opentext™

OpenText™ Dynamic Application Security Testing (Fortify WebInspect)

Software Version: 25.2.0
Windows operating systems and select Tools for macOS

Tools Guide

Document Release Date: May 2025
Software Release Date: May 2025

Legal notices

Open Text Corporation

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

Copyright notice

Trademark notices

Documentation updates

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

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

This document was produced on May 07, 2025.

About this PDF Version of Online Help

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

Contents

Preface

Contacting Customer Support

Visit the Customer Support website to:

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

For more information

For more information about OpenText Application Security Testing products, visit OpenText Application Security.

Product feature videos

You can find videos that highlight OpenText Application Security Software products and features on the Fortify Unplugged YouTube™ channel.

Change Log

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

Software Release / Document Version	Changes

25.2.0	Added:
	• Content related to the Web Macro Recorder main application window, widget, and QuickLook for Mac version. See the following topics:
	  • "Working with the main application window (Mac only)" on page 197
	  • "Using the Web Macro Recorder widget (Mac only)" on page 199
	  • "Using QuickLook (Mac only)" on page 200
	• Content related to TOTP using OAuth 2.0 authentication. See "Using IMAP multi-factor authentication with OAuth2" on page 239.
	Updated the following Web Macro Recorder content:
	• Accessing the Web Macro Recorder with new options for Mac. See "Accessing the Event-based Web Macro Recorder" on page 194.
	• Description of Web Macro Recorder UI specific to Mac version. See "Understanding the user interface" on page 201.
	• Shortcut keys with recents list functionality (Mac only). See "Using shortcut keys" on page 208.
	• Procedures for starting a new macro in Mac version. See "Using the record buttons (Mac only)" on page 218.
	• Options for uninstalling the Web Macro Recorder on Mac with new troubleshooting options. See "Cleaning up or uninstalling the Web Macro Recorder on Mac" on page 313.
	Removed:
	• Content related to the Web Macro Recorder uninstall tool on Mac.

24.4.0	Updated: • Version number and release date.

Software Release / Document Version	Changes

24.2.0	Added:
	• Installation instructions for Event-based Web Macro Recorder. See "Installing the Event-based Web Macro Recorder" on page 193.
	• Instructions for accessing Event-based Web Macro Recorder on MacOS. See "Accessing the Event-based Web Macro Recorder" on page 194.
	• Content describing shortcut keys for Event-based Web Macro Recorder. See "Using shortcut keys" on page 208.
	• Content for using the record and play buttons on Mac version of Event-based Web Macro Recorder. See Using the Record and Play Buttons (Mac Only).
	• Content for configuring certificates on Windows and Mac in Event-based Web Macro Recorder. See "Configuring certificates" on page 312.
	• Instructions for uninstalling the Event-based Web Macro Recorder. See Uninstalling the Event-based Web Macro Recorder.
	
	Updated:
	• Policies content with OWASP API Top 10 <*year*> policy and deprecated AggressiveLog4Shell policy. See "Policies" on page 84.
	• Regular expression extensions with descriptions and removed the [TEXT] extension from the list. See "Regular expression extensions and operators" on page 101.
	• Content to include the Mac version of the Event-based Web Macro Recorder. See the following topics:
	  • "Event-based Web Macro Recorder" on page 192
	  • "Understanding the user interface" on page 201
	• TOTP content in the Event-based Web Macro Recorder with click and drag option for selecting QR code. See "Using TOTP authentication" on page 234.
	
	Removed:
	• SWFScan tool content.
	• SSL settings and Firefox proxy settings from Browser Settings of the Event-based Web Macro Recorder

Software Release / Document Version	Changes

23.2.0	Added:
	• Information about using event handlers. See "Working with event handlers" on page 243.
	• Information about web storage. See "Interactive Options" on page 303 and "Working with web storage keys" on page 257.
	• Information about function libraries. See the following topics:
	  • "Understanding the Function Libraries tab" on page 206
	  • "Working with function libraries" on page 245
	  • "Understanding end events" on page 247
	Updated:
	• Policy Manager policies content with information about OAST-related checks. See "Policies" on page 84.
	• Default locations for SecureBase data when performing an offline SmartUpdate. See "SmartUpdate" on page 109.
	• Logout Condition Editor content with event-based logout conditions. See "Working with logout conditions" on page 248
	• Two-factor authentication content with support for IMAP and facts about Gmail accounts. See "Using two-factor authentication" on page 228.
	• UI and Related Objects content to include the Event Handlers Editor. See "Understanding the user interface" on page 201 and "Relating objects to other objects" on page 297
	• Browser settings content with note about an empty User Agent field. See "Browser Settings" on page 299.
	Removed:
	• Content related to Site Explorer.

Chapter 1: Welcome to OpenText™ Dynamic Application Security Testing (DAST) Tools

OpenText DAST (Fortify WebInspect) Tools is a robust set of diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and OpenText™ Fortify WebInspect Enterprise.

The tools provided in Fortify WebInspect Enterprise are a subset of the tools provided in OpenText DAST. The chapters in this guide that describe tools that are provided in OpenText DAST but not in Fortify WebInspect Enterprise have titles that end with "(OpenText DAST Only)."

Using Tools with a Proxy

When using tools that incorporate a proxy, you may encounter servers that do not ask for a client certificate even though a client certificate is required. To accommodate this situation, you must edit the `SPI.Net.Proxy.Config` file.

Product name changes

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

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

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

Related documents

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

Note: Most guides are available in both PDF and HTML formats. Product help is available within the OpenText DAST product.

All products

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

Document / file name	Description
About OpenText Application Security Software Documentation appsec-docs-n-<*version*>.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. **Note:** This document is included only with the product download.
What's New in OpenText Application Security Software <version> appsec-wn-<*version*>.pdf	This document describes the new features in OpenText Application Security Software products.
OpenText Application Security Software Release Notes appsec-rn-<*version*>.pdf	This document provides an overview of the changes made to OpenText Application Security Software for this release and important information not included elsewhere in the product documentation.

OpenText ScanCentral DAST

The following document provides information about OpenText ScanCentral DAST. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-ScanCentral-DAST.

Document / file name	Description
OpenText™ ScanCentral DAST	This document provides information about how to

Document / file name	Description
Configuration and Usage Guide sc-dast-ugd-<*version*>.pdf	configure and use OpenText ScanCentral DAST to conduct dynamic scans of Web applications.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an OpenText ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.

OpenText DAST

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

Document / file name	Description
OpenText™ Dynamic Application Security Testing Installation Guide dast-igd-<*version*>.pdf	This document provides an overview of OpenText DAST and instructions for installing and activating the product license.
OpenText™ Dynamic Application Security Testing User Guide dast-ugd-<*version*>.pdf	This document describes how to configure and use OpenText DAST to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the

Document / file name	Description
	OpenText DAST help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use OpenText DAST and Fortify OAST that are available as container images on the Docker platform. The OpenText DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an OpenText ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing Tools Guide dast-tgd-<*version*>.pdf	This document describes how to use the OpenText DAST diagnostic and penetration testing tools and configuration utilities packaged with OpenText DAST and Fortify WebInspect Enterprise.
OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide dast-agent-igd-<*version*>.pdf	This document describes how to install the OpenText DAST Agent and describes the detection capabilities of the OpenText DAST Agent Rulepack Kit. OpenText DAST Agent Rulepack Kit runs atop the OpenText DAST Agent, allowing it to monitor your code for software security vulnerabilities as it runs. OpenText

Document / file name	Description
	DAST Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Fortify WebInspect Enterprise

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

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

Chapter 2: Audit Inputs Editor

This tool enables you to create or edit inputs to the audit engines and to a distinct set of checks.

There are two ways to access the Audit Inputs Editor:

- From the Policy Manager (using the Policy Manager **Tools** menu). Use this method to create or modify an inputs file (<*filename*>`.inputs`). You can then specify this file when modifying scan settings.

  To modify an inputs file, click the **Open** icon on the Audit Input Editor's toolbar or select **File > Open**.
- From the Default or Current Settings, by clicking the **Audit Inputs Editor** button on the Attack Exclusions settings. Using this method, you can modify the Default settings file directly, but you cannot create a separate inputs file.

If you access the Audit Inputs Editor from Default Settings or Current Settings, the check inputs you create or modify become part of the settings file.

However, if you access the Audit Inputs Editor from the Policy Manager, you must import into OpenText DAST the saved file containing your check input modifications, as follows:

1. On the OpenText DAST menu bar, click **Edit > Default Settings**.
2. Under **Audit Settings**, select **Attack Exclusions**.
3. Click **Import Audit Inputs**.
4. Select the file you created (`*.inputs`) and click **Open**.

When accessed through the Current Settings window or the Default Settings window, Attack Exclusions panel, the Audit Inputs Editor does not contain a menu bar or toolbar.

Check inputs

Certain checks require inputs that accommodate the specific design of the target website. OpenText DAST conducts these checks using default values, which you may need to change.

To create or modify inputs for specific checks:

1. Click the **Check Inputs** tab.
2. Select a check from the list.

   The inputs for the selected check appear on the right.
3. Enter the requested input values.
4. Do one of the following:

- If you launched the Audit Inputs Editor from the Default Settings or Current Settings, click **OK**.
- If you launched the Audit Inputs Editor from the Policy Manager, click **File > Save** or **File > Save As**.

See also

"Engine inputs" below

Engine inputs

To create or modify inputs to audit engines:

1. Click the **Engine Inputs** tab.
2. Click the drop-down arrow.
   a. To apply your modifications to all audit engines, select **<Default>**. The Default parameters are extracted from the default OpenText DAST Audit Settings - Attack Exclusions.
   b. To modify inputs for a specific audit engine, select one from the list.
3. Select an engine input.
4. If you selected one of the following:
   - Excluded Query Parameters
   - Excluded Post Parameters
   - Excluded Cookies
   - Excluded Headers
   - Root Directories

   then do the following:
   - To add an item to the list, click **Add**.
   - To edit an item, select an item and click **Edit**.
   - To delete an item, select the item and click **Remove**.
   - If you selected a specific engine (rather than Defaults), select one of the following options:
     - **Merge with defaults** - The parameters you specified are added to the Defaults list, which apply to all engines.
     - **Replace defaults** - The engine will use the parameters you specified instead of those in the Defaults list.

Note: If you specify a Root Directory, then the engine will attack the object in the directory you specify, rather than the actual root. For example, if an engine normally attacks filename.txt in the default root directory *rootdir* (/rootdir/filename.txt), then if you specify a root directory of */foobar/*, the engine will attack /foobar/filename.txt.

5. If you selected one of the following:
   - Header Audit Rules
   - Cookie Audit Rules

   then do the following:
   a. Clear the **Use value from defaults** check box.
   b. Select an option from the drop-down list. Options are as follows:

      Header Audit Rules

      - **Attack All Every Time** - Attack the header in every request.
      - **Attack Once Per Directory** - Attack each named header in every directory only once the first time it is encountered.
      - **Attack Only Once** - Attack the header only once per host the first time it is encountered during the scan.

      Cookie Audit Rules

      - **Attack All** - Attack all cookies that are encountered in every request during the scan.
      - **Attack Only Cookies In Children Set In Parent** - Attack the inherited cookie in every child session in which it is encountered.

        For example, if the parent session request sets the following cookie with JSESSION ID:

        ```
        GET /auth/link.page; HTTP/1.1
        Referer: http://zero.webappsecurity.com/auth/security-check.html
        …
        Cookie:
        CustomCookie=WebInspect83644ZX632F0EE21C7249358BE159C67CEE9085YCE5
        1;
        JSESSIONID=2DC913EA;username=username;password=password
        ```

        And the child session includes the inherited cookie:

        ```
        GET /auth/link.page HTTP/1.1
        Referer: http://zero.webappsecurity.com/auth/link.page;
        …
        Cookie:
        CustomCookie=WebInspect83644ZX632F0EE21C7249358BE159C67CEE9085YCE5
        1;
        JSESSIONID=2DC913EA;username=username;password=password
        ```

        Then the cookie will be attacked in the child session.

        A child session might have multiple cookies, but only the one that was set in the parent session will be attacked.
      - **Attack Each Cookie Once** - Attack each unique cookie only once per host the first time it is encountered during the scan.

6. Click **OK** if you launched the Audit Inputs Editor from Default or Current Settings, or click **File > Save** or **File > Save As** if you launched the Audit Inputs Editor from the Policy Manager.

See also

"Check inputs" on page 30

Chapter 3: Compliance Manager (OpenText DAST only)

OpenText DAST employs an extensive arsenal of attack agents designed to detect security flaws in web-based applications. It probes your system with thousands of HTTP requests and evaluate each individual response. This session-based assessment reports each vulnerability, pinpoints its location in the application, and recommends corrective actions you should take. It is, basically, a quantitative analysis of your system.

OpenText DAST can also perform a qualitative analysis by grading how well your application complies with certain government-mandated regulations or corporate-defined guidelines. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers using web-based applications to provide "procedures for creating, changing, and safeguarding passwords." With OpenText DAST, you can assess your application and then generate a Compliance Report that measures how well your application satisfies this HIPAA rule.

How it works

You create a compliance template that associates requirements with one or more attack agents or vulnerabilities. For example, you might include the statement (or question) "The application will not use any 'hidden' fields." The attack agent that tests for compliance to this requirement is Hidden Form Value, ID #4727 (which is one of the agents in the "General text searching group" on page 40).

Compliance templates are completely flexible. You can enable or disable individual requirements. You can also modify requirements by adding or removing attack agents or "Threat classes" on page 40. For maximum flexibility, you can even create your own agents and associate them with a user-defined requirement.

OpenText DAST includes sample compliance templates that you can edit to fit your company's specific requirements.

For step-by-step instructions for creating a policy, see "Creating a compliance template" on the next page.

To test your website for compliance:

1. If necessary, create or modify a compliance template.
2. Scan your website.
3. On the OpenText DAST **Start** page, click **Generate a Report**.
   The Generate a Report window opens.
4. If the scan data is stored in a different database, click **Change DB** and then select a database.
5. Select a scan (designated by name, URL, or IP address).
6. Click **Next**.

7. Select **Compliance**.
8. If you want to produce individual reports on separate tabs (rather than combining all reports on one tab), select **Open Reports in Separate Tabs**.
9. Select either **Adobe PDF** or **HTML** as the report format.

   Adobe Reader 7 or later is required to read reports in portable data format (PDF).
10. Specify a compliance template. You can select a default template from the list, click the browse button to browse for templates you have created, or open the Compliance Manager and create a custom template.
11. Click **Finished**.
12. After OpenText DAST generates the report and displays it on a tab, you can save a report by clicking the Save Report icon on the toolbar.

See also

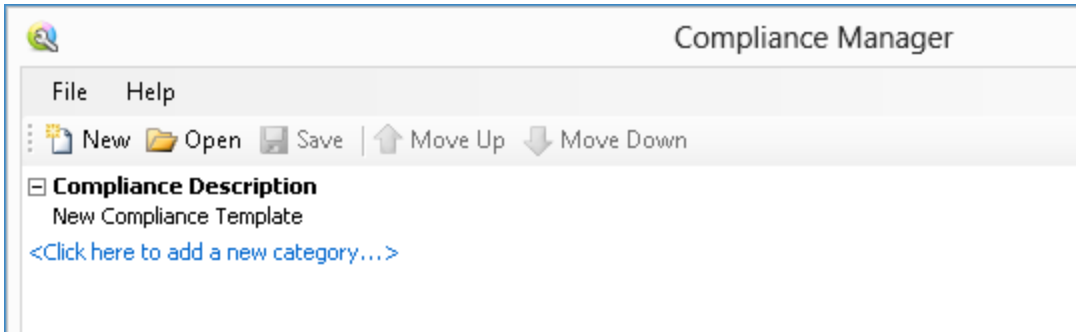
"Creating a compliance template" below

Creating a compliance template

To create a compliance template:

1. On the OpenText DAST menu bar, click **Tools > Compliance Manager**.

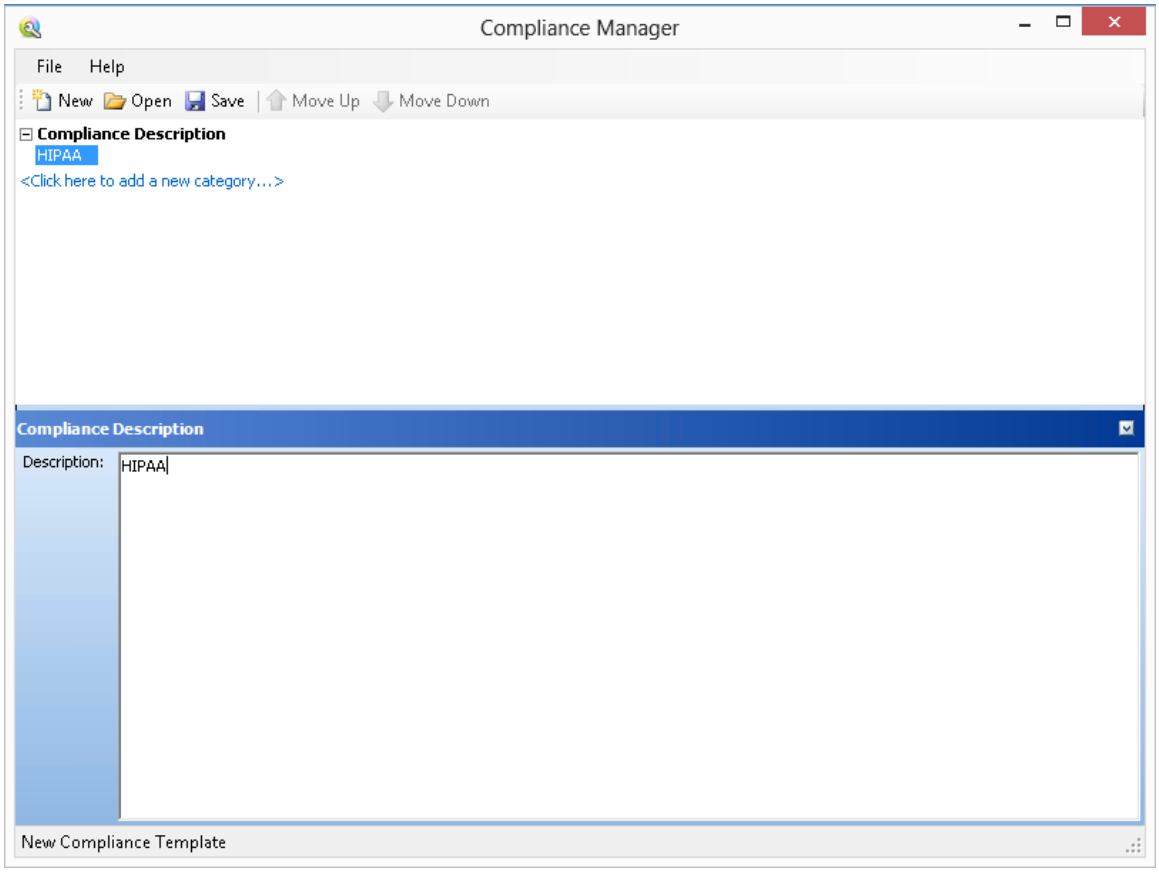
   The Compliance Manager window opens, displaying the outline of a new template.



2. Click the phrase "New Compliance Template."

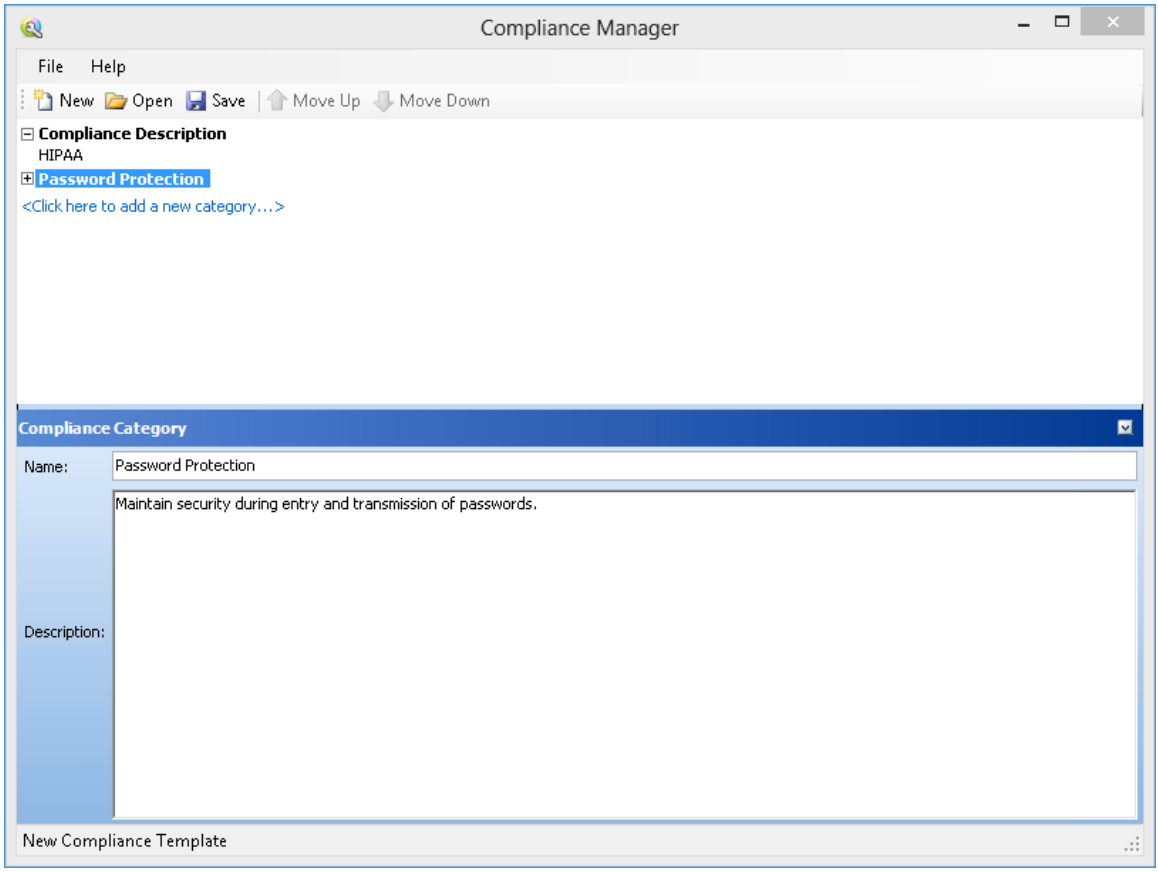
   The Compliance Manager creates an editing area in the lower half of the window.

3. In the editing area, replace the phrase "New Compliance Template" with a description of the template you are creating ("HIPAA" in this example).



4. Click the phrase "<Click here to add a new category...>."

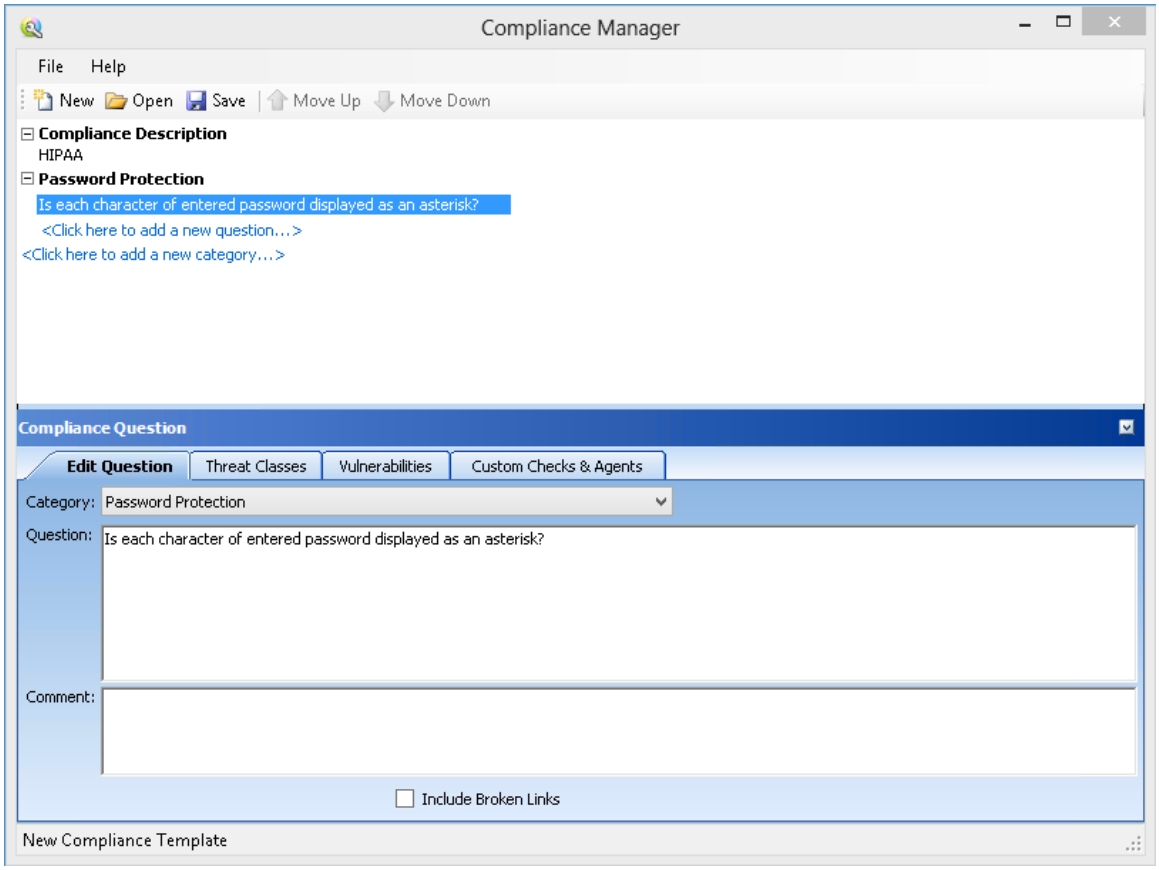
5. In the editing area, enter the name and description of the new category. In this example, the name is "Password Protection" and the description is "Maintain security during entry and transmission of passwords."



