editing an Alias](#) on page 75 for detailed instructions.

Icons allow you to add or delete aliases, or recalculate all scans.

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

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 SSC application and navigate to the Issues tab of the Project Version window.
Scan Requests	Navigate to the Scan Requests form, where you can process requests issued from SSC.

### Publishing Scans to Software Security Center

When a scan completes, it is automatically published to the associated project version in HP Fortify Software Security Center (SSC) if that project version is in the Finished state. If the project 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 project version is not finished.

Note: Imported scans and scans that are uploaded from WebInspect are not automatically published.

You can manually publish a scan to SSC from the following locations:

- Project 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, WebInspect Enterprise displays a dialog listing the number of vulnerabilities to be published, categorized by status and severity. To determine the status, WebInspect Enterprise compares previously submitted vulnerabilities (obtained by synchronizing with SSC) with those reported in the current scan. If this is the first scan submitted to a project 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 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 SSC (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 SSC, select **Associate scan with an “In Progress” scan request for the current project version**. See [Displaying Scan Requests](#) on page 78 for more information.
- 3 Click **Publish**.

### 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 project versions by identifying all the equivalent URLs and hostnames for the Web application, which allows correlation to occur for all active and future scans.

To create an alias:

- 1 Select **Project Versions** from the navigation pane.
- 2 Click the name of a project version for which you want to create an alias.
- 3 On the *Project Version Details* form, click the **Aliases** tab.
- 4 Click **Add**.
- 5 On the *Add New Alias* dialog, in the **Primary URL** field, enter the alias URL (the umbrella under which other scans will be associated). Using the above 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 above example, you might enter `http://QA.testsite.com`.
- 10 To add other URLs, repeat [step 8](#) and [step 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.

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 project 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.

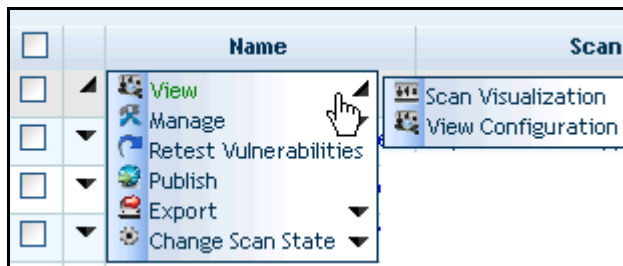
## Displaying Scans

For each scan in the WebInspect Enterprise database, the Scans form displays (by default) the following information:

- Name - The name assigned to the scan by the user.
- Scan URL - Target Web site URL or IP address.
- Status - Current state of the scan (imported, complete, etc.).

- Project Version - Project version to which this scan is assigned. Click this field to open the associated Project 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 SSC.
- 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.
- Security Group - Name of the security group associated with this scan.
- Organization - Name of the organization associated with this scan.
- WebInspect Agent Detected - Indicator (Yes/No) whether WebInspect Agent was detected during the scan.
- Project Name - Name of the project associated with this scan.
- Publish Status - Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC.
- Publish Date - The date on which the scan data was published to SSC.

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



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. For more information, see [About Scan Visualization](#) on page 89.
  - **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 paste 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 paste 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 project 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. 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.
- **Publish**—Send scan data to SSC. For more information, see [Publishing Scans to Software Security Center](#) on page 74.
- **Export**—Export the selected scan (or settings for the selected scan) to a destination you select.
- **Change Scan State**—Start, stop, resume, or suspend a scan.

Note for Internet Explorer users: When attempting to export scans, errors will result if the Internet option “Do not save encrypted pages to disk” is selected.

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

Icon	Function
Add	Start a new Guided Scan, Web site scan or Web service scan. Each choice launches the Scan Wizard, which guides you through the steps required to start a scan. You can use this as an alternative to selecting <b>Guided Scan</b> , <b>Scan Web Site</b> , or <b>Scan Web Service</b> in the Actions section of the navigation pane.
Import	<p>Import a scan.</p> <p>This feature invokes the Scan Uploader, which allows you to consolidate scans from WebInspect and WebInspect Enterprise and upload them to a project version.</p> <p>Note: WebInspect Enterprise may display the message, “You cannot start application Scan Uploader from this location because it is already installed from a different location.” This can occur when you have multiple WebInspect Enterprise managers, or you rename your WebInspect Enterprise manager, or you access the same WebInspect Enterprise manager using different URLs, and you are importing to a WebInspect Enterprise manager that is different from the one into which you previously imported. The workaround solution is to uninstall the Scan Uploader utility and click the <b>Import</b> button again (which will reinstall the utility that is paired with the correct URL). Alternatively, launch the utility using the desktop shortcut instead of the <b>Import</b> button.</p> <p>Scans can also be uploaded through the Scan Uploader service provided by the WebInspect Enterprise Services Manager. If you scan a Web site with WebInspect, you can copy the results to a location called a “dropbox.” The Scan Uploader service (which is separate from the Scan Uploader utility) can access each dropbox periodically and, if files exist, it uploads those files to the WebInspect Enterprise Manager. You can configure this feature through the WebInspect Enterprise Services Configuration utility. Initial configuration is performed as part of product installation; for more information, see <a href="#">Chapter 3, WebInspect Enterprise Services Manager</a>.</p>
Delete	Use the check boxes to select scans and delete those scans.
Move	Use the check boxes to select scans and assign those scan to a different project version.
Create Report	Select a check box for one scan and create a report for that scan. For information about creating reports, see <a href="#">About the Toolbar</a> on page 101.
Publish	Use the check boxes to select scans and send their scan data to Software Security Center. For more information, see <a href="#">Publishing Scans to Software Security Center</a> on page 74.
Change Scan State	<p>Use the check boxes to select scans and select one of the following:</p> <ul style="list-style-type: none"> <li>• Start the scans.</li> <li>• Stop the scans (if running).</li> <li>• Resume the scans (if suspended).</li> <li>• Suspend the scans (if running).</li> <li>• Repeat the scans.</li> </ul>


## Displaying Scan Requests

The Scan Requests form lists all requests issued by SSC to WebInspect Enterprise to conduct a scan. The possible values for the Status column are Pending, In Progress, and Complete.

For instructions on how an SSC user can generate a scan request, see [Creating a Scan Request](#) on page 79.

Use the following procedure to process a request.

- 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.

To restrict the display of scan requests to those that match criteria you specify, simply click  in the header of one or more columns and enter the appropriate filter information.

- 3 On the **Details** tab in the lower pane, click the **Status** list and select **In Progress**.
- 4 Click **Create a Web Site Scan** or **Create a Web Service Scan** (or you can postpone running the scan until a later, more convenient time).

When the scan is complete, review the results. You may want to retest or delete vulnerabilities, mark vulnerabilities as ignored or false positive, attach screenshots, or investigate the scan data in other ways facilitated by WebInspect Enterprise.

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.

- 5 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**. For more information, see [About Scan Visualization](#) on page 89.
  - 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. See the Note below.
- 6 Return to the *Scan Requests* form and select the request for the scan you have reviewed and published.
- 7 Click the **Status** list and select **Completed**.
- 8 Click **Change Status**.

Note: 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](#), above), 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 project version that have not been associated with a specific request.

- 4 Select a scan and click **OK**.

### Creating a Scan Request

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

- 1 Click the **Projects** tab.

- 2 Select a project version and click **View Details**.
- 3 On the **Issues** tab of the *Details* window, click the drop-down arrow on the **Dynamic Scan Request** button and select **Create**.
- 4 Enter the requested information and click **Submit**.

The request is transmitted to WebInspect Enterprise and placed in the *Scan Requests* form.

## Displaying Scan Schedules

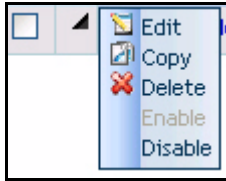
The Scan Schedules view displays information about each scheduled scan.



Note: This feature is not available and the Action options do not appear in the Filtered Views group unless the **Enable “New Scan Schedule” action** is selected as an option. To enable or disable this feature, click the Options link on the WebInspect Enterprise toolbar.

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

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



The functions unique to this menu are:

**Edit**—Copy all settings that were used for the selected scheduled scan and paste them into the *Configure Scheduled Scan* window, allowing you to edit the settings for this scheduled scan.

**Copy**—Copy all settings that were used for the selected scheduled scan and paste them into the *Configure Scheduled Scan* window, allowing you to edit the settings and create an additional scheduled scan.

**Enable**—Activate a disabled scheduled scan. Requests are enabled, by default, when created.

**Disable**—Deactivate 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 perform additional functions using the icons at the top of the form.

Icon	Function
Add	Schedule a scan. See <a href="#">Adding a Scan Schedule</a> for a description of settings.
Delete	Remove the scheduled event.

## Adding a Scan Schedule

To schedule a scan, click the **Add** icon and then specify the scan settings. The available settings are the full complement of scan settings described in [About Advanced Scan Settings](#) on page 107, along with the unique additions for scheduled scans as described below.

Note that 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.

Headings in the following sections are named and organized the same way they appear in the product interface in the SCHEDULE group.



## General

### 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 **Scan Template** list. You are not required to use a template.

### Schedule

- **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.

The Project Version and Scan Template settings described at the beginning of this section appear on each settings form, allowing you to change them in any of the forms. Descriptions of these settings are not repeated for other forms described below.

## Recurrence

### Recurring

To schedule a scan, SmartUpdate, or blackout on a recurring basis, select the **Recurring** check box. Do *not* select this option if you want to schedule a one-time-only event.

### Pattern

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.

### Range

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 scan should occur.

# Managing Scan Templates and Blackout Schedules (Resources Group)

## Managing Scan Templates

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

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

- Name - The name assigned to the template.
- Project Version - The project version associated with the specified project. Not applicable to global templates.

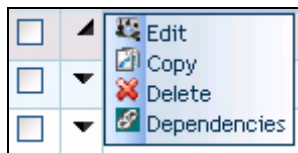
To view or modify details about a template, click the template name.

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

- The **Global Template** check box, and if it is *not* selected, the **Project** and **Project Version** fields that were selected when the template was created
- The **Global Template** check box, and if it *is* selected:
  - The organization and group combination that was selected when the template was created, and
  - The **Use Organization** check box, which is selected only if this 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.

For more information about the Configure Scan Template fields, see [Adding a Scan Template](#) on page 83.

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



The functions unique to this menu 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 forms, allowing you to modify (if necessary) and save the scan template settings.

**Delete**—Delete the scan template.

**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 86 for more information.

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

Button	Function
Add	Create a template that contains default settings as the base. See <a href="#">Adding a Scan Template</a> .
Import	Select <b>Oracle Settings</b> to create a template that contains settings that are optimized for these sites.
Delete	Delete the selected templates from the list.

## Adding a Scan Template

From the Scan Templates form under **Resources** in the Navigation pane, 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.

From the drop-down lists, you can select a **Project** and **Project 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 from drop-down lists, you must select an organization and group combination from a drop-down list.

Specify a **Scan Template Name**, the type of scan and associated data as needed, and click **Finish**.

The scan template becomes available to select in the **Scan Template** field when you run a scan.

If you select **Global Template**, all the other forms you can select in the left column also show the **Global Template** option as selected and show 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.

## Managing Blackout Periods

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.

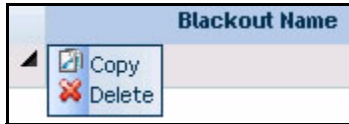
For each blackout defined in the system, the Blackouts form under **Resources** in the Navigation pane displays (by default) the following information:

- 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.
- 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 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 for a specific blackout.



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

Icon	Function
Add	Add a blackout period. See <a href="#">Adding a Blackout Period</a> .
Delete	Delete the selected blackout period.

## Adding a Blackout Period

Headings in the following sections are named and organized the same way they appear in the product interface.

### General

#### Security Group

Select an organization and group. To associate the blackout with all groups in an organization, select **Use Organization**.

#### 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 below, 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

- **Start Time**—The date and time at which the blackout period begins. You can enter the data manually or select the date from a calendar popup and the time from a clock popup.
- **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.
- **Time Zone**—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 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**—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:

d.hh.mm

where

d = the number of days

hh = the number of hours

mm = the number of minutes

## Blackout Type

- **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 “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.

## Recurrence

Use these settings to schedule a blackout on a recurring basis.

### Recurring

Select the **Recurring** check box to impose recurring blackouts. Do *not* select this option if you want to schedule a one-time-only event.

## Pattern

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.

## Range

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.

## Displaying Deleted Project Versions (Administration Group)

The only option under the **Administration** heading is **Deleted Project Versions**.



Note: This option does not appear in the navigation pane until project versions that have associated scans, scan templates, or scan schedules are deleted from SSC.

The Deleted Project Versions form displays, in the left column, a list of project versions that have been removed from HP Fortify Software Security Center. For each version, this form displays:

- The project 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 project

Click a project version name to view project version details.

System administrators can recover deleted project versions using the Administration - Roles and Permissions feature of the WebInspect Enterprise Administrative Console.

To permanently delete a project version, click the drop-down arrow for a specific project version and select **Purge** (or select one or more project versions and click the **Purge** icon at the top of the form). Purged versions cannot be recovered.

## About Dependencies


Certain objects in 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 a project version that contains scans, you cannot delete that project version unless you first delete the associated scans or assign them to a different project version.

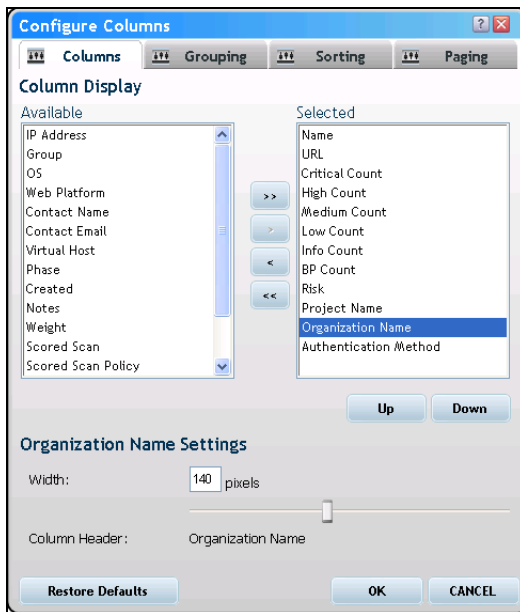
The dependencies are categorized in the following table. Dependent objects must be disassociated from the parent object before the parent object can be deleted.

Parent Object	Dependent Objects
Scan Template	<ul style="list-style-type: none"><li>• Scheduled scan</li><li>• Scan (only if scan has not completed)</li></ul> <p>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).</p>

Parent Object	Dependent Objects
Project Version	Scan You cannot delete a project version until you delete the associated scans or move them to a different project version.
Custom Policy	<ul style="list-style-type: none"> <li>• Scan</li> <li>• Scheduled scan</li> </ul> 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).

## About Editing Form Layouts

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

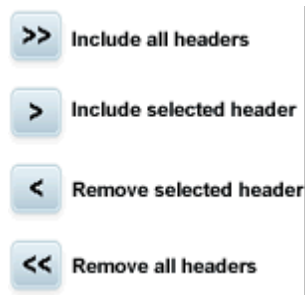


As described in the following sections, this dialog has four tabs with options to configure the form layout:

- Columns
- Grouping
- Sorting
- Paging

## Configuring Which Columns to Display

Use the **Columns** 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.




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**.

## Configuring Grouping

Use the **Grouping** tab to group objects in views (projects, scans, scan schedules, etc.) 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, scans are grouped by security group and then by policy within each security group.

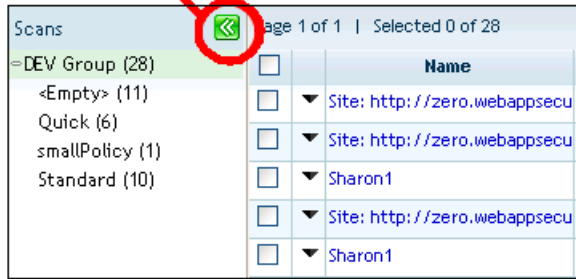
- 1 In the navigation pane under Filtered Views, click **Scans**.
- 2 Click the **Edit Layout** icon .
- 3 On the *Configure Columns* dialog, click the **Grouping** tab.
- 4 In the **Available** list, select **Security Group** and click >.
- 5 Select **Policy** and click >. Both column headers are now removed from the **Available** list and appear in the **Selected** list.
- 6 Click **OK**.

When you return to the **Scans** form, the Group pane displays the grouped results. When you select a group name (such as DEV Group, in this example), 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.

### Group pane toggle



## Configuring Sorting

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

## Configuring Paging

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

## About Scan Visualization

The *Scan Visualization* window emulates the WebInspect graphical presentation of scan data. To open this view, do one of the following:

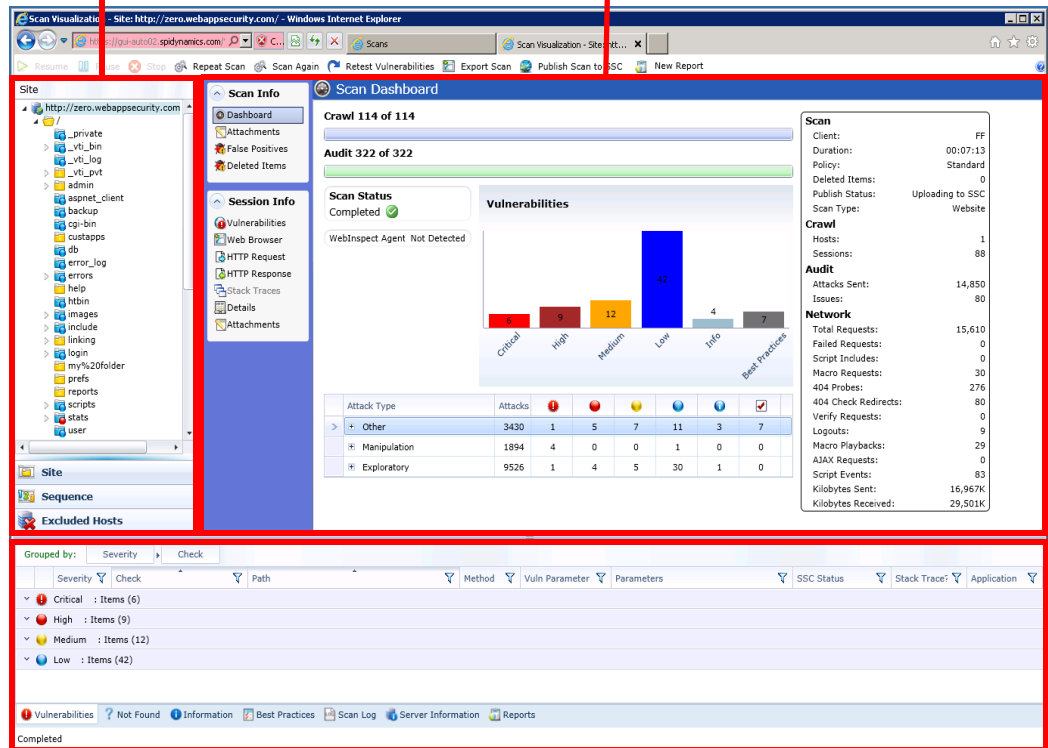
- In the WebInspect Enterprise Web Console, select the **Scans** shortcut from the **Filtered Views** group and click the name of a scan (or click the drop-down arrow for the scan and select **View** → **Scan Visualization**).
- On the Projects tab in SSC, select a project version and click **View Details** (or double-click the project version), click the Scans tab, select a scan, and click **View Scan**. By this method, if you are already working in SSC, you do not need to open WebInspect Enterprise to see the scan results.

The work area of the Scan Visualization window is divided into three regions, as depicted in the following screen capture:

- Navigation Pane
- Information Pane
- Summary Pane

Navigation Pane

Information Pane



Summary Pane

## About the Navigation Pane

When conducting or viewing a scan, the navigation pane is on the left side of the *Scan Visualization* window. It includes the **Site**, **Sequence**, and **Excluded Hosts** buttons, which determine the contents (or “view”).

## About the Site View

In the Site View, 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, WebInspect Enterprise 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.

## About the Sequence View

Sequence view displays server resources in the order they were encountered during a scan.

In both Site view and Sequence view, blue text denotes a directory or file that was identified by WebInspect, rather than a resource that was discovered through a link. For example, 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.”














## About the Excluded Hosts View

This view 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' Scan Settings.

## About the Navigation Pane Icons

Use the following table to identify resources displayed in the Sequence and Site views.

### Icons Used on the Navigation Pane

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.
	Grey 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.
Icons superimposed on a folder or file indicate a discovered vulnerability	
	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.
	A blue dot indicates the object contains a low vulnerability. These are generally interesting issues, or issues that could potentially become higher ones.
	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 WebInspect to test for vulnerabilities and the HTTP response from the server.

## About the Navigation Pane Shortcut Menu

If you right-click an item in the navigation pane while using the Site view, a shortcut menu presents the following commands:

### Navigation Pane Shortcut Commands

Command	Definition
<b>Expand Children</b>	Expands branching nodes in the site tree.
<b>Collapse Children</b>	Contracts branching nodes into the superior node.
<b>Copy URL</b>	Copies the URL of the selected session to the clipboard (the same as selecting <b>Edit</b> → <b>Copy URL</b> ).
<b>View in Browser</b>	Displays the server's HTTP response in a Web browser.
<b>Add</b>	<p>Allows you to add a page, directory, or vulnerability discovered by means other than a WebInspect scan (manual inspection, other tools, etc.) for information purposes. You can then add vulnerabilities to those locations so that a more complete picture of the site is available for analysis.</p> <ul style="list-style-type: none"><li>• <b>Page</b> - A distinct URL (resource).</li><li>• <b>Directory</b> - A folder containing a collection of pages.  Choosing either <b>Page</b> or <b>Directory</b> invokes a dialog that allows you to name the page or directory and edit the HTTP request and response.</li><li>• <b>Variation</b> - 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&amp;Password=12345&amp;Action=Login”  Variations, like any other location, can have vulnerabilities attached to them, as well as subnodes.  Choosing <b>Variation</b> invokes the <i>Add Variation</i> dialog, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.</li><li>• <b>Vulnerability</b> - A specific security threat.  Choosing <b>Vulnerability</b> invokes the <i>Edit Vulnerabilities</i> dialog, allowing you to edit the variation attributes, specify Post or Query, and edit the HTTP request and response.</li></ul>
<b>Remove Location</b>	<p>Removes the selected session from the navigation pane (both Site and Sequence views) and also removes any associated vulnerabilities.</p> <p>Note: You can recover removed locations (sessions) and their associated vulnerabilities. Select <b>Deleted Items</b> from the Scan Info panel.</p>
<b>Edit Vulnerability</b>	Allows 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.
<b>Review Vulnerability</b>	Allows you to retest the vulnerability or mark it as “ignored” or “false positive.” For more information, see <a href="#">Reviewing and Retesting Vulnerabilities</a> on page 98.
<b>Mark as False Positive</b>	Flags the vulnerability as a false positive and allows you to add a note.

## Navigation Pane Shortcut Commands (cont'd)

Command	Definition
<b>Attachments</b>	Allows you to create a note or snapshot associated with the selected vulnerability.

## About the Information Pane

When conducting or viewing a scan, the information pane contains two collapsible information panels (Scan Info and Session Info) and an information display area.

### About the Scan Info Panel

This panel contains the following selections: Dashboard, Attachments, False Positives, and Deleted Items.

#### About the Dashboard

The Dashboard displays a summary of the scan results and a graphic representation of the scan progress.

The following table describes the graphics used in the Dashboard.

#### Dashboard Graphics

Graphic	Explanation
Crawl Gauge	Number of sessions crawled, of the total number of sessions for crawl.
Audit Gauge	Number of sessions audited, of the total number of sessions for audit.
Scan Status	Status: Running, Paused, or Completed.
WebInspect Agent field	Not Detected or Detected. If WebInspect Agent is detected, it can provide stack traces for certain checks. For more information, see <a href="#">About the Session Info Panel</a> on page 95 and <a href="#">Displaying Project Version Details</a> on page 72.
Vulnerabilities Graph	Total number of issues identified for the scan sorted by severity level.
Attack Stats Grid	Number of attacks made and issues found, categorized by attack type and audit engine.

The following table describes the statistics presented in the Dashboard.

#### Dashboard Statistics

Group	Statistic	Explanation
Scan	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.
	Deleted Items	Number of sessions and vulnerabilities removed by the user from the scan.

## Dashboard Statistics (cont'd)

Group	Statistic	Explanation
	Publish Status	Unpublished, Uploading to SSC, Error Uploading to SSC, Processing in SSC, Error Processing in SSC, or Processing Complete in SSC.
	Scan Type	Website or Web Service.
Crawl	Hosts	Number of hosts included in the scan.
	Sessions	Total number of sessions (excluding AJAX requests, script and script frame includes, WSDL includes).
Audit	Attacks Sent	Total number of attacks sent.
	Issues	Total number of issues found (all vulnerabilities, as well as best practices).
Network	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 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.	

### About 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 [About the Session Info Panel](#) on page 95.

### About False Positives

This feature lists all URLs that WebInspect Enterprise originally flagged as containing a vulnerability, but which a user later determined were false positives.

### About Deleted Items

This feature lists either deleted sessions or deleted vulnerabilities, depending on your selection.

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:

- Right-click an item on the **Vulnerabilities** tab, **Information** tab, or **Best Practices** 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 Vulnerability** from the shortcut menu, and (on the *Edit Vulnerabilities* dialog) click **Delete**.
- Right-click an item on any tab in the summary pane except **Scan Log**, select **Edit Vulnerability** from the shortcut menu, and (on the *Edit Vulnerabilities* dialog) click **Delete**.

## About the Session Info Panel

WebInspect 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.

The following table lists the options available in the **Session Info** panel. Some options appear only for specific scans (Web Site Scan or Web Service Scan). Also, options are enabled only if they are relevant to the selected session.

### Options in Session Info Panel

Option	Definition
Vulnerabilities	Displays the vulnerability information for the session selected in the navigation pane.
Web Browser	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 WebInspect to the server hosting the site you are scanning.
HTTP Response	Displays the server's raw HTTP response to WebInspect's request. Note: If you select a Flash (.swf) file, WebInspect displays HTML instead of binary data. This allows WebInspect to display links in a readable format.
Stack Traces	Displays stack traces provided for certain checks by WebInspect Agent, if WebInspect Agent is detected to be available. For more information, see <a href="#">About the Dashboard</a> on page 93 and <a href="#">Displaying Project Version Details</a> on page 72.
Details	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 <b>Returned Content Type</b> indicates the media type specified in the Content-Type entity-header field of the HTTP response. The <b>Detected Content Type</b> indicates the actual content-type as determined by WebInspect Enterprise.
Attachments	Displays all notes and screenshots associated with the object selected in the navigation pane (Site or Sequence view). To create an attachment, you can do one of the following: <ul style="list-style-type: none"> <li>• Right-click a session (Web site scan) or an operation or vulnerability (Web service scan) in the navigation pane and select <b>Attachments</b> from the shortcut menu.</li> <li>• Right-click an item on the <b>Vulnerabilities</b> tab of the summary pane and select <b>Attachments</b> from the shortcut menu.</li> <li>• Select a session (Web site scan) or an operation or vulnerability (Web service scan) in the navigation pane, then select <b>Attachments</b> from the Session Info panel and click the <b>Add</b> menu (in the information pane).</li> </ul>

## About the Summary Pane

When conducting or viewing a scan, use the horizontal summary pane at the bottom of the window to see a centralized display of discovered vulnerabilities. It allows you to access vulnerability information quickly and view WebInspect logging information.

To select the information you want to display, right-click any column header and choose **Columns** from the shortcut menu. The available columns are:

- **Severity:** A relative assessment of the vulnerability, ranging from low to critical. See below for associated icons.
- **Check:** A WebInspect probe for a specific vulnerability, such as cross-site scripting, unencrypted log-in form, etc.
- **Path:** The hierarchical path to the resource.
- **Method:** The HTTP method used for the attack.
- **Vuln Param:** The name of the vulnerable parameter.
- **Parameters:** Names of parameters and values assigned to them.
- **Reproducible:** Values may be Reproduced, Not Found/Fixed, or New. Column is available for Site Retests only (Retest Vulnerabilities).
- **SSC Publish Status:** The status as it exists in Software Security Center, if previously published.
- **SSC Status:** Expected status of the vulnerability when the scan is published to SSC.
- **Stack Trace?:** Whether or not a stack trace exists for the vulnerability.
- **CWE ID:** The Common Weakness Enumeration identifier(s) associated with the vulnerability.
- **7PKs:** The category in which this vulnerability is classified, using a taxonomy of software security errors developed by the HP Fortify Software Security Research Group.

The summary pane has the following tabs:



- Vulnerabilities
- Not Found
- Information
- Best Practices
- Scan Log
- Server Information
- Reports

On all tabs, you can filter the data that is presented by clicking on the icons in the column headers.

## About the Vulnerabilities Tab

The **Vulnerabilities** tab lists information about each vulnerability that WebInspect 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.

If you right-click an item in the list, a shortcut menu displays the following commands.

#### Vulnerability Shortcut Menu

Command	Definition
<b>Export All Vulns</b>	Creates a comma-separated values (.csv) file containing all items and displays it in Microsoft Excel.
<b>Change Severity</b>	Change the severity level.
<b>Edit Vulnerability</b>	Display the <i>Edit Vulnerabilities</i> dialog, allowing you to modify various vulnerability characteristics.
<b>Review Vulnerability</b>	Retest the vulnerable session, or mark it as false positive or ignored. For more information, see <a href="#">Reviewing and Retesting Vulnerabilities</a> on page 98. This option is also invoked if you double-click a vulnerability.
<b>Mark As</b>	Flag the vulnerability as either a false positive or ignored. In both cases, the vulnerability is removed from the list. To view a list of all false positives, click <b>False Positives</b> in the Scan Info panel. Note: To view (and optionally recover) deleted sessions and vulnerabilities, click <b>Deleted Items</b> in the Scan Info panel.
<b>Remove Location</b>	Delete from the navigation pane the session associated with the selected vulnerability and also remove any associated vulnerabilities. Note: To view (and optionally recover) removed sessions, select <b>Deleted Items</b> in the Scan Info panel.
<b>Attachments</b>	Create a note or associate an image with the selected vulnerability.
<b>Update SSC Status</b>	Change the status of an issue to be submitted to SSC. Statuses are: New, Existing, Reintroduced, Resolved, Still an Issue, and Not Found. The availability of a specific status is determined by the current status.

### About the Not Found Tab

This tab lists vulnerabilities that were detected by a previous scan in this project 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 or sequence view of the navigation pane. Right-clicking an item in the list presents the same options described for the [Vulnerability Shortcut Menu](#) on page 97.

### About the Information Tab

The **Information** tab lists information discovered during a WebInspect scan. These are not considered vulnerabilities. They simply identify interesting points in the site or certain applications or Web servers. When you click a listed URL, the related item in the navigation pane is highlighted.

Right-clicking an item in the list presents the same options described for the [Vulnerability Shortcut Menu](#) on page 97.

## About the Best Practices Tab

The **Best Practices** tab lists issues detected by WebInspect that relate to commonly accepted best practices for Web development. Items listed here are not vulnerabilities, but are indicators of overall site quality and site development security practices (or lack thereof).

Right-clicking an item in the list presents the same options described for the [Vulnerability Shortcut Menu](#) on page 97.

## About the 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.

## About the Server Information Tab

This tab lists items of interest pertaining to the server. Only one occurrence of an item or event is listed per server.

## About the Reports Tab

This tab displays a list of reports that have been run or are running for the scan. For information about creating a report, see [About the Toolbar](#) on page 101. 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.

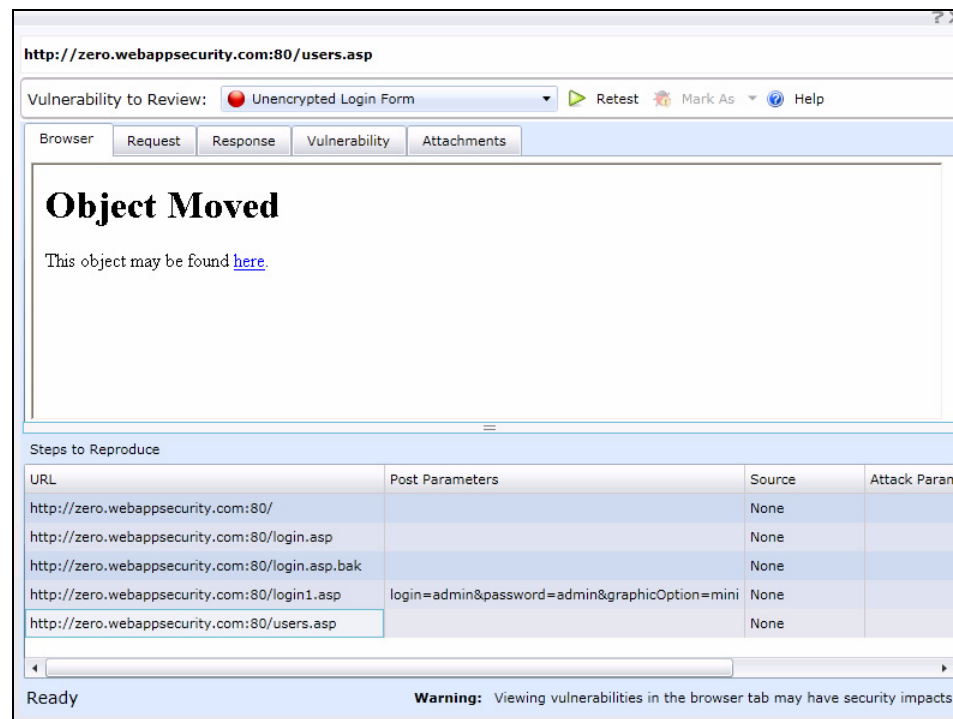
## Reviewing and Retesting Vulnerabilities

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 **Vulnerability**, **Not Found**, **Information**, or **Best Practices** 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.

In the following screen capture, the Unencrypted Login Form check was selected from the summary pane of the *Scan Visualization* window.



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: 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 WebInspect Enterprise Administrative Console, the organization administrator can disable this tab. See [Configuring Organization Options](#) on page 44.
- **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.

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."

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; 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 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 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 - WebInspect Enterprise occasionally reports a “false positive.” This occurs when 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 WebInspect Enterprise’s ranking of a vulnerability, you can assign a different level.
- Record Keeping - You can modify any of the report fields associated with an individual vulnerability (Summary, Execution, Recommendation, Implementation, Fixes, and References). For example, you could add a paragraph to the Fixes 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.

Use the procedure below 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 any modifications you made to existing vulnerability descriptions, select a check name and click **Restore Defaults**.