6. Click the plus sign ⊞ to expand the node labeled Password Protection.
7. Click the phrase "<Click here to add a new question...>."
8. Click the phrase "New Question."

   The editing area displays tabs allowing you to create a question related to the category "Password Protection."

9. In the **Question** area, type a question related to the category. This example asks the question, "Is each character of entered password displayed as an asterisk?"



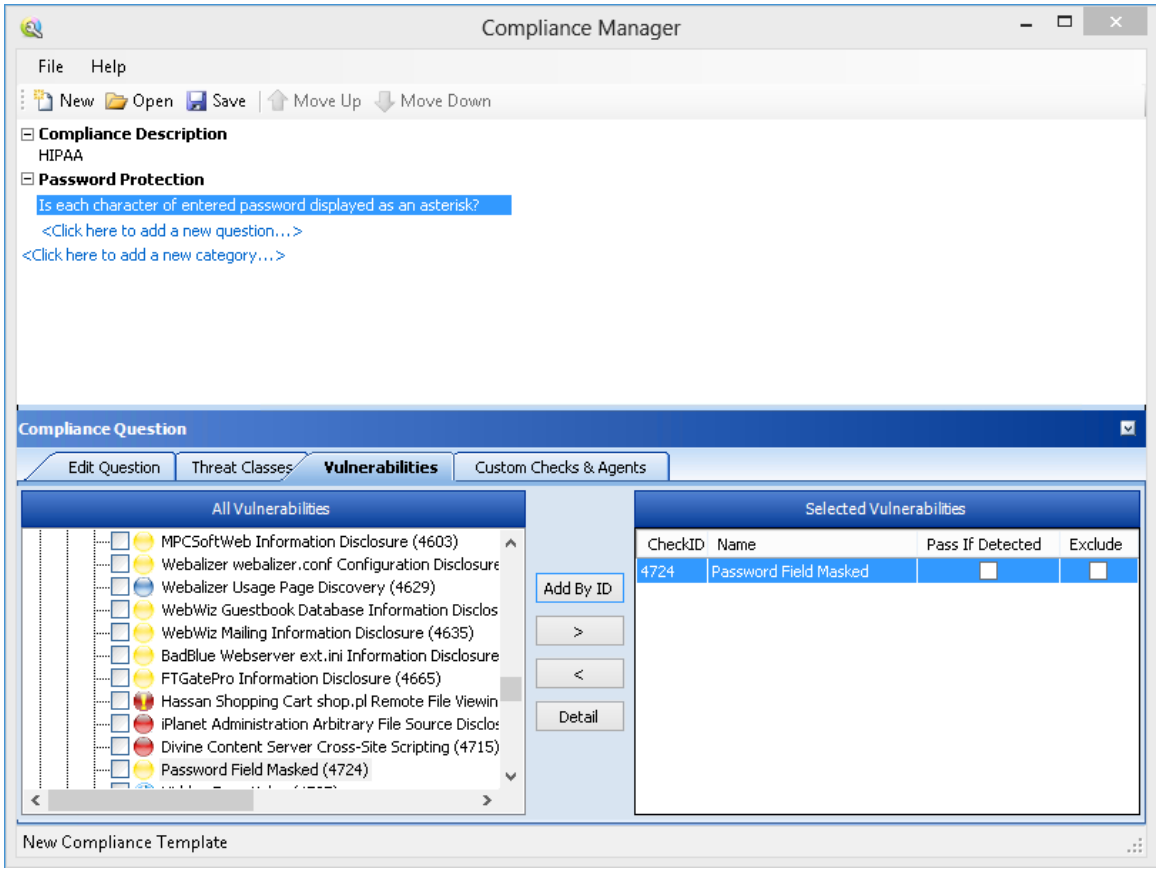
10. You can associate this question with threat classes, vulnerabilities defined by OpenText, or a custom check or agent that you previously created. For this example, click the **Vulnerabilities** tab and then click **Add By ID**.

> **Note:** You can also select a vulnerability or a threat class and click to include it in the **Selected Vulnerabilities** or **Selected Threat Classes** section for this question.

11. On the Add Check By ID window, enter 4724 and click **OK**. 4724 is the ID number of the "Password Field Masked" check.

> **Note:** You can add multiple IDs (one per line).

The check you specified appears in the **Selected Vulnerabilities** area.



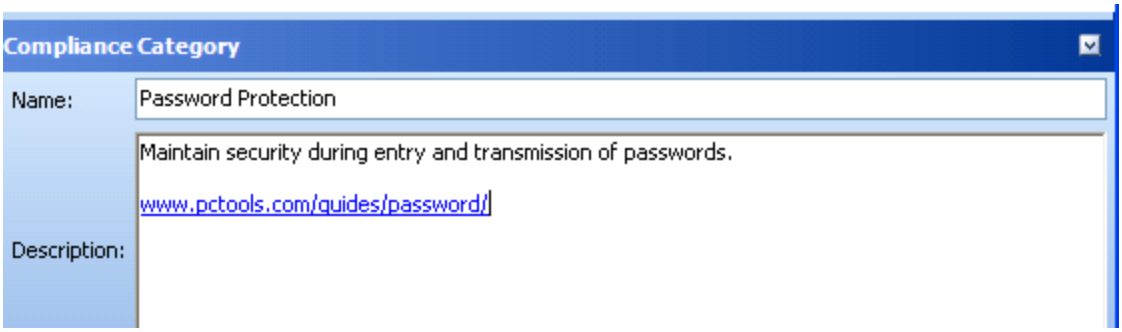
12. The **Selected Vulnerabilities** area contains two check boxes:
    - **Pass If Detected** - Select this option if the check is designed to confirm an attribute that contributes to application security. You might use this if, for example, you develop a custom check that checks for the existence of a file (such as Privacy Policy.html) that is part of your compliance program.
    - **Exclude** - Select this option if you add a group of checks, but want to exclude specific ones.

    In this example, do not select either check box.
13. To view a list of broken links in the compliance report, select the **Include Broken Links** check box.

    If you select the check box, then when you run a compliance report, any broken links found will be listed at the end of the report. If broken links are associated with a question in the template, then that question will be marked as failed.
14. Continue adding threat classes, vulnerabilities, or custom checks until you have included all that sufficiently test your application for the compliance question.
15. Create additional questions and categories using the above procedures until the compliance template is complete.
16. Click **Save**.

Usage notes

- To rearrange categories or items, select an item and click **Move Up** or **Move Down**.
- To insert categories or items, you can alternatively right-click a category/question and select **Insert** from the shortcut menu. The item will be inserted above the selected item.
- You can add an HTML link to any description or question, as depicted in the following illustration.



General text searching group

This group of agents, used mainly by the Directory Enumeration engine, follows all known and unknown paths located on your site. Individual checks are grouped alphabetically from A (which begins with the search for a directory named Accounting) to Z (which ends with the search for a directory named Zips). This group also includes checks for other types of commonly occurring directories, such as those associated with Microsoft FrontPage and Microsoft Internet Information Server log files (W3SVCnn).

For detailed information about all the possible agents, start the Policy Manager in Standard view, expand the General Text Searching node and click on any agent.

Threat classes

The Web Application Security Consortium has developed industry-standard terminology to clarify and organize threats to the security of a web site. These are listed on the **Threat Classes** tab.

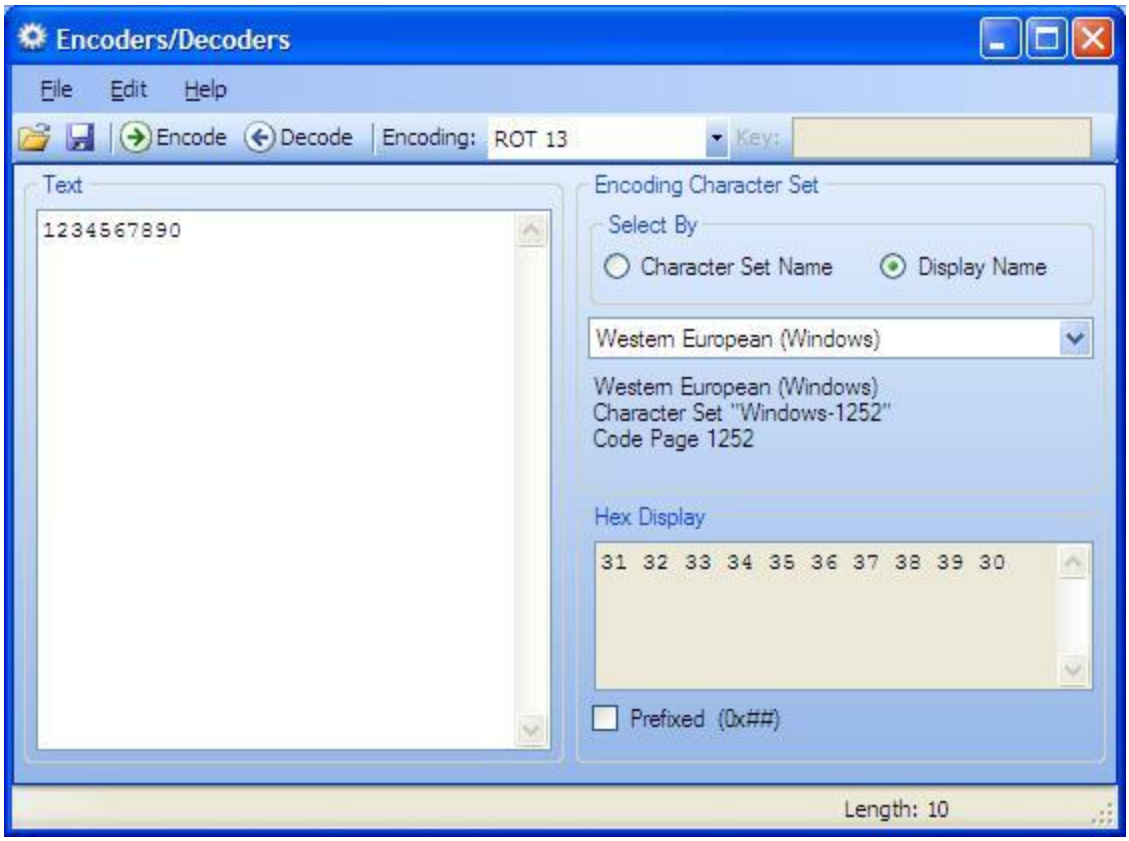
To determine if a scan revealed a susceptibility to these threats:

1. Select a threat class (or one of its components).
2. Click ▸ to include it in the **Selected Threat Classes** for this question.

Chapter 4: Encoders/Decoders

This tool enables you to encode and decode values using Base 64, hexadecimal, MD5, and other schemes. You can also encode a string into a Unicode string and use special characters in URL construction.

During the analysis of your scan results, when you encounter a string that you suspect is in an encoded or encrypted format, you can simply copy the string, paste it into the Encoders/Decoders tool, and then click **Decode**.



Encoding a string

To encode a string:

1. Type (or paste) a string in the **Text** area, or load the contents of a file by selecting **File > Open** from the menu.
2. Select an encoding character set using either the **Character Set Name** or the **Display Name**.
3. Select a cipher type from the **Encoding** list. For more information, see "Encoding types" on page 43.

4. If necessary, type a key in the **Key** field. When a valid key is entered, the **Encode** and **Decode** buttons become enabled.
5. Click **Encode**.

   The **Text** area displays the encoded string. The **Hex Display** area displays the hexadecimal value of each character in the encoded string (formatted in the character set that you select).

   If you select **Prefixed**, "0x" is added to the beginning of the hexadecimal numbers. C and languages with a similar syntax (such as C++, C#, Java and JavaScript) prefix hexadecimal numerals with “0x” (for example, 0x5A3). The leading zero allows the parser to recognize a number, and the “x” stands for hexadecimal.

Decoding a string

To decode a string:

1. Type (or paste) a string in the **Text** area, or load the contents of a file by selecting **File > Open** from the menu.
2. Select a cipher type from the **Encoding** list.
3. If necessary, type a key in the **Key** field.
4. Click **Decode**.

You can also use OpenText DAST's encoding and decoding capabilities in the HTTP Editor. Right-click while editing a session to access encoding and decoding options.

Manipulating encoded strings

The encoded form of a string may contain characters that are non-printable. This often occurs when using a hash-based encoding scheme or any encoding scheme that requires a key. Since non-printable characters cannot be copied to the Windows clipboard, you cannot simply copy from or paste into the Encoder/Decoder. However, there are two methods you can use to work around this limitation:

- Save the encoded string to a file and, when you want to decode it, select **File > Open** from the menu to load it into the Encoder tool. Then decode it using the original method and (if applicable) key.
- Also, after encoding the string using the chosen encoding method and key, you can encode the resulting string using the base 64 method; then copy the string to the clipboard, paste the clipboard contents, decode using base 64, and decode again using the original method and (if applicable) key.

Encoding types

The Encoder/Decoder enables you to select the encoding types described in the following table.

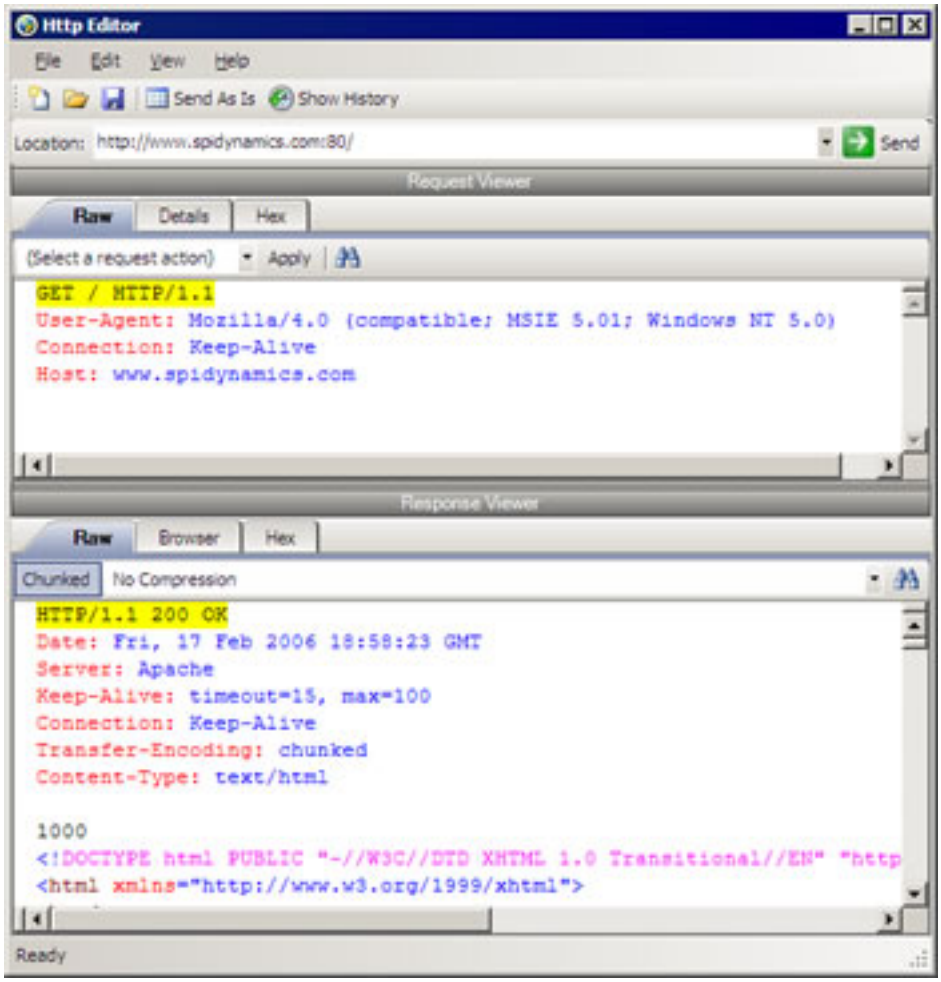
Encoding Type	Definition
3DES	Triple DES; a mode of the DES encryption algorithm that encrypts data three times (the string is encrypted, then the encryption is encrypted, and the resulting cipher text is encrypted a third time). The key must be 128 or 192 bits (16 or 24 characters).
Base64	Encodes and decodes triplets of 8-bit octets as groups of four characters, each representing 6 bits of the source 24 bits. Only characters present in all variants of ASCII and EBCDIC are used, avoiding incompatibilities in other forms of encoding.
Blowfish	An encryption algorithm that can be used as a replacement for the DES algorithm.
DES	Data Encryption Standard. A widely used method of data encryption that can use more than 72 quadrillion different private (and secret) encryption keys. Both the sender and the user must use the same private key.
Hex	Hexadecimal.
MD5	Produces a 128-bit "fingerprint" or "message digest" of whatever data you enter.
RC2	A variable key-size block cipher designed by Ronald Rivest. It has a block size of 64 bits and is about two to three times faster than DES in software.
RC4	A stream cipher designed by Ronald Rivest. It is a variable key-size stream cipher with byte-oriented operations. Used for file encryption in products such as RSA SecurPC and also used for secure communications, as in the encryption of traffic to and from secure web sites using the SSL protocol.
ROT13	A simple Caesar cipher used for obscuring text by replacing each letter with the letter thirteen places down the alphabet.
SHA1	Secure Hash Algorithm. A one-way hash function developed by NIST and defined in standard FIPS 180. SHA-1 is a revision published in 1994; it is also described in ANSI standard X9.30 (part 2).
SHA256	Secure Hash Algorithm that uses 256-bit encryption.

Encoding Type	Definition
SHA384	Secure Hash Algorithm that uses 384-bit encryption.
SHA512	Secure Hash Algorithm that uses 512-bit encryption.
ToLower	Changes uppercase letters to lowercase.
ToUpper	Changes lowercase letters to uppercase.
TwoFish	An encryption algorithm based on an earlier Blowfish.
Unicode	Provides a unique number for every character, regardless of the platform, program, or language.
URL	Creates values that can be used for URL-encoding non-standard letters and characters for display in browsers and plug-ins that support them.
XHTML	Encapsulates the entered data with text tags: <text>data</text>
XOR	XOR performs an Exclusive OR operation. You must provide a key. If the length of the key string is only one character, that character is ORed against each character in the encode/decode string.

Chapter 5: HTTP Editor

Use the HTTP Editor to create or edit requests, send them to a server, and view the response either in raw HTML or as rendered in a browser. The HTTP Editor is a manual hacking tool, and requires a working knowledge of HTML, HTTP, and request methods.

To set proxy and authorization parameters, if necessary, select **Edit > Settings**.



Request Viewer

The Request Viewer contains the HTTP request message, which you can view in four different formats using the following tabs:

- **Raw** - Depicts the line-by-line textual format of the request message.
- **Details** - Displays the header names and field values in a table format.

- **Hex** - Displays the hexadecimal and ASCII representation of the message.
- **XML** - Displays any XML content in the message body. (This tab appears only if the request contains XML-formatted data.)

Response Viewer

The Response Viewer contains the HTTP response message, which you can also view in four different formats using the following tabs:

- **Raw** - Depicts the line-by-line textual format of the response message.
- **Browser** - Displays the response message as rendered in a browser.
- **Hex** - Displays the hexadecimal and ASCII representation of the response message.
- **XML** - Displays any XML content in the message body. (This tab appears only if the response contains XML-formatted data.)

HTTP Editor menus

File menu

The **File** menu contains the following options:

- **New Request** - Deletes all information from previous sessions and resets the Location URL.
- **Open Request** - Enables you to load a file containing an HTTP request saved during a previous session.
- **Save Request** - Enables you to save an HTTP request.
- **Save Request As** - Enables you to save an HTTP request.
- **URL Synchronization** - When selected, any characters you type into the **Address** combo box are added to the Request-URI of the HTTP request line.
- **Send As Is** - If you select this option, the HTTP Editor will not modify the request, regardless of any other settings you may select. This option enables you to send a purposely malformed message. Authentication and proxy settings are disabled when using this option.

  Note: You may manually edit the request to go through a proxy, but many standard HTTP proxy servers cannot process non-compliant HTTP requests.

- **Exit** - Closes the HTTP Editor.

Edit menu

The **Edit** menu contains the following options:

- **Cut** - Deletes selected text and saves it to the clipboard.
- **Copy** - Saves the selected text to the clipboard.
- **Paste** - Inserts text from the clipboard

- **Find** - Displays a dialog box that enables you to search for text that you specify.
- **Settings** - Enables you to configure request, authentication, and proxy parameters for the HTTP Editor.

View menu

The **View** menu contains the following options:

- **Show History** - Displays a pane listing all HTTP requests sent.
- **Word Wrap** - Causes all text to fit within the defined margins.

Help menu

The **Help** menu contains the following commands:

HTTP Editor Help - Opens the Help file with the **Contents** tab active.

Index - Opens the Help file with the **Index** tab active.

Search - Opens the Help file with the **Search** tab active.

About HTTP Editor - Displays information about the HTTP Editor.

Request actions

The following options are available from the **Request Action** list in the Request Viewer pane.

PUT file upload

The PUT method requests that the enclosed entity be stored under the supplied Request-URI.

To write a file to a server:

1. Select **PUT File Upload** from the drop-down list on the Request Viewer pane.
2. In the text box that appears to the right of the list, type the full path to a file
   - or -
   Click the Open Folder icon and select the file you want to upload.
3. Click **Apply**. This will also recalculate the content length.

Change content-length

In normal mode, if you edit the message body of the request, the HTTP Editor recalculates the content length and substitutes the appropriate value in the Content-length header. However, when using the **Send As Is** option, the HTTP Editor does not modify the content length. You can force this recalculation before sending the request by selecting **Change Content-Length** and clicking **Apply**.

URL encode/decode param values

The specification for URLs (RFC 1738, Dec . '94) limits the use of characters in URLs to a subset of the US-ASCII character set. HTML, on the other hand, allows the entire range of the ISO-8859-1 (ISO-Latin) character set to be used in documents, and HTML4 expands the allowable range to include the complete Unicode character set as well. To circumvent this limitation, you can encode non-standard letters and characters for display in browsers and plug-ins that support them.

URL encoding of a character consists of a "%" symbol, followed by the two-digit hexadecimal representation of the ISO-Latin code point for the character. For example:

- The asterisk symbol (*) = 42 decimal in the ISO-Latin set
- 42 decimal = 2A hexadecimal
- URL code for asterisk = %2A

You can use URL encoding to bypass an intruder detection system (IDS) that inspects request messages for certain keywords using only the ISO-Latin character set. For example, the IDS may search for "login" (in ISO-Latin), but not "%4C%4F%47%49%4E" (the URL-encoded equivalent).

To substitute URL code for parameters throughout the entire message, select **URL Encode Param Values** and click **Apply**.

To translate URL-encoded parameters to ISO-Latin, select **URL Decode Param Values** and click **Apply**.

Unicode encode/decode request

The Unicode Worldwide Character Standard includes letters, digits, diacritics, punctuation marks, and technical symbols for all the world's principal written languages, using a uniform encoding scheme. Incorporating Unicode into client-server applications and websites offers significant cost savings over the use of legacy character sets. Unicode enables a single software product or a single website to be targeted across multiple platforms, languages and countries without re-engineering. It allows data to be transported through many different systems without corruption.

To translate the entire request message into Unicode, select **Unicode Encode Request** and click **Apply**.

To translate the entire request message from Unicode into ISO-Latin, select **Unicode Decode Request** and click **Apply**.

Create MultiPart post

The POST method is used to request that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line. You can attempt to upload data by manipulating a POST request message.

To insert data from a file:

1. Select **Create MultiPart Post** from the **Action** drop-down list on the Request Viewer pane.
2. In the text box to the right of the **Action** list, type the full path to a file

   - or -

Click the Open Folder icon and select the file you want to insert.

3. Click **Apply**.

Remove MultiPart post

To remove a file that is part of a multipart request, select **Remove MultiPart Post** from the **Action** list on the Request Viewer pane.

Response actions

The area immediately below the tabs on the **Response Viewer** pane contains three controls:

- a **Chunked** button
- a **Content Coding** drop-down list
- a  button that launches the Find In Response dialog box, allowing you to search the response for the text string you specify

Chunked

If a server starts sending a response before knowing its total length, it might break the complete response into smaller chunks and send them in series. Such a response contains the "Transfer-Encoding: chunked" header. A chunked message body contains a series of chunks, followed by a line with "0" (zero), followed by optional footers and a blank line. Each chunk consists of two parts:

- A line with the size of the chunk data, in hex, possibly followed by a semicolon and extra parameters you can ignore (none are currently standard), and ending with CRLF.
- The data itself, followed by CRLF.

Content codings

If the HTTP response contains compressed data, you can decompress the data using one of the options from the list:

- GZIP - A compression utility written for the GNU project.
- Deflate - The "zlib" format defined in RFC 1950 [31] in combination with the "deflate" compression mechanism described in RFC 1951 [29].

See also

"Editing and sending a request" on the next page

"Searching the request or response" on page 51

Editing and sending a request

To edit and send a request:

1. Modify the request message in the Request Viewer pane.

   To encode or decode a text string, select the text, then right-click the selection and select either **Encoding** or **Decoding** from the pop-up menu.

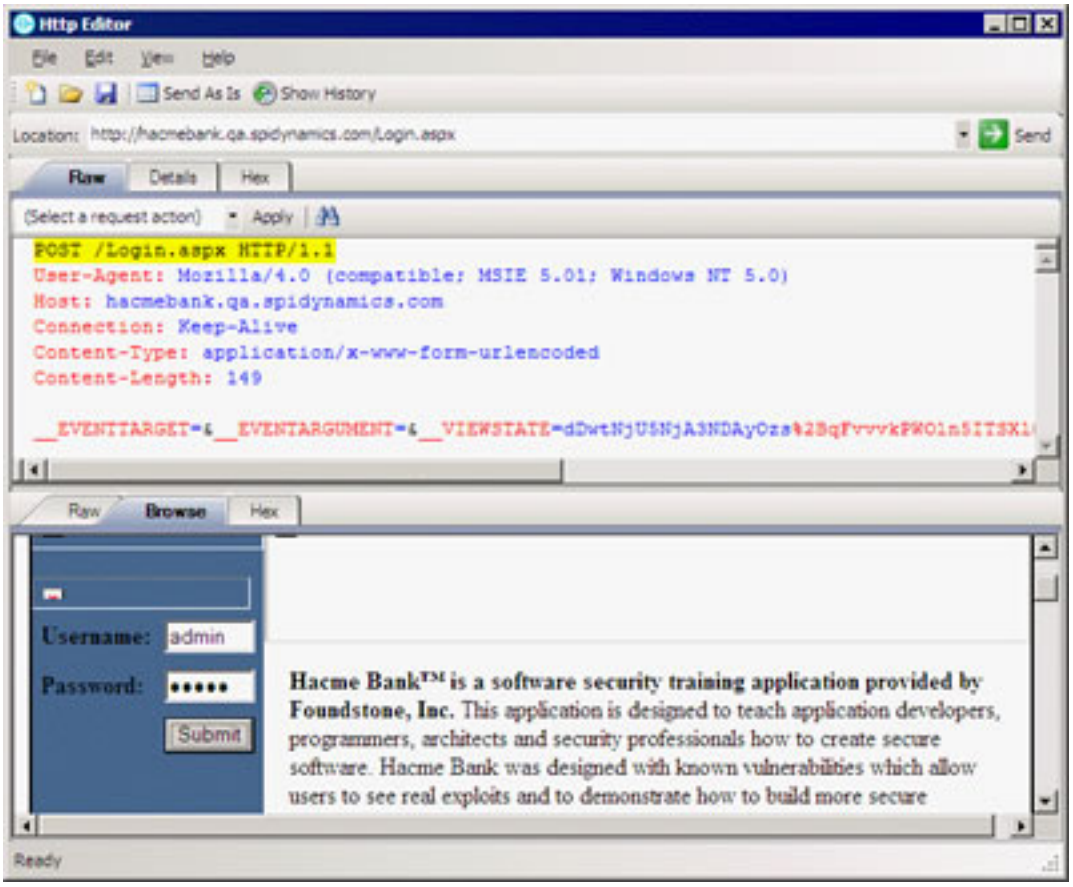
   To change certain features of the request, select an item from the **Action** list and click **Apply**.

   See "HTTP Editor" on page 45 for more information.
2. Click **Send** to send the HTTP request message.

   The Response Viewer pane displays the HTTP response message when it is received.
3. To view the response as rendered in a browser, click the **Browser** tab.
4. You can prepare your next HTTP request using the HTML or JavaScript controls rendered on the **Browser** tab. To use this feature, you must select the Interactive Navigation option (click **Edit > Settings**).
   a. In the **Location** field, enter a URL and click **Send**.

      The application returns a logon form.
   b. In the **Response** pane, click the **Browser** tab.
   c. On the rendered page, enter a user name and password, and then click **Submit**.

The HTTP Editor formats the request (which uses the POST method to the Login.aspx URL) and displays it in the Request Viewer pane, as illustrated below.



d. Click **Send** to send the formatted response (including the user name and password) to the server.

5. To save a request, select **File > Save Requests**.

See also

"Searching the request or response" below

Searching the request or response

To search for text in the request or response:

1. Click  in either the Request Viewer or Response Viewer pane.
2. Using either the Find in Request or Find in Response window, type or select a string or regular expression.
3. If using a regular expression as the search string, select the **Regex** check box.
4. Click **Find**.

Settings

To modify the HTTP Editor settings, click **Edit > Settings**, select one of the following tabs, make your changes, and click **OK**:

- Options
- Authentication
- Proxy

The settings on each tab are described in the following sections.

Options tab

The **Request Group** includes the following options:

- **Send As Is** - If you select this option, the HTTP Editor will not modify the request, regardless of any other settings you may select. This option enables you to send a purposely malformed message. **Authentication** and **Proxy** settings are disabled when using this option.

  Note: You can manually edit the request to go through a proxy, but most standard HTTP proxy servers cannot process non-compliant HTTP requests.

- **Manipulate Request** - If you select this option, the HTTP Editor will modify requests to accommodate the following parameters:
  - **Apply State** - If your application uses cookies, URL rewriting, or post data techniques to maintain state within a session, the HTTP Editor will attempt to identify the method and modify the response accordingly.
  - **Apply Proxy** - If you select this option, the HTTP Editor will modify the request according to the proxy settings you specify.
  - **Apply Filter** - This option appears only when you invoke the HTTP Editor while using OpenText DAST and a scan tab has focus (that is, after opening or while conducting a scan). If this option is selected, the HTTP Editor applies the Filters settings from OpenText DAST's Current Scan Settings to add search-and-replace rules for HTTP requests and responses.

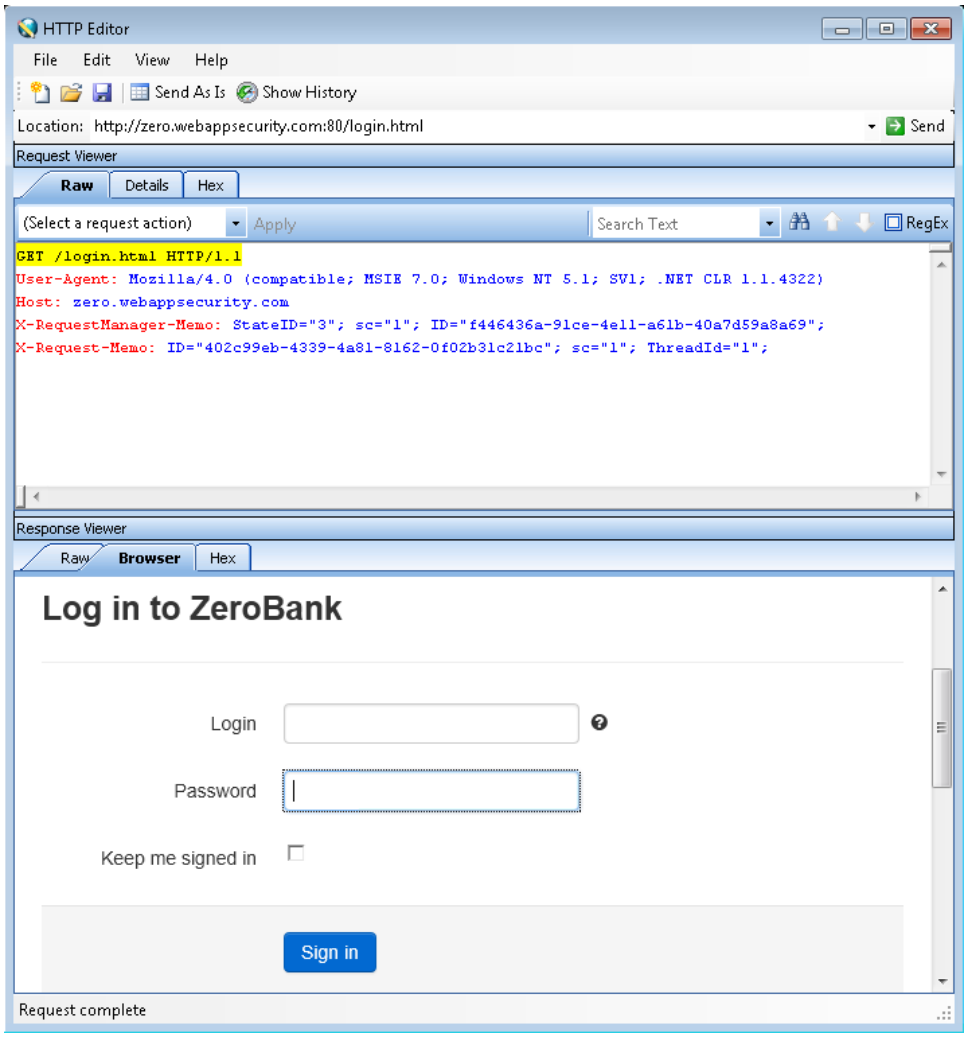
    Note: Changing the Current Scan Settings before invoking the HTTP Editor has no effect. The HTTP Editor uses the settings that were in effect when the scan began.

  - **Apply Header** - This option appears only when you invoke the HTTP Editor while using OpenText DAST and a scan tab has focus (that is, after opening or while conducting a scan). If this option is selected, the HTTP Editor applies the Cookies/Headers settings for OpenText DAST's Current Scan Settings for HTTP requests.

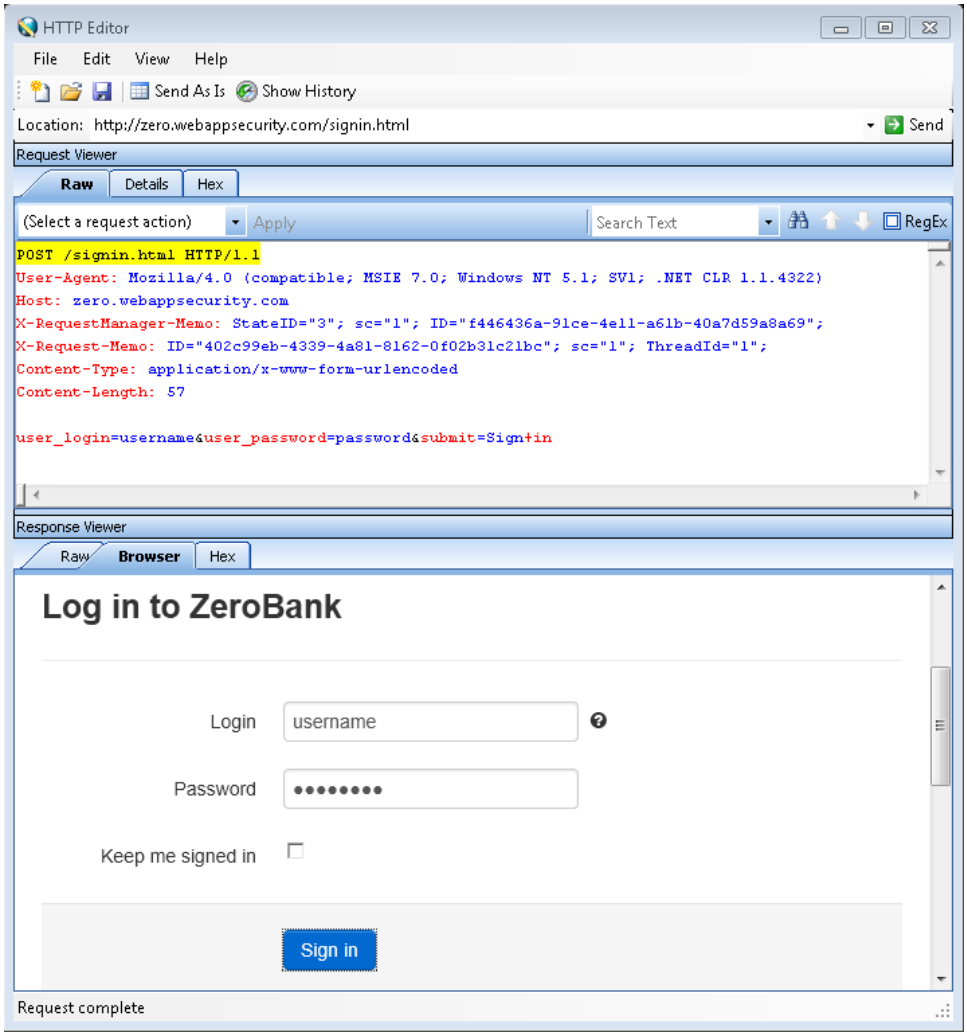
    Note: Changing the Current Scan Settings before invoking the HTTP Editor has no effect. The HTTP Editor uses the settings that were in effect when the scan began.

In the **Navigation group**, select **None, Interactive,** or **Browser Mode**.

You can view the server's response as rendered in a browser by selecting the **Browser** tab in the Response Viewer (the lower pane). If the **Interactive** feature is enabled, you can prepare your next HTTP request using the HTML or JavaScript controls rendered in the browser.



For example, using the logon page at http://zero.webappsecurity.com:80/login.html (shown above), you could enter a **Login** name ("username") and **Password** ("password"), and then click **Sign in**. The HTTP Editor formats the request (which uses the POST method to the signin.html resource) and displays it in the Request Viewer, as illustrated below. You could then edit the logon message (if required) or simply send it to the server by clicking **Send**.



If you select the **Browser Mode** option, then **Interactive** mode is enabled, but the HTTP Editor will send the request immediately, without first placing it in the Request Viewer and allowing you to edit it.

Select the **Enable Active Content** check box to allow execution of JavaScript and other dynamic content in all browser windows.

Most web pages contain information that tells the browser which 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 the HTTP Editor should use. In the **Advanced HTTP Parsing** group, select the **Assumed 'charset' Encoding**.

Authentication tab

If authentication is required, select a type from the **Authentication** list. After selecting an authentication method, enter a user name and password. The authentication methods are:

- **Automatic**
- **HTTP Basic**
- **NTLM**

After selecting an authentication method, enter a **User name** and **Password**. To prevent typographical errors, you must re-enter the password in the **Confirm Password** field.

Proxy tab

Use these settings to access the HTTP Editor through a proxy server.

- **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 Protocol (WPAD) to locate and use a proxy autoconfig file to configure the browser's web proxy settings.
- **Use System proxy settings** - Select this option to import your proxy server information from the local machine.
- **Use Firefox proxy settings** - Select this option to import your proxy server information from Firefox.

  Note: Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.

- **Explicitly configure proxy** - Select this option to access the Internet through a proxy server, and then enter the requested information:
  a. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080).
  b. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
  c. If authentication is required, select a type from the **Authentication** list:
     - **Automatic**

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

     - **Basic**
     - **Digest**
     - **Kerberos**

- **Negotiate**
- **NTLM**

d. If your proxy server requires authentication, enter the qualifying **User name** and **Password**.

e. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** field. Use commas to separate entries.

- **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.

Regular expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the Regular Expression Library.

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /\n/ matches a line feed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/[^(en|ca)].*/.* . Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never

Character	Description
	early."
\B	Matches a non-word boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a non-digit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a line feed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v].
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v].
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any non-word character. Equivalent to [^A-Za-z0-9_].

See also

"Regular expression extensions and operators" below

Regular expression extensions and operators

OpenText engineers have developed and implemented extensions to the normal regular expression syntax, along with a set of operators.

Regular expression tags

When building a regular expression, you can use the extensions to specify in which element of the request or response to search for a match. The following table describes the extensions.

Extension	Element
[ALL]	All elements of the request or response
[BODY]	Request Body

Extension	Element
	Response Body
[COOKIES]	Cookie in the Request
[HEADERS]	Request Headers Response Headers
[METHOD]	Request Method
[POSTDATA]	Post Data
[REQUESTLINE]	Request Line (the start line of an HTTP request)
[SETCOOKIES]	Set-Cookie Response Header
[STATUSCODE]	Status Code
[STATUSDESCRIPTION]	Status Description (a string that describes the status of the HTTP output returned to the client)
[STATUSLINE]	Status Line (the start line of an HTTP response)
[URI]	The request target (a URI)
[VERSION]	HTTP Version

Regular expression operators

OpenText engineers have developed regular expression operators that you can use to construct complex regular expression patterns. The operators are:

- AND
- OR
- NOT
- [ ]
- ( )

Examples

The following paragraphs provide examples of how the use the extensions and operators:

- To detect a response in which (a) the status line contains a status code of "200" and (b) the phrase "logged out" appears anywhere in the message body, use the following regular expression:

[STATUSCODE]200 AND [BODY]logged\sout

- To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and having a reference to the path "/Login.asp" anywhere in the response, use the following:

  [STATUSCODE]302 AND [ALL]Login.asp

- To detect a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response, use the following regular expression:

  ([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302 AND [ALL]Login.asp)

  Note: You must include a space before and after an "open" or "close" parenthesis. Otherwise, the parenthesis will be erroneously considered as part of the regular expression.

- To detect a redirection response where "login.aspx" appears anywhere in the redirection Location header, use the following regular expression:

  [STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx

- To detect a response containing a specific string (such as "Please Authenticate") in the Reason-Phrase portion of the status line, use the following regular expression:

  [STATUSDESCRIPTION]Please\sAuthenticate

See also

"Regular expressions" on page 56

Chapter 6: Log Viewer (OpenText DAST only)

Use the Log Viewer to inspect the various logs maintained by OpenText DAST. This feature is used mainly by the Customer Support group to investigate reported incidents.

To view log files:

1. Click the **Tools > Log Viewer**.

   If you open the Log Viewer when a tab containing a scan has focus, the program assumes you want to view logs for that scan. Go to Step 4.
2. Click **Open Scan**.
3. On the Open Scan window, select the scan whose logs you want to view and click **Open**. To open scans in a different database, click **Change Database**.
4. Select a log from the **Log Type** list. The available types depend on the logging level that was selected for the scan (in OpenText DAST's Application settings).
5. To locate text within the log, click **Find** on the toolbar

   - or -

   Select **Edit > Find**.
6. To save a log file, click **Export** on the toolbar

   - or -

   Select **File > Export Logs**.
7. To view logs that are not related to a specific scan, click **DAST Logs** (on the toolbar).

Chapter 7: Policy Manager

A policy is a collection of audit engines and attack agents that OpenText DAST 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. These components are organized into the following groups:

- Audit Engines
- Audit Options
- General Application Testing
- General Text Searching
- Third-Party Web Applications
- Web Frameworks/Languages
- Web Servers
- Web Site Discovery
- Custom Agents
- Custom Checks

All these components (except for the Audit Engines) are known collectively as attack groups. Each attack group contains subgroups of individual modules (called attack agents) that check your website for vulnerabilities.

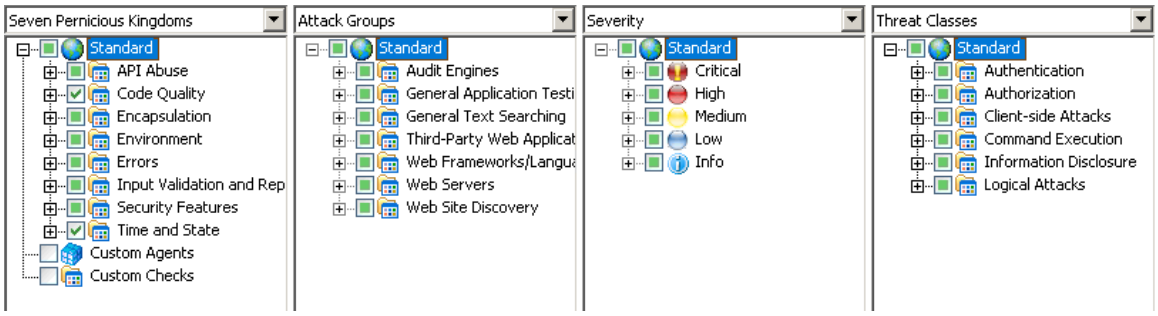
OpenText DAST contains several prepackaged policies designed to accommodate the requirements of most users. All policies contain all possible audit engines and agents, but each policy has a different subset of these components enabled. You edit a policy by enabling or disabling audit engines and/or individual attack agents (or groups of agents). You create a policy by editing an existing policy and saving it with a new name.

Views

The Policy Manager has two different views—**Standard** and **Search**—which are selectable from the **View** menu by clicking icons in the toolbar.

Standard view

This view displays, by default, a list of checks categorized by Seven Pernicious Kingdoms. Alternatively, a drop-down list enables you to display checks by Attack Groups, Severity, and Threat Class (according to classifications established by the Web Application Security Consortium).

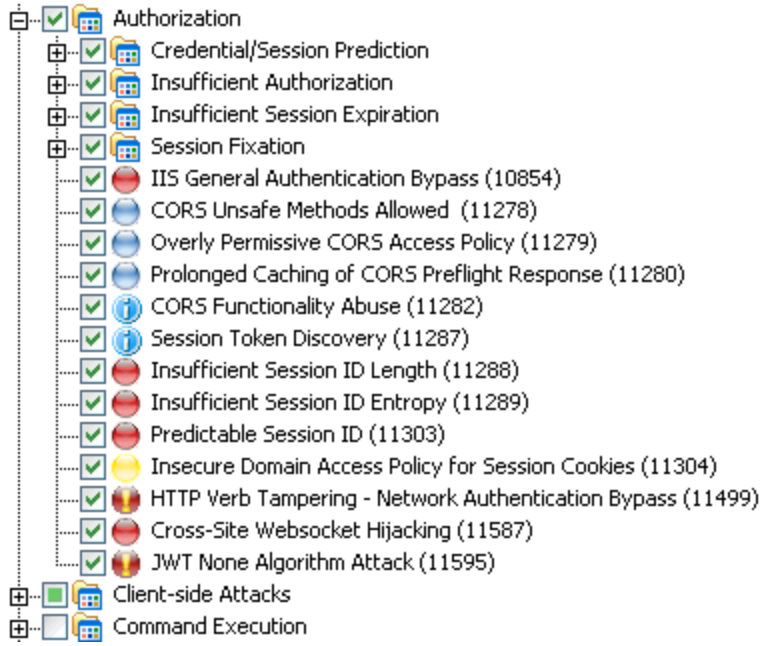


You enable or disable a component by selecting or clearing its associated check box.

The check box next to an unexpanded node indicates the "selected" status of the objects within the node.

- A **check** means all objects are selected.
- A **green square** means some objects are selected.
- An **empty box** means no objects are selected.

Click the plus sign ⊞ to expand a node.

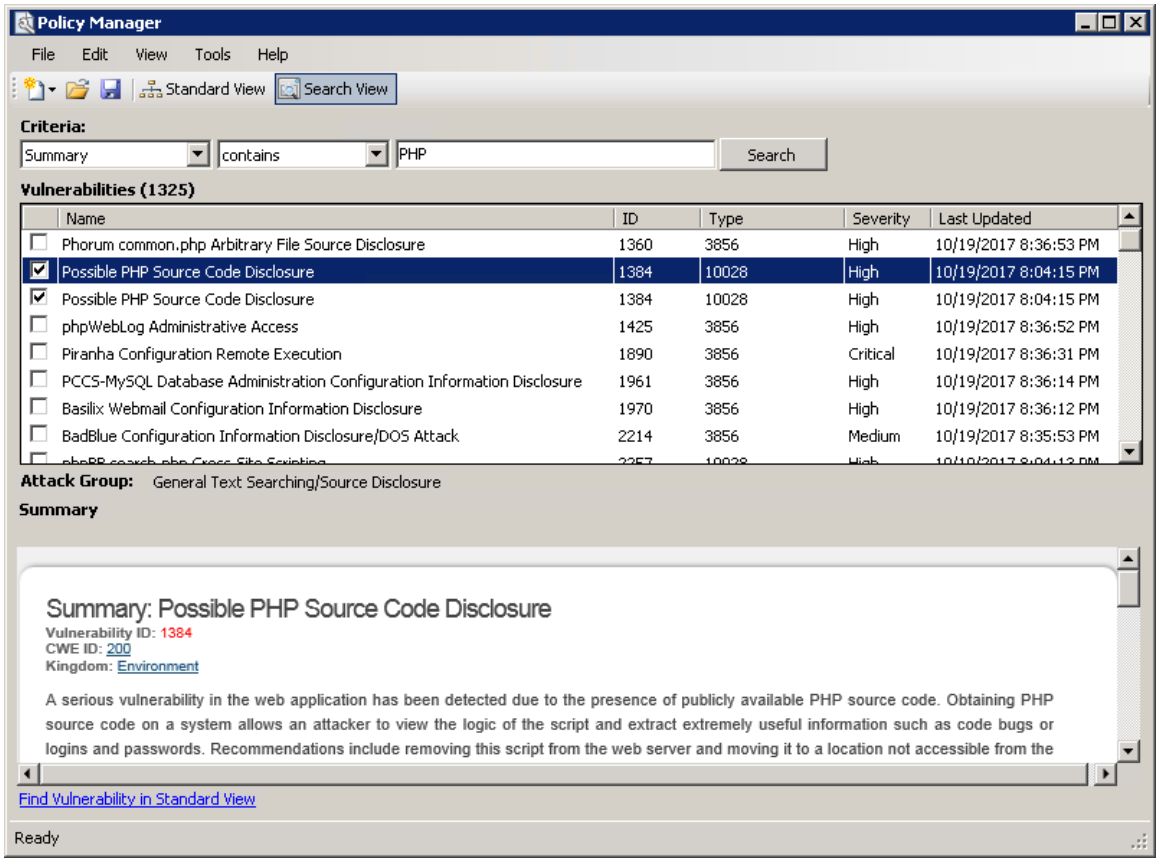


Search view

This view enables you to locate attack agents based on the attribute you select from the Criteria list:

- Vulnerability ID
- Vulnerability Name
- Engine Type
- Last Updated
- CWE ID
- Kingdom
- Summary
- Implication
- Execution
- Fix
- Reference Info

This feature is used most often to identify checks that you want to disable. For example, if you are scanning an application that does not contain PHP scripting, you could search summary fields for "PHP." When the Policy Manager lists the attack agents that match your search criteria, you could disable an agent by clearing its associated check box. Then, you can either save the modified policy (making the policy changes permanent) or simply apply the modified policy to the current scan.



See also

"Policies" on page 84

"Creating or editing a policy" below

"Searching for specific agents" on page 74

"Working with custom checks" on the next page

Creating or editing a policy

OpenText DAST contains a number of prepackaged policies designed to accommodate the majority of users. You cannot permanently change these policies. However, you can open any of them as a template, modify their contents to create a custom policy, and save the customized policy under a new name. You can edit and save a custom policy without changing its name.