## About the Toolbar

Actions available from the toolbar at the top of the 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. 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.
- **Export Scan** - Export the selected scan (or settings for the selected scan) to a destination you select.
- **Publish Scan to SSC** - Send scan data to SSC. For more information, see [Publishing Scans to Software Security Center](#) on page 74.
- **New Report** - Create a new report from the scan you select and open. The reports available in WebInspect Enterprise are a subset of the reports available in WebInspect.

The first time you create a report (or launch Guided Scan) from WebInspect Enterprise or Software Security Center (SSC), the WebInspect Enterprise Thin Client application, including an installation wizard and a Help system, is automatically downloaded and installed on your computer. Then the interface for the function you selected opens, and Help becomes available for either function any time you use it.

In the *Generate a Report* dialog, 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* dialog 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**. You can choose to see the report generation status (**Pending**, **Running**, or **Complete**) as it changes, on the **Reports** tab in the Summary pane (you must select the **Reports** tab). You can save a completed report to a location you specify. If you selected multiple reports in the *Generate a Report* dialog, 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**. Users must also be allowed to view the scans for which they want to create reports.

## About Guided Scan

Guided Scan is the preferred alternative to the standard Web Site scan. Guided Scan directs you through the best steps to configure a scan that is tailored to your application. The first time you launch Guided Scan in WebInspect Enterprise or Software Security Center, the Guided Scan client application, which includes its own Help system, is downloaded and installed on your local computer. For detailed information, see [Chapter 5, Guided Scan for Web Sites, Using Predefined Templates](#) and [Chapter 6, Guided Scan Using Mobile Templates](#).

## About the Web Site Scan Wizard

The Web Site Scan Wizard steps you through the process of creating settings for a Web site scan (known in WebInspect as a Basic Scan). The options displayed by default on this and subsequent windows are extracted from the Advanced Settings. Any changes you make will be used for the current scan only. When each dialog appears, provide the requested information as described in the following procedure.

To start the Web Site Scan Wizard, do one of the following:

- Click **Scan Web Site** in the Actions section of the navigation pane in the WebInspect Enterprise Web Console.
- In SSC, select a project version on the Projects tab and click **New Scan** in the Quick Links section. In this case, the **Project** and **Project Version** on the first screen of the scan are automatically populated.



Click **Advanced Settings** at the bottom of any dialog in the wizard to access the full complement of WebInspect Enterprise settings. Any selections you make will be applied to this scan only, and you will not be able to return to the Scan Wizard. See [About Advanced Scan Settings](#) on page 107.

## Specifying Scan Options in the Web Site Scan Step

To complete the **Web Site Scan** step 1:

- 1 Select a **Project** and a **Project Version** from the appropriate lists.
- 2 In the **Scan Name** field, enter a name or brief description of the scan.
- 3 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 **Scan Template** list. You are not required to use a template. At the end of the Web Site Scan Wizard, you can save the options you have selected as a new template.

- 4 Select one of the following scan modes:
  - **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 & Audit:** 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 [SCAN SETTINGS](#) on page 109.
  - **Audit Only:** 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

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, 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).

WebInspect supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets.

- 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)** - 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/`, WebInspect will assess only the “two” directory.
  - **Directory and subdirectories** - 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** - 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 a 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

The scanner 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:

- To select a macro containing the URLs you want to scan, click **Import**.
- To import or remove a macro and to specify allowed hosts, click **Manage**.
- To create a workflow macro, if you have access to the WebInspect Enterprise Administrative Console, click **Tools** → **Workflow Macro Recorder**. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.


- 6 Click **Next**.

## Specifying Authentication and Connectivity Options

To complete the **Authentication and Connectivity** step 2:

- 1 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: Electing to use 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 will not be used.

- **Autodetect:** 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 Internet Explorer proxy settings on the sensor machine:** Import your proxy server information from Internet Explorer, 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 Mozilla 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 that the sensor should run on a user account that has proxy settings configured, not on the local system.
- 2 Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.
  - 3 Select **Site Authentication** to use a recorded 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 WebInspect Enterprise can rerun this macro to log on again.
    - To browse to select a previously recorded login macro, click .
    - To create a login macro, from the WebInspect Enterprise Administrative Console, click **Tools** → **Login Macro Recorder**. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.



- To remove the login macro name, if any, clear the **Site Authentication** check box.
- A table appears if input parameters were used when the macro was recorded using the Web Macro Recorder (see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*) or if Smart Credentials were used when the macro was created using the Event-Based IE Compatible Web Macro Recorder (see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*).

Enter a user name and password. When scanning the page containing the input control associated with this entry, WebInspect Enterprise will substitute these credentials for those used in the macro. This feature allows you to create a macro using your user name and password, yet when other persons run the scan using this macro, they can substitute their own user credentials.

- 4 Click **Next**.

## Specifying a Policy in the Coverage and Thoroughness Step

To complete the **Coverage and Thoroughness** step 3:

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

For descriptions of system policies, see [Appendix A, Policies](#).

- 2 If you want WebInspect to submit values for input controls on forms it encounters while scanning the target site:
  - a Select **Auto-fill Web forms during crawl**. 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.
- 3 Click **Next**.

## Specifying a Template, Scan Priority, and Sensor in the Congratulations Step

To complete the **Congratulations!** step 4:

- 1 If you want to create a template containing the settings you configured for this scan, specify a template name and click **Save**.
- 2 Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.
- 3 Select which sensor should conduct the scan. You can choose a specific sensor or select the **Run on Any Available Sensor** option.
- 4 Click **Scan**.

Note that 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.

When the scan completes, the Scan Visualization appears. For detailed information, see [About Scan Visualization](#) on page 89.

## About the Web Service Scan Wizard

The Web Service Scan Wizard steps you through the process of creating settings for a Web service scan. The options displayed by default on this and subsequent windows are extracted from the Advanced Settings. Any changes you make will be used for the current scan only. When each dialog appears, provide the requested information as described in the following procedure.

To start the Web Service Scan Wizard, click **Scan Web Service** in the Actions section of the navigation pane in the WebInspect Enterprise Web Console.



Click **Advanced Settings** at the bottom of any dialog in the wizard to access the full complement of WebInspect Enterprise settings. Any selections you make will be applied to this scan only, and you will not be able to return to the Scan Wizard.

## Specifying Scan Options in the Web Service Scan Step

To complete the **Web Service Scan** step 1:

- 1 Select a project and project version from the appropriate lists.
- 2 In the **Scan Name** field, enter a name or brief description of the scan.
- 3 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 **Scan Template** list. You are not required to use a template.
- 4 Click **Import** to open a standard file-selection dialog 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 “Web Service Test Designer” chapter in the *Tools Guide for WebInspect Products*.
- 5 Click **Next**.

## Specifying Authentication and Connectivity Options

To complete the **Authentication and Connectivity** step 2:

- 1 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: Electing to use 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 will not be used.

- **Autodetect:** 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 Internet Explorer proxy settings on the sensor machine:** Import your proxy server information from Internet Explorer, 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 Mozilla 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 that the sensor should run on a user account that has proxy settings configured, not on the local system.
- 2 Select **Network Authentication** if server authentication is required. Then select an authentication method and enter your network credentials.
  - 3 Click **Next**.

## Viewing the Coverage and Thoroughness Step

You cannot select a policy. The Simple Object Access Protocol (SOAP) policy is used by default.

Click **Next**.

## Specifying a Template, Scan Priority, and Sensor in the Congratulations Step

To complete the **Congratulations!** step 4:

- 1 If you want to create a template containing the settings you configured for this scan, specify a template name and click **Save**.
- 2 Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.
- 3 Select which sensor should conduct the scan. You can choose a specific sensor or select the **Run on Any Available Sensor** option.
- 4 Click **Scan**.

Note that 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.

When the scan completes, the Scan Visualization appears. For detailed information, see [About Scan Visualization](#) on page 89.

## About Advanced Scan Settings

To access advanced scan settings, click **Advanced Settings** at the lower left of the Web Site Scan Wizard or the Web Service Scan Wizard. The following categories of advanced scan settings are grouped on the left:

- SCAN
- SCAN SETTINGS
- CRAWL SETTINGS
- AUDIT SETTINGS
- SCAN BEHAVIOR
- EXPORT

Each group has one or more subcategories. Headings in the following sections are named and organized the same way they appear in the product interface.

# SCAN

## General

### 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

Enter a name for the scan.

### Scan URL

Select one of the following scan types.

- Standard Scan

The scanner 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).

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)** - The scanner 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/`, the scanner will assess only the “two” directory.
- **Directory and subdirectories** - The scanner 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** - The scanner 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 a comma-separated list or one URL per line, or the XML file generated by the FilesToURLs utility. Do one of the following:

- Click **Browse** and 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**

The scanner 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.

Click **Browse** and select a macro containing the URLs you want to scan.
- **Web Service Scan**

When performing a Web Service scan, the scanner 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 open a standard file-selection dialog and choose 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 WebInspect Enterprise manager will place the second scheduled scan request in a queue until the first scan finishes or until another sensor becomes available.
- If the currently running scan has a lower priority, the WebInspect Enterprise manager will suspend that scan, assign the second scheduled scan request to that sensor, and then reassign the suspended request to the sensor when the higher priority scan is complete.

Scans that are manually initiated have priority over any scheduled scan.

The Project Version and Scan Template settings described at the beginning of this section appear on each settings form, allowing you to change them in any of the forms. Descriptions of these settings are not repeated for other forms described below.

## SCAN SETTINGS

### Method

#### Scan Mode

Select one of the following modes:

- **Crawl Only**—This option completely maps a site's hierarchical data structure, but does not audit the site. The scan is saved to the database, allowing you to open the scan at a later date and conduct an audit.

- **Crawl and Audit**—In this mode, the scanner crawls the entire site, mapping the site’s hierarchical data structure, and conducting an audit.
- **Audit Only**—The scanner 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 a scanner 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 may possibly change before the crawl can be completed.
- **Sequentially**—In this mode, the scanner 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)**: The scanner 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)**: The scanner 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 the HP scanner 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 WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.

If you specified login parameters when recording the macro, the scanner 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 the scanner will use to navigate to that area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application. The scanner 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 WebInspect Enterprise. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.
- **Auto-fill Web forms during crawl**—If you select this option, the scanner submits values for input controls found on all HTML forms it encounters while scanning the target site. The scanner 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).

## General

### Scan Details

You may choose the following options:

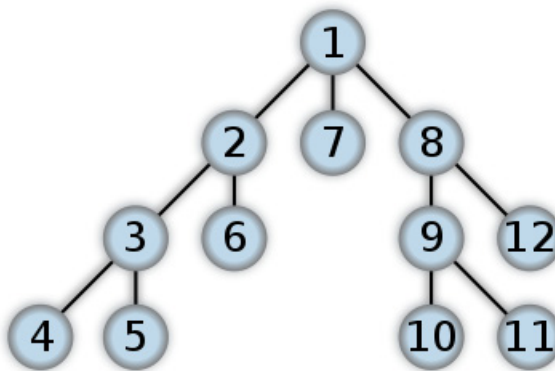
- **Enable Path Truncation**—Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. The scanner truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of `http://www.site.com/folder1/folder2/file.asp`, 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, the scanner 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, the scanner 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, the scanner 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 1000.

### Crawl Details

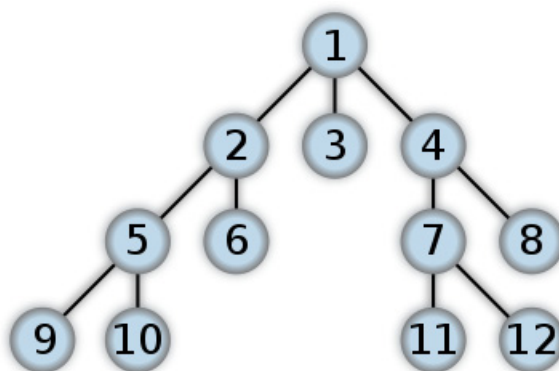
You may choose the following options:

- **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, the scanner 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, scanners would never be able to finish the scan. This option, however, allows scanners 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.aspx?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 the scanner 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 the scanner traverses the hierarchical levels of your Web site. If set to 1, the scanner drills down one level; if set to 2, the scanner 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.
- **Limit maximum Web form submission to**—Normally, when the scanner 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 the scanner 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.

## Content Analyzers

### Content Analyzers

**JavaScript/VBScript**—The JavaScript/VBScript analyzer is always enabled. It allows the scanner 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 below.

**Flash**—If you enable the Flash analyzer, the scanner analyzes Flash files, Adobe’s vector graphics-based resizable animation format. There are no associated settings.

**Silverlight**—If you enable the Silverlight analyzer, the scanner analyzes the multimedia, graphics, animation, and interactivity elements developed within Microsoft’s Silverlight Web application framework. There are no associated settings.