To edit or create a policy:

1. On the toolbar, click **Policy Manager**

   - or -

   select **Tools > Policy Manager**.

   The Policy Manager opens. By default, it loads the Standard policy.
2. Do one of the following:
   - To edit a policy that you previously created (that is, a custom policy), select **File > Open** and select the policy.
   - To create a policy based on one of the prepackaged policies, select **File > New** (or click the New Policy icon) and select the policy on which the new one will be modeled.
3. Disable (or enable) an attack group by clearing (or selecting) its associated check box. To disable or enable an individual agent within a group, first expand the group and then edit its check box.
4. To rename an attack group:
   a. Right-click the attack group.
   b. Choose **Rename** from the shortcut menu.
5. To add an attack group:
   a. Right-click any existing attack group.
   b. Choose **New Attack Group** from the shortcut menu.

      A highlighted entry named New Attack Group will appear.
   c. Right-click the new group and choose **Rename**.
   d. Populate the group by dragging and dropping attack agents onto it.
6. You can also create a custom check. For more information, see "Working with custom checks" on the next page.
7. If you select the **Auto Update** check box, OpenText DAST determines if any updated or new attack agents downloaded from the OpenText database should be enabled or disabled, based on

the analysis of its sibling agents. For example, if you disable attack agents targeting Microsoft's Internet Information Server (IIS), and you select **Auto Update**, then OpenText DAST will not enable any IIS-related attack agent that it downloads to your system. Conversely, any new or updated attack agents that are related to agents that are enabled in your policy will also be enabled.

Note: New vulnerability checks downloaded via Smart Update are not added automatically to any custom policies you may have created.

8. Select **File > Save As**. Type a name for your custom policy in the **File name** field and then click **Save** to save the new policy in OpenText DAST's *.policy format. You cannot save a policy using the name of a default policy (Assault, Blank, Standard, etc.).

See also

"Using a custom agent" on page 75

"Searching for specific agents" on page 74

"Working with custom checks" below

Working with custom checks

Although OpenText DAST rigorously inspects your entire website for real and potential security vulnerabilities, you may require a custom check to detect vulnerabilities that are unique to your application.

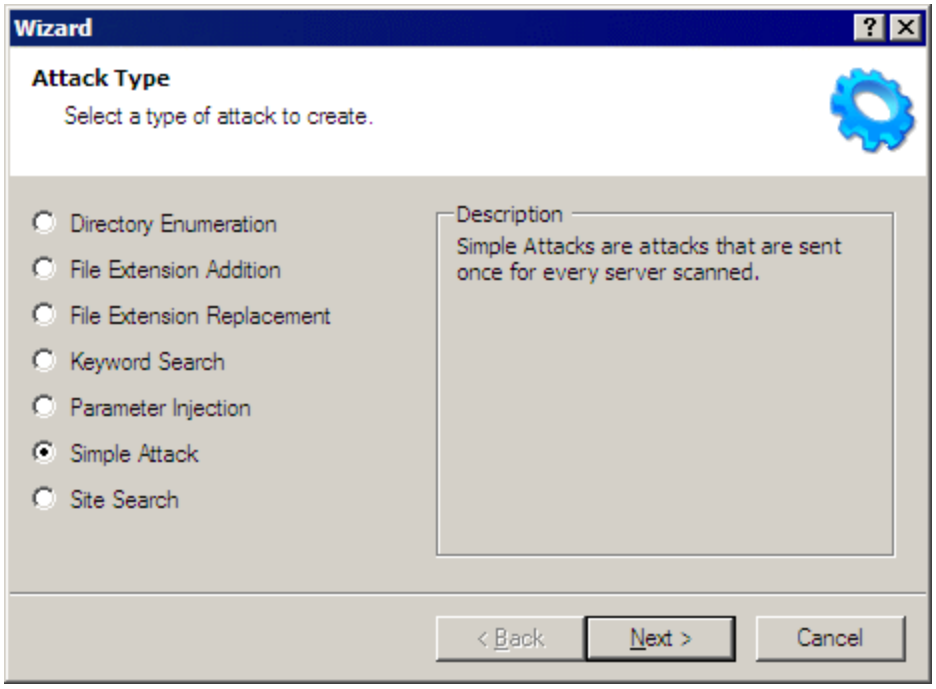
If you create a custom check that duplicates an attack conducted by OpenText DAST, your new check will not be submitted unless you disable the standard check. For example, OpenText DAST normally runs a directory enumeration check that searches for a backup directory with "(copy)" suffix. If you create a custom check that also searches for a backup directory with "(copy)" suffix, OpenText DAST will not submit it (because it has already searched for that directory) unless you disable check #11485 named Backup Directory ((copy)).

Creating a custom check

To create a custom check in the Policy Manager:

1. Do one of the following:
   - To edit a policy that you previously created, select **File > Open** and select the policy.
   - To create a new policy based on a prepackaged policy, select **File > New** (or click the New Policy icon) and select the policy on which you will model a new one.
2. Make sure the **Standard view** is selected, with Seven Pernicious Kingdoms listed in the left pane.
3. Right-click on **Custom Checks** and select **New Custom Check** from the shortcut menu.

The Custom Check Wizard appears.



4. Select one of the following attack types, listed with detailed explanations and examples:

- **Directory enumeration**

  This type of check searches for a directory of the name you specify.

  - Attack Type: Directory Enumeration
  - Attack: /directory_name/ [where directory_name is the name of the directory you want to find]
  - Signature: [STATUSCODE]3\d\d OR [STATUSCODE]2\d\d OR [STATUSCODE]40[13]

- **File extension addition**

  This type of check searches for files with a file extension that you specify.

  During the crawl, whenever OpenText DAST encounters a file of any name and any extension (for example, global.asa), it sends an HTTP request for a file of the same name plus the found extension plus an extension that you specify. For example, if you specify a file extension of .backup, then when OpenText DAST discovers a file named global.asa, it will subsequently search for a file named global.asa.backup.

  A server would normally deny any request for the global.asa file, but if a programmer has left a backup file on the server and the file has a different extension (such as global.asa.backup), then the server might return the file (which contains the full source of the global.asa file).

  To create a custom check that searches for files with a specific added extension, enter the following in the Custom Check Wizard:

  - Attack Type: File Extension Addition
  - Attack: .ext [where ext is the file extension of files you want to locate]. You must include the leading dot or period (.)

- Signature: [STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

- **File extension replacement**

  This type of check searches for files with a file extension that you specify.

  For example, OpenText DAST contains a standard check that searches for files having an extension of .old. During the crawl, whenever it encounters a file of any name and any extension (for example, startup.asp), it sends an HTTP request for a file of the same name but with an extension of .old (for example, startup.old).

  To create a custom check that searches for files with a specific extension, enter the following in the Custom Check Wizard:

  - Attack Type: File Extension Replacement
  - Attack: ext [where ext is the file extension of files you want to locate]. Do NOT include a leading dot or period (.)
  - Signature: [STATUSCODE]200 AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

- **Keyword search**

  This type of check determines if a specified word or phrase (defined by a regular expression) exists anywhere in the HTTP response.

  The following example searches the HTTP response for a nine-digit number formatted as a social security number (\d = any digit).

  - Attack Type: Keyword Search
  - Attack: N/A
  - Signature: [BODY]\d\d\d-\d\d-\d\d\d\d

- **Parameter injection**

  This type of attack replaces an argument value with an attack string.

  Example:

  http://www.samplesite.com/webapp.asp?ValidParameter=ValidArgument

  will be changed to

  http://www.samplesite.com/webapp.asp?ValidParameter=AttackArgument

  There are several types of parameter injection, as follows:

  - Command Execution

    A command execution check combines strings composed of special characters with operating system-level commands. It is an attempt to make the web application execute the command using the provided string (if the application fails to check for and prohibit the input).

    The following example tests for parameter injection by providing spurious input to a program named support_page.cgi; if the HTTP response contains data that matches the regular expression, then the application is vulnerable to command execution.

- Attack Type: Parameter Injection
- Attack: /support_page.cgi?file_name=|id|
- Signature: [BODY]uid= AND [BODY]gid=

- SQL Injection

  SQL injection is the act of passing SQL code into an application. These attack strings are composed of fragments of SQL syntax that will be executed on the database server if the web application uses the string when forming a SQL statement without first filtering out certain characters.

  - Attack Type: Parameter Injection
  - Attack: ' [an apostrophe]
  - Signature: [STATUSCODE]5\d\d

- Cross-Site Scripting

  This issue occurs when dynamically generated web pages display input that is not properly validated. This allows an attacker to embed malicious JavaScript into the generated page, enabling him to execute the script on the machine of any user who views the malicious page. Any site that allows users to post text messages can be vulnerable to an attack such as this.

  The following example tests for cross-site scripting in the Fusion News application:

  - Attack Type: Parameter Injection
  - Attack: /fullnews.php?id=<script>alert(document.cookie)</script>
  - Signature: [ALL]Powered\sby\sFusion\sNews And [ALL]<script>alert\(document\.cookie\)</script>

- Directory Traversal

  Directory traversal entails sending malformed URL strings to access non-public portions of the web server's content. An attacker will try to access different files on a server by using relative hyperlinks. For example, by adding triplets of two periods and a forward slash (../) to the target URL and by varying the number of directories to traverse, an attacker might find and gain access to a system password file such as www.server.com/../../../../password.

  The following example searches for the boot.ini file:

  - Attack Type: Parameter Injection
  - Attack: /../../../../../../../../../../boot.ini
  - Signature: [ALL]\[boot\sloader\]

- Abnormal Input

  Abnormal input attack strings are composed of characters that can cause unhandled exceptions (errors the program is not coded to handle) in web applications where unexpected input is not prohibited. Unhandled exceptions often cause servers to display error messages that disclose sensitive information about the application's internal mechanics. Source code may even be disclosed.

  The following example sends an extraordinarily long string in an attempt to create a buffer overflow.

- Attack Type: Parameter Injection
- Attack: AAAAAAAAAAAA...AAAAAAAA [1000 repetitions of the letter "A"]
- Signature: [STATUSCODE]5\d\d

- **Simple attack**

  This type of attack is sent once for every server scanned.

  The following example attempts to obtain a UNIX password file by appending the attack string to the target URL or IP address:

  - Attack Type: Simple Attack
  - Attack: /etc/passwd
  - Signature: [ALL]root: AND [ALL]:0:0

- **Site search**

  This type of attack is designed to find files commonly left on a web server. For example, check ID #279 searches for a file named log.htm.

  The following example searches for a file named xanadu.html by appending the attack string to the target URL or IP address:

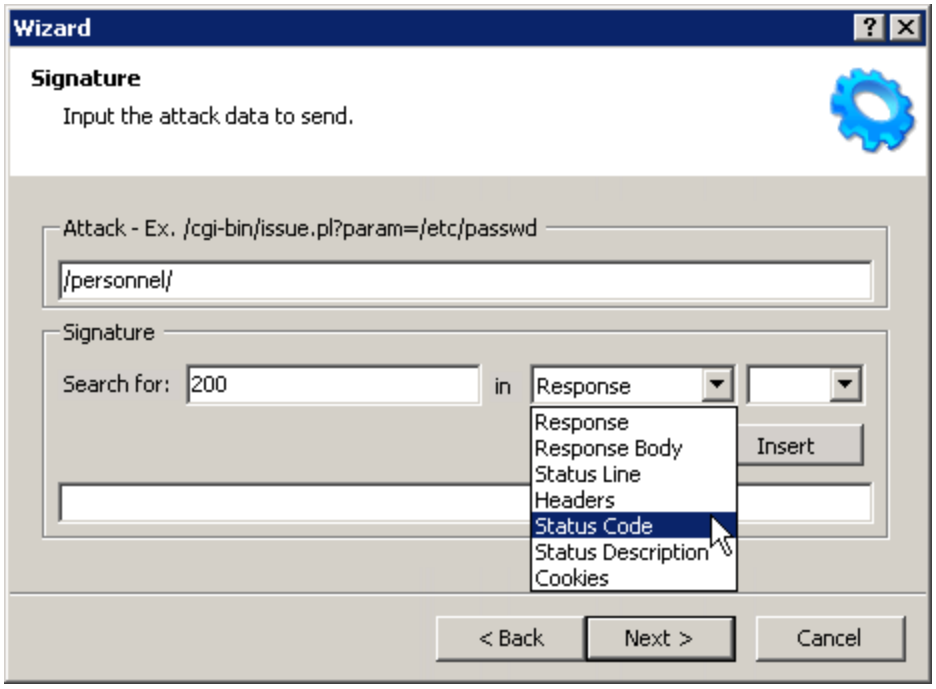
  - Attack Type: Site Search
  - Attack: xanadu.html
  - Signature: [STATUSCODE]2\d\d OR [STATUSCODE]40[1]

  To create a custom check that searches for a file named confidential.txt, enter the following in the Custom Check Wizard:

  - Attack Type: Site Search
  - Attack: confidential.txt
  - Signature: [STATUSCODE]2\d\d AND ([HEADERS]Content-Type:\stext/plain OR [HEADERS]Content-Type:\sapplication/octet-stream)

5. Click **Next**.

6. In the **Attack** field, enter the data you want to use for the attack.



In the above example of directory enumeration, the check will search for a directory named "personnel" by appending the attack string (/personnel/) to the target URL or IP address.

7. You must specify a signature, which is simply a regular expression (that is, a special text string for describing a search pattern). When OpenText DAST searches the HTTP response and finds the text described by the signature, it flags the session as a vulnerability. You can use the **Search for** field and drop-down lists to help you create the regular expression, or you can type the regular expression directly into the text box at the bottom of the window.

   To use the **Search for** field:

   a. Enter the text you want to locate.

      Enter only text in the **Search for** field; do not enter a regular expression.

      In this example (searching for a directory named "personnel"), the server would return a status code of 200 if the directory exists, so enter "200" in the **Search for** field. Realistically, however, you might also accept any status code in the 200 or 300 series, or a status code of 401 or 403.

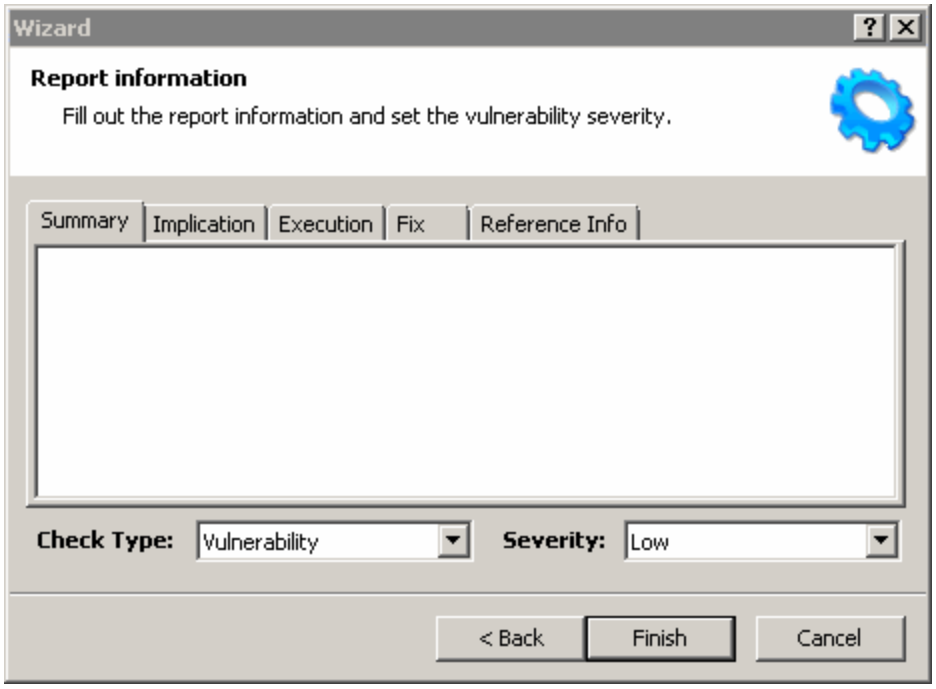
   b. Click the drop-down arrow to specify the section of the HTTP response that should be searched.

   c. (Optional) To create a complex search, click the second drop-down and select a Boolean operator (AND, OR, or NOT).

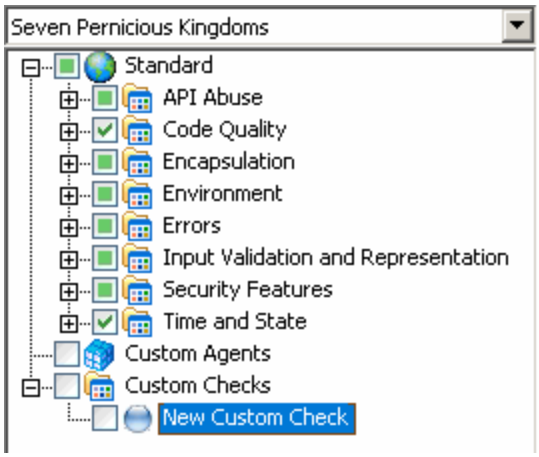
   d. Click **Insert**.

   e. (Optional) For complex searches, repeat steps a-d as needed. You can also edit or replace the regular expression that appears in the bottom text box.

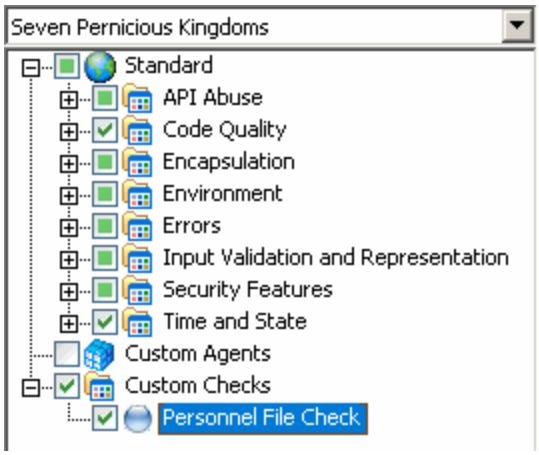
8. Click **Next**.



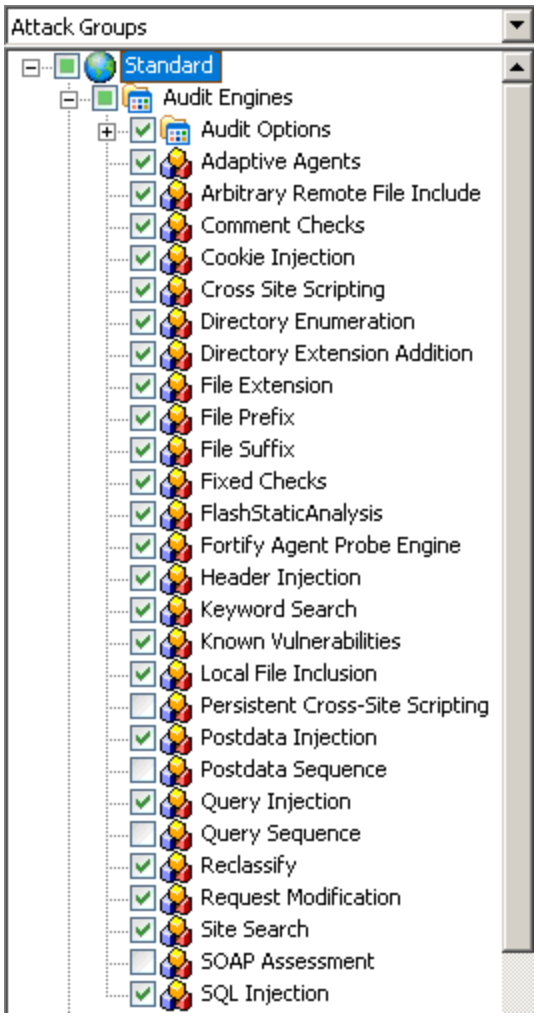
9. On the Report Information panel, click each tab and enter the text that will appear in the description.
10. Select an entry from the **Check Type** list.
11. Select a severity level from the **Severity** list.
12. Click **Finish**.
13. Change the default name "New Custom Check" to reflect the purpose of the check.



14. Ensure that the custom check is enabled (with a check mark).



15. Select **Attack Groups** from the drop-down list, and then click ⊞ to expand the Audit Engines folder.



16. Ensure that the appropriate audit engine is enabled (with a check mark) for the type of check you created, according to the following table.

This Attack Type...	Uses This Audit Engine...
Directory Enumeration	Directory Enumeration
File Extension Addition	File Extension
File Extension Replacement	File Extension
Keyword Search	Keyword Search
Parameter Injection	Post Data Injection
Simple Attack	Fixed Checks
Site Search	Site Search

17. Select **File > Save**.
18. Enter a name for the new policy and click **Save**.

OpenText DAST adds all custom checks to every policy, but does not enable them. To enable the custom check in other policies, see "Creating or editing a policy" on page 64.

Disabling a custom check

To disable a custom check:

1. Select a custom check.
2. Clear its associated check box.

Deleting a custom check

To delete a custom check:

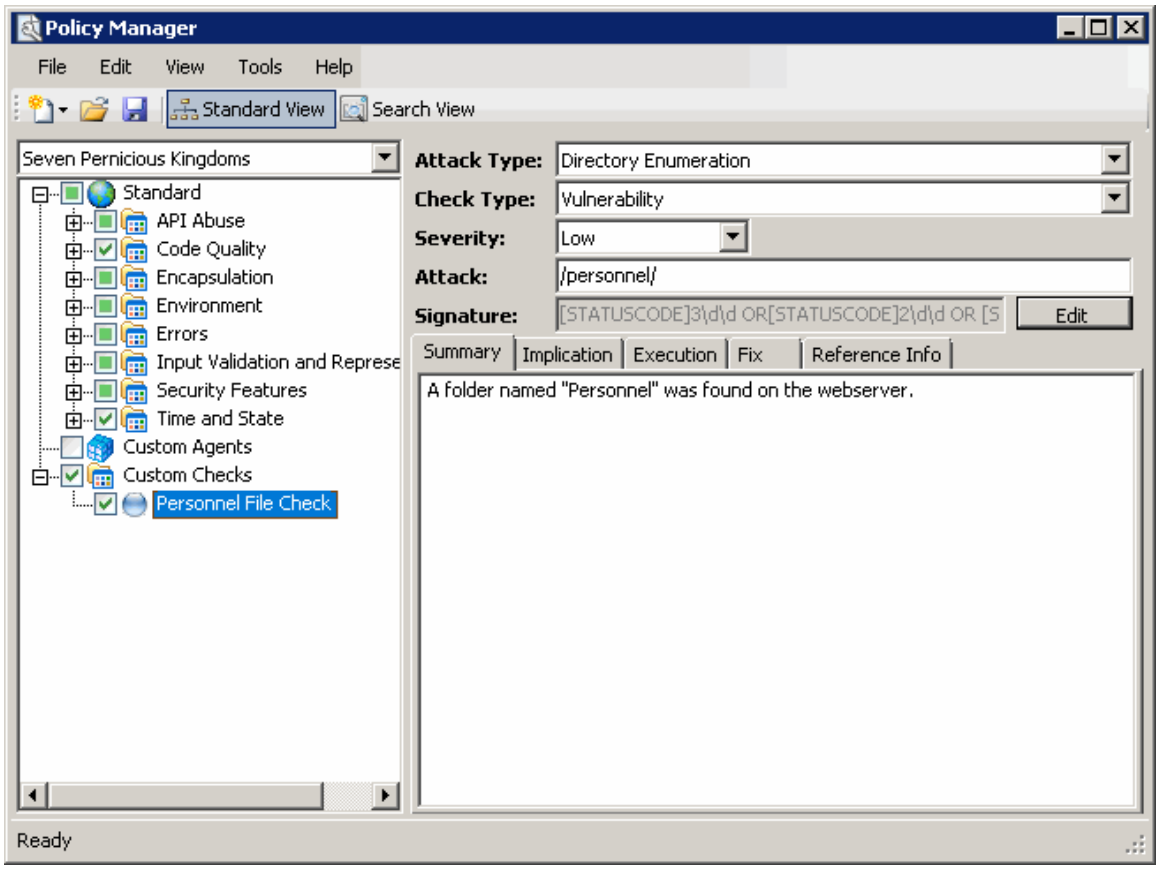
Caution! If you delete a custom check from a policy, you delete it from all policies and from the entire system.

1. Right-click a custom check.
2. Select **Delete** from the short-cut menu.

Editing a custom check

To edit a custom check:

1. Open a policy.
2. Select a custom check.
3. Using the right pane of the Policy Manager, modify the custom check properties.



4. Click the Save icon.

See also

"Regular Expressions" on page 95

"Regular Expression Extensions" on page 96

Searching for specific agents

Use the Search view on the Policy Manager to locate specific vulnerability checks (attack agents). You can then elect to include or exclude individual agents.

To search for attack agents:

1. On the toolbar, click **Policy Manager**

   - or -

   select **Tools > Policy Manager**.
2. If you do not have a policy selected, select a policy from the *Open Policy* window and click **OK**.
3. Select **View > Search**.

   The description of every attack agent contains "report fields" such as summary, implication, execution, recommendation, and fix. The Search feature enables you to locate attack agents that contain the text you specify in a selected report field.
4. From the **Criteria** list, select the report field that you want to search.
5. Choose an operator from the drop-down list (is, is greater than, is less than, contains).
6. In the text box, type the text or number you want to find.
7. Click **Search**.
8. The Policy Manager lists in the **Checks** area all attack agents that match your search criteria. An active agent has a check mark next to its name. Select (or clear) a check box to activate (or deactivate) an agent.
9. Click **Save** to save the revised policy.