### Parser Settings

- **Crawl links found from script execution**—If you select this option, the crawler will follow dynamic links (that is, links generated during execution of 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>
```

The scanner will download and parse such files, regardless of their origin or file type, unless you select this 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)**—The scanner 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**—The scanner 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, the scanner logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
- **Log JavaScript Errors**—The scanner 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.

## Requestor

### Requestor Performance

Select one of the following:

- **Use a shared requestor**—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 HP scanners 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**—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. You also specify the maximum number of threads that can be created for each requestor. The crawl requestor can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 50. Increasing the thread count will increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.



Tip: While most servers can handle a large number of requests, servers in development environments sometimes have limitations on their licensing that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5. Failing to do so may mean that the scanner does not accurately crawl or audit the site because requests are being rejected by the server.

### 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 the scanner will resubmit an HTTP request after receiving a “failed” response (which is defined as any socket error or request timeout).
- **Request timeout**—Specify how long the scanner will wait for an HTTP response from the server. If this threshold is exceeded, the scanner resubmits the request until reaching the retry count. If it then receives no response, the scanner logs the timeout and issues the first HTTP request in the next attack series.

### 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 the scanner to terminate a scan by specifying a threshold for the number of timeouts.

- **Consecutive “single host” retry failures to stop scan**—Enter the number of consecutive timeouts permitted from one specific server.
- **Consecutive “any host” retry failures to stop scan**—Enter the total number of consecutive timeouts permitted from all hosts.

- **Nonconsecutive “single host” retry failures to stop scan**—Enter the total number of nonconsecutive timeouts permitted from a single host.
- **Nonconsecutive “any host” retry failures to stop scan**—Enter the total number of nonconsecutive timeouts permitted from all hosts.
- **If first request fails, stop scan**—Selecting this option will force the scanner to terminate the scan if the target server does not respond to the scanner’s first request.
- **Response codes to stop scan if received**—Enter the HTTP status codes that, if received, will force termination of the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.

## Session Storage

### 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, the scanner retrieves the saved data and sends HTTP requests that previously were suppressed.
- Hewlett-Packard 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 scan settings.
Excluded URL	URLs or hosts that are excluded by scan settings.
Outside Root URL	If the <b>Restrict to Folder</b> option is selected when starting an advanced scan, any resource not qualified by the available options ( <b>Directory only (self)</b> , <b>Directory and subdirectories</b> , or <b>Directory and parent directories</b> ).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the <b>Limit maximum crawl folder depth to</b> option has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the <b>Limit Maximum Single URL hits to</b> option has been exceeded.
404 Response Code	The option <b>Determine File Not Found (FNF) using HTTP response codes</b> is selected and the response contains a code that matches the requirements.
Solicited File Not Found	The option <b>Auto detect FNF page</b> is selected and the scanner determined that the response constituted a “file not found” condition.
Custom File Not Found	The option <b>Determine FNF from custom supplied signature</b> is selected and the response contains one of the specified phrases.
Rejected Response	Files have a MIME type that is excluded by scan settings.

## Session Storage

The scanner normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

## Session Exclusions

The following settings apply to both the crawl and audit phases of a vulnerability 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**—The scanner will not request files of the type you specify.
- **Exclude**—The scanner 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

The scanner will not process files associated with the MIME type you specify.

### 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**—The scanner 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, the scanner will not examine the specified URL or host for links to other resources. During the audit portion of the scan, the scanner 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 (i.e., 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, the scanner will exclude or reject URLs such as logout.asp or applogout.jsp.

#### Example 3

If you enter /myApp / then the scanner 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 the scanner will exclude or reject the following directories:

`http://www.test.me/W3SVC55/`

`http://www.test.me/W3SVC5/`

`http://www.test.me/W3SVC550/`

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**.

## Allowed Hosts

### 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 the scanner scans the target site, if it encounters a link to any URL containing “myco,” it will pursue that link and scan that site’s server, repeating the process until all linked sites are scanned. For this hypothetical example, the scanner 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 that 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**.

## HTTP Parsing

### 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 the scanner 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=slbhkelvbk173dhj`. 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.

The scanner 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. The defaults identify ASP.NET cookieless session IDs.

### 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:

Ex. 1 -- `http://www.anysite.com?Master.asp?Page=1`

Ex. 2 -- `http://www.anysite.com?Master.asp?Page=2`

Ex. 3 -- `http://www.anysite.com?Master.asp?Page=13;Subpage=4`

Ordinarily, the scanner would assume that these three requests refer to identical resources and would conduct a vulnerability assessment 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.

Examples 1 and 2 contain one resource parameter: “Page.”

Example 3 contains two parameters: “Page” and “Subpage.”

To identify resource parameters:

- 1 Click **Add**.
- 2 Enter the parameter name.

### 3 Click **Update**.

The string you entered appears in the Parameter list. 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) the scanner should use.

## 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 the scanner or those who have access to the raw data. If the text you specify is found, the scanner reports it on the **Information** tab as a “Hidden Reference Found” vulnerability.

### 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.

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**.

## Cookies/Headers

### Standard Header Parameters

You can elect to include referer and/or host headers in scanner requests.

- **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 the scanner 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 the scanner is auditing that site. You can add multiple custom headers. To add a custom header:

- 1 In the top text 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 the scanner to the server. To add a custom cookie:

- 1 In the top text 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.

## Proxy

### 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, the scanner 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 Internet Explorer proxy settings**—Select this option to use the proxy server settings configured for the Internet Explorer browser 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.
  - ▶ Electing to use 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 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 fields in the **Explicit Proxy Settings**: subsection as follows. For proxy servers accepting https connections, select the **Specify Alternative Proxy for HTTPS** check box and specify the fields after the check box instead.



- 1 In the **Server** field, type the URL or IP address of your proxy server.
- 2 In the **Port** field, enter the port number (for example, 8080).
- 3 Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.
- 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.

## Authentication

### 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.



Warning: The scanner 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 HP technical 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 the scanner has to pass through a proxy server to submit its requests to the Web server, the scanner may not be able to crawl or audit that Web site. Use caution when configuring a scanner 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 2003 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 the scanner to determine the correct authentication method. Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.

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.

## File Not Found

### 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. The scanner 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 either plain text, a regular expression, or SPI Regex (see the *Tools Guide for WebInspect Products* for information on SPI Regex).

### 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 the scanner to detect these “custom” file-not-found pages.

The HP scanner 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 this option, you can specify what percentage of the response content must be the same. The default is 90 percent.

## Policy

### Scan Policy

A policy is a collection of audit engines and attack agents that a scanner 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. See [Appendix A, Policies](#), for policy descriptions.

When conducting a Web Service scan, you cannot select a policy.

# CRAWL SETTINGS

## Link Parsing

### Link Parsing

The scanner follows all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (if you select the JavaScript/VBScript analyzer option on the Scan Settings: Content Analyzers panel). 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 the scanner 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**.

## 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) allows 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 **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 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**.

## AUDIT SETTINGS

### 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) allows 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 **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 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**.

## Attack Exclusions

### Excluded Parameters

Use this feature to prevent the scanner 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 the scanner 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."

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 the scanner 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 using the procedure described below.

- 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**.

## Import Audit Inputs

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 Audit Inputs Editor, click the **Browse** button next to the **Import Audit Inputs** field.

## 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):

- ja-jp: Japanese and Japan
- ko-Kr: Korean and Korea
- zh-cn: Chinese and China (PRC)
- zh-tw: Traditional Chinese

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.

## Vulnerability Filters

### Select Vulnerability Filters to Enable

By applying certain filters, you can limit the display of vulnerabilities reported during a scan. For example, the “Parameter Vulnerability Roll-Up” filter, when selected, consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.

Click a filter name to view a description of the function it performs.

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 <<.

## Smart Scan

### 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, the scanner 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 both of the identification methods described in the following section.

## Server/Application Type Detection Options

- **Use regular expressions on HTTP responses to identify server/application types**—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 to identify server/application types**—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 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**.

# SCAN BEHAVIOR

## Blackout Action

### 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 scanner will resume a suspended scan when the blackout period ends.

# EXPORT

## General

### 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 specified by the WebInspect Enterprise administrator.
- **Export Format**—Select how you want the exported file to be formatted. Your choices are WebInspect Scan File or 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.





# 5 Guided Scan for Web Sites, Using Predefined Templates

This chapter describes scanning Web sites, using the “predefined templates.” It has the following sections:

- [About Guided Scan](#)
- [About the Toolbar Buttons](#) on page 131
- [About the Guided Scan Steps](#) on page 132
- [Configuring the Guided Scan](#) on page 133
- [Importing HP Unified Functional Testing \(UFT\) Files in a Guided Scan](#) on page 140
- [Specifying Advanced Scan Settings for Guided Scan](#) on page 141
- [Specifying Advanced Crawl Settings for Guided Scan](#) on page 171
- [Specifying Advanced Audit Settings for Guided Scan](#) on page 175

## About Guided Scan

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.

The first time you launch a Guided Scan (or create a report) from WebInspect Enterprise or Software Security Center (SSC), the WebInspect Enterprise Thin Client application, including an installation wizard and a Help system, is automatically downloaded and installed on your computer. Then the interface for the function you selected opens, and Help becomes available for either function any time you use it.



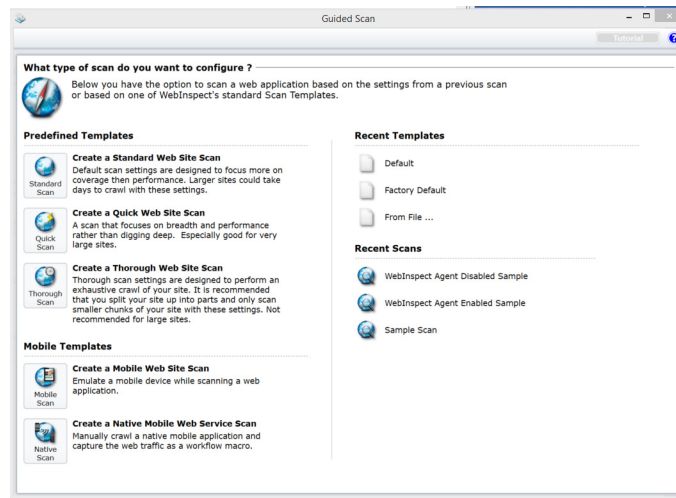
To use any of the Thin Client capabilities while using the Mozilla Firefox browser, you must download and install the Firefox add-on for the .NET Framework Assistant. To obtain it, click **Add-ons** on the *Mozilla Firefox Start Page* in the Firefox browser and search .NET.

You can launch Guided Scan in the following ways:

- In the WebInspect Enterprise Web Console, click **Actions** → **Guided Scan**.
- In SSC, on the **Projects** tab select a project and project version, and click **Guided Scan** in the Quick Links.
- In SSC, open a particular project version in the **Projects** tab, click the **Scans** tab for that project version, and click **Guided Scan**.

## Guided Scan Templates

On the first screen that appears, you select the type of scan you want to run—one of several types of web site scans using predefined templates, or mobile scans using mobile templates.



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.

### Predefined Templates

The predefined templates are:

- **Standard Scan (Create a Standard Web Site Scan):** Click **Standard Scan** to use default scan settings that are designed to focus on coverage rather than performance. Large sites could take days to crawl with these settings.
- **Quick Scan (Create a Quick Web Site Scan):** Click **Quick Scan** when you want to focus on breadth and performance rather than digging deep. It is especially good for very large sites.
- **Thorough Scan (Create a Thorough Web Site Scan):** Click **Thorough Scan** to perform an exhaustive crawl of your site. It is recommended 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.

These predefined templates are used for website scans, as described in this chapter, starting with [About the Toolbar Buttons](#) on page 131. The only difference among the predefined templates is the default value for **Crawl Coverage** (described later), which you can change.

### Mobile Templates

The mobile templates are described in [Chapter 6, Guided Scan Using Mobile Templates](#).

## About the Toolbar Buttons

Using the predefined templates, the following toolbar buttons (in the indicated toolbar groups) at the top of Guided Scan are available at various times as may be necessary or useful for the scan:

- **Scan Now** (in Scan group) - Skip the remaining Guided Scan steps and go to the *Guided Scan - Settings - Final Review - Validate Settings and Start Scan* page. See [Validate Settings and Start Scan](#) on page 140.
- **Open** (in Settings group) - Open scan settings from a file you select, from your own configured default settings, or from the original HP “factory” default settings.
- **Save** (in Settings group) - Save the current scan settings in a file you specify.
- **Advanced** (in Settings group) - Open advanced Scan Settings. See [Specifying Advanced Scan Settings for Guided Scan](#) on page 141.
- **Rendering engine** (in Verify Web Site group) - Specify the browser to use to open your target site: Firefox (recommended) or Internet Explorer.
- **New** (in Record/Edit Login Macro group) - Record a new macro. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- **Import** (in Record/Edit Login Macro group) - Import an existing macro. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- **Export** (in Record/Edit Login Macro group) - Save a macro. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- **Logout Conditions** (in Record/Edit Login Macro group) - Open the Logout Condition Editor to manually specify logout conditions when recording or editing a macro. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- **Rendering engine** (in Record/Edit Login Macro group) - Specify the browser to use to record or edit a macro: Firefox (recommended) or Internet Explorer. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- **Import Locations** (in Enhance Coverage of Your Web Site group) - Import a file of key locations that were covered and saved when enhanced coverage of your website was performed.
- **Export Locations** (in Enhance Coverage of Your Web Site group) - Export to a new file the key locations you have specified when enhancing coverage of your website.
- **Allowed Hosts** (in Enhance Coverage of Your Web Site group) - List of allowed hosts identified thus far. Each can be enabled or disabled, as long as at least one remains enabled.
- **Rendering engine** (in Enhance Coverage of Your Web Site group) - Specify the browser to use when enhancing coverage of your website: Firefox (recommended) or Internet Explorer.
- **Import** (in Web Forms group) - Import an existing set of web form values that were entered when your website was previously explored.
- **Export** (in Web Forms group) - Export to a new file the web form values you have entered when exploring your website.
- **New Global** (in Web Forms group) - Add a new global Web form field, that is, a field whose value will be submitted for any input control having the specified name, regardless of the URL at which the scanner encounters it.
- **Show Globals** (toggle button in Web Forms group) - In the **Web Form Values** step, add a list of all global web form values that were used in verifying the site.
- **Show All** (toggle button in Web Forms group) - In the **Web Form Values** step, add lists of all non-global web form values that were used in verifying the site.

## About the Guided Scan Steps

The tree in the left pane of the Guided Scan display allows 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 step and substeps comprise the name of the wizard page in the title bar. The initial page is *Guided Scan - Site - Start Parameters - Verify Web Site*, for which **Start Parameters** and **1. Verify Web Site** are highlighted in the **Site** step in the left pane. Details you need to complete are displayed in the right pane of each page.

Following is an outline of the steps that 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**
    - **1. Select Login Macro** - Specify whether to use a login macro for this site and whether to select, create, or edit one.
    - **2. Record/Edit Login Macro** - Record or edit a login macro.
- **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, and navigate to key site locations.
  - **Optimization Tasks**
    - **Profile your site for optimal settings** - Run the Profiler and see what it recommends.
    - **Enhance coverage of your web site** - Navigate to key locations in your site to ensure that they are well covered.
    - **Web Form Values** - Optionally modify any web form values that Guided Scan recorded while you configured the scan.
- **Settings** - Address configuration errors, optionally save scan settings, specify the project 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, specify the project and project version, and begin the scan.

The right pane often includes a yellow instruction bar that guides you through particular steps.

# Configuring the Guided Scan

Use the procedure in the following sections to follow along with the product interface and configure the Guided Scan. Headings in the following sections are named and organized the same way they appear in the tree in the left pane.

## Site

### 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, 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).

WebInspect supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 addresses must be enclosed in brackets. Examples:

- `http://[::1]` — WebInspect scans “localhost.”
- `http://[fe80::20c6:29ff:fe32:bae1]/subfolder/` — WebInspect scans the host at the specified address starting in the “subfolder” directory.
- `http://[fe80::20c6:29ff:fe32:bae1]:8080/subfolder/` — 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):** 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/`, WebInspect will assess only the “two” directory.
- **Directory and subdirectories:** 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:** 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.

- 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 Internet Explorer proxy settings:** Import your proxy server information from Internet Explorer.
- **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. If you select this option, click **Edit** to enter the location (URL) of the PAC.
- **Explicitly configure proxy settings:** Specify proxy server settings as indicated. If you select this option, click **Edit** to enter proxy information.



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 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 in the **Site** step in the left pane, **Start Parameters** and **2. Choose Scan Type** are highlighted.

## 2. Choose Scan Type

- 1 Select one of the following scan types:

- **Standard:** 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** step 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** page becomes selected using the default sequence. This procedure assumes that you use the default sequence.

- 2 (Optional) You can change the default scan name in the **Scan Name** text box.

- 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:** 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 about simultaneous vs. sequential crawl and audit, see [Method](#) on page 142.
- **Audit Only:** 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.

- 4 In the Policy area, select a policy from the drop-down list. For information about policies, see [Appendix A, Policies](#).

- 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 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** step in the left pane, **Application Authentication** and **1. Select Login Macro** are highlighted. If you do *not* need to perform *network* authentication, go to [Application Authentication](#) on page 136.

If you *do* need to perform network authentication, click **Network Authentication** under the Login step in the left pane. The *Guided Scan - Login - Network Authentication - Configure Network Authentication* page appears, and under the Login step, **Network Authentication** and **Configure Network Authentication** are highlighted. In this case, proceed to [Network Authentication](#) on page 135.

## Login

### Network Authentication

#### Configure Network Authentication

If your site requires network authentication:

- 1 Click the **Network Authentication** check box.
- 2 Select an authentication method from the **Method** options, and then enter your network credentials. The authentication methods are:

- **Basic.** A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter 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. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.
- **NTLM.** NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect has to pass through a proxy server to submit its requests to the Web server, WebInspect may not be able to crawl or audit that Web site. Use caution when configuring WebInspect for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

- **Digest.** The Windows Server 2003 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 WebInspect to determine the correct authentication method.
- **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.



- **Negotiate.** The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice. For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3 Complete the **User Name** and **Password** fields.

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** - WebInspect uses a certificate on the local machine based on your selection in the Certificate area.
  - **Current User** - WebInspect 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 *Guided Scan - Login - Application Authentication - Select Login Macro* page appears, and **Application Authentication** and **1. Select Login Macro** are highlighted in the left pane.

## Application Authentication

### 1. Select Login Macro

If your site requires a login macro:

- 1 Select **Use a login macro for this site**.
- 2 Do one of the following:
  - If a default login macro is shown in the **Automated Login Sequence (Login Macro)** text box, click **Edit** to edit it.
  - If a default login macro is shown in the **Automated Login Sequence (Login Macro)** text box, click the **x** to the right of the text box, select **Use a login macro for this site** again, and then click **Create** to record a new macro. The Web Macro Recorder opens in the *Guided Scan - Login - Application Authentication - Record/Edit Login Macro* page, and **Application Authentication** and **2. Record/Edit Login Macro** are highlighted in the left pane.
  - If no default login macro is shown, click **Create** to record a new macro. The Web Macro Recorder opens in the *Guided Scan - Login - Application Authentication - Record/Edit Login Macro* page, and **Application Authentication** and **2. Record/Edit Login Macro** are highlighted in the left pane.
  - Click  to open a standard file-selection window, allowing you to select a previously recorded macro.



## 2. Record/Edit Login Macro

- 1 Follow the instructions in the yellow instruction bar of the Web Macro Recorder to create or edit a login macro. For more information, see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- 2 Click the **Next** icon.

If you selected a **Standard** scan in the **Site** step, then the *Guided Scan - Active Learning - Optimization Tasks - Profile site for optimal settings* page appears, and **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane. In this case, go to [Active Learning](#) on page 138.

If you selected a **Workflows** scan in the **Site** step, then the *Guided Scan - Workflows - Workflows - Manage Workflows* page appears, and **Workflows** and **1. Manage Workflows** are highlighted in the left pane. In this case, proceed to [Workflows](#).

## Workflows

The **Workflows** step appears only if you selected **Workflows** as the **Scan Type** in the **Site** step; if you chose **Standard**, the **Workflows** step does not appear. You can create a workflow macro to ensure WebInspect Enterprise audits the pages you specify in the macro. 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 workflows 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.

## Workflows

### 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 **2. Record/Edit Workflow** are highlighted in the left pane, and the Web Macro Recorder opens. Go to [2. Record/Edit Workflow](#) on page 138.
  - **Edit** opens the Web Macro Recorder and loads the selected macro. The *Record/Edit Workflow* page appears, **Workflows** and **2. Record/Edit Workflow** are highlighted in the left pane, and the Web Macro Recorder opens. Go to [2. Record/Edit Workflow](#) on page 138.
  - **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 macro (\*.webmacro file) and/or Burp Proxy captures (\*.\*). See [Importing Burp Proxy Results](#) on page 138.
  - **Export** opens a standard file-selection window, allowing you to save a recorded macro to a \*.webmacro file.



Note: If you have installed HP Unified Functional Testing (UFT) on your computer, then WebInspect detects this automatically and displays an option to import a UFT (.usr) file. See [Importing HP Unified Functional Testing \(UFT\) Files in a Guided Scan](#) on page 140.

- 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 **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane. In this case, go to [Optimization Tasks](#) on page 138.

## 2. Record/Edit Workflow

- 1 Follow the instructions in the yellow instruction bar of the Web Macro Recorder to create or edit a workflow macro. For information about the Web Macro Recorder tool, see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
- 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 **Optimization Tasks** and **Profile site for optimal settings** are highlighted in the left pane.

## 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 *Manage Workflows* step 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**.

# Active Learning

## 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 WebInspect 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 WebInspect setting to accommodate this feature.

- 1 To launch the Profiler, click **Profile**.

Results appear in the Settings area, in addition to the default options for:


- **Disable case sensitivity for crawling**
- **Known Web Technologies and Sites**

- 2 Accept or reject the suggested settings. To reject them, clear the associated check box.
- 3 Provide the requested information as necessary.
- 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 WebInspect to submit values for input controls on forms it encounters while scanning the target site. WebInspect 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 *Tools Guide for WebInspect Products*. 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 Hosts settings to add domains to be crawled and audited. If your Web presence uses multiple domains, add those domains here. See [Allowed Hosts](#) on page 157 for more information.

To add allowed domains:

- 1 Click **Add**.
- 2 On the *Specify Allowed Host* page, enter a URL (or a regular expression representing a URL) and click **OK**.

#### **Apply sample macro**

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 - Enhance coverage of your web site* page appears, and **Optimization Tasks** and **Enhance coverage of your web site** are highlighted in the left pane.

#### [Enhance coverage of your web site](#)

To enhance coverage of your application, navigate to its key locations.

See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products* for detailed information about using the Web Macro Recorder tool to navigate key locations in your application, for Guided Scan to use during the scan.

See the Guided Scan Tutorial for more information about how to use this page of the Guided Scan wizard. To launch the tutorial, click **Tutorial** in the upper right corner of the page.

At any time you can click **Explored Locations** at the bottom left of the page to see a list of the Excluded URLs or directories, Method, Status, and URL of each location you have accessed.

When you complete the **Enhance coverage of your web site** step, click the **Next** icon. If any web form values were recorded, the *Guided Scan - Active Learning - Optimization Tasks - Web Form Values* page appears, and **Optimization Tasks** and **Web Form Values** are highlighted in the left pane. Proceed to [Web Form Values](#).

If there are no web form values, the *Guided Scan - Settings - Final Review - Validate Settings and Start Scan* page appears, and **Final Review** and **Validate Settings and Start Scan** are highlighted in the left pane. Go to [Settings](#) on page 140.

### Web Form Values

Guided Scan recorded all of the web form values that you entered while you explored your Web site to enhance coverage. Here you can review and modify the values, which are part of the scan settings that are saved with the scan. In the toolbar, you can click **Export** to save the values to a separate file or click **Import** to use an existing set of values. The scan settings, including the web form values, serve as defaults that you can modify in future scans.

## Settings

### Final Review

#### Validate Settings and Start Scan

- 1 Address any scan configuration errors that have been detected.
- 2 As desired, select **Click here to save settings** to save the settings to an external file for later use.
- 3 Specify the **Project** and **Project Version**.
- 4 In the *Scan Now* area, review your scan settings, and then click **Start Scan** to begin the scan.

## Importing HP Unified Functional Testing (UFT) Files in a Guided Scan

If you have the HP Unified Functional Testing application installed, WebInspect detects it and allows you to import a UTF file (.usr) into your workflow scan to enhance the thoroughness and attack surface of your scan. For more information about HP UFT, see the following HP website:

<http://www8.hp.com/us/en/software-solutions/software.html?compURI=1172957>

To import a UTF (.usr) file into a WebInspect Enterprise 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:  

```
HP Unified Functional Testing has been detected. You can import scripts to improve the thoroughness of your security test.
```
- 2 Click **Next**.
- 3 In the **Login** section, WebInspect Enterprise automatically selects the **Application Authentication** option. Complete the fields as indicated, and then click **Next**.
- 4 On the *Manage Workflows* screen, the Workflow table appears. Click **Import** to display the *Import Scripts* dialog.
- 5 On the *Import Scripts* dialog, you may:
  - Type the filename.
  - Browse to your file to locate your file with a .usr extension. Select **HP Unified Functional Testing** from the drop-down file type, and then navigate to the file.

- Click **Edit** to launch the HP Unified Functional Testing application.
- 6 (Optional) On the *Import Scripts* dialog, you may select either of the following options:
    - **Show HP Unified Functional Testing 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 WebInspect Unified Web Macro Recorder. For more information, see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
    - **Edit** - allows you to modify the file using the WebInspect Unified Web Macro Recorder. See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.
    - **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, WebInspect will crawl or audit the responses from that host. If a check box is not selected, 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 “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*. That document also provides information about using macros that were recorded in earlier versions of WebInspect using other web macro recorder tools.

## Specifying Advanced Scan Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Scan Settings described in this section. The Advanced Scan Settings for Guided Scan are similar to, but not identical to, those for a Web Site Scan.

Headings in the following sections are named and organized the same way they appear in the product interface (except that there are some additional sections that describe related procedures that may be required).

## Method

The Method settings broadly determine the type of scan to be conducted.

### Scan Mode

#### 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 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 may possibly change before the crawl can be completed. This is described in the Default Settings as Crawl and Audit (Simultaneously).

#### Audit Only

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

#### Simultaneously

As 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 may possibly change before the crawl can be completed.

#### Sequentially

In this mode, 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 **Sequentially**, you can specify the order in which the crawl and audit should be conducted:

- **Test each engine type per session**—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**—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.

### Crawl and Audit Details

#### Include search probes (send search attacks)

When selected, 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

When selected, 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

### Auto-fill web forms during crawl

If you select this option, 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 click **Edit** (to modify the currently selected file) or **Create** (to create a Web form file).



Do not rely on this feature for authentication. If the crawler and the auditor are configured to share state, and if the scanner 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 the scanner will not be able to log in again and the auditing will be unauthenticated. To prevent WebInspect from terminating prematurely if it inadvertently logs out of your application, go to Scan Settings - Authentication and select **Use a login macro for forms authentication**.

### Prompt for web form values during scan (interactive mode)

If you select this option, WebInspect pauses the scan when it encounters an HTTP or JavaScript form and displays a window that allows you to enter values for input controls within the form. However, if you also select **Only prompt for tagged inputs**, 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.



Do not select this option if you want to conduct an unattended scan.

### Use Web Service design

This option applies only to Web Service scans.

When performing a Web Service Scan, 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. 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 click **Edit** (to modify the currently selected file) or **Create** (to create a SOAP values file).

## General

### Scan Details

#### Enable path truncation

Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. 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.



## Attach debug information in request header

If you select this option, WebInspect includes a “Memo:” header in the HTTP request containing information that can be used by support personnel to diagnose problems. Although the format and content is subject to change without notice, the information may assist advanced users. Two of the more useful constructions are illustrated below.

Attack memo header example:

```
Memo: 197:Auditor.SendAsynchronousRequest:Attack(CID:123:AS:2,
EID:1354e211-9d7d-4cc1-80e6-4de3fd128002,ST:AuditAttack,AT:PostParamManip
ulation,APD:username,I:(1,0),R:False,SM:2,SID:FDF074B3AC41D4ABE4114B3C1A1
14160,PSID:DDAA45FB26C9149DB15AF2D8DDFD5D3A)
Requestor thread ID handling request:197
Originating function in scanner: SendAsynchronousRequest
CheckID:123
Attack Sequence: 2
Originating Engine ID:1354e211-9d7d-4cc1-80e6-4de3fd128002
Session Type: AuditAttack
Attack Type: PostParamManipulation
Attack descriptor (what was attacked): username 'param' was attacked; it
is parameter (1,0) in collection
Smart Mode: 2
Attack Session ID: FDF074B3AC41D4ABE4114B3C1A114160
Parent Session ID :DDAA45FB26C9149DB15AF2D8DDFD5D3A
```

Crawl memo header example:

```
Memo: 180:ProcessSession:Crawler.CreateStateRequest:
SID:2BC3FC705779A6F201810A1E64F7CF83,PSID:A77674B6A5BF9B3B3CEDAEF583C0826
2,ST:Crawl,CLT:HTML
Requestor thread ID handling request:180
Originating function in scanner: ProcessSession:Crawler.CreateStateRequest
Session Type: Crawl
Crawl Link Type: HTML
Session ID: 2BC3FC705779A6F201810A1E64F7CF83
Parent Session ID : A77674B6A5BF9B3B3CEDAEF583C08262
```

## Case-sensitive request and response handling

Select this option if the server at the target site is case-sensitive to URLs. Usually, the case sensitivity of a Web server is determined by the server’s operating system. Windows is not case-sensitive; UNIX and Linux are. The one exception to this rule concerns Apache, which can be configured with non-case-sensitive page names, even on a UNIX system.

## Recalculate correlation data

This feature is used only for comparing scans and should be selected only upon the advice of HP Support personnel if scan comparisons produce questionable results.

## Compress response data

If you select this option, WebInspect saves disk space by storing each HTTP response in a compressed format in the database.



## Enable Traffic Monitor Logging

- Note: Traffic monitoring is not supported in WebInspect Enterprise version 10.20, but you can configure it for potential use in scan settings you save for use in WebInspect.

While scanning, WebInspect 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, WebInspect adds the **Traffic Monitor** button to the Scan Info panel (as shown below), allowing you to display and review every request sent by WebInspect and the associated response received from the server.

Time	Host	Method	Uri	Response Code	Engine
1/6/2011 2:53:36 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:37 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:53:53 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:14 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:14 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...
1/6/2011 2:54:15 PM	h10078.www1.hp.com	POST	/cda/hpdc/register.do	200 OK	Cross Site...

```
POST /cda/hpdc/register.do HTTP/1.1
Referer: https://h10078.www1.hp.com:443/cda/hpdc?
/display/main/register.jsp?TYPE=33554433?
&REALMID=06-00060790-bec3-16ef-9bed?
-a14d91447abd&GUID=1c5MAUTHREASON=0&METHOD=GET?
&SMAGENTNAME=?SM?
?2Cq3HoFq8XcwZh079hEXbjYx21TNB4tj4RuxdLVC?
?2bxxmiuwPsc6o3JIR6zMUadd&TARGET=?SM?HTTP?3a?
?2f?2fh10078?2evww1?2ehp?2ecom?2fcda?2fhpdc?
```

```
HTTP/1.0 200 OK
Date: Thu, 06 Jan 2011 19:53:57 GMT
Server: Apache
Connection: close
Content-Type: text/html;charset=UTF-8
Content-Length: 253008
```

## Encrypt Traffic Monitor File

- Note: Traffic monitoring is not supported in WebInspect Enterprise version 10.20, but you can configure it for potential use in scan settings you save for use in WebInspect.

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.

## Maximum crawl-audit recursion depth

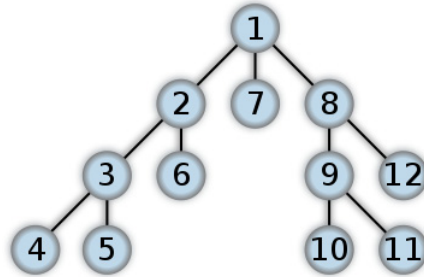
When an attack reveals a vulnerability, WebInspect crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other 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

### Crawler

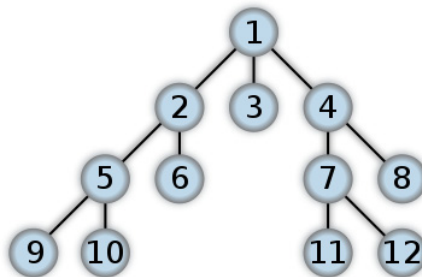
Select either **Depth First** or **Breadth First**.

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.



**Depth-First Tree**

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.



**Breadth-First Tree**

When performing a depth-first crawl, 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 \(only available during a 'crawl only'\)](#)

A keyword search, as its name implies, examines server responses and looks for certain text strings that typically indicate a vulnerability. This option is available only for a crawl-only scan.

### [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, WebInspect would never be able to finish the scan. This option, however, allows WebInspect to identify and exclude processing of redundant resources.

### 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 link will be followed during a crawl. 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.aspx?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 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

This option limits the number of directories that may be included in a single request. 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. The default value is 15.

### 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 the scan of a large site.

### Limit maximum web form submission to

Normally, when 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 WebInspect will perform. The default value is 3.

## Audit Details

### Depth First: Retrace the crawl path for each parameter attack

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. However, this option should be used for sites that enforce a strict order of access to pages. Using the “depth first” and “path retrace” options can obtain a successful scan on these types of sites when a breadth-first crawl fails.

## Content Analyzers

### Silverlight

If you enable the Silverlight analyzer, WebInspect analyzes Silverlight applications, which provide functionalities similar to those in Adobe Flash, integrating multimedia, graphics, animations and interactivity into a single runtime environment.

### Flash

If you enable the Flash analyzer, WebInspect analyzes Flash files, Adobe’s vector graphics-based resizable animation format.

### JavaScript/VBScript

The JavaScript/VBScript analyzer is always enabled. It allows WebInspect to crawl links defined by JavaScript or Visual Basic script, and to create and audit any documents rendered by JavaScript. Crawling links defined by VBScript execution requires selecting the **Enable classic script engine** option (described later in this section).

To increase the speed at which WebInspect conducts a crawl while analyzing script, change your browser options so that images/pictures are not displayed.

Configure the settings described below.

#### 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>
```

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

If you select this option, 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, WebInspect logs more detailed information about DOM operations that occur during script execution. This can create several hundred megabytes of data for medium and large sites.

### Log JavaScript errors

WebInspect logs JavaScript parsing errors from the script parsing engine.

### Enable JS Framework UI Exclusions

If selected, the WebInspect JavaScript parser ignores JQuery calendars.

### 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 new script engine provided in WebInspect 10.00 operates more like a browser and supports more web applications than did the script engine used in previous WebInspect versions. You can select this option to use the previous script engine instead.

### Enable Advanced JS Framework Support

When this option is selected, 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 new script engine of WebInspect 10.00 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.

## Recommendations



Recommendations do not appear in WebInspect Enterprise scan visualizations, but you can configure them to save and use in WebInspect scan settings.

While conducting a scan, WebInspect may encounter certain omissions, abnormalities, or anomalies that interfere with or diminish the thoroughness of the scan. If you enable the Recommendations feature, WebInspect records this information and, when the scan is complete (or paused), presents a list of recommendations designed to improve the quality of your scan when you next conduct it.

### Run Recommendation Modules when the scan is paused or completed

To enable this feature, select **Run Recommendation Modules when the scan is paused or completed**. You can then select or deselect an individual module by selecting or clearing its associated check box.

To view the recommendations resulting from this analysis, click **Recommendations** in the **Scan Info** panel.

## Network Authentication

This module detects that network, proxy, or site authentication is required, but credentials are missing or invalid.

## Web Macro

This module tracks the number of times the scanner runs a Web macro to log in to the site and warns if the number seems to be excessive, indicating that the macro may not be functioning properly. Usually this occurs because the macro is unable to log in or contains a poor log-out condition, or the site prevents multiple concurrent log-in sessions.

Note: If the macro worked correctly when it was recorded, the user name or password assigned to the site may have been subsequently changed, or the account may have been blocked or deleted.

The threshold for determining this condition is heuristically set at 10 percent. For example, if the scanner examines 4,000 responses and more than 400 of them (10 percent) indicate that the scanner is logged out of the site, thus causing the scanner to run the macro that logs in to the site, then there is a high probability that the macro is faulty and should be replaced.

You may establish a threshold that is higher or lower than 10 percent, based on your experience. To do so, click **Settings** and select a different macro ratio.

## File Not Found

This module examines the server's responses to requests for files and determines that the scan settings for recognizing a "file not found" condition may be incorrect. It is used only during a crawl-and-audit scan.

## Web Service

This module detects the presence of Web service communication within the Web site and advises you to conduct a Web service scan.

## Form Values

This module detects the existence of forms containing an input element for which you have not provided a value.

Caution: Using Form Values recommendations can cause an unintended large increase in scan data stored, as well as potential "out of memory" errors during large scans. This module is turned off by default. If it is turned on, data storage problems and out of memory incidents may occur.

## Custom Parameters

This module detects the use of URL Rewriting techniques and RESTful services technologies.

Click **Settings** to select options for this feature. The settings are:

- **Similar URLs Percentage of Total in Site** -- In some cases, WebInspect uses a "Similar URLs Percentage of Total in Site" threshold to prevent false positives. You can change this threshold to improve the accuracy of these suggestions in case you encounter false positives. Enter a percentage between 1 and 100.

- **Maximum Custom Parameter Recommendations** -- WebInspect also applies a prioritization algorithm to the recommendations and lists them in order of their estimated accuracy. If you encounter problems or anomalies while attempting to detect custom parameters, you can use the **Maximum Custom Parameter Recommendations** field to limit the number of recommendations the module will produce. Select either **Unlimited**, or enter a value between 1 and 10,000.
- **Validate custom parameter recommendations** -- If you select this option, WebInspect validates custom parameter recommendations by sending appropriate requests during the analysis stage and removing those recommendations for which an invalid response is received.

## Mobile Site

This module detects the presence of a mobile version of the Web application. You may want to scan the mobile version using a Mobile Scan. See [Chapter 6, Guided Scan Using Mobile Templates](#).

## Requestor

A requestor is the software module that handles HTTP requests and responses.

### Requestor Performance

#### 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 WebInspect and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads.

#### 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.

You can also specify the maximum number of threads that can be created for each requestor. When performing a sequential crawl and audit, the crawl requestor can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 50. The default setting is 5 for the crawl requestor and 10 for the audit requestor. Increasing the thread count will increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.



If you select “simultaneous crawl and audit” as the scan mode (see [Scan Mode](#) on page 142), the Crawl Requestor Thread Count is set to “1” and may not be modified.

If you notice numerous entries on the **Scan Log** tab showing requests timing out, you should reduce the thread count. While most servers can handle a large number of requests, servers in development environments sometimes have limitations on their licensing that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5. Failing to do so may mean that WebInspect does not accurately crawl or audit the site because requests are being rejected by the server.

## Requestor Settings

### 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 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 WebInspect will wait for an HTTP response from the server. If this threshold is exceeded, WebInspect resubmits the request until reaching the retry count. If it then receives no response, WebInspect 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 crashes or becomes too busy to respond in a timely manner. You can instruct WebInspect to terminate a scan by specifying a threshold for the number of timeouts.

### 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’ retry 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 WebInspect to terminate the scan if the target server does not respond to WebInspect’s first request.

### Response codes to stop scan if received

Enter the HTTP status codes that, if received, will force WebInspect to terminate the scan. Use a comma to separate entries; use a hyphen to specify an inclusive range of codes.