Using a custom agent

OpenText DAST audit extensions are developed by software developers in your organization and published to SecureBase as custom agents that can be enabled in policies and used in conducting scans. To enable a custom agent in the Policy Manger:

1. Do one of the following:
   - To create a new policy that includes only the custom agent check, select **File > New > Blank Policy**, and go to Step 2.
   - To enable the custom agent check along with other checks in an existing policy, go to Step 2.
2. Select **Seven Pernicious Kingdoms** from the drop-down list.
3. Expand the **Custom Agents** group.
4. Select a custom agent from the list.
5. Select **File > Save**.

When conducting a scan, select the policy that includes the enabled custom agent check.

Note: If the developer republishes an extension, you must close and re-open the Policy Manager to get the revised custom agent.

Methodologies

A web application includes not only the code that creates your website, but also the architectural components necessary to make a website available and useful to the public. When considering web application security, you must account for all the components that work together to create a website, not just the visible face presented to the world at large.

OpenText DAST can analyze any web application, identify potential security flaws, and supply you with the latest information necessary to resolve security issues before unauthorized users are able to capitalize on them. In an ever-changing, dynamic environment like the web, having a security tool that's always up to date is an absolute necessity. With this in mind, OpenText's design team engineered the software to automatically update its built-in knowledgebase of known successful hacking methodologies every time it's used. The software will then emulate these methodologies against the applications to be tested. This knowledgebase is gathered from OpenText security experts, as well as a wide variety of leading third-party security organizations and analysts.

When new methods of attack are discovered, OpenText is ready with same-day upgrades to its SecureBase™ vulnerabilities database. Following is a list of the key methodologies that OpenText DAST employs when assessing the security vulnerabilities of your web application.

Parameter manipulation

Parameter manipulation involves tampering with URL parameters to retrieve information that would otherwise be unavailable to the user. Parameter manipulation modifies, adds or removes parameter names and/or arguments. Basically, any input can be modified. Parameter manipulation attacks can be used to achieve a number of objectives, including disclosure of files above the web root, extraction of information from a database and execution of arbitrary operating-system level commands. This is applied to:

- **Query strings**. Web applications often use query strings as a simple method of passing data from the client and the server. Query strings are a way to add data calls to a hyperlink, and then retrieve that information on the linked page when it is displayed. By manipulating query strings, an attacker can easily steal information from a database, learn details about the architecture of your web application, or possibly execute commands on your web server. When conducting an audit, OpenText DAST implements advanced query string manipulation to ascertain the feasibility of command execution on your server(s), and determines the vulnerability of your web applications to query string manipulation.
- **Post data**. Since manipulating a query string is as easy as typing text in the address bar of a browser, many web applications rely on the POST method coupled with the use of forms rather than GET to pass data between pages. Since browsers normally don't display POST data, some programmers are lulled into thinking that it is difficult or impossible to change the data, when in fact the opposite is true. OpenText DAST determines your application's susceptibility to attacks that rely on the POST method of parameter manipulation.
- **Headers**. Both HTTP requests and responses use headers to deliver information about the HTTP message. A developer may not consider HTTP headers as areas of input, even though many web

applications will log headers such as the "referrer" or "user-agent" to a database for traffic statistics. OpenText DAST intercepts header information, and attempts to pass different parameter values during an audit.

- **Cookies**. Many web applications use cookies to save information (for example, user ID's and timestamps) on the client's machine. By changing these values, or “poisoning” the cookie, malicious users can gain access to the accounts and information of other users. As well, attackers can also steal a user's cookie and gain direct access to the user's account, bypassing the need to enter an ID and password or other form of authentication. OpenText DAST lists all cookies discovered during a scan, and attempts to change their parameters during an audit.

Parameter manipulation can be divided into several subcategories, as described in the following sections.

Parameter injection

Parameter injection attacks replace an argument value with an attack string.

Example:

http://www.site.com/webapp.asp?ValidParameter=ValidArgument will be changed to http://www.site.com/webapp.asp?ValidParameter=AttackString

These attempts to manipulate parameters associated with a URL are usually directed to the following areas:

Command execution

Command execution attack strings are composed of special characters combined with operating system-level commands that will be run if the web application uses the string in a call to an operating system command without first parsing out the special characters.

Example: ;id;

OpenText DAST submits harmless commands, such as the ID command, to ascertain the feasibility of commands being inserted by an attacker and then executed.

SQL injection

SQL injection is the act of passing SQL code not intended by the developer into an application. These attack strings are composed of fragments of SQL syntax that will be executed on the database server if the web application uses the string when forming a SQL statement without first parsing out certain characters.

Example: '+(SELECT TOP 1 name FROM sysobjects WHERE 1=1)+'

Problems can arise when a developer does not protect against potentially malicious input such as an apostrophe ('), which could close the SQL string and give the user unintended system and application access.

Cross-site scripting

This issue occurs when dynamically generated web pages display input that is not properly validated. This allows an attacker to embed malicious JavaScript into the generated page, enabling him to execute the script on the machine of any user who views the malicious page. Any site that allows

users to post text messages can be vulnerable to an attack such as this. This vulnerability is commonly seen on the following:

- Search engines that repeat the search keyword that was entered
- Error messages that repeat the string that contained the error
- Forms that are filled out where the values are later presented to the user
- Web message boards that allow users to post their own messages.

An attacker who uses cross-site scripting successfully might compromise confidential information, manipulate or steal cookies, create requests that can be mistaken for those of a valid user, or execute malicious code on the user systems.

Abnormal input

Abnormal input attack strings are composed of characters that can cause unhandled exceptions (errors the program is not coded to handle) in web applications where unexpected input is not parsed out. Unhandled exceptions often cause error messages to be displayed that disclose sensitive information about the application's internal mechanics. Source code may even be disclosed.

Example: %00

Parameter overflow

Parameter overflow attacks supply web applications with extremely large amounts of data in the forms of parameter or cookie header arguments or parameter names. If a web application is programmed in such a manner that it cannot appropriately handle unexpected and extremely large amounts of data, it may be possible to execute arbitrary operating system-level code or cause a denial-of-service condition.

Buffer overflow

Buffer overflow attacks can be used to execute arbitrary operating system commands. OpenText DAST determines whether or not you are vulnerable to buffer overflow attacks, and provides details for remedying any buffer overflow vulnerabilities.

Example:

http://www.site.com/webapp.asp?ValidParameter=ValidArgument

will be changed to

http://www.site.com/webapp.asp?XXXXXXXXXXXXXXXXX[several thousand more characters]XXX=ValidArgument

and also to

http://www.site.com/webapp.asp?ValidParameter=XXXXXXXXXXXXXXXXX[several thousand more characters]XXX

Parameter addition

Parameter addition attacks insert new parameters into an HTTP request (such as admin=true) in an attempt to gain access to restricted or undocumented application features, and to manipulate internal application settings.

Application debug/backdoor mode parameters

Application debug/backdoor mode parameters are often undocumented application features that are added by programmers in order to assist with quality assurance. Access to debug and backdoor modes can lead to disclosure of sensitive information about the internal mechanics of the web application or even administrative control.

Example:

http://www.site.com/webapp.asp?ValidParameter=ValidArgument&debug=true

Path manipulation

Path manipulation attacks construct or modify the Request-URI section of the HTTP request in order to gain access to files above the web root, bypass authorization settings, display directory listings or display file source. Each of the following is a method of path manipulation.

Path truncation

Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. OpenText DAST 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' truncating the path to look for 'http://www.site.com/folder1/folder2/' and 'http://www.site.com/folder1/'. will cause the web server to reveal directory contents or to cause unhandled exceptions.

Character encoding

Character encoding attacks substitute encoded equivalents of characters in a request for a known resource. If the web application performs a string comparison for authorization or processing purposes using the encoded URI without first parsing the encoded characters, authorization settings may be defeated or source code may be disclosed. OpenText DAST submits various encoded character strings to ascertain whether your web application properly parses special characters. The following elements are included when OpenText DAST performs character encoding tests.

- Unicode: The Unicode Worldwide Character Standard includes letters, digits, diacritics, punctuation marks, and technical symbols for all the world's principal written languages, using a uniform encoding scheme. OpenText DAST submits strings that have been converted to their Unicode equivalent, and attempts to gain unauthorized authentication credentials through this manipulation.
- Hexadecimal coding: This involves replacing characters with their hexadecimal equivalent. OpenText DAST submits hex-encoded strings, and attempts to gain unauthorized authentication credentials through this manipulation.

MS-DOS 8.3 short filename

MS-DOS 8.3 short filename attacks convert the file names to the MS-DOS 8.3 format (1 to 8 characters, as opposed to the 255 characters allowed for file names by more recent versions of Windows). If the web application performs a string comparison for authorization or processing purposes using the MS-DOS 8.3 filename without first converting it to its FAT32/NTFS equivalent, this may defeat authorization settings or cause source code to be disclosed.

Example: longfilename.asp would become longfi~1.asp

Directory traversal

Directory traversal attacks are expressions in the URI that will cause the web server to display the contents of files above the web root if the web application uses the string to specify a file location without first completely parsing out traversal characters.

Example: ../../../../../boot.ini

Character stripping

Character stripping attacks add special characters to a URI that the server or application may parse out. If the server or application uses the URI in a string comparison for authorization or request processing without first stripping out the special characters, authorization settings may be defeated and source code may be disclosed.

Character append

Character append attacks add a special character to the end of a file or directory name.

Example: file.asp would become file.asp%00

Site search

This can be considered the information-gathering stage, emulating an intruder's attempt to learn as much as possible about your web application before launching an attack. Site search is used to locate resources such as documents, applications and directories on the server that are not intended to be viewed by web users. Disclosure of such resources can result in the disclosure of confidential data, information about internal server and application configurations and settings, administrative access to the site, and information and application source code. OpenText DAST determines the availability of the following items, among others, to users of your web application.

- Test and sample files: These often contain information that can be used to implement an attack. For example, authenticated test scripts that have been left on the server could provide an attacker with the location of sensitive areas of your site.
- Administrative interfaces: These are applications that network administrators often place on a network to conduct remote maintenance.
- Application data: This can be information in a database or data passed from page to page via another method.
- Program dumps: Programs often leave a dump file on the server when they terminate prematurely. Attackers will often break an application through various methods and then retrieve important information from a dump file.

- Application logs: Several software applications leave default application logs that detail the installation of the product. Application logs can reveal important information about the architecture of your web application, including the location of hidden areas.
- Installation documentation: Certain software packages place comprising information in default installation documentation that is left available on the server.
- Backup files: Network administrators and developers often leave backup files and scripts on the web server. These files commonly contain information that can be used to breach a site's security. Backup file search involves replacing extensions on files, and then looking for older or backup versions stored on the site. For example, an attacker who finds hi.asp might search for hi.old and hi.back, and retrieve the script's source code.
- Site statistics pages: These can be used to determine information about who is visiting your site. However, it can also reveal information that an attacker can use in formulating an attack, such as the location of other areas of your site.

Application mapping

OpenText DAST exposes and follows all known (and unknown) links located on your site. This creates a baseline for vulnerability checking and application testing.

Crawl

One of the most important elements of discovering the security vulnerabilities of your web application is in mapping its internal structure. A crawl completely maps a site's tree structure. In essence, a crawl runs until no more links on the URL can be followed.

Automatic form-filling

OpenText DAST can be configured to submit data automatically for any form encountered during a crawl (for example, if a page requires entry of a telephone number, etc.).

SSL support

OpenText DAST can crawl any site that uses SSL and determine whether data is being properly encrypted and protected.

Proxy support

A proxy server can be used to ensure network security, provide adequate caching purposes, and regulate administrative control. OpenText DAST can crawl sites that use a proxy server, and check for vulnerabilities specifically related to that configuration.

Client certificate support

A certificate is a statement verifying the identity of a person or the security of a website. Attackers will attempt to alter the values of client certificates to gain unauthorized access to your web application.

State management

State is a property of connectivity. HTTP is a stateless protocol; no concept of session state is maintained by HTTP when handling client-server communications. OpenText DAST determines if any

cookies used on your web application are secure (are they set to expire, properly handled, etc.), and if session IDs are managed securely.

Directory enumeration

Directory enumeration lists all directory paths and possibilities on the application server, including hidden directories that could possibly contain sensitive information. OpenText DAST uses a database of known folders (such as admin, test, logs, etc.) and hidden areas discovered during a crawl when composing a directory enumeration listing.

Web server assessment

During a web server assessment, OpenText DAST test your proprietary web server for vulnerabilities utilizing information gathered during a Site Search and other applied methodologies. Protocol and extension implementation analysis is used to determine what services the server offers, whether or not they conform to established standards for these services, and details regarding their implementation. As web server configurations are responsible for serving content and launching applications, damage from an attack on an unprotected proprietary web server can include denial of service, the posting of inappropriate messages or graphics on the site, deletion of files, or damaging code or software packages being left on the server.

HTTP compliance

HTTP compliance testing assesses the web server or proxy server for proper compliance to HTTP/1.0 and HTTP/1.1 rules. This testing consists of attacks such as sending a data buffer larger than the marked length (buffer overflows). Servers are tested to see if they properly sanitize data by mixing and matching various methods and headers that are never seen within a normal request and determining if the web server handles the requests properly. These attacks can determine if a web server or web device complies with HTTP specifications and can also uncover unknown vulnerabilities.

WebDAV compliance

WebDAV allows users to place and manipulate files in a directory on your web server. OpenText DAST determines whether or not WebDAV privileges can be exceeded and manipulated on your web server.

SSL strength

SSL strength identification determines the encryption level accepted by a web server. This can be important to ensure that secure clients do not connect at an encryption level lower than the expected standard, and that data is being properly encrypted to prevent its interception.

Certificate analysis

OpenText DAST analyzes the SSL certificate for improper properties such as unknown CA certificate analysis or expired time.

HTTP method support

OpenText DAST determines which HTTP methods are supported by the web server.

Example: Does the webserver support GET,PUT,INDEX,POST,CONNECT, etc.

Content investigation

Content Investigation involves searching through content discovered during a Site Search to determine what information is available to users of your web application that should remain private. OpenText DAST searches for the following items when conducting Content Investigation (although by no means a comprehensive list), and will determine each item's potential level of exploitation.

Spam gateway detection

Spam gateways are e-mail web applications that allow the client to specify the location of the mail recipient via hidden form inputs or parameters.

Client-side pricing

Client-side pricing is a web application flaw that allows the client to specify item pricing via hidden form inputs or parameters.

Sensitive developer comments

Developer comments in HTML often reveal sensitive information about an application’s internal mechanics and configuration. For example, something as seemingly innocuous as a comment referencing the required order of fields in a table could potentially give an attacker a key piece of information needed to crack the security of your site. OpenText DAST lists all comments found in the site's code in the Comments area on the Information pane.

Web werver/web package identification

OpenText DAST will identify all services and banners on the web server, and ascertain the vendors and version numbers of all available software packages used by your web application. This is accomplished through a variety of methods, listed below.

- Header Evidence - For example, Server: Microsoft-IIS/5.0
- Link Evidence - For example, <a href="/webapp.php"> indicates that the PHP web application server is running.
- Default/Template Page Evidence - For example, "If you can see this, it means that the installation of the Apache web server software on this system was successful."

Absolute path detection

OpenText DAST detects whether a fully qualified pathname was able to be discovered anywhere within an application. Certain vulnerabilities can only be exploited if the attacker has the fully qualified pathname.

Example: /opt/Web/docroot/, c:\inetpub\wwwroot"

Error message identification

Often, error messages will reveal more than they were designed to do. For example, pages containing /servletimages/logo2circle.gif are default template BEA WebLogic error pages. An attacker forearmed with that knowledge can customize his attack to take advantage of that server's inherent vulnerabilities.

Permissions assessment

OpenText DAST will determine what level of permissions (such as uploading files to the web server, editing data, traversing directories, etc.) are available in different areas of your web application, and then determine the best way to remedy any inherent security vulnerabilities.

Brute force authentication attacks

Brute force attacks test for susceptibility to dictionary attacks (files containing common logons and passwords). OpenText DAST tests Basic, NTLM, and web form authentication for susceptibility to a brute force attack.

Known attacks

Known attacks include all exploitable holes and bugs in web servers, applications, and other third-party components that have been published, posted, or otherwise communicated. Most of these vulnerabilities have existing patches, but hackers will exploit systems where patches have not been installed in a timely fashion. Known attack information is included in all other methodologies.

OpenText DAST rely on a proprietary database that contains fingerprints of known attacks dating back to the birth of the World Wide Web. They check for and download new risks and exploits each they run, ensuring that the product is always updated and at the forefront of hacking expertise.

Policies

Each policy is kept up to date through the Smart Update function, ensuring that scans are accurate and capable of detecting the most recently discovered threats. OpenText DAST (or sensor) contains the following packaged policies that you can use with your scans and crawls to determine the vulnerability of your web application.

Note: This list might not match the policies that you see in your product. SmartUpdate might have added or deprecated policies since this document was produced.

About OAST-related checks

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

Best Practices

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

- **API**: This policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.
- **CWE Top 25 *<version>***: The Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25) is a list created by MITRE. The list demonstrates the most widespread and critical software weaknesses that can lead to vulnerabilities in software.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **Best Practices** group.
- **General Data Protection Regulation (GDPR)**: The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and provides a framework for organizations on how to handle personal data. The GDPR articles that pertain to application security and require businesses to protect personal data during design and development of their products and services are as follows:
  - Article 25, data protection by design and by default, which requires businesses to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.
  - Article 32, security of processing, which requires businesses to protect their systems and applications from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

  This policy contains a selection of checks to help identify and protect personal data specifically related to application security for the GDPR.
- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 - (NIST SP 800-53 Rev.5) provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. This policy contains a selection of checks that must be audited to meet the guidelines and standards of NIST SP 800-53 Rev.5.
- **OWASP API Top 10 *<year>***: The OWASP API Top 10 *<year>* provides a list of the top security risks affecting APIs for the year specified. It aims to raise awareness around API security weaknesses and to educate those involved in API development and maintenance, such as developers, designers, architects, managers and/or organizations in general who need to secure Web APIs. The OWASP API Top 10 focuses on weaknesses affecting Web APIs and it is not intended to be used only by itself, instead it is intended to be used in combination with other standards and best practices to thoroughly capture all relevant risks. For example, it should be

used in combination with the OWASP Top 10 to identify issues related to input validation such as injections.

- **OWASP Application Security Verification Standard (ASVS)**: The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test, and verify secure applications.

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

By Type

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

- **Aggressive SQL Injection**: This policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs a more accurate and decisive job, but has a longer scan time.
- **Apache Struts**: This policy detects supported known advisories against the Apache Struts framework.
- **Blank**: This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Client-side**: This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the

phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.

- **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against production servers.
- **Cross-Site Scripting**: This policy performs a security scan of your web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a website to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **By Type** group.
- **Mobile**: A mobile scan detects security flaws based on the communication observed between a mobile application and the supporting backend services.
- **NoSQL and Node.js**: This policy includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL, such as MongoDB, and server side infrastructures based on JavaScript, such as Node.js.
- **OAST**: This policy includes all checks that use Out-of-band Application Security Testing (OAST) technology in scanning logic.
- **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **PCI DSS *<version>***: The Payment Card Industry Data Security Standard (PCI DSS) provides a baseline of technical and operational requirements designed to protect account data. This policy contains a selection of checks that need to be audited to meet the secure coding requirements of PCI DSS.
- **PCI Software Security Framework *<version>* (PCI SSF *<version>*)**: The PCI SSF provides a baseline of requirements and guidance for building secure payment systems and software that handle payment transactions. This policy contains a selection of checks that must be audited to meet the secure coding requirements of PCI SSF.
- **Privilege Escalation**: The Privilege Escalation policy scans your web application for programming errors or design flaws that allow an attacker to gain elevated access to data and applications. The policy uses checks that compare responses of identical requests with different privilege levels.
- **Server-side**: This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.

- **SQL Injection**: The SQL Injection policy performs a security scan of your web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database.
- **Transport Layer Security**: This policy performs a security assessment of your web application for insecure SSL/TLS configurations and critical transport layer security vulnerabilities, such as Heartbleed, Poodle, and SSL Renegotiation attacks.
- **WebSocket**: This policy detects vulnerabilities related to WebSocket implementation in your application.

Custom

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

Hazardous

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

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

  Caution! An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. OpenText strongly recommends using the All Checks policy only in test environments.

Deprecated checks and policies

The following checks and policies are deprecated and are no longer maintained.

- **Aggressive Log4Shell (Deprecated)**: This policy performs a comprehensive security assessment of your web application for JNDI Reference injections in vulnerable versions of Apache Log4j libraries. In vulnerable versions, Log4j does not restrict JNDI features. This allows an attacker who can control log messages to inject JNDI references that point to an attacker-controlled server. This can lead to remote code execution on the vulnerable target. Compared with other policies that include Log4Shell agent, this policy performs a more accurate and decisive job, but produces a significant number of requests and has a longer scan time.
- **Application (Deprecated)**: The Application policy performs a security scan of your web application by submitting known and unknown web application attacks, and only submits specific attacks that assess the application layer. When performing scans of enterprise level web

applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your scan in terms of speed and memory usage.

- **Assault (Deprecated)**: An assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web application server, and web application layers. An assault scan includes checks that can create denial-of-service conditions. It is strongly recommended that assault scans only be used in test environments.
- **Deprecated Checks**: As technologies go end of life and fade out of the technical landscape it is necessary to prune the policy from time to time to remove checks that are no longer technically necessary. Deprecated checks policy includes checks that are either deemed end of life based on current technological landscape or have been re-implemented using smart and efficient audit algorithms that leverage latest enhancements of core OpenText DAST framework.
- **Dev (Deprecated)**: A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web application layer only. The policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **OpenSSL Heartbleed (Deprecated)**: This policy performs a security assessment of your web application for the critical TLS Heartbeat read overrun vulnerability. This vulnerability could potentially disclose critical server and web application data residing in the server memory at the time a malicious user sends a malformed Heartbeat request to the server hosting the site.
- **OWASP Top 10 Application Security Risks - 2010 (Deprecated)**: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about what the most critical web application security flaws are. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. This policy includes elements specific to the 2010 Top Ten list. For more information, consult the OWASP Top Ten Project.
- **Platform (Deprecated)**: The Platform policy performs a security scan of your web application platform by submitting attacks specifically against the web server and known web applications. When performing scans of enterprise-level web applications, use the Platform Only policy in conjunction with the Application Only policy to optimize your scan in terms of speed and memory usage.
- **QA (Deprecated)**: The QA policy is designed to help QA professionals make project release decisions in terms of web application security. It performs checks for both known and unknown web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
- **Quick (Deprecated)**: A Quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the web server, web application server and web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **Safe (Deprecated)**: A Safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown vulnerabilities at the web server, web application server and web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.
- **Standard (Deprecated)**: Standard (Deprecated) policy is copy of the original standard policy before it was revamped in R1 2015 release. A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web

application server and web application layers. A standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

See also

"Policy Manager" on page 61

Policy Manager icons

The following table describes the icons that are used in the Policy Manager tree view.

Icon	Definition
	The policy.
	Attack Group Folder: Folders that contain vulnerability assessments.
	Audit Methodology: A set of checks that compose an audit methodology. For example, Site Search is part of the Audit methodology. For more information on methodologies, see "Methodologies" on page 76.
	A critical vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify private information.
	A high vulnerability. Generally, the ability to view source code, files out of the web root, and sensitive error messages.
	A medium vulnerability. Indicates non-HTML errors or issues that could be sensitive.
	A low vulnerability. Indicates interesting issues or issues that could potentially become higher ones.

Audit engines

OpenText DAST uses the following audit engines:

- **Adaptive Agents**: Certain vulnerabilities require a large amount of logic when checking for them. For example, a buffer overflow JRun check might cause a server to crash if conducted through a vulnerability database. Instead, an adaptive agent with the proper amount of logic can be written to prevent such a problem. With this smart approach, OpenText DAST continuously applies appropriate assessment resources that adapt to the specific application environment.

- **Arbitrary Remote File Include**: This engine checks for vulnerabilities that may allow fetching and incorporating data from arbitrary URLs supplied by an attacker.
- **Comment Checks**: The comment audit examines each session for file names and/or URLs in comments. Upon finding a filename or URL, the audit will check to see if the file or URL exists.
- **Cookie Injection**: Cookies and headers are just as vulnerable to injection attacks as text fields in forms. Cookie injection occurs when unvalidated data is sent by a user's browser as part of a cookie. The Cookie Injection audit engine attempts certain traditional parameter injection attacks against different cookie values
- **Cross-Site Scripting**: This engine conducts cross-site scripting parameter injection attacks. Applications are vulnerable to these attacks when developers do not adequately filter or verify client-supplied data that is returned by the application to the server.
- **Directory Enumeration**: Directory Enumeration finds all directory paths and possibilities on the application server, including hidden directories which could possibly contain sensitive information. This helps OpenText DAST create a full and accurate map of the targeted site.
- **Directory Extension Addition**: Directory extension checking involves adding extensions to directories and removing the trailing slash to find archived directories left on the server. OpenText DAST attempts to locate all directories that have been left on your server that could be used by an attacker.
- **File Extension**: Network administrators and developers often leave backup files and scripts on the web server. These files commonly contain information that can be used to breach a site's security. Extension checking involves replacing extensions on files, and then looking for older or backup versions stored on the site. For example, an attacker who finds hi.asp might search for hi.old and hi.back, and retrieve the script's source code. OpenText DAST attempts to locate all files that could be utilized by an attacker that have been left on your server.
- **File Prefix**: Network administrators and developers often leave backup files and scripts on the web server. These files commonly contain information that can be used to breach a site's security. Prefix checking involves affixing a value to file names, and then looking for older or backup versions stored on the site.
- **File Suffix**: File suffix checking involves affixing a value to file names, and then looking for older or backup versions stored on the site. See File Prefix above.
- **Fixed Checks**: This audit performs checks for files with known vulnerabilities. This audit is the same as the ABS Checks audit, with the exception being that the Fixed Checks audit does not probe the directory structure before sending the attacks.
- **FlashStaticAnalysis**: Performs Flash source code analysis to detect vulnerabilities.
- **Fortify Agent Probe Engine**: This engine sends probes for hints whether a particular parameter or injection point would be vulnerable to the attack suggestions provided in the audit inputs.
- **Hacker Level Insights**: This engine provides data that extends beyond the classic weaknesses and vulnerabilities that DAST traditionally highlights.
- **Header Injection**: Cookies and headers are just as vulnerable to injection attacks as text fields in forms. HTTP header injection occurs when HTTP headers are dynamically generated with user input that includes malicious content. The Header Injection audit engine attempts certain traditional parameter injection attacks against different types of HTTP headers.