## Session Storage

### Log Rejected Session to Database

You can specify which rejected sessions should be saved to the WebInspect 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, WebInspect retrieves the saved data and sends HTTP requests that previously were suppressed.
- Hewlett-Packard 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:

#### Reasons for Rejecting a Session

Reject Reason	Explanation
Invalid Host	Any host that is not specified in Default (or Current) Scan Settings/Scan Settings/Allowed Hosts.
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 an advanced 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.

## Reasons for Rejecting a Session (cont'd)

Reject Reason	Explanation
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 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

WebInspect normally saves only those attack sessions in which a vulnerability was discovered. To save all attack sessions, select **Save non-vulnerable attack sessions**.

## Session Exclusions

These settings apply to both the crawl and audit phases of a WebInspect vulnerability scan. To specify exclusions for only the crawl or only the audit, use the **Crawl Settings - Session Exclusions** or the **Audit Settings - Sessions Exclusions** options in the left pane.

## Excluded or Rejected File Extensions

You can identify a file type and then specify whether you want to exclude or reject it.

- **Reject**—WebInspect will not request files of the type you specify.
- **Exclude**—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

WebInspect will not process files associated with the MIME type you specify.

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 If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.
- 4 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**—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, WebInspect will not examine the specified URL or host for links to other resources. During the audit portion of the scan, 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.

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/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**.

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 HP's regular expression extensions you specify in the **Match String** field.
  - **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 .
- 7 (Optional) Repeat [step 2](#) through [step 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 **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

#### 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, 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]*/

## 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. For example, if you were scanning “Wlexample.com,” you would need to add “Wlexample2.com” and “Wlexample3.com” here if those domains were part of your Web presence and you wanted to include them in the 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 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, 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 that if you specify a port number, then the allowed host must be an exact match.

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**.

When specifying the URL, do not include the protocol designator (such as http:// or https://).

To edit or remove an allowed domain:

- 1 Select a domain from the **Allowed Hosts** list.
- 2 Click **Edit** or **Remove**.

## HTTP Parsing

### 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 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=slbhkelvbk173dhj`. In this case, “userid” is the parameter you would identify.



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.

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. The defaults identify ASP.NET cookieless session IDs.

## 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:

Ex. 1 -- `http://www.anysite.com?Master.asp?Page=1`

Ex. 2 -- `http://www.anysite.com?Master.asp?Page=2;`

Ex. 3 -- `http://www.anysite.com?Master.asp?Page=13;Subpage=4`

Ordinarily, 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.

Examples 1 and 2 contain one resource parameter: “Page.”

Example 3 contains two parameters: “Page” and “Subpage.”

To identify resource parameters:

- 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 specify which character set WebInspect should use.

## 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, WebInspect will attempt (during a scan) to identify custom parameters and create rules to accommodate them. WebInspect will save these rules in the Custom Parameters settings and will suggest them as recommendations.

## 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 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 either Simplified Syntax or Regular Expression syntax.

Examples:

HTML: `<a href="someDetails/user1/">User 1 details</a>`

Rule: `http://samplesite.com/someDetails/{username}/`

HTML: `<a href="TwoParameters/Details/user1/Value2">User 1 details</a>`

Rule: `http://samplesite.com/TwoParameters/Details/{username}/{parameter2}`

HTML: `<a href="/Value2/PreFixParameter/Details/user1">User 1 details</a>`

Rule: `http://samplesite.com/{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 SOAP-based and Web Services Description Language (WSDL)-based Web services.

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 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 [Creating Rules for Matrix and Path Parameters](#) on page 161 for guidelines and examples.

The enabled check box is selected by default. WebInspect examines the rule and, if 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 Without Deleting It

To disable a rule without deleting it:

- 1 Select a rule.
- 2 Clear the check mark in the **Enabled** column.

## Importing a File Containing Rules

To import a file containing rules:

- 1 Click Import  **Import...**
- 2 Using a standard file-selection dialog, 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 which were not used during a 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 WebInspect can programmatically assume that a valid portion of the site has not been attacked. Therefore, if you select this option, 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, 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.

## Creating Rules for Matrix and Path 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 SecurityScope
- 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 are actually modified URLs that use special characters to designate parts of the actual URL that contain parameters. If URL matches a rule, WebInspect parses the parameters and attacks them. Notable components of a rule (and of a URL) are:

- Scheme (HTTP/HTTPS)
- Authority (username + hostname + port)
- 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 following special elements.

- \* (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 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: `http://www.amazon.com/gp/c/*={param}`

Invalid rule: `http://www.amazon.com/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:

`http://www.amazon.com/gp/c/{book_name}` is a match for these two URLs:

`http://www.amazon.com:8080/gp/c/Moby_Dick`

`http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0`

but is not a match for any of these:

`https://www.amazon.com/gp/c/Hobbit`

`http://www.amazon.com /gp/c/Moby_Dick/`

`http://www.amazon.com/gp/c/Sex_and_the_City/Horror`

WebInspect treats 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, 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:

- Schema – as in `*://www.amazon.com/{param}`, which will match both HTTP and HTTPS.

- Authority – as in `http://*/{param}`, which will match all hosts, ports and userinfo.
  - Userinfo – as in `http://*@amazon.com/{param}`, which will match any username and password.
    - Username – as in `http://*:my_password@amazon.com/{param}`, which will match any username with given password.
    - Password – as in `http://john:*@amazon.com/{param}`, which will match any password for a given username.
  - Hostname – as in `http://john:password@*/{param}`, which will match any host provided the username and password are as defined.
    - Host fragments – as in `http://*.amazon.com/{param}`, which will match any host within amazon.com domain.
    - Port – as in `http://www.amazon.com:*/{param}`, which will match any port for www.amazon.com host.
- Path – cannot be matched as a whole, since `*` in path matches a single segment or less.
  - Path segments – as in `http://www.amazon.com/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 `http://www.amazon.com/gp/ref=*`, which will match URLs with schema HTTP, hostname www.amazon.com, path containing two segments (first is exactly “gp”, second containing any string with prefix “ref=”).
- Query – as in `http://www.amazon.com/gp/c/{param}?*`, which match any URL with schema HTTP, hostname www.amazon.com, 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 `http://www.amazon.com/gp/c/{param}` and `http://www.amazon.com/gp/c/{param}?*`. The 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 `http://www.amazon.com/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 `http://www.amazon.com/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 `http://www.amazon.com/gp/c/{param}#*` which match any URL with fragment part being present.

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 WebInspect and attacked properly.

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 example, 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}
```

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.

## Filters

Use these 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 WebInspect or those who have access to the raw data or generated reports.

If the text you specify is found, WebInspect reports it on the **Information** tab as a “Hidden Reference Found” vulnerability.

### 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.

To add a 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 representing 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 an area to search:
  - For Requests: select **All**, **Headers**, or **Postdata**.
  - For Responses: select **All**, **Headers**, or **Body** (that is, the code of the page itself).
- 4 Type (or paste) the replacement string in the **Replace search text with** field.
- 5 For case-sensitive searches, select the **Case-Sensitive Match** check box.
- 6 Click **OK**.

## Cookies/Headers

### Standard Header Parameters

#### Include 'referer' in HTTP request headers

Select this check box to include referer headers in 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 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 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 WebInspect is auditing that site. You can add multiple custom headers.

The default custom headers are described in the following table.

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.

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 WebInspect to the server when conducting a vulnerability scan.

To add a custom cookie:

- 1 Click **Add**.  
The *Specify Custom Cookie* window opens.

- 2 In the Custom Cookie field, 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**
- 3 Click **OK**.

## Proxy

### Proxy Settings

Select one of the following proxy options.

#### Direct Connection (proxy disabled)

Select this option if you are not using a proxy server.

#### Auto detect proxy settings

Select this option to use the Web Proxy Autodiscovery (WPAD) protocol to automatically locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

#### Use Internet Explorer proxy settings

Select this option to use the proxy server settings configured for the Internet Explorer browser 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.



Electing to use 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 will not be used.

#### Configure proxy using a PAC File

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 fields as follows. For proxy servers accepting https connections, select the **Specify Alternative Proxy for HTTPS** check box and specify the fields after the check box instead.

- 1 In the **Server** field, type the URL or IP address of your proxy server.
- 2 In the **Port** field, enter the port number (for example, 8080).
- 3 Select a protocol for handling TCP traffic through a proxy server: **Standard**, **Socks4**, or **Socks5**.

- 4 If authentication is required, select a method from the **Authentication** list:

Authentication	Description
Basic	<p>A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.</p> <p>The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.</p>
NTLM	<p>NTLM (NT LAN Manager) is an authentication process used by all members of the Windows NT family of products. It 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.</p> <p>Use NTLM authentication for servers running IIS.</p>
Kerberos	<p>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.</p>
Digest	<p>The Windows Server 2003 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.</p>
Automatic	<p>Allow the Web Form Editor to determine the correct authentication method. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.</p>
Negotiate	<p>If both the server and client are using Windows 2000 or later, Kerberos authentication is used. Otherwise, NTLM authentication is used. This method is also known as Integrated Windows authentication.</p>

- 5 If your proxy server requires authentication, enter the qualifying user name and password.
- 6 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 the **Specify Alternative Proxy for HTTPS** check box and provide the requested information (described in the previous table).

## 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 WebInspect encounters a server or form that requires authentication. Otherwise, a crawl might be prematurely halted for lack of logon information.

### Scan requires network authentication

Select this check box if users must log on to your Web site or application using assigned credentials. You may then select the authentication method and specify the credentials.



WebInspect will crawl all servers granted access by this password. 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 HP technical support.

#### Authentication Method

See [step 4](#) on page 167 for a description of the available authentication methods.

#### Authentication Credentials

Enter user name and password.

## 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 **Enable** in the **Client Certificates** group.
- 2 Click **Select** to open the *Client Certificates* window.
- 3 Choose a certificate.
- 4 Click **OK**.

## Specifying Client Certificates When Tools Should Require Them

When using manual mode or other tools that incorporate a proxy (specifically the Unified 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 procedures.

Find your certificate's serial number as follows:

- 1 Open Microsoft Internet Explorer.
- 2 Click **Tools** → **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.



Create an entry in the `SPI.Net.Proxy.Config` file and edit it as follows:


- 1 Open the `SPI.Net.Proxy.Config` file for editing. The default location is `C:\Program Files (x86)\HP\HP WebInspect Enterprise 10.20 Console`.
- 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.hp.com`).  
*Number* is the serial number obtained in Task 1.
- 3 Save the edited file.

## Site Authentication

### Use a login macro for forms authentication

This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent 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 logout signature. Click the browse button  to locate and load a macro. To record a macro, enter the starting URL in the **Initial recorder location** field and click **Record**. The Web Macro Recorder then opens.


### 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 Smart Credentials (if you used the Event-Based IE Compatible Web Macro Recorder) or username and password parameters (if you used the Web Macro Recorder).

If you start a scan using a macro that includes Smart Credentials (or parameters for user name and password), then when you scan the page containing the input elements associated with these entries, WebInspect substitutes the user name and password specified here. This allows 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.

### Use a startup macro

This type of macro is used to acquire state by logging in to a particular area of the application, but does not contain logic that will prevent WebInspect from logging out. Use this type of macro if you cannot determine a logout signature or if the application cannot log you out.

Click the browse button  to locate the macro. Click **Record** to record a macro.

## File Not Found

### 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.

### Forced valid response codes (never a FNF)

Specify the HTTP response codes that should never be treated as a file-not-found response.

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.

#### Forced FNF response codes (always a FNF)

Specify the HTTP response codes that will always be treated as a file-not-found response. WebInspect Enterprise 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 WebInspect from 404 pages that are unique to your site.

### 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 WebInspect to detect these "custom" file-not-found pages.

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.

#### Match FNF page with [ ] % certainty

If you select the **Auto detect** check box, you can specify what percentage of the response content must be the same. The default is 90 percent.

## Policy

Select a policy to be used as the default whenever you start a scan.

You can substitute a different policy when starting a scan through the Scan Wizard, but the policy you select here will be used if you do not select an alternate.

You can also create, import, edit, or delete policies.


### Creating a Policy

Use the following procedure to create a policy:

- 1 Click **Create**.  
The Policy Manager tool opens.
- 2 Select **File** → **New** (or click the New Policy icon).
- 3 Select the policy on which you will model a new one.
- 4 Refer to the on-line Help for additional instructions.

## Importing a Policy

Use the following procedure to import a policy:

- 1 Click **Import**.
- 2 On the *Import Custom Policy* window, click the browse button .
- 3 Using the **Files Of Type** list on the standard file-selection window, choose a policy type:
  - **Policy Files (\*.policy)**—Policy files designed and created for versions of WebInspect beginning with release 7.0.
  - **Old Policy Files (\*.apc)**—Policy files designed and created for versions of WebInspect prior to release 7.0.
  - **All Files (\*.\*)**—Files of any type, including non-policy files.
- 4 (optional) Edit the policy name.
- 5 Click **OK**.

A copy of the policy is created in the Policies folder. The default location is C:\Documents and Settings\All Users\Application Data\HP\HP WebInspect\Policies\.

The policy and all of its enabled checks are imported into SecureBase using the specified policy name.

## Deleting a Policy

Use the following procedure to delete a policy:

- 1 Select a custom policy. Only custom policies may be deleted.
- 2 Click **Delete**.

## Editing a Policy

Use the following procedure to edit a policy:

- 1 Select a custom policy. Only custom policies may be edited.
- 2 Click **Edit**.

The Policy Manager tool opens. Refer to the online Help for additional instructions.

# Specifying Advanced Crawl Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Crawl Settings described in this section. The Advanced Crawl Settings for Guided Scan are similar but not identical to those for a Web Site Scan.

The WebInspect crawler is a software program designed to follow hyperlinks throughout a Web site, retrieving and indexing pages to document the hierarchical structure of the site. The parameters that control the manner in which WebInspect crawls a site are available in the Crawl Settings category.



These settings are not displayed if you select the **Audit Only** option in the Scan Settings - Method category.

Headings in the following sections are named and organized the same way they appear in the product interface.

## Link Parsing

WebInspect will follow all hyperlinks defined by HTML (using the <a href> tag) and those defined by scripts (if you select the JavaScript/VBScript analyzer option on the Crawl Settings - Content Analyzers panel). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, use the Custom Links feature to identify (using regular expressions) links that you want WebInspect to follow.

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**.

## 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) allows 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**.  
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.

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 If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.
- 4 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 (during the crawl) that contains that component.

- **Reject**—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, WebInspect will not examine the specified URL or host for links to other resources. 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.

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/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**.

To add exclusion/rejection criteria:

- 1 Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** 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 HP's regular expression extensions you specify in the **Match String** field.
  - **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 .
- 7 (Optional) Repeat [step 2](#) through [step 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 **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.

### 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, 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]*/

The default setting URL: \?[DNMSCO]=[ADNSM] is used for Apache directory indexing. These are sort options for the listing, which have no real impact on the page contents. An example would be http://www.w3.org/Icons/?C=M;O=A.

# Specifying Advanced Audit Settings for Guided Scan

Click **Advanced** in the toolbar to access the Advanced Audit Settings described in this section. The Advanced Audit Settings for Guided Scan are similar but not identical to those for a Web Site Scan.

An audit is the probe or attack conducted by WebInspect that is designed to detect vulnerabilities. The parameters that control the manner in which WebInspect conducts that probe are available from the Audit Settings category.



These settings are not displayed if you select the **Crawl Only** option in the Scan Settings - Method category.

Headings in the following sections are named and organized the same way they appear in the product interface.

## 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) allows 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**.  
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.

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 If you enter a regular expression to specify a MIME type, select the **Use Regular Expression** check box.
- 4 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 (during the audit) that contains that component.

- **Reject**—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 the audit portion of the scan, 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.

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/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**.

To add exclusion/rejection criteria:

- 1 Click **Add** (on the right side of the **Excluded or Rejected URLs and Hosts** 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 HP's regular expression extensions you specify in the **Match String** field.
  - **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 .
- 7 (Optional) Repeat [step 2](#) through [step 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 **Excluded or Rejected URLs or Hosts** list, select either **Reject**, **Exclude**, or both.



### 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, 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]*/

## Attack Exclusions


### Excluded Parameters

Use this feature to prevent 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**.  
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 in which the parameter may be found: **HTTP query data** or **HTTP POST data**. You can select both areas, if necessary.
- 4 Click **OK**.

## Excluded Cookies

Use this feature to prevent 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.”

To exclude certain cookies.

- 1 In the **Excluded Cookies** group, click **Add**.

The Regular Expression Editor appears.

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 **Comparison 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 comparison text for strings that match the regular expression. Matches will be highlighted in red.
- f Did your regular expression identify the string?  
NO—Verify that the Comparison Text contains the string you want to identify or modify the regular expression.  
YES—Click **OK**.

## Excluded Headers

Use this feature to prevent 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 using the procedure described below.

- 1 In the **Excluded Headers** group, click **Add**.

The Regular Expression Editor appears.


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 **Comparison 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 comparison text for strings that match the regular expression. Matches will be highlighted in red.
- f Did your regular expression identify the string?  
NO—Verify that the Comparison Text contains the string you want to identify or modify the regular expression.  
YES—Click **OK**.

## Audit Inputs Editor and Import Audit Inputs Buttons

Using the Audit Inputs Editor, you can create additional 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 in the *Tools Guide for WebInspect Products*.

## Attack Expressions

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 and Japan
- ko-kr: Korean and Korea
- zh-cn: Chinese and China
- zh-tw: Traditional Chinese

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.

## Vulnerability Filtering

By applying certain filters (listed below), you can modify the results of a vulnerability scan to accommodate your specific testing environment.

- **Standard Vulnerability Definition:** This filter reports vulnerabilities in the same manner as `QAInspect`.
- **Standard Vulnerability Definition - New:**
- **403 Blocker:** This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Parameter Vulnerability Roll-Up:** This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.
- **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.
- **Standard Vulnerability Definition CaseFix,**

### Select Vulnerability Filters to Enable

To add a filter to your default settings:

- 1 In the **Audit Settings** panel in the left column, select **Vulnerability Filtering**.  
All available filters are listed in either the **Disabled Filters** list or the **Enabled Filters** list.
- 2 To enable a filter, select a filter in the **Disabled Filters** list and click **Add**.  
The filter is removed from the **Disabled Filters** list and added to the **Enabled Filters** list.
- 3 To disable a filter, select a filter in the **Enabled Filters** area and click **Remove**.  
The filter is removed from the **Enabled Filters** list and added to the **Disabled Filters** list.

## 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, 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.

### Enable Smart Scan

If you select **Enable Smart Scan**, you can choose one or more of the identification methods described in the following sections.

#### Use regular expressions on HTTP responses to identify server/application types

This method, employed by previous releases of 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** 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**.

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.

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**.



## 6 Guided Scan Using Mobile Templates

### About Guided Scans Using Mobile Templates

For a general introduction to Guided Scan, including the automatic download of the required Thin Client application, see [About Guided Scan](#) on page 129.

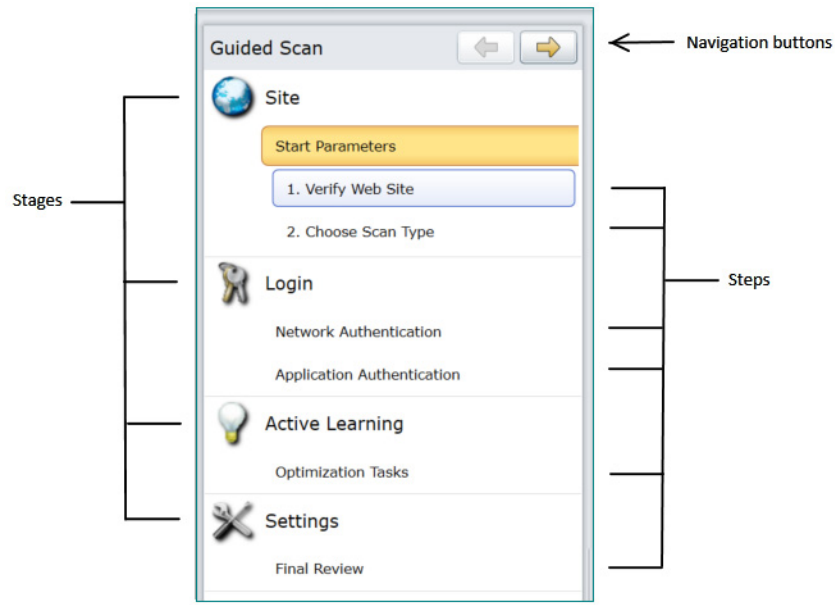
The mobile template options are:

- **Mobile Scan (Create a Mobile Web Site Scan):** A **Mobile Scan** scans a mobile site from the machine where your instance of WebInspect or WebInspect Enterprise is installed. WebInspect or WebInspect Enterprise emulates a mobile browser to access the mobile version of the site. See [About Mobile Scans](#) on page 183.
- **Native Scan (Create a Native Mobile Web Service Scan):** A **Native Scan** manually crawls a native mobile application and captures the Web traffic as a workflow macro. You generate the traffic on an Android or iOS device or a software emulator running a mobile application. See [About Native Scans](#) on page 194

### About Mobile Scans

Using the Mobile Scan template to create a mobile Web site scan allows you to scan the mobile version of a Web site using the desktop version of your browser from within WebInspect or WebInspect Enterprise. A Mobile Scan is nearly identical to a Web Site Scan and 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. WebInspect Enterprise comes with four mobile user agent options to choose from, and you can create a custom option and create a user agent for another version of Android, Windows Phone, or other mobile device. For information about creating a user agent header, see [Creating a Custom User Agent Header](#) on page 185.

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, shown below, 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 website to determine if particular settings should be modified.
- **Settings:** where you review and validate your choices and run the scan.

The Guided Scan wizard includes a tutorial that runs the first time you launch a Guided Scan. You can close it at any time and reopen it later by clicking the **Tutorial** button at the top right of the display.

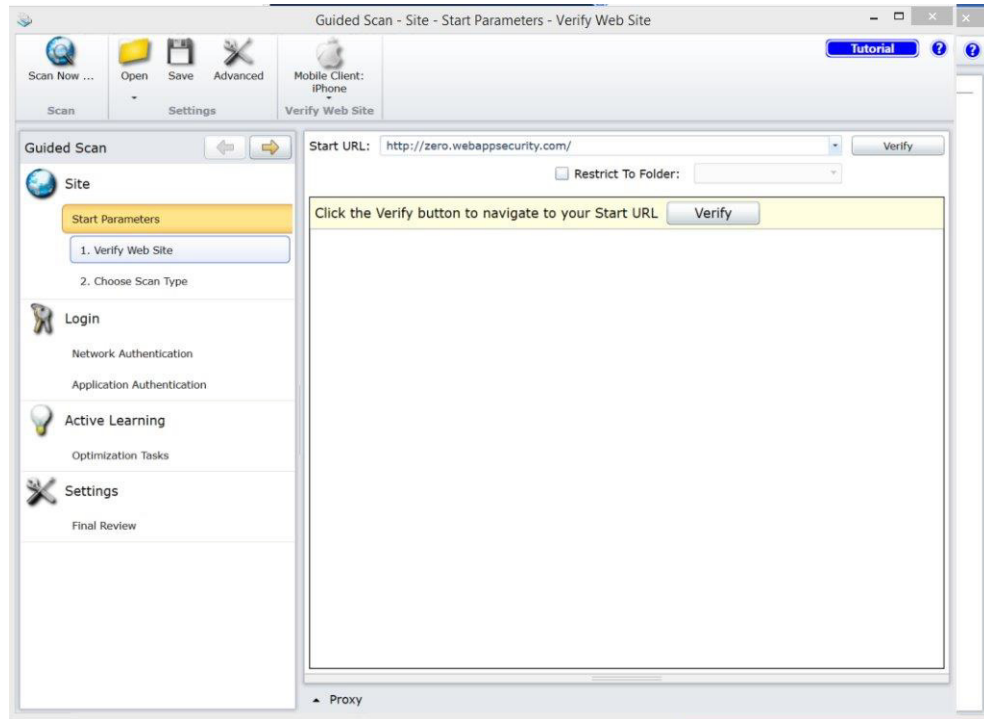
## Creating a Mobile Scan

To create a Mobile Scan:

- 1 Log into 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.
  - 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](#) on page 185.
  - d When you have selected the rendering engine and user agent as needed, go to [About the Site Stage](#) on page 186.

## Creating a Custom User Agent Header

WebInspect Enterprise includes user agents for Android and iOS. 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 of the settings area, double-click the User-Agent string.

The *Specify Custom Header* box 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** box, 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, WebInspect or 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).

WebInspect and 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).** WebInspect or 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/`, WebInspect or WebInspect Enterprise will assess only the “two” directory.
  - **Directory and subdirectories.** WebInspect or 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.** WebInspect or 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 Click **Verify**.
- 4 If you must access the target site through a proxy server, click **Proxy** in the lower left of the main screen to display the *Proxy Settings* area, and then select an option from the **Proxy Settings** list:
  - **Direct Connection (proxy disabled)**
  - **Autodetect 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 Internet Explorer proxy settings:** Import your proxy server information from Internet Explorer.
- **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. If you select this option, click **Edit** to enter the location (URL) of the PAC.
- **Explicitly configure proxy settings:** Specify proxy server settings as indicated. If you select this option, click **Edit** to enter proxy information.



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.

When 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

- 1 Type in a name for your scan in the **Scan Name** box.
- 2 Select one of the following scan types:
  - **Standard:** WebInspect or 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.** WebInspect or 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 Scan Settings: [Method](#) on page 142.
  - **Audit Only.** WebInspect or 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 “Policy Manager” chapter in the *Tools Guide for WebInspect Products*, the *WebInspect Enterprise User Guide*, or the WebInspect Enterprise Web Console Help system.
- 5 In the *Crawl Coverage* area, adjust the **Crawl Coverage** slider to select the level of coverage you want. Use the guidance provided on screen for each option.
- 6 Click the **Next** button.

The *Login* stage appears with **Network Authentication** highlighted in the left pane.

## About the Login Stage

If the application you intend to scan requires login credentials, you can use the *Login* stage to either select an existing login macro or record one for use with the scan.

If your application does not require login credentials, you can skip this section of the Guided Scan wizard by clicking through the options without assigning values, or clicking the next step in the Guided Scan tree.

In this stage you can:

- Configure network authentication
- Configure application authentication
- Create or assign a login macro

### Network Authentication Step

If your application requires either network or application level authentication, you can assign it here.

#### Configuring Network Authentication

If your network requires network authentication and/or a client certificate, you can configure them here.

To configure network authentication:

- 1 Click the **Network Authentication** check box.
- 2 Select a **Method** from the drop-down list of authentication methods. The authentication methods are:
  - **Automatic.** Allow WebInspect or WebInspect Enterprise to determine the correct authentication type.