- **Keyword Search**: Information disclosure attacks focus on ways of getting a website to reveal system-specific information or confidential data, including user data, that should not be exposed to anonymous users. The Keyword Search audit engine examines every response from the web server for information, such as error messages, directory listings, credit card numbers, etc., that is not properly protected by the website
- **Known Vulnerabilities**: This engine checks for files with known vulnerabilities. The audit will perform a probe of directories known to contain these files and then send requests based on any discovered directories.
- **Local File Inclusion**: Local file reading/inclusion vulnerabilities exist when an attacker can influence the application to read (presumably arbitrary) files specified by the attacker. The engine submits to the web application various values that contain various combinations of relative and absolute file names for specific known files. The engine considers the attack a success if the contents of those files are displayed.
- **Persistent Cross-Site Scripting**: This engine must be enabled to check for Persistent Cross-Site Scripting vulnerabilities (also known as Stored Cross-Site Scripting). When successfully exploited, Persistent Cross-Site Scripting can allow an attacker to inject malicious scripts into the target application's client-side code.
- **Postdata Injection**: Since manipulating a query string is as easy as typing text in the address bar of a browser, many web applications rely on the POST method coupled with the use of forms (rather than GET) to pass data between pages. Since browsers normally don't display POST data, some programmers are lulled into thinking that it is difficult or impossible to change the data, when in fact the opposite is true. OpenText DAST determines your application's susceptibility to attacks that rely on the POST method of parameter manipulation.
- **Postdata Sequence**: Since manipulating a query string is as easy as typing text in the address bar of a browser, many web applications rely on the POST method coupled with the use of forms (rather than GET) to pass data between pages. Since browsers normally don't display POST data, some programmers are lulled into thinking that it is difficult or impossible to change the data, when in fact the opposite is true. OpenText DAST determines your application's susceptibility to attacks that rely on the POST method of parameter manipulation by sending fragmented data to the target.
- **Query Injection**: Web applications often use query strings as a simple method of passing data from the client to the server. Query strings are a way to add data calls to a hyperlink, and then retrieve that information on the linked page when it is displayed. By manipulating query strings, an attacker can easily steal information from a database, learn details about the architecture of your web application, or possibly execute commands on your web server.

  When conducting an audit, OpenText DAST implements advanced query string manipulation to ascertain the feasibility of command execution on your server(s), and determines the vulnerability of your web applications to query string manipulation.
- **Query Sequence**: Web applications often use query strings as a simple method of passing data from the client to the server. Query strings are a way to add data calls to a hyperlink, and then retrieve that information on the linked page when it is displayed. By manipulating query strings, an attacker can easily steal information from a database, learn details about the architecture of your web application, or possibly execute commands on your web server.

When conducting an audit, OpenText DAST implements advanced query string manipulation to ascertain the feasibility of command execution on your server(s), and determines the vulnerability of your web applications to query string manipulation by sending fragmented data to the target.

- **Reclassify**: This engine analyzes the responses to generic/application non-specific attacks and reclassifies certain vulnerability instances into specific known application vulnerabilities.
- **Request Modification**: Several types of attacks involve malformed requests that result in a failed response from the web server. The Request Modification engine generates requests that are derived from other requests that match a pattern, and then evaluates the response to determine if these types of attacks are possible.
- **Site Search**: This can be considered the information gathering stage, much as an attacker would learn as much as possible about your web application before launching an attack. Site search is used to locate resources such as documents, applications and directories on the server that are not intended to be viewed by web users. Disclosure of such resources can result in the disclosure of confidential data, information about internal server and application configurations and settings, administrative access to the site, and information about application source code.
- **SOAP Assessment**: Web services are programs that communicate with other applications (rather than with users) and answer requests for information. Most web services utilize SOAP (Simple Object Access Protocol) to send XML data between the web service and the client web application making the information request. SOAP assessment involves checking for security vulnerabilities inherent within that transport mechanism.
- **SQL Injection**: SQL Injection is an attack in which hackers use SQL statements via an Internet browser to extract, add, or modify data, create a denial of service, bypass authentication, or execute remote commands. The SQL Injection engine detects the following attacks:
  - Injection through user input, such as malicious strings in web forms
  - Injection through cookies, such as modified cookie fields that contain attack strings
  - Injection through server variables, such as headers that are manipulated to contain attack strings
- **WAF Detection**: This engine detects the presence of a web application firewall.

Audit options

OpenText DAST uses the following audit options:

- **CVS Entries Parser**: This engine parses any Entries files found within the scan for links to add to the crawler engine.
- **Robots.txt Parser**: This engine parses any robots.txt files found within the scan for links to add to the crawler engine.
- **WebInspect Scan Signature**: This signature sends the text SCANNED-BY-HP- to the server. The text appears in the webserver logs and indicates that a scan has occurred.
- **Ws_ftp.log Parser**: This engine parses any Ws_ftp.log files it finds and will add links to the site directory tree.

General application testing

This group of checks is applicable to all web applications generally. It includes Directory Enumeration, which looks for common directories in the root of the server. It also includes input injection checks such as SQL Injection and Cross-Site Scripting.

Third-party web applications

This group of checks looks for known vulnerabilities associated with third-party web applications.

Web frameworks/languages

This group of agents looks for known vulnerabilities associated with web application servers. It also determines if known flaws in certain scripting languages can be exploited on the target system.

Web servers

This group of agents looks for known vulnerabilities associated with the following web servers:

- Apache
- IIS
- Lotus Domino
- Minor (a collection of servers including ATPhttpd, 4D, Abyss, Alibaba, BadBlue, and others)
- Netscape/iPlanet
- Secure IIS
- Website Pro
- WebSphere Proxy
- Zeus

For detailed information about all the possible agents, expand the Web Servers node and click on any agent.

Custom agents

Even though OpenText DAST launches thousands of agents to assess your web application during a normal scan, a developer may want to check for a specific condition that is unique to your environment or application. The developer may create a custom agent using the WebInspect Software

Developer's Kit (SDK). You may then integrate the custom agent into one or more policies using the Policy Manager.

See also

"Using a custom agent" on page 75

Custom checks

A custom check is a user-defined probe for a specific vulnerability that the standard repertoire does not address. A custom check can be created using a simple wizard.

See also

"Working with custom checks" on page 65

Regular Expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the Regular Expression Library.

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /\n/ matches a linefeed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/[^(en|ca)].*/.* . Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a"

Character	Description
	in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never early."
\B	Matches a non-word boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a non-digit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a linefeed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v]
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any non-word character. Equivalent to [^A-Za-z0-9_].

Regular Expression Extensions

OpenText engineers have developed and implemented extensions to the normal regular expression syntax. When building a regular expression, you can use the following tags and operators.

Regular expression tags

- [ALL]
- [BODY]
- [STATUSLINE]
- [HEADERS]
- [STATUSCODE]
- [STATUSDESCRIPTION]
- [COOKIES]

Regular expression operators

- AND
- OR
- NOT
- [ ]
- ( )

Examples

- To detect a response in which (a) the status line contains a status code of "200" and (b) the phrase "logged out" appears anywhere in the message body, use the following regular expression:

  [STATUSCODE]200 AND [BODY]logged\sout
- To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and has a reference to the path "/Login.asp" anywhere in the response, use the following:

  [STATUSCODE]302 AND [ALL]Login.asp
- To detect a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response, use the following regular expression:

  ([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302 AND [ALL]Login.asp)

  Note: You must include a space (ASCII 32) before and after an "open" or "close" parenthesis; otherwise, the parenthesis will be erroneously considered as part of the regular expression.
- To detect a redirection response where "login.aspx" appears anywhere in the redirection Location header, use the following regular expression:

  [STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
- To detect a response containing a specific string (such as "Please Authenticate") in the Reason-Phrase portion of the status line, use the following regular expression:

  [STATUSDESCRIPTION]Please\sAuthenticate

Chapter 8: Regular Expression Editor

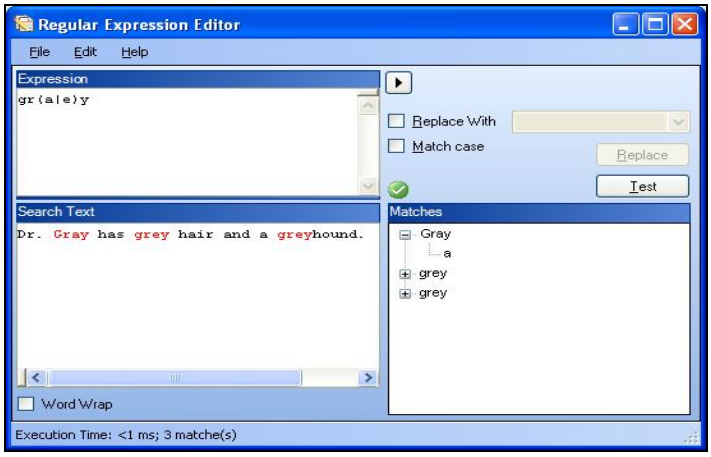
A regular expression is a pattern that describes a set of strings. Regular expressions are constructed similarly to mathematical expressions by using various operators to combine smaller expressions. Only advanced users with a working knowledge of regular expressions should use this feature.

Testing a regular expression

Use the Regular Expression Editor to test and verify regular expressions, as follows:

1. Click **Tools > Regular Expression Editor**.

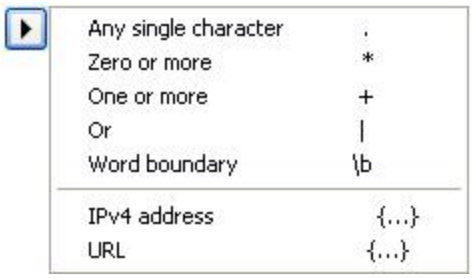
   The Regular Expression Editor window opens.



2. In the **Expression** area, type or paste a regular expression that you think will find the text for which you are searching.

   For assistance, click  to reveal a list of objects. These include metacharacters and regular expressions that define a URL and an IP address. Click an object to insert it.

   Note: You can also use Regular Expression Extensions to restrict your search to certain areas of an HTTP message.



The Regular Expression Editor examines the syntax of the entered expression and displays (if valid) or (if invalid).

3. In the **Search Text** area, type (or paste) the text through which you want to search.

   Alternatively, you can load an HTTP request or response message that you previously saved using the HTTP Editor, as follows:

   a. Click **File > Open Request**.

      The Request file is actually a session containing data for both the HTTP request and response.

   b. Using the standard file-selection window, choose a file containing the saved session.

   c. Select either **Request** or **Response**.

   d. Click **OK**.

4. To find only those occurrences matching the case of the expression, select the **Match Case** check box.
5. To substitute the string identified by the regular expression with a different string:

   a. Select the **Replace With** check box.

   b. Type or select a string using the drop-down combo box.

6. Click **Test** to search the target text for strings that match the regular expression. Matches are highlighted in red.
7. If you selected the **Replace** option, click **Replace** to substitute all found strings with the replacement string.

See also

"Regular expressions" below

"Regular expression extensions and operators" on page 101

Regular expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the Regular Expression Library.

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /\n/ matches a linefeed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use:

Character	Description
	/content/[^(en|ca)].*/.* . Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never early."
\B	Matches a non-word boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a non-digit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a linefeed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v]
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any non-word character. Equivalent to [^A-Za-z0-9_].

Regular expression extensions and operators

OpenText engineers have developed and implemented extensions to the normal regular expression syntax, along with a set of operators.

Regular expression extensions

When building a regular expression, you can use the extensions to specify in which element of the request or response to search for a match. The following table describes the extensions.

Extension	Element
[ALL]	All elements of the request or response
[BODY]	Request Body Response Body
[COOKIES]	Cookie in the Request
[HEADERS]	Request Headers Response Headers
[METHOD]	Request Method
[POSTDATA]	Post Data
[REQUESTLINE]	Request Line (the start line of an HTTP request)
[SETCOOKIES]	Set-Cookie Response Header **Note:** This extension does not work in the Regular Expression Editor tool. However, regular expressions using this extension will work outside of the editor.
[STATUSCODE]	Status Code
[STATUSDESCRIPTION]	Status Description (a string that describes the status of the HTTP output returned to the client)
[STATUSLINE]	Status Line (the start line of an HTTP response)
[URI]	The request target (a URI)

Extension	Element
[VERSION]	HTTP Version

Regular expression operators

OpenText engineers have developed regular expression operators that you can use to construct complex regular expression patterns. The operators are:

- AND
- OR
- NOT
- [ ]
- ( )

Examples

The following paragraphs provide examples of how the use the extensions and operators:

- To detect a response in which (a) the status line contains a status code of "200" and (b) the phrase "logged out" appears anywhere in the message body, use the following regular expression:

  [STATUSCODE]200 AND [BODY]logged\sout
- To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and has a reference to the path "/Login.asp" anywhere in the response, use the following:

  [STATUSCODE]302 AND [ALL]Login.asp
- To detect a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response, use the following regular expression:

  ([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302 AND [ALL]Login.asp)

  Note: You must include a space (ASCII 32) before and after an "open" or "close" parenthesis; otherwise, the parenthesis will be erroneously considered as part of the regular expression.
- To detect a redirection response where "login.aspx" appears anywhere in the redirection Location header, use the following regular expression:

  [STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
- To detect a response containing a specific string (such as "Please Authenticate") in the Reason-Phrase portion of the status line, use the following regular expression:

  [STATUSDESCRIPTION]Please\sAuthenticate

Chapter 9: Server Analyzer (OpenText DAST only)

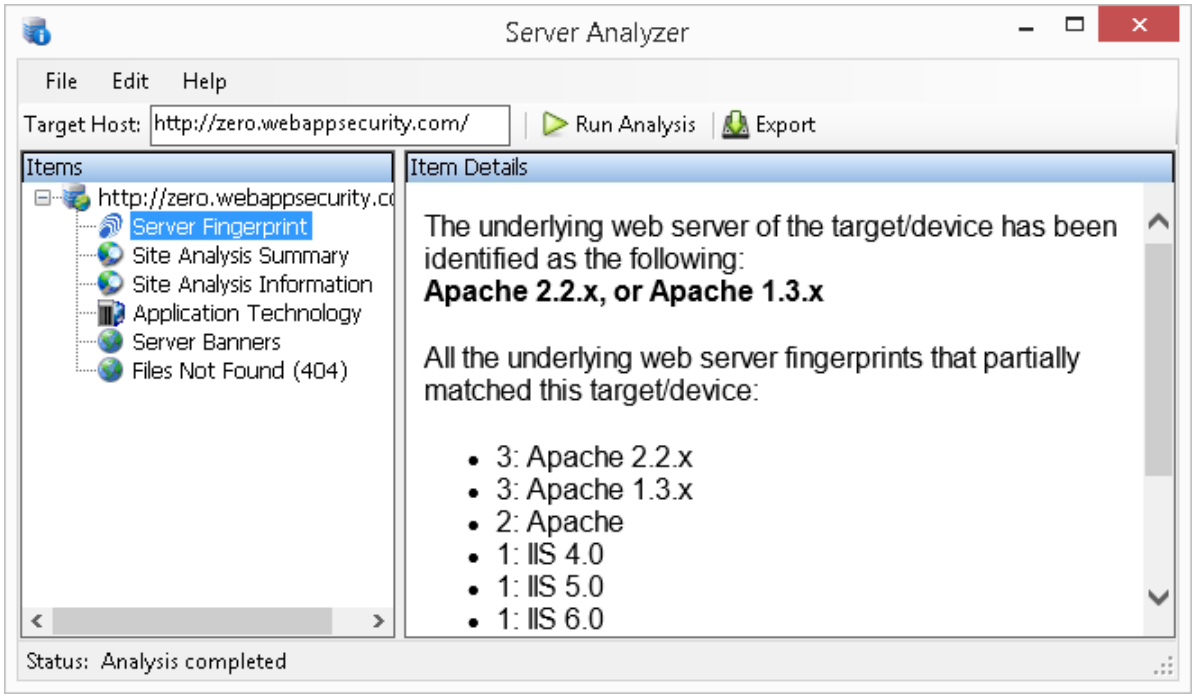
The Server Analyzer interrogates a server to reveal the server's operating system, banners, cookies, and other information.

Analyzing a server

To analyze a server:

1. In the **Target Host** field, enter the URL or IP address of the target server.
2. If host authentication (user name and password) is required, or if you are accessing the target server through a proxy server, click **Edit > Settings**, and enter the requested information. For more information, see "Authentication settings" on the next page and "Proxy settings" on page 105.
3. Click the **Run Analysis** icon.

   When finished, the Server Analyzer displays the status "Analysis completed" and a list of items that were analyzed.
4. Select an item in the **Item** pane to view its information in the **Item Details** pane.



Modifying settings

To modify the Server Analyzer settings:

1. Click **Edit > Settings**.
2. Select one of the following:
   - **Host Authentication**. See "Authentication settings" below.
   - **Proxy**. See "Proxy settings" on the next page.
3. Click **OK**.

Exporting analyzer results

To export the results of the analysis to an HTML file:

1. Click **File > Export**.
2. On the Export File window, select or enter a location and file name.
3. Click **Save**.

See also

"Authentication settings" below

"Proxy settings" on the next page

Authentication settings

Authenticator settings enable you to configure an authentication method and authentication credentials.

Authentication method

If authentication is required, select the authentication type:

- **Automatic**

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

- **Digest**
- **HTTP Basic**
- **Kerberos**
- **NTLM (NT LanMan)**

Authentication credentials

Type a user ID in the **User name** field and the user's password in the **Password** field. To prevent mistyping, repeat the password in the **Confirm Password** field.

To use these credentials whenever the Server Analyzer encounters a password input control, select **Submit these credentials to forms with password input fields**.

Proxy settings

To access this feature, click **Edit > Settings**. Then select **Proxy**.

Direct connection (proxy disabled)

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

Auto detect proxy settings

If you select this option, Server Analyzer will use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the browser's web proxy settings.

Use system proxy settings

Select this option to import your proxy server information from the local machine.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Note: Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.

Configure proxy using a PAC file

Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the **URL** field.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information:

1. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080).
2. Select a protocol **Type** for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or Standard.
3. If authentication is required, select a type from the **Authentication** list:
   - **Automatic**

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

   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NTLM (NT LanMan)**
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** field. Use commas to separate entries.

Specify alternative proxy for HTTPS

For proxy servers accepting HTTPS connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information.

Chapter 10: Server Profiler

Use the Server Profiler to conduct a preliminary examination of a website to determine if certain OpenText DAST 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 Server 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 Server Profiler's prompt to configure the required information before continuing.

Similarly, your settings may specify that OpenText DAST should not conduct "file-not-found" detection. This process is useful for websites 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 OpenText DAST setting to accommodate this feature.

The Server Profiler can be selected during a Guided Scan, or enabled in the Application settings.

Launching Server Profiler as a tool

To launch the profiler as a tool, outside of a scan wizard:

1. Click the OpenText DAST **Tools** menu and select **ServerProfiler**.
2. In the **URL** box, enter or select a URL or IP address.
3. (Optional) If necessary, modify the **Sample Size**. Large websites may require more than the default number of sessions to sufficiently analyze the requirements.
4. Click **Analyze**.

   The Profiler returns a list of suggestions (or a statement that no modifications are necessary).
5. To reject a suggestion, clear its associated check box.
6. For suggestions that require user input, provide the requested information.
7. (Optional) To save the modified settings to a file:
   a. Click **Save Settings**.
   b. Using a standard file-selection window, save the settings to a file in your Settings directory.

Invoking Server Profiler when starting a scan

To launch the profiler when beginning a scan:

1. Start a scan using one of the following methods:
   - On the OpenText DAST **Start Page**, click **Start a Basic Scan**.
   - Click **File > New > Basic Scan**.
   - Click the drop-down arrow on the **New** icon (on the toolbar) and select **Basic Scan**.
   - On the OpenText DAST **Start Page**, click **Manage Scheduled Scans**, click **Add**, and then select **Basic Scan**.
2. On step 4 of the Scan Wizard (Detailed Scan Configuration), click **Profile** (unless **Run Profiler Automatically** is selected).

   The Profiler returns a list of suggestions (or a statement that no modifications are necessary).
3. To reject a suggestion, clear its associated check box.
4. For suggestions that require user input, provide the requested information.
5. Click **Next**.

Chapter 11: SmartUpdate

For installations connected to the Internet, the SmartUpdate feature contacts the OpenText data center to check for new or updated adaptive agents, vulnerability checks, and policy information. SmartUpdate will also ensure that you are using the latest version of OpenText DAST, and will prompt you if a newer version of the product is available for download.

You can configure OpenText DAST settings to conduct a SmartUpdate each time you start the application (select **Application Settings** from the **Edit** menu and choose **Smart Update**).

You can also run SmartUpdate on demand through the OpenText DAST user interface by selecting **Start SmartUpdate** from the OpenText DAST **Start Page**, by selecting **SmartUpdate** from the Tools menu, or by clicking the **SmartUpdate** button on the standard toolbar.

For installations lacking an Internet connection, see "Performing an offline SmartUpdate" on the next page.

Caution! For enterprise installations, if SmartUpdate changes or replaces certain files used by OpenText DAST, the sensor service might stop and the sensor will display a status of "off line." You must launch the OpenText DAST application and restart the service. To do so:

1. Click **Edit > Application Settings**.
2. Select **Run as a Sensor**.
3. Click the **Start** button in the Sensor Status area.

Performing a SmartUpdate (Internet connected)

To perform a SmartUpdate when OpenText DAST is connected to the Internet:

1. Do one of the following:
   - From the toolbar, click **SmartUpdate**.
   - Select **SmartUpdate** from the **Tools** menu.
   - Select **Start SmartUpdate** from the OpenText DAST **Start Page**.

   If updates are available, the SmartUpdater window opens with the Summary tab in view. The Summary tab displays up to three separate collapsible panes for downloading the following:
   - New and updated checks
   - OpenText DAST software
   - SmartUpdate software
2. Select the check box associated with one or more of the download options.

3. (Optional) To view details about the checks being updated:
   a. Click the **Check Detail** tab.

      In the left pane is a list showing the ID, Name, and Version of checks being updated. The list is grouped by Added, Updated, and Deleted.
   b. To view the policies that include a specific check being updated, select the check in the list.

      A list of affected policies appears in the Related Policies pane.
4. (Optional) To view details about the policies affected:
   a. Click the **Policy Detail** tab.

      In the left pane is an alphabetical list of the policies affected by the update.

      Note: The list shows only those policies that are affected by updated checks. The Policy Detail tab does not show other policy changes that could be included in the update, such as associating new checks with a policy or changing a policy name.
   b. To view the checks being updated in a specific policy, select the policy in the list.

      A list showing the ID, Name, and Version of checks being updated appears in the Related Checks pane. The list is grouped by Added, Updated, and Deleted.
5. To install the updates, click **Download**.

Downloading checks without updating OpenText DAST

Engine updates are required for some checks to be run during scans. If you are not using the latest version of OpenText DAST, it is likely that some of the checks in your SecureBase cannot be run during a scan. To test your application with all the latest checks, ensure that you are using the latest version of OpenText DAST.

Performing an offline SmartUpdate

Follow this process to perform a SmartUpdate for OpenText DAST that is offline.

Stage	Description
1.	Open a support case. Customer Support personnel will provide you with the offline FTP server URL and login credentials (if needed). For more information, see Contacting Fortify Customer Support in "Preface" on page 21.
2.	On a machine that can access the Internet, access the offline FTP server.
3.	Download the OpenText DAST static SmartUpdate ZIP file.

Stage	Description
4.	On the machine where OpenText DAST is installed, extract all files from the ZIP file.
5.	Close OpenText DAST.
6.	Copy the extracted **SecureBase.db** and **version.txt** files to the directory where your SecureBase data resides. The default location is: `C:\ProgramData\HP\HP WebInspect\SecureBase` **Tip:** By default, these folders are hidden in Windows. Be sure to change folder options to show hidden files.

Chapter 12: SQL Injector (OpenText DAST only)

SQL injection is a technique for exploiting web applications that use client-supplied data in SQL queries without first removing potentially harmful characters. The SQL Injector supports MS-SQL, Oracle, Postgress, MySQL, and DB2 database types and also supports multiple language systems including Japanese.

Caution! This tool tests for SQL injection vulnerabilities by creating and submitting HTTP requests that may be processed by your SQL server. If your web application allows database records to be updated or created using data supplied by the user, the SQL Injector may create spurious records. To avoid this possibility, do not test against your production database. Instead, use a copy of the database, or use a test account that does not have access to the production data, or exclude from audit any pages that may update data or delete data from the database. If these alternatives are not feasible, back up your production database before testing at a time when the site has little or no customer traffic.