  - **Basic.** A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a user name and password. The Web browser then attempts to establish a connection to a server using the user's credentials. If the credentials are rejected, the browser displays an authentication window to re-enter 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. The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers.
  - **NTLM.** NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and WebInspect or WebInspect Enterprise has to pass through a proxy server to submit its requests to the Web server, WebInspect or WebInspect Enterprise may not be able to crawl or audit that Web site. Use caution when configuring WebInspect or WebInspect Enterprise for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.

- **Digest.** The Windows Server 2003 operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

- **Kerberos.** Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.
- **Negotiate.** The Negotiate authentication protocol begins with the option to negotiate for an authentication protocol. When the client requests access to a service, the server replies with a list of authentication protocols that it can support and an authentication challenge based on the protocol that is its first choice. For example, the server might list Kerberos and NTLM, and send a Kerberos challenge. The client examines the contents of the reply and checks to determine whether it supports any of the specified protocols. If the client supports the preferred protocol, authentication proceeds. If the client does not support the preferred protocol, but does support one of the other protocols listed by the server, the client lets the server know which authentication protocol it supports, and the authentication proceeds. If the client does not support any of the listed protocols, the authentication exchange fails.

3 Complete the **User Name** and **Password** fields.

To configure a client certificate:

- 1 Select the **Client Certificate** check box.
- 2 Select **Local Machine** if the certificate is located on the local machine, or **Current User** to select among the certificates owned by the currently logged-in user.
- 3 Select **My** or **Root** from the drop-down menu to identify the type of certificate required.

The *Certificate* box is populated with the certificates that meet the selected criteria.

- 4 Select the certificate you want to use from the *Certificate* box.

For verification purposes, certificate information, including validity dates, is listed in the *Certificate Information* section below the *Certificate* box.

- 5 Click the **Next** button.

The *Application Authentication* page appears.

## Application Authentication Step

If your site requires authentication, you can use this step to create 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. You can select a previously recorded login macro or record a new one.

### Selecting a Login Macro

Note: For details about recording login macros or using an existing login macro, see the "Unified Web Macro Recorder" chapter in the *Tools Guide for WebInspect Products*.

To select a previously recorded login macro or record a new one:


- 1 Click the **Use a login macro for this site** check box.
- 2 Click the browse button to navigate to and select an existing login macro to use in the scan, or click the **Create** button to record and test a new login macro.
- 3 Click the **Next** button.

The *Optimization Tasks* page appears with **Profile site for optimum settings** highlighted in the left pane.

## 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 WebInspect Enterprise audits the pages you specify in the macro. 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 workflows 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 Unified Web Macro Recorder, allowing you to create a macro.
  - **Edit.** Opens the Unified 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 macro and/or Burp Proxy captures. See [Importing Burp Proxy Results](#).
-  Note: If you have installed HP Unified Functional Testing (UFT) on your computer, then WebInspect or WebInspect Enterprise detects this automatically and displays an option to import a UFT .usr file. See [Importing HP Unified Functional Testing \(UFT\) Files in a Guided Scan](#) on page 140.
- **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. See [Allowed Hosts](#) on page 157.

## 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.

### Adding Burp Proxy Results

To add Burp Proxy results to a workflow macro:

- 1 If you are not on the *Workflows* screen, click the *Manage Workflows* step 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:

- Run the WebInspect or WebInspect Enterprise Profiler to see if any settings need to be changed.
- Set scan optimization options if necessary.
- Navigate to key locations in your site that should be fully exercised.

## Profiling the site for optimal settings

The Profiler conducts a preliminary examination of the target Web site to determine if certain settings should be modified. If changes appear to be required, the Profiler returns a list of suggestions, which you may accept or reject.

For example, the Profiler may 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 may specify that WebInspect or 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 WebInspect or WebInspect Enterprise setting to accommodate this feature.

To launch the Profiler:

- 1 Click **Profile**.

The Profiler runs.

Results appear in the *Optimize scan for* box in the *Settings* section.

- 2 Accept or reject the suggestions that appear in the *Optimize scan for* drop-down box. To reject the suggestion, select **None** or an alternate from the drop-down menu.
- 3 If necessary, provide any requested information.
- 4 Click the **Next** button.

Several options may be presented even if you do not run the Profiler, as described in the following sections.

### Autofill Web Forms

Select **Auto-fill Web forms during crawl** if you want WebInspect or WebInspect Enterprise to submit values for input controls on forms it encounters while scanning the target site. WebInspect or 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 *Tools Guide for WebInspect Products*.

You may:

- 1 Click the browse button (...) to locate and load a file.
- 2 Click **Edit** to edit the selected file (or the default values) using the Web Form Editor.
- 3 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 [Allowed Hosts](#) on page 157 for more information.

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**.

## Reuse Identified False Positives

Select scans containing vulnerabilities that were changed to false positives. If those false positives match vulnerabilities detected in this scan, the vulnerabilities will be changed to false positives.

To reuse identified false positives:

- 1 Select **Import False Positives**.
- 2 Click **Select Scans**.
- 3 Select one or more scans containing false positives from the same site you are now scanning.
- 4 Click **OK**.

## Apply Sample Macro

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.

## Traffic Analysis

Select **Launch and Direct Traffic through Web Proxy** to use the Web Proxy tool to examine the HTTP requests issued by WebInspect or WebInspect Enterprise and the responses returned by the target server.

While scanning a Web site, WebInspect or 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 **Enable Traffic Monitor**, WebInspect or WebInspect Enterprise adds the **Traffic Monitor** button to the Scan Info panel, allowing you to display and review each HTTP request sent by WebInspect or WebInspect Enterprise and the associated HTTP response received from the server.

## Message

If the Profiler does not recommend changes, the Guided Scan wizard displays the message “No settings changes are recommended. Your current scan settings are optimal for this site.”

Click **Next**. The **Enhance coverage of your web site** task appears highlighted in the left pane.

## Enhancing coverage of your web site

To enhance coverage of your application, navigate to key locations in your application to enhance coverage.

See the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products* for detailed information about using the Web Macro Recorder to navigate key locations in your application for Guided Scan to use during the scan.

See the Guided Scan Tutorial for more information about how to use this page of the Guided Scan wizard. To launch the tutorial, click **Tutorial** in the upper right corner of the page.

## Web Form Values

Guided Scan recorded all of the web form values that you entered while you explored your Web site. Here you can review and modify the values, which are part of the scan settings that are saved with the scan. In the Web Forms section of the toolbar, you can click **Export** to save the values to a separate file or click **Import** to use an existing set of values. The scan settings, including the web form values, serve as defaults that you can modify in future scans.

Click the **Next** button.



## About the Settings Stage

In the *Settings* stage, under the *Final Review* step, the *Validate Settings and Start Scan* step allows you to:

- Save your scan settings
- Select the project and project version
- Start a scan

### Final Review Step

#### Validate Settings and Start Scan

To complete this step:

- 1 The *Scan Now* section has a summary of your scan settings. Click the **Click here to save settings** link in the *Save Settings* section if you want to save your scan settings for future use.
- 2 Select a **Project** and **Project Version**.
- 3 Click the **Start Scan** button to launch the scan.

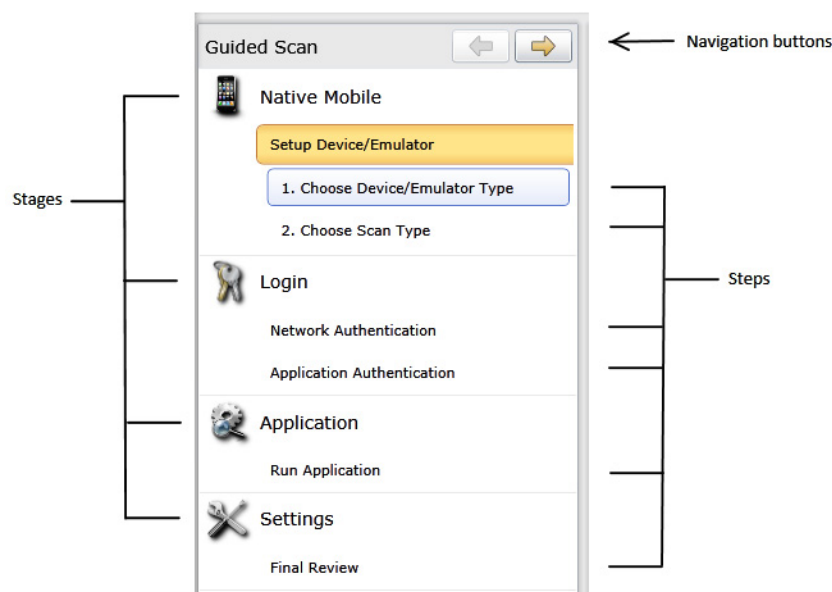
The wizard closes and the Scan Dashboard opens.

## 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 or iOS device or a software emulator running a mobile application.

**Note:** Most of the information in this section is iOS-specific, but equally relates to Android and emulator usage. Please consult your OS documentation if you have questions on setting up proxies, installing certificates, or other OS-specific tasks.

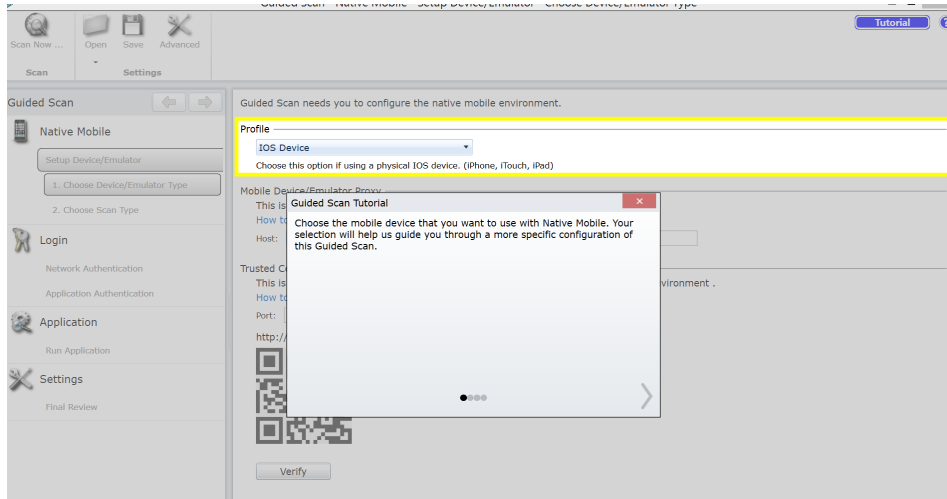
The Guided Scan wizard will guide you through the stages and steps that are required to record and scan your application traffic. The tree in the left pane, shown below, tracks your progress. If you need to return to a previous step or stage, click the Back navigation button, or click the step in the 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 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 and run the scan.

The Guided Scan wizard includes a tutorial that runs the first time you launch a Guided Scan. You can close it at any time and return to it later by clicking the **Tutorial** button at the top right of the display. This tutorial is unique to the Native Scan.



## Supported Devices

WebInspect and WebInspect Enterprise support scanning the back-end traffic on Android and iOS devices.

### Android Device Support

Any Android device, such as an Android-based phone or 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 WebInspect or WebInspect Enterprise and that you have set up a proxy between WebInspect or WebInspect Enterprise and your development machine.

## Creating a Native Scan

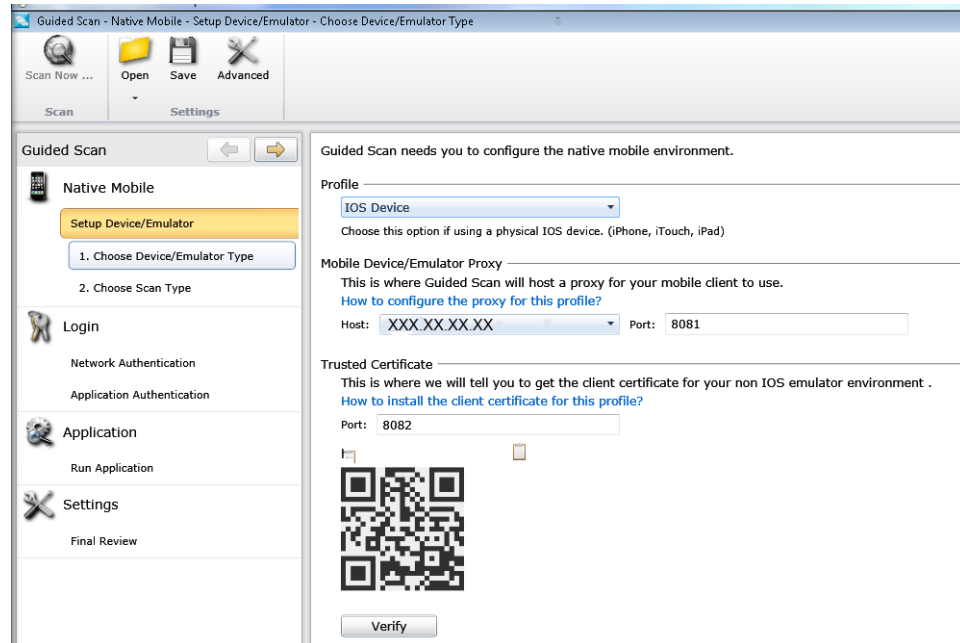
To create a Native Scan, you will need to make sure your device or emulator is on the same network as WebInspect or WebInspect Enterprise. In addition, you need to have authorization and access to the ports on the machine where you are running WebInspect or WebInspect Enterprise in order to successfully create a proxy connection.

To create a Native Scan:

- 1 Open WebInspect or 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 WebInspect or 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

After launching the Guided Scan, you will be provided with the following options:

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 <a href="#">Selecting a Profile</a> on page 197.
Mobile Device/Emulator Proxy	This is where Guided Scan will host a proxy for your mobile client to use. For more information, see <a href="#">Setting the Mobile Device Proxy Address</a> on page 197.
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 <a href="#">Adding a Trusted Certificate</a> on page 198.

### Selecting a Profile

To set the device profile, select one of the following from the **Profile** drop-down text box:

iOS Device	An iPad or iPhone running the latest version of iOS.
Android Device	A phone or tablet running the Android operating system.
iOS Emulator	The iOS emulator that is part of the iOS SDK.
Android Emulator	The Android emulator that is part of the Android SDK.

### Setting the Mobile Device Proxy Address

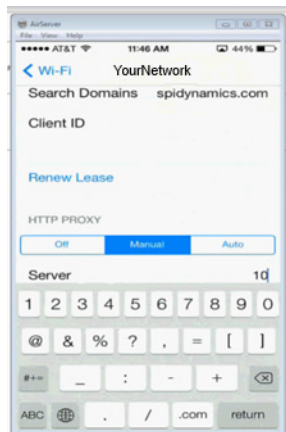
The *Mobile Device/Emulator Proxy* section lists the *Host* IP address and the *Port* number that will be used to establish a proxy connection between your device or emulator and WebInspect or WebInspect Enterprise. Use the suggested settings unless the IP address or port number are unavailable on your 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 WebInspect or WebInspect Enterprise interface allows you to click the address and select an alternate from a drop-down list.

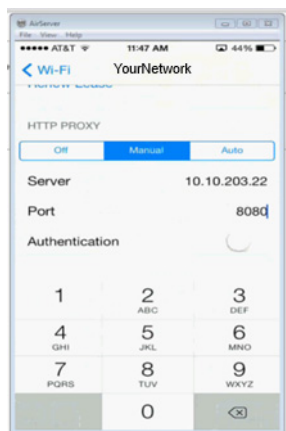
To set up a proxy on an iOS device or iOS emulator:

- 1 Run the **Settings** application.
- 2 Select **Wi-Fi**.
- 3 Select the Wi-Fi network you are using to connect to WebInspect or 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 WebInspect or WebInspect Enterprise. If you do not have this information, see [Choosing the Device/Emulator Type](#) on page 197.



- 6 In WebInspect or 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 WebInspect or 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 **Next** to select a scan type.

To set up a proxy on an Android 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, 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)

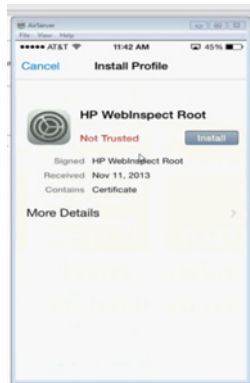
Choose the option that best suits your needs.



After completing the scan, you should remove the certificate from the repository on your device. See [Post Scan Steps](#) on page 203.

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.



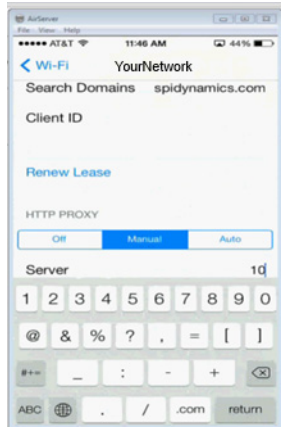
The HP WebInspect Root certificate status will display as *Not Trusted* until you add it to your root chain.

- 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.

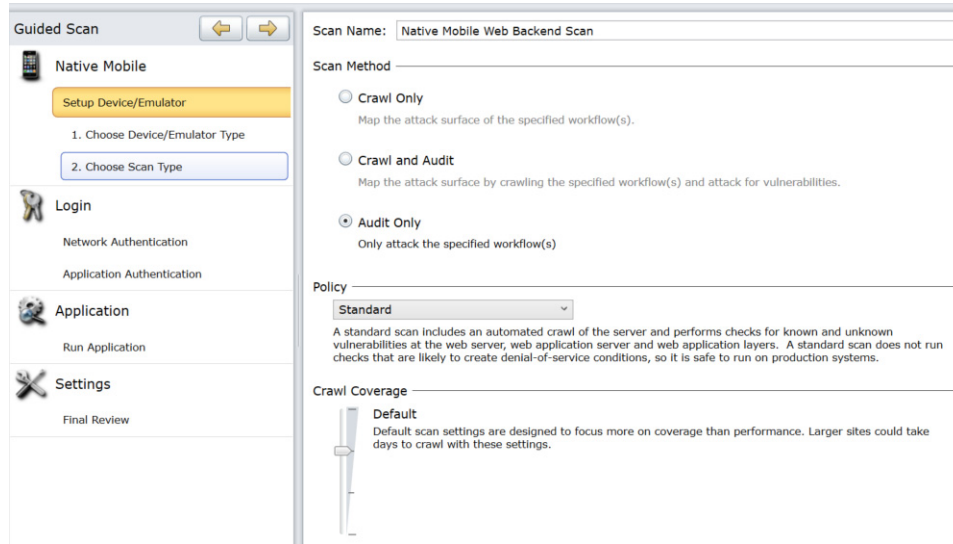
- 3 Tap **Install** on the **Warning** screen.

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 WebInspect or WebInspect Enterprise.



## Choosing the Scan Type

After setting up your device or emulator to work with WebInspect or 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.



Set the options listed below.

Option	Description
Scan Name	Type a name for the scan so that later you can identify the scan on the <i>Manage Scans</i> page.
Scan Method	Choose the type of scan your want from the following list: <ul style="list-style-type: none"><li>• Crawl Only: maps the attack surface of the entire Web site.</li><li>• Crawl and Audit: maps the attack surface of the entire Web site and scans for vulnerabilities.</li><li>• Audit Only: only attack the specified workflows.</li></ul>
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 <i>Tools Guide for WebInspect Products</i> .
Crawl Coverage	Select the level of coverage you want, using the <b>Crawl Coverage</b> slider.

## About the Login Stage

If the application you intend to scan requires login credentials, you can use the *Login* stage to either select an existing login macro or record one for use with the scan.

If your application does not require login credentials, you can skip this section of the Guided Scan wizard by clicking through the options without assigning values, or clicking the next step in the Guided Scan tree to skip to the next stage.

In this stage you can:

- Configure network authorization
- Configure application authorization
- Create or assign a login macro



## Network Authentication Step

If your application requires either network or application level authentication, you can assign it here.

### Configuring Network Authentication

If your network requires user authentication, you can configure it here. If your network does not require user authentication, click the **Next** navigation button or the next appropriate step in the Guided Scan tree to continue on.

To configure network authentication:

- 1 Click the **Network Authentication** check box.
- 2 Select a **Method** from the drop-down list of authentication methods.
- 3 Type in the **User Name** and **Password**.

### Configuring a Client Certificate

If your network is set up to accept a client certificate rather than a user name and password, you can configure your scan to provide the client certificate upon request.

To configure a client certificate:

- 1 Click the **Client Certificate** check box.
- 2 Select **Local Machine** if the certificate is located on the local machine, or **Current User** to select among the certificates owned by the currently logged-in user.
- 3 Select **My** or **Root** from the drop-down menu to identify the type of certificate required.  
The *Certificate* box is populated with the certificates that meet the selected criteria.
- 4 Select the certificate you want to use from the *Certificate* box.

For verification purposes, certificate information, including validity dates, is listed in the *Certificate Information* section below the selection box.

## Application Authentication Step

If the back-end of your mobile application requires authentication, you can use this step to create 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 tapping a button such as Log In or Log On. You can select a previously recorded login macro or record a new one.



For more information about recording login macros or using an existing login macro, see the “Unified Web Macro Recorder” chapter in the *Tools Guide for WebInspect Products*.

### Selecting a Login Macro

To select a login macro:

- 1 Click the **Use a login macro for this site** check box.
- 2 Click the browse (...) button to select a macro you have saved.

## Recording a Login Macro

To create a login macro:

- 1 Click the **Use a login macro for this site** check box.
- 2 Click the **Create** button.
- 3 When the macro recorder opens, click the **Record** button.
- 4 On your device or emulator, use your application to log in to your site. Once you have logged in, click the **Stop** button.
- 5 Click **Play** to test your macro.
- 6 Confirm the macro played back correctly or start over and recreate the macro.

## Specifying a Logout Condition

In some cases, after playing back your macro, a logout condition will need to be manually specified. If so, see the *Logout Condition Editor* section of the “Unified Web Macro Recorder” chapter of the *Tools Guide for WebInspect Products*.

## 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

### Recording Web Traffic

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.

### Finalizing Allowed Hosts and RESTful Endpoints

After running the application and collecting Web traffic, a list will be generated of the Allowed Hosts and potential RESTful Endpoints.

To select the 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 resultant list.

If WebInspect or WebInspect Enterprise didn't 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 RESTful endpoints.

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 Step

#### Validate Settings and Start Scan

In the *Validate Settings and Start Scan* step, you can:

- Save your scan settings
- Select the project and project version
- Start a scan

To complete this step:

- 1 Read the *Warnings and Informationals* section to see if there are any final tasks or corrections that need to be made.
- 2 The *Scan Now* section has a summary of your scan settings. Click the **Click here to save settings** link in the *Save Settings* section if you want to save your scan settings for future use.
- 3 Select a **Project** and **Project Version**.
- 4 Click the **Start Scan** button to launch the scan.

The wizard closes and the Scan Dashboard opens.

## Post Scan Steps

After you have completed your scan and run WebInspect or WebInspect Enterprise, you will need to reset your Android, iOS device, or emulator to its former state. The following steps show how to reset your iOS device to the way it was before you began. Steps for Android and emulator users are similar, but depend on the version of the OS you are running.

To remove the HP 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 HP 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.

# A Policies

This appendix has the following sections:

- [About Policies](#)
- [List of Policies](#)

## About Policies

A policy is a collection of vulnerability checks and attack methodologies that HP scanners deploy against a Web application. All policies contain all possible audit engines and agents, but each policy has a different subset of these components enabled. Although your environment may also include custom policies designed by your developers, the standard installation contains the prepackaged policies described in the following section.

Each policy is kept current using the SmartUpdate function, ensuring that assessments are accurate and capable of detecting the most recently discovered threats.

## List of Policies

HP scanners contain the following packaged policies that you can use with your scans and crawls to determine the vulnerability of your Web application:

- **Aggressive SQL Injection**—The Aggressive SQL Injection 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.
- **All Checks**—An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the HP check database. This includes checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.
- **Application**—The Application policy performs a security assessment of your Web application by submitting known and unknown Web application attacks, and only submits specific attacks that assess the application layer. When performing assessments of enterprise level Web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your assessment in terms of speed and memory usage.
- **Assault**—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.



You are strongly advised to use assault scans in test environments only.

- **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.
- **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 will also list directories that could potentially lead to discovery of critical or high vulnerabilities. This policy does not contain checks that may write data to databases or create denial-of-service conditions, and it is safe to run against production servers.
- **Cross-Site Scripting**—This policy performs a security assessment of your Web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a Web site 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.
- **Dev**—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 Developer policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **DevInspectEclipse**—The DevInspectEclipse policy is the standard policy for use by DevInspect Java Eclipse. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **DevInspectVS**—The DevInspectVS policy is the standard policy for use by DevInspect VS. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **OWASP Top Ten**—Many organizations suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application. This policy reflects OWASP 2013, which is the latest version.
- **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.
- **Platform**—The Platform policy performs a security assessment of your Web application platform by submitting attacks specifically against the Web server and known Web applications. When performing assessments of enterprise-level Web applications, use the Platform policy in conjunction with the Application policy to optimize your assessment in terms of speed and memory usage.
- **QA**—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**—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. Smart Assessment is enabled in a Quick scan.
- **Safe**—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. Smart Assessment is enabled in a Safe scan.
- **SOAP**—Most Web services use SOAP to send XML data between the Web service and the client Web application making the information request. Use the SOAP policy to determine the security vulnerabilities of your Web service. Applying the SOAP policy against a Web site is not recommended.

- **SQL Injection**—The SQL Injection policy performs a 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.
- **Standard**—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. Smart Assessment is enabled in a Standard scan.