To test for susceptibility to SQL injection:

1. If using a proxy server or if the target site requires authentication, click the **Settings** tab and enter the appropriate information. For more information, see "SQL Injector settings" on page 116.
2. Select **File > New**

   - or -

   click the New Request icon  .
3. In the **Location** field, type or paste the URL that you suspect is susceptible to SQL injection. See examples below.
   - GET method (query parameters are embedded in the URL):
     http://172.16.61.10/Myweb/MSSQL/Welcome.asp?login=aaa&password=bbb
   - POST method (query parameters are included in message body):
     http://172.16.61.10:80/Myweb/MSSQL/Welcome.asp

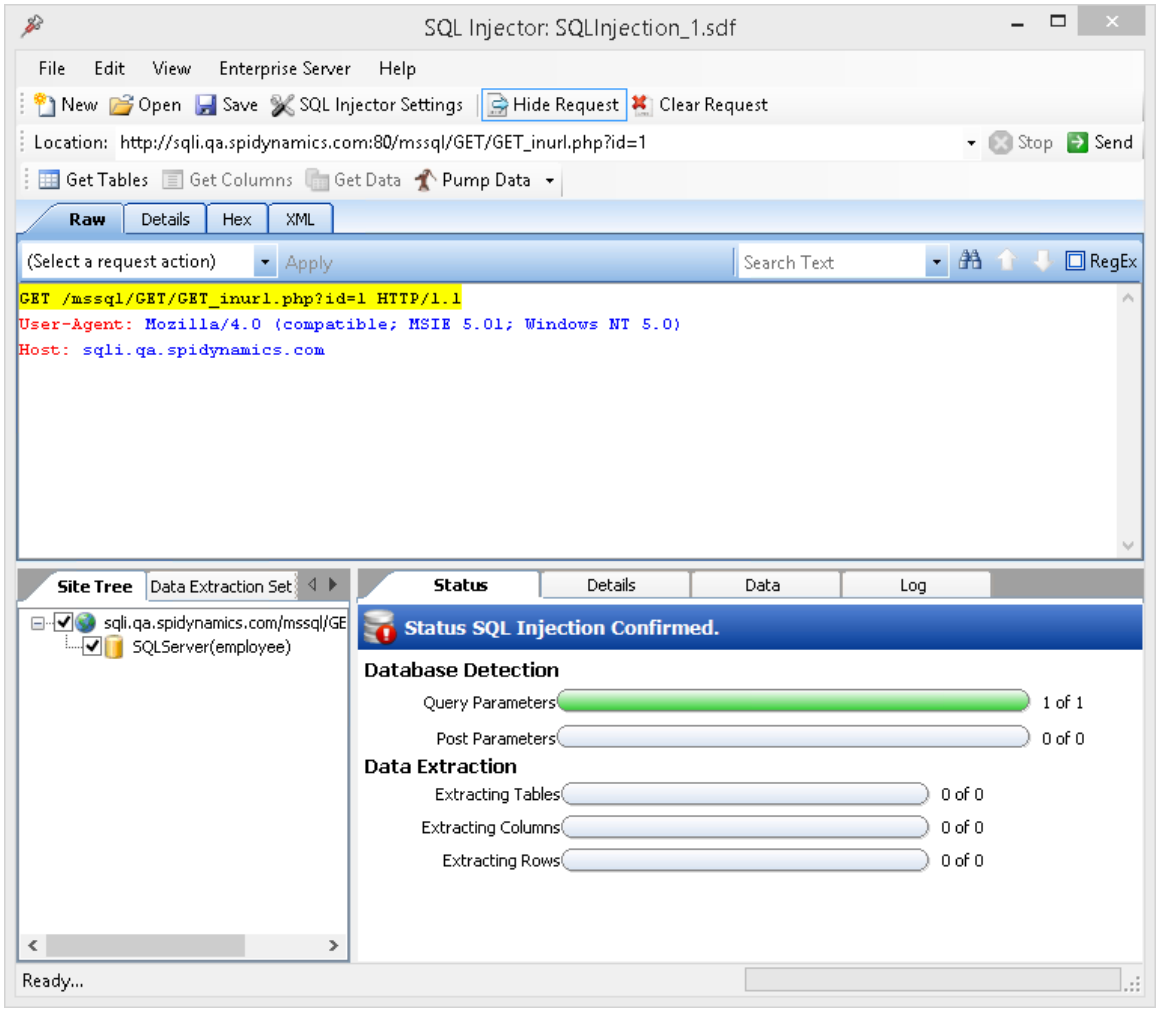
   Because the SQL Injector defaults to the GET method, you must also edit POST requests on the **Raw** tab (visible if you select **View > Show Request**). The edited request would be similar to the following:

```
POST /Myweb/MSSQL/POST/2.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 172.16.61.10
Content-Length: 22
Content-Type: application/x-www-form-urlencoded
login=qqq&password=aaa
```

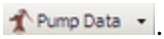
Note: If OpenText DAST has detected a SQL injection vulnerability, you can right-click the vulnerable session in OpenText DAST's navigation pane (or right-click the vulnerable URL on the **Vulnerabilities** tab of the summary pane) and select **Tools > SQL Injector** from the shortcut menu.

4. Click **Send**.

   If SQL injection is successful, "SQL Injection Confirmed" appears on the **Status** tab and the beginnings of a data hierarchy tree appear on the **Site Tree** tab in the lower left pane.



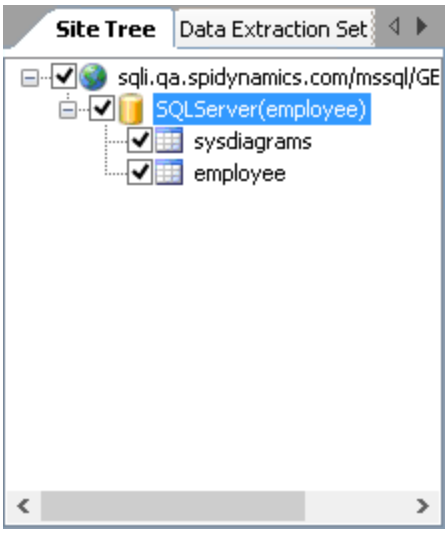
   For detailed information about the tabs on this screen, see "SQL Injector tabs" on page 115.

5. To extract all the data from all tables, click the **Pump Data** icon  .

   Alternatively, you can selectively investigate tables and columns using the following procedure:

   a. Select **Get Tables**.

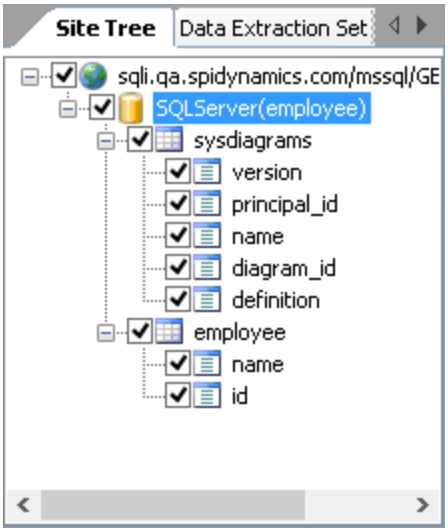
      The SQL Injector returns the names of all tables in the targeted database.



b. Choose tables by selecting or clearing their associated check boxes.

c. Click **Get Columns**.

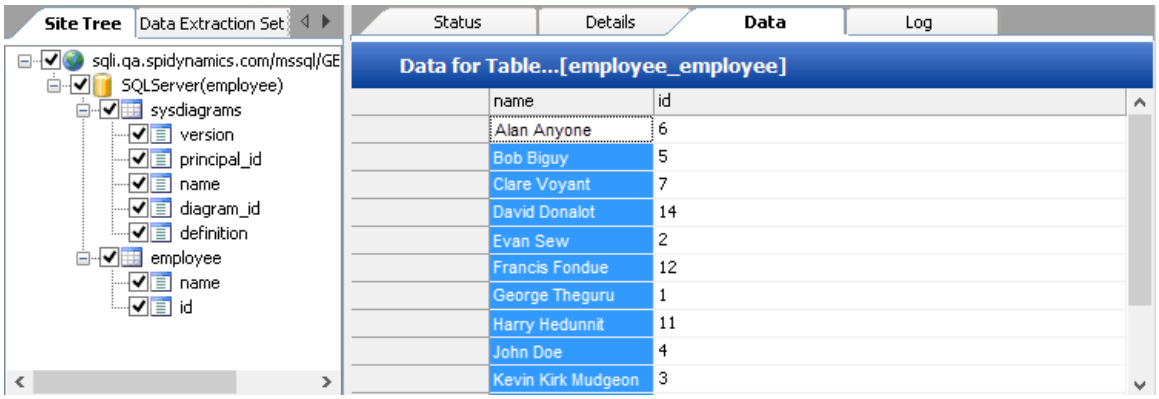
The SQL Injector returns the names of all columns in the selected tables.



d. Choose a column by selecting or clearing its associated check box.

e. Click **Get Data**.

6. Select a column and click the **Data** tab to view the column values.



Note: If the SQL Injector is unable to extract data, it may be able to verify the existence of a SQL injection vulnerability by retrieving the name of the vulnerable database. To enable this feature, see Inferential/Time-Based Extraction in the "SQL Injector settings" on the next page topic.

See also

"SQL Injector tabs" below

"SQL Injector settings" on the next page

SQL Injector tabs

After a successful SQL injection, the SQL Injector displays the following panes and tabs:

Request pane

The Request pane contains the following tabs:

- **Raw** - Displays the text of the HTTP request.
- **Details** - Displays the request segmented by method, request URI, and protocol. Also lists the request header fields and their associated values.
- **Hex** - Displays a hexadecimal representation of the HTTP request.

To toggle the display of the Request pane, click **Show Request**/**Hide Request**.

To delete the request, replacing it with the default http://localhost:80/, click **Clear Request**.

Database pane

The lower left pane contains the following tabs:

- **Site Tree** - Displays the URL, databases, tables, and columns.
- **Data Extraction Settings** - Displays the maximum number of tables, columns, and rows to return when extracting data. These values are extracted from the settings, but can be modified here or in the *Settings* dialog.

Information pane

The lower right pane contains the following tabs:

- **Status** - Displays progress bars for detection and extraction functions.
- **Details** - Displays database information and injectable parameter details.
- **Data** - Displays data extracted from the selected tables and columns.
- **Log** - Displays a synopsis of pertinent functions and the time at which they occurred.

SQL Injector settings

To modify the SQL Injector settings:

1. Click **Edit > Settings**.
2. Select one of the following tabs and specify settings as described in the following sections:
   - Options (See "Options tab" below)
   - Authentication (See "Authentication tab" on page 118)
   - Proxy (See "Proxy tab" on page 118)
3. Click **OK**.

Options tab

Timeout in seconds

Specify the number of seconds that the SQL Injector will wait for a response before terminating the session.

Apply state

If your application uses cookies, URL rewriting, or post data techniques to maintain state within a session, the SQL Injector will attempt to identify the method and modify the response accordingly.

Apply proxy

If you select this option, the SQL Injector will modify the request according to the proxy settings you specify.

Logging

Select the events you want to log:

- Requests
- Responses
- Errors
- Debug Messages

Log files are stored in xml format in `<drive>:\Users\<user name>\Documents\HP\Tools\SQLInjector\logs`.

The beginning of each file name is formatted as YYYY_MM_DD<current-process-id>. The remainder of the name is formatted as follows:

- _sqli_debug.log: Contains debugging messages for that session.
- _errors.log: Contains errors and exceptions that occurred for that session.
- _RequestsResponses.log: Contains all the requests and responses sent and received by the SQL Injector.

Data extraction

Specify the maximum number of tables, columns, and rows that should be returned when extracting data through a URL that is vulnerable to SQL injection. These values are also displayed in the Database pane on the **Data Extraction Settings** tab. You can change these values using either this tab or the *Settings* dialog.

Also specify the maximum number of concurrent threads that should be used for data extraction.

Inferential/time-based extraction

The SQL Injector can use two different techniques for extracting data when a SQL injection vulnerability is discovered. All attempts are conducted using the inferential technique, which examines the content of the HTTP responses. If this method fails, you can force the tool to use a second technique called time-based extraction. Instead of extracting table data, this method attempts to retrieve the name of the database by sending 4-5 long-running database queries for each character in the database name. Since this can be a rather time-consuming exercise, you can specify the number of characters required to confirm the existence of the SQL injection vulnerability.

Use a macro

If you want to use a macro, select this check box and then click the browse button  to select a macro.

Database file path

This read-only text box displays the path to the database created by the SQL Injector tool to store attack data and replicate portions of the attacked database.

Authentication tab

Authentication method

If the site does not require authentication, select **None**. Otherwise, select an authentication method from the **Authentication** list:

- **Automatic**

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

- **HTTP Basic**
- **NTLM (NT LanMan)**

Authentication credentials

Enter a user ID in the **User name** field and the user's password in the **Password** field. To prevent mistyping, repeat the password in the **Confirm Password** field.

Proxy tab

Use these settings to access the SQL Injector through a proxy server.

Direct connection (proxy disabled)

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

Auto detect proxy settings

If you select this option, SQL Injector will use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the browser's web proxy settings.

Use system proxy settings

Select this option to import your proxy server information from the local machine.

Use Firefox proxy settings

Select this option to import your proxy server information from Firefox.

Note: Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.

Configure a proxy using a PAC file

Select this option to load proxy settings from the Proxy Automatic Configuration (PAC) file in the file location you specify in the **URL** field.

Explicitly configure proxy

Select this option to access the Internet through a proxy server, and then enter the requested information:

1. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080).
2. Select a protocol **Type** for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or Standard.
3. If authentication is required, select a type from the **Authentication** list:
   - **Automatic**

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

   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NTLM (NT LanMan)**
4. If your proxy server requires authentication, enter the qualifying user name and password.
5. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass Proxy For** field. Use commas to separate entries.

Specify alternative proxy for HTTPS

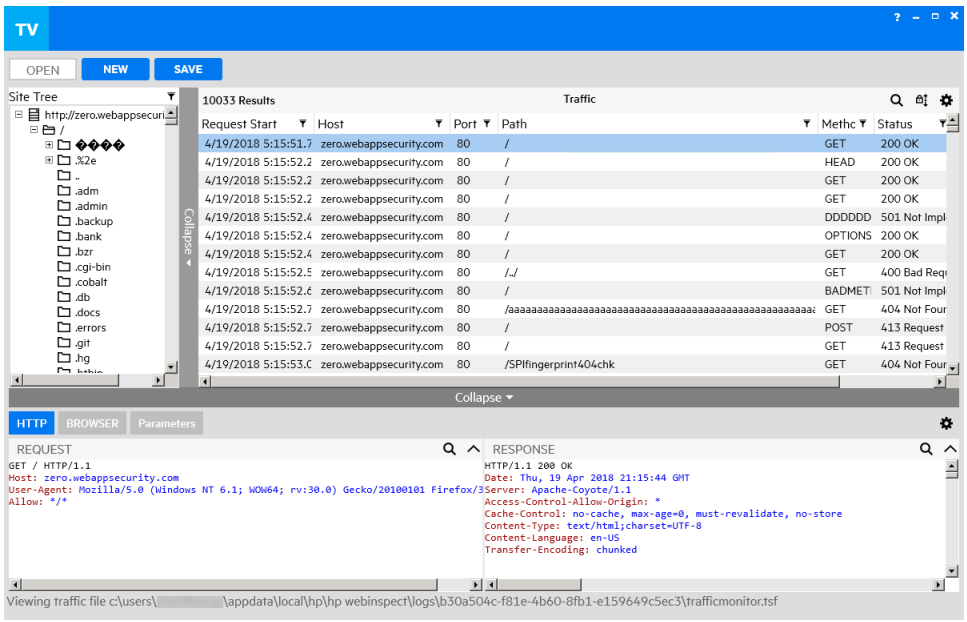
For proxy servers accepting HTTPS connections, select the **Specify Alternative Proxy for HTTPS** check box and provide the requested information.

Chapter 13: Traffic Viewer

OpenText DAST normally displays in the navigation pane only the hierarchical structure of the Web site or Web service, plus those sessions in which a vulnerability was discovered. The Traffic Viewer, however, enables you to display and review every HTTP request sent by OpenText DAST and the associated HTTP response received from the server.

Traffic Viewer image

The following image shows the Traffic Viewer displaying a traffic file from a scan.



Option must be enabled

To use the Traffic Viewer, you must enable the Traffic Monitor Logging option prior to running a scan. The Traffic Viewer is not available for a scan if the Traffic Monitor Logging option was not enabled prior to running the scan. See "Enabling Traffic Monitor" on the next page for more information.

Proxy server

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

You can also use this feature to create a Workflow macro or a Login macro that you can use with OpenText DAST.

Enabling Traffic Monitor

In OpenText DAST, you can enable the Traffic Monitor for all scans or for an individual scan.

Enabling the Traffic Monitor for all scans

To enable the Traffic Monitor in the Default Settings:

1. Click **Edit > Default Scan Settings**.
2. In the Scan Settings pane, click **General**.
3. Select **Enable Traffic Monitor Logging**.

   Note: The Traffic Viewer does not support the encryption of traffic files. The **Encrypt Traffic Monitor File** option is for use under special circumstances with legacy traffic files only.
4. Click **OK**.

Enabling the Traffic Monitor for individual scans

To enable the Traffic Monitor when you start a scan through the Scan Wizard, do one of the following:

- Select **Settings (Default)** at the bottom of the Scan Wizard and follow steps 2 through 4 of "Enabling the Traffic Monitor for all scans" above.
- In the Detailed Scan Configuration window of the Scan Wizard, select **Enable Traffic Monitor**.

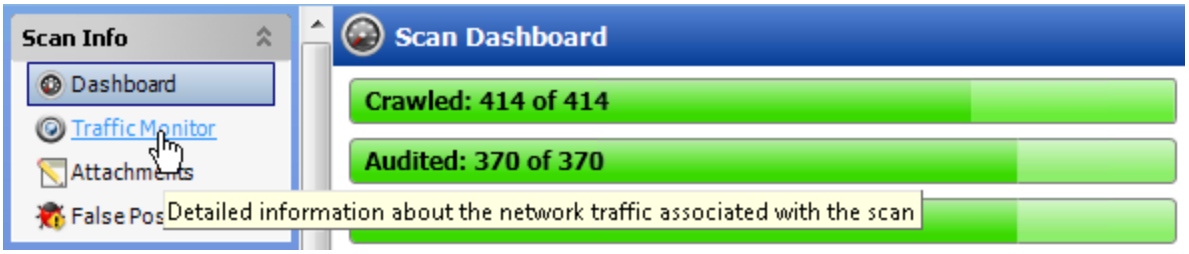
Launching the Traffic Viewer

You can launch the Traffic Viewer from the Scan Info Panel within an open scan in OpenText DAST and Fortify WebInspect Enterprise. Launching the tool in this manner opens the Traffic Viewer with a traffic file in view. You can also open the tool as a stand-alone tool outside of a scan and without any traffic or proxy data in view.

From an open scan

To launch the Traffic Viewer from an open scan in OpenText DAST and Fortify WebInspect Enterprise:

- In the Scan Info panel, click **Traffic Monitor**



Note: The Traffic Viewer is not available if Traffic Monitor Logging was not enabled prior to conducting the scan.

As a stand-alone tool

To launch the stand alone Traffic Viewer, do one of the following:

- In OpenText DAST, click **Tools > Traffic Viewer**.
- In the Fortify WebInspect Enterprise Admin Console, click **Tools > Traffic Viewer**.

The Traffic Viewer is launched without any traffic or proxy data in view.

Note: You may also launch the Traffic Viewer from your Windows Start menu.

Using the interface

This section describes how to open existing files, use the Site Tree, customize grid and detail views, resize user interface (UI) elements, and use auto scroll.

Opening an existing file

You can open the following types of existing files in the Traffic Viewer to examine sessions:

- Traffic session files (`.tsf`)
- Legacy proxy session files (`.psf`)
- Burp proxy files
- HTTP archive (`.har`) files

Note: If you open a legacy proxy session file (`.psf`), Traffic Viewer will convert it to a traffic file (`.tsf`).

To open an existing file:

1. Click **OPEN**.
   The Open dialog box opens.
2. From the drop-down list, select the type of file to open.
3. Navigate to and open the file.
   The sessions are populated in the Traffic Viewer.

Using the Site Tree

By default, the Site Tree displays an unfiltered tree view of all traffic that was generated during the scan. The tree includes a list of hosts and all sub-directories within those hosts. In this view, you can select a top-level host and expand the sub-directories to examine the requests and responses occurring at each level. You can select an item in the Site Tree to display the traffic for the item.

Site Tree icons

The following table identifies the icons displayed in the Site Tree.

Icon	Name	Represents
	Server/host	The top level of your site's tree structure
	Folder	A directory
	Page	A file

Viewing traffic for a resource

You can view the traffic for a resource in the Site Tree. To view the traffic for an item:

- Select the item in the **Site Tree**.
  All traffic involving that item appears in the Traffic grid.

For more information, see "Working with sessions" on page 129.

Viewing only host names

To view a list of only the host names:

- From the default tree view, click the filter icon once.

  The Site Tree displays only the host names. Sub-directories are not accessible in this view. From this view, you can select one or more hosts and filter out the rest. See "Filtering for selected hosts" below.

To return to viewing the entire tree:

- Click the filter icon again.

Filtering for selected hosts

To focus your research, you can filter for specific hosts in the Site Tree. To view only selected hosts and their sub-directories in the Site Tree:

1. With the Site Tree displaying only the host names, select one or more hosts to view.
2. Click the filter icon.

   Only the selected hosts appear in the Site Tree.
3. Expand a host to display its sub-directories.

Viewing all host names

To return to viewing all host names:

1. Click the filter icon.

   The Site Tree displays only the host names with the previously viewed hosts selected.
2. Click each selected host to clear its selection.
3. Click the filter icon.

   The Site Tree displays an unfiltered tree view of all traffic.

See also

"Resizing, collapsing, and expanding UI elements" on page 127

Customizing grid views

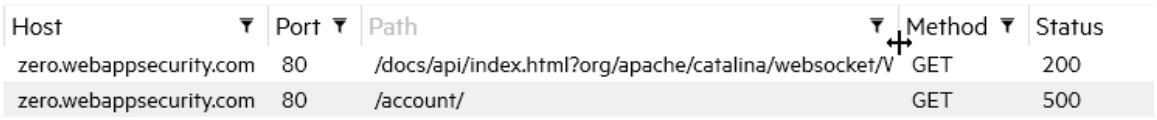
You can resize, reposition, add, and remove columns displayed in grid views.

Resizing columns

To resize a column:

1. Move your cursor to the border to the right of the column heading you want to resize.

   Your cursor becomes a double-headed arrow and the column heading background color changes to a lighter gray.



2. Do one of the following:
   - Drag the column border either right or left to the width you want.
   - Double-click the border to resize the column to the width of the widest amount of data in the column. A horizontal scroll bar might be added to the bottom of the window.

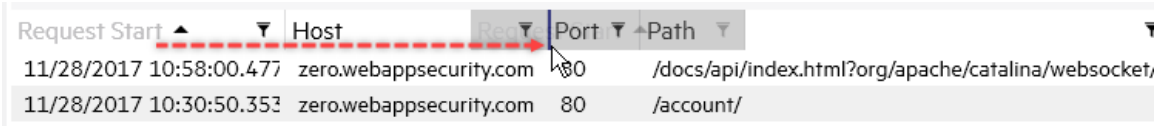
Repositioning columns

To rearrange the order of the columns across the grid:

1. Move your cursor to the column heading that you want to move.

   The column heading background color changes to a lighter gray.
2. Click once.

   The column heading background color changes to white.
3. Drag the column to the right or left into the position you want it.



   The column of data is moved and the remaining columns are shifted right or left by one column.

Adding/removing columns

By default, not all columns of data are displayed in the grid. Grid view settings allow you to select which columns of data you want visible in the grid. To add or remove displayed columns:

1. In the grid view, click  .

   A list of available columns appears.

   Note: The column names indicate the memo headers that are generated during a scan.
2. Do the following:
   - Select the check box for each column you want to add to the display.
   - Clear the check box for each column you want to remove from the display.

3. Click anywhere outside the list of columns to close the list.
   The displayed columns are updated.

Customizing detail views

You can choose the layout and color theme for non-grid detail views, and you can hide or show the HTTP detail views.

Changing the layout

When two detail views are visible for an item, such as the Request and Response detail views, you can rearrange the placement of the detail views to have them stacked vertically (one on top of the other) or have them aligned horizontally (side-by-side). To change the layout:

1. In the detail view, click ⚙.
   The settings menu opens.
2. Do one of the following:
   - To align the detail views vertically one on top of the other, click **Vertical Layout**.
   - To align the detail views horizontally side-by-side, click **Horizontal Layout**.

Changing the color theme

The default color theme is black and colored text on a white background. However, you might prefer white and colored text on a black background. To change the color theme:

1. In the detail view, click ⚙.
2. Do one of the following:
   - To use black and colored text on a white background, click **Light Theme**.
   - To use white and colored text on a black background, click **Dark Theme**.

Hiding and showing HTTP detail views

You can collapse (or hide) one of the HTTP detail views, such as the Request or Response detail view, so that only the contents of other HTTP detail view is visible.

To hide a detail view:

- Click the hide icon (^) in the detail view.

To show a hidden detail view:

- Click the show icon (v).

Resizing, collapsing, and expanding UI elements

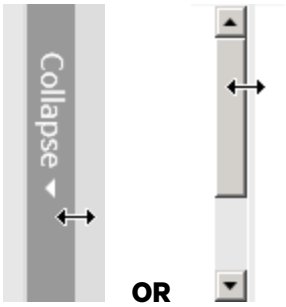
You can resize, hide (or collapse), and show (or expand) certain user interface (UI) elements, such as a site tree or a grid view of data.

Resizing an element

To resize an element, do one of the following:

- For UI elements with a horizontal layout of data, such as a grid view, drag the horizontal Collapse bar to widen or narrow the element.

- For UI elements with a vertical layout of data, such as a site tree, drag the vertical Collapse bar or the scroll bar to widen or narrow the panel.



OR

Collapsing an element

To collapse an element:

- Click **Collapse**.

Expanding an element

To expand an element:

- Click **Expand**.

Using auto scroll

Enabling auto scroll causes the traffic grid to scroll up as new sessions are added so that the newest traffic sessions are always visible. The auto scroll feature is only applicable when you are working with a scan that is currently running.

Enabling auto scroll

To enable auto scroll:

- Click the scroll lock icon ( ).

Disabling auto scroll

You may want to pause auto scroll to examine a session in the Traffic grid. To disable auto scroll:

- Click the scroll lock icon ( ).

Note: You can resume auto scroll at any time during the active scan.

Working with traffic

This section describes how to explore traffic, work with sessions and parameters, search and filter traffic data, and use regular expressions.

Exploring traffic

By default, the Traffic grid displays all traffic generated during the scan, allowing you to explore the traffic for the entire scan. However, you can also view and explore traffic for a specific resource. You can search, sort, and filter the data in the Traffic grid. For more information, see "Searching and filtering" on page 133.

Viewing traffic for a resource

You can view the traffic for a resource in the Site Tree. To view the traffic for an item:

- Select the item in the **Site Tree**.
  All traffic involving that item appears in the Traffic grid.

Using the breadcrumbs

When you select a resource in the Site Tree, breadcrumbs appear at the top of the traffic grid, similar to the sample shown here.

These breadcrumbs indicate that the displayed traffic has been filtered down to the last resource listed in the breadcrumbs.

To filter the traffic for a specific resource listed elsewhere in the breadcrumbs:

- Click the resource in the breadcrumbs.

  For example, if you want to view all traffic for the resources folder shown in the previous image, click **resources**.

  The selected resource becomes the final breadcrumb and the traffic sessions are updated to show only the traffic for the selected resource.

To remove the filter completely:

- Click **X** in the final breadcrumb.

  The breadcrumbs are removed and the traffic sessions are no longer filtered.

See also

"Working with sessions" below

"Drilling down into traffic data" on page 132

Working with sessions

You cannot modify data you are viewing in a traffic file from a scan. You can, however, research the traffic data in the Traffic Viewer to get a better understanding of what happened during the scan. For example, you can resend a request using the HTTP Editor or you can view the session in a browser.

Viewing the HTTP detail

You can view the request and response of a session in the HTTP detail view. This view is the default view for sessions selected in most grids. However, if you are seeing another detail view and want to see the request and response instead, you can switch to the HTTP detail view. To view a session in the HTTP detail view:

1. Select a session in the grid.
2. Click **HTTP**.

   The HTTP detail view opens, showing the request and response of the selected session.

Wrapping text

Long lines of text in the detail views, such as in the Request and Response detail views, might make it impossible to view the content without using the horizontal scroll bars. You can use the Word Wrap setting to wrap the text to prevent the horizontal scroll bars. The Word Wrap setting is available in each detail view and is not a global setting for all detail views. The Word Wrap setting is saved in your user settings file for each detail view, and is the default behavior for the detail view the next time you open the application.

To wrap text:

- Right-click the detail view and select **Word Wrap**.
  The long lines of text are wrapped and the horizontal scroll bar is removed.

Decoding percent-encoded characters

By default, requests and responses use percent-encoding for reserved characters. If you see percent-encoded characters, such as `%3B` and `%40`, in the text of a request or response, you can decode these characters to improve readability of the text. When you decode the characters in a request or response, the requests or responses for all parent and child sessions of the selected session will also be decoded. These characters remain decoded only while the scan is open. If you close the scan and reopen it, the default display applies, and reserved characters will once again be percent-encoded.

To decode percent-encoded characters:

- Right-click in the **RESPONSE** or **REQUEST** tab and select **URL Decode**.
  The percent-encoded characters are converted to readable text.

Resending a request

You can resend a request using the HTTP Editor. To resend a request:

1. Select a session in the grid to view the request and response.
2. If the HTTP detail view is not open, click **HTTP**.
3. Right-click in the **REQUEST** detail view and select **View in HTTP Editor**.
   The HTTP Editor opens for the request. For more information about using the HTTP Editor, see the HTTP Editor online help or the HTTP Editor chapter in the *OpenText™ Dynamic Application Security Testing Tools Guide*.

Viewing a session in the browser

You can view a session in the Browser detail view to see where the traffic occurred in your site. To view a session in the Browser:

1. Select a session in the grid.
2. Click **BROWSER**.
   The Browser detail view opens showing the selected session.

Expanding compressed content

Compressing (or minifying) content removes spaces, new line markers, comments, and block delimiters from code to reduce file size. However, the practice also makes the content more difficult for humans to read. You can use the Beautify setting to expand compressed text. The Beautify setting is available in each detail view and is not a global setting for all detail views. The Beautify setting is saved in your user settings file for each detail view, and is used as the default behavior for the detail view the next time you open the application.

To expand compressed content:

- Right-click in the detail view and select **Beautify**.

  The compressed content is expanded and becomes more readable.

  Note: Some text cannot be beautified, so you might not see the option.

See also

"Working with parameters" below

Working with parameters

You can view the Type, Name, and Value for parameters used in a traffic session. The Parameters detail view displays a grid with one record for each cookie or query string used in the traffic session. You can also view every traffic record in which the same parameter is used. You can access the Parameters detail view from the Traffic and Related Traffic grids.

Understanding parameters

A parameter can be one of the following:

- Cookie data
- A query string submitted as part of the URL in the HTTP request (or contained in another header)
- Data submitted using the Post method (such as set_<parametername>)

Viewing parameter details

To view the parameter details for a session:

1. Select a session in the Traffic or Related Traffic grid.
2. Click **PARAMETERS**.

The Parameters detail view opens showing the parameters used in the selected session.

Note: The detail view layout settings have no effect on the Parameters grid.

Adding parameter columns to traffic grid

You can add columns to the Traffic grid to display a parameter that is listed in the Parameters detail view. Adding these columns of data to the Traffic grid is useful when you are working with a workflow macro and need to follow a state parameter through the sessions to determine when and why you are being logged out of the application.

For example, you might want to view the values for the JSESSIONID parameter to examine it from session to session to see where its value changes. You can add a column for the JSESSIONID parameter along with its companion column set_JSESSIONID to show where the value changes.

To add columns for a parameter:

1. Right-click the row for the parameter in the Parameters detail grid.
2. Select **Build Columns...**.

   Note: If you have previously added columns for the selected parameter, the Build Columns option is unavailable.

A column for the parameter name is added to the Traffic grid, along with a column for any methods that set the parameter value, if applicable. These columns are permanently added to the database for the current scan. The column names are also added to the grid settings menu. You can use the grid settings menu to add or remove the columns from view. See "Adding/removing columns" on page 125.

Drilling down into traffic data

You can view traffic for a resource in the Site Tree, and then drill down to view related traffic for a session in the Traffic grid view.

Viewing traffic for a resource

You can view the traffic for a resource in the Site Tree. To view the traffic for an item:

- Select the item in the **Site Tree**.

  All traffic involving that item appears in the Traffic grid.

Viewing related traffic for a session

You can view the related traffic for a session in the Traffic grid.

To view related traffic for a session:

- Double-click a session in the **Traffic** grid.

  The Related Traffic grid appears. If parent traffic sessions are available, you can click through the list of parents and see the HTTP and browser detail views for them.

To return to the Traffic grid:

- Click the vertical **Traffic** title bar.

  The Traffic grid appears displaying all traffic.

  For more information, see "Working with stacked grids" below.

Working with stacked grids

When you drill down into grid data, an additional grid opens with a vertical title bar. When you drill down through multiple layers of grid data, each new grid is stacked on the previous grid with its vertical title bar visible. The following example shows three stacked grids.

Note: Not all applications include all of the grids shown above.

Viewing and closing stacked grids

You can view a specific grid in the stack by closing any grids stacked on it. You can also close all stacked grids at once.

To view a specific grid in the stack:

- Click the title bar of the grid you want to view.
  All grids stacked on the one you want to view are closed.

To close all stacked grids:

- Click the leftmost grid title bar.
  All stacked grids are closed.

See also

"Customizing grid views" on page 124

Searching and filtering

You can search on the data displayed in grid views and in most non-grid views. You can also sort and filter on each column displayed in a grid. If an active scan is being viewed, you can search, filter, and sort on live data in the scan that is running. For more information about formatting search queries, see "Understanding the search expressions" on page 136.

Searching in grid views

You can search for data in a single column or in multiple columns displayed in a grid. To search on the data displayed in a grid:

1. Click the search icon ( ).
2. In the **Search** field, type the column name (without spaces), the operator, and the value you are searching for.

Examples:

```
Status='404 Not Found'
ResponseStart>'9/4/2015 9:08:52.242 AM'
Status~'3[0-9][0-9].*'
```

3. (Optional) To search on multiple columns, press the **Space Bar**, type the next column name (without spaces), the operator, and the value you are searching for. Searching on multiple columns is treated as an AND search; only records that include search criteria specified for each column will be displayed. Repeat for each column that you want to search.

   Example:

   ```
   Method=GET Status~'3[0-9][0-9].*'
   ```

4. Press **Enter** or click  .

You can also use regular expressions to search for patterns in the grid. For more information, see "Understanding the search expressions" on page 136.

Searching in non-grid views

You can search for data in non-grid views, such as in the Request and Response tabs. To search in tabs:

1. Select a row of data in the grid.

   Details for the selected data appear in the associated tab(s), such as in the Request and Response tabs.
2. Type the value you are searching for in the tab search field.
3. (Optional) To use regular expressions in your search criteria, select the **RegEx** check box. For more information, see "Understanding the search expressions" on page 136.
4. Press **Enter**.

Clearing the search

To clear the search criteria, click the **x** in the search icon.

Sorting in the grid

To sort by any column in the grid:

- Click the column heading.

Filtering in the grid

To filter on one or more columns in the grid:

1. Click  in the column heading.

   A filter panel appears below the column heading.
2. Type a filter expression in the filter field.

A filter expression consists of an optional operator (>,<,>=,<=,!=,~,=) or one of the functions "in", "notin", or "regex" followed by a string. The range operator (..) is an exception, as it sits between two strings. For more information, see "Understanding the search expressions" on the next page.

Examples:

```
443
'400 Bad Request'
30*
'9/3/2015 10:53:08.000 AM'..'9/3/2015 10:53:12.089 AM'
in(200,300) notin(400,500)
```

Note: The equal (=) operator may not filter accurately on columns containing date and time information.

For more information, see "Rules for filtering in the grid" below.

3. Press **Enter**.

   Data in the grid is filtered based on the expression entered. The icon in the filtered column heading changes to  .

4. To filter on additional columns, repeat steps 1-3 on each column.

Rules for filtering in the grid

The following rules apply to filtering in the grid:

- You do not need to specify the field name. Since you edit the filter in a specific column, the field name is identified implicitly.
- You can use search operators in the filter field. For more information, see "The Operators" on page 138.
- If no operators or wild cards are specified in the filter field, the filter is converted to a "contains" clause of the form `field:*string*`. If the search is enclosed in quotation marks, the filter is converted to `field:'*string*'`.

  For example, the filter string `404 Not Found` in the Status column is converted to `Status:'*404*' Status:'*Not*' Status:'*Found*'` and displays all sessions with a Status that contains either 404, Not, or Found. The filtered results would include such statuses as '302 Found', '404 Not Found', and '405 Method Not Allowed'.

  The filter string `'404 Not Found'` in the Status column is converted to `Status:'*404 Not Found*'` and displays all sessions with a Status that contains '404 Not Found'.
- You can specify multiple search filters in the filter field, separated by spaces.
- Filters on date and time fields must be enclosed in either single (') or double (") quotation marks.

Clearing a filtered view

To clear a filtered view on one or more columns in the grid:

1. Click in a column heading that is filtered.
   A search panel appears below the column heading.
2. Click **Clear**.
   Data in the column is no longer filtered.
3. To clear the filter on additional columns, repeat steps 1 and 2 on each filtered column.

Understanding the search expressions

This topic explains the components of the expressions used to search in the grid and tabs.

Basic Format of a Query

The basic format of a search query is:

<PropertyName><Operator><SearchValue>

If you are searching the entire grid, the PropertyName is the column name that you wish to include in the search. If you are searching in a tab, such as the Request or Response tabs, the PropertyName is the field/property name, such as 'Request' or 'Response'.

If you are searching within a column in the grid, omit the PropertyName. The format for this type of search is:

<Operator><SearchValue>

To use regular expression (RegExp) syntax in your search, the format is:

<PropertyName> RegExp('[*RegexSearchValue*]','[*RegexFlags*]')

For more information about using regular expressions, see "Using regular expressions" on page 139.

Simple Query

You can perform a simple query on string data that contains no special characters and on integers. Simple queries are:

```
Method=GET
```

```
Scan.CheckId=6
```

Show me on YouTube™.

Searching for Data that Contains Spaces or Special Characters

If there is a space or special character in the content you are searching for, enclose the content in either single (') or double (") quotation marks:

```
Status='404 Not Found'
```

```
Path='/signin.html'
```

Show me on YouTube™.

The quotation marks can be combined with wildcards:

```
ResponseStart:*'7/8/2015 4:22:'*
```

Searching with More than One Expression

A search can include more than one expression at the same time, with the expressions separated from each other by a space:

```
Path='/banklogin.asp' Method=GET
```

Show me on YouTube™.

If the same field is listed more than once, it becomes an "OR" expression:

```
Path='/banklogin.asp' Path='/login1.asp'
```

This search would return all records where Path is either '/banklogin.asp' or '/login1.asp'.

Other fields added to the expressions are treated as an "AND" expression:

```
Path='/banklogin.asp' Path='/login1.asp' Method=POST
```

This search would return all records where Path is either '/banklogin.asp' or '/login1.asp' AND Method is 'POST'.

Another example of an AND/OR search is:

```
Method=POST Scan.Engine:Sql* Scan.Engine:Cross*
```

This search would return all records where Method is 'POST' and the value of Scan.Engine starts with either 'Sql' or 'Cross'.

Show me on YouTube™.

Searching for Null Data

To search for data that contains null (empty) entries, use the = operator followed by two single quotation marks (''):

```
ParameterValue=''
```

To filter for data that contains null (empty) entries in a specific column, use the = operator followed by two single quotation marks ('') in the column filter field.

Show me on YouTube™.

Using Column Names in Search Queries

To search on a column or field name that includes a space, remove the space in the search query. For example, to search on the Response End column in the grid, use the following format:

```
ResponseEnd='7/8/2015 4:22:52 PM'
```

Using Regular Expressions

To search for patterns, you can use the regular expression operator (~) and include regular expressions in the search:

```
Response~'[0-9].*='
```

Show me on YouTube™.

You can also construct regular expression syntax:

```
Response RegExp('[0-9].*=','i')
```

For more information about using regular expressions, see "Using regular expressions" on the next page.

The Operators

The following table describes the operators and functions available for use in searching and filtering. The PropertyName used in the example column would be the column name when searching the grid or the field/property name when searching tabs. If you are filtering directly in a column, do not include the field/property name in the column filter field.

Operator	Description	Example(s)
=	Find only exact matches to the search string	`PropertyName=asdf`
>	Find data greater than the search number or date	`PropertyName>123`
>=	Find data greater than or equal to the search number or date	`PropertyName>=123`
<	Find data less than the search number or date	`PropertyName<123`
<=	Find data less than or equal to the search number or date	`PropertyName<=123`
!=	Find data not equal to the search string	`PropertyName!=asdf`
:	Find only exact matches to the search string using wildcards; search is case sensitive If the search string contains a space or dash (-), it must be enclosed in either single or double quotation marks.	`PropertyName:asdf` (find exact matches) `PropertyName:*asdf` (find data that ends with search string) `PropertyName:*asdf*` (find data that

Operator	Description	Example(s)
		contains search string) `PropertyName:asdf*` (find data that starts with search string)
..	Find data that is within a specified range of values	`PropertyName:'7/15/2015 5:00 PM'..'7/15/2015 5:15 PM'`
~	Find the search string using regular expressions For more information about using regular expressions, see "Using regular expressions" below.	`PropertyName~'sea[a-z]ches'`
in	Find matches to the search value(s) listed in parentheses; to search for multiple values, include a comma-separated list in parentheses Show me on YouTube™.	`PropertyName in(123,456)` or `PropertyName in(abc,def)` `Port in(80,443)` (find all sessions with a port of 80 or 443) `Method in(GET)` (find all sessions with a method of 'GET')
notin	Find everything except the search value (s) listed in parentheses; to exclude multiple values, include a comma-separated list in parentheses Show me on YouTube™.	`PropertyName notin(123,456)` or `PropertyName notin(abc,def)` `Port notin(80,443)` (exclude all sessions with a port of 80 or 443) `Method notin(GET)` (exclude all sessions with a method of 'GET')

Using regular expressions

Using the tilde (~) operator with a regular expression means that whatever is on the left of the tilde is searched using the regular expression on the right. You can also construct more complex regular expression (RegExp) syntax.

Traffic string properties for searching

You can use regular expressions to search any of the Traffic string properties, which are numbers, strings, or dates. This includes all fields that are listed when you click the settings icon (⚙) in a

Traffic grid view.

Using the tilde (~) operator

When using the tilde (~) operator, the format is:

<*PropertyName*>~'*RegexPattern*'

You can use single or double quotation marks.

Examples

The following query returns a list of sessions with a Referer in the request header that contains an index.jsp file:

```
Request~'Referer:\\s.+/index\\.jsp'
```

The following query returns a list of sessions with a Location in the response header that contains an index.php or index.html file:

```
Response~'Location:\\s.+/index\\.(php|html)'
```

The following query returns a list of sessions with index.html or index.php files that were attacked by an audit engine whose name begins with 'Cross' or 'Sql':

```
Path~'/index\.(html|php)' Scan.Engine~'^(Cross|Sql)'
```

Using RegExp syntax

RegExp syntax, which is similar to JavaScript, uses the following formats:

<*PropertyName*> RegExp('*RegexPattern*') - Performs a case-sensitive search

<*PropertyName*> RegExp('*RegexPattern*','*i*') - Performs a case-insensitive search

Examples

The following query returns a list of sessions with a Referer in the request header that contains an index.jsp file:

```
Request RegExp('Referer:\\s.+/index\\.jsp','i')
```

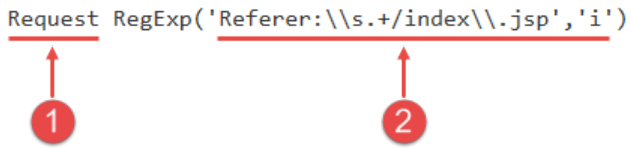
The following query returns a list of sessions with a Location in the response header that contains an index.php or index.html file:

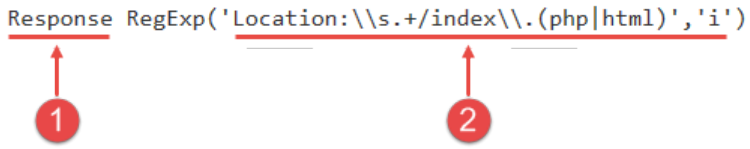
```
Response RegExp('Location:\\s.+/index\\.(php|html)','i')
```

Show me on YouTube™.

Understanding the RegExp syntax

The following diagrams define the parts of the RegExp syntax.





Item	Description
1	Specifies whether raw HTTP Request or raw HTTP Response data is searched; includes both Header and Body data
2	Defines the regular expression pattern to search for using the regular expression characters described in the table below

Regular expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the Regular Expression Library online at http://regexlib.com/Default.aspx.

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /\n/ matches a linefeed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/[^(en|ca)].*/.* . Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."

Character	Description
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
|	Indicates OR between two or more literal text search terms. For example, the following query will return a list of sessions where the path contains /index.html OR /index.php: `Path~'/index\.(html|php)'`

i	Ignores character case. Use this character in the second argument in the RegExp. For example:
	`PropertyName RegExp('stuff[abc]','i')`
	You can combine this with other flags. For example:
	`PropertyName RegExp('stuff[abc]','mi')`

m	Searches in multi-line mode. Use this character in the second argument in the RegExp. For example:
	`PropertyName RegExp('stuff[abc]','m')`
	You can combine this with other flags. For example:
	`PropertyName RegExp('stuff[abc]','mi')`

[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never early."
\B	Matches a non-word boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a non-digit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a linefeed character.

Character	Description
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v]
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any non-word character. Equivalent to [^A-Za-z0-9_].

The Traffic Viewer proxy

This section describes how to start proxy mode, create a new proxy file, and configure the Traffic Viewer proxy settings.

Using the Traffic Viewer proxy

You can create a new proxy file using the Traffic Viewer in proxy mode. This file can be saved as a traffic file or as a macro. For example, you may want to record the login process for your website and save the captured data as a login macro.

Starting proxy mode

To start proxy mode, do one of the following:

- While viewing traffic data from an open scan, click **NEW**.
- After launching the Traffic Viewer from the Tools menu (or the Toolkit in Fortify WebInspect Enterprise), click **OPEN** to view a previously recorded proxy file or click **NEW** to create a new one.

  The proxy tool buttons appear at the top of the window.

Creating a new proxy file

To create a new proxy file:

1. Click **NEW**.

   The proxy tool buttons appear at the top of the window.
2. To begin recording the proxy file, click **START**.
3. Click **BROWSE**.

The tool launches the TruClient with Firefox browser.

4. In the browser, navigate to the portions of your site that you wish to view in the proxy file.

   Traffic coming through the proxy populates the grid in the Traffic Viewer.
5. When you are finished, click **STOP**.
6. Do one of the following:
   - To save the proxy file as a traffic file (`.tsf`), click **SAVE**.
   - To save the proxy file as a macro (`.webmacro`), click the **SAVE** drop-down menu and select **as Macro**.

Configuring the proxy listener

A proxy listener is a local HTTP proxy server that listens for incoming connections from your browser. You configure the Proxy Listener on the settings page. Click  to access the settings.

To configure the proxy listener:

- In the GENERAL area, type the **Local IP Address** and **Port** number for the proxy listener.

Note: By default, the proxy uses localhost (IP address 127.0.0.1) and port 8080, but you can change this if necessary.

To configure Web Proxy on your host to be used by another host, you will need to change the value of the Local IP Address. The default address of 127.0.0.1 is not available to outside hosts. If you change this value to your workstation's current IP address, remote stations can use your workstation as a proxy.

Both the proxy and your Web browser must use the same IP address and port. These settings are automatically applied to the browser when you use the Browse button in proxy mode. If you launch the browser outside of the Traffic Viewer, the settings are not applied.

Configuring the proxy

You configure the proxy settings in the application settings. Click  to access the settings.

To configure the proxy:

1. Select from the options in the **PROXY** section. The options are described in the following table.

Option	Description
Direct Connection (proxy disabled)	Select this option if you are not using a proxy server.
Auto detect proxy settings	Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's web proxy settings.
Use System proxy settings	Import your proxy server information from the local machine.
Use Firefox proxy settings	Import your proxy server information from Firefox. **Note:** Using browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy server will not be used.
Configure proxy using a PAC file	Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the **PAC File URL** field.
Explicitly configure proxy settings	To configure a proxy, provide the following information: a. From the **Type** list, select a protocol type for handling TCP traffic through a proxy server: Socks4, Socks5, or Standard. b. If authentication is required, select one of the following types from the **Authentication Type** list: ◦ **Automatic** ◦ **Basic** ◦ **Digest** ◦ **Kerberos** ◦ **Negotiate** ◦ **NTLM (NT LAN Manager)** c. In the **Server** field, type the URL or IP address of your proxy server, followed (in the **Port** field) by the port number (for example, 8080). d. If your proxy server requires authentication, type credentials in the **User Name** and **Password** fields.

Option	Description
	e. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), type the addresses or URLs in the **Bypass proxy for** field. Use commas to separate entries.

2. Click **SAVE**.

Configuring client certificates

Configure client certificates in the Traffic Viewer proxy settings. Click to access the settings.

To enable client certificates and specify a certificate to use:

1. In the CLIENT CERTIFICATES area, select **Enable Client Certificates**.
2. Select the **Certificate Store** for the certificate you want to use. Options are:
   - Local Machine - The certificate store that is local to the computer and is global to all users on the computer.
   - Current User - The certificate store that is local to the current user account on the computer.

     Note: Certificates used by a common access card (CAC) reader are user certificates and are stored under Current User.
3. Do one of the following:
   - To select a certificate from the "Personal" ("My") certificate store, select **My** from the drop-down list.
   - To select a trusted root certificate, select **Root** from the drop-down list.
4. Does the website use a common access card (CAC) reader?
   - If *yes*, do the following:
     i. Select a certificate that is prefixed with “(SmartCard)” from the **Certificate** list.

     Information about the selected certificate and a Pin field appear in the Certificate Information area.

     ii. If a PIN is required, type the PIN for the CAC in the **Pin** field.

     iii. Click **Test**.

     If you entered the correct PIN, a Success message appears.
   - If *no*, select a certificate from the **Certificate** list.

     Information about the selected certificate appears below the Certificate list.
5. Click **SAVE**.

Configuring proxy exclusions

You may not want certain types of files, such as image files or PDFs, to be included in the proxy data. You can exclude them from being recorded. Excluding these files enables you to focus on HTTP request/response lines and headers by removing clutter from the message body. Exclude these files in the Traffic Viewer proxy settings. Click to access the settings.

To exclude file types:

1. In the DO NOT RECORD area, use regular expressions to type the file extension(s) that you want to exclude from capture in the proxy file.

   Example:

   .*\.jpg$,.*\.png$,.*\.bmp$

   For more information, see "Using regular expressions" on page 139.
2. Click **SAVE**.

Configuring search and replace

Search and replace enables you to create rules for locating and replacing text or values in HTTP messages coming through the proxy. This feature provides a highly flexible tool for automating your simulated attacks. Some suggested uses include:

- Masking sensitive data, such as user names and passwords
- Appending a cookie to each request
- Modifying the Accept request-header field to add or delete media types that are acceptable for the response
- Replacing a variable in the Request-URI with a cross-site scripting attack

Configure search and replace in the Traffic Viewer proxy settings. Click to access the settings.

Finding and replacing text

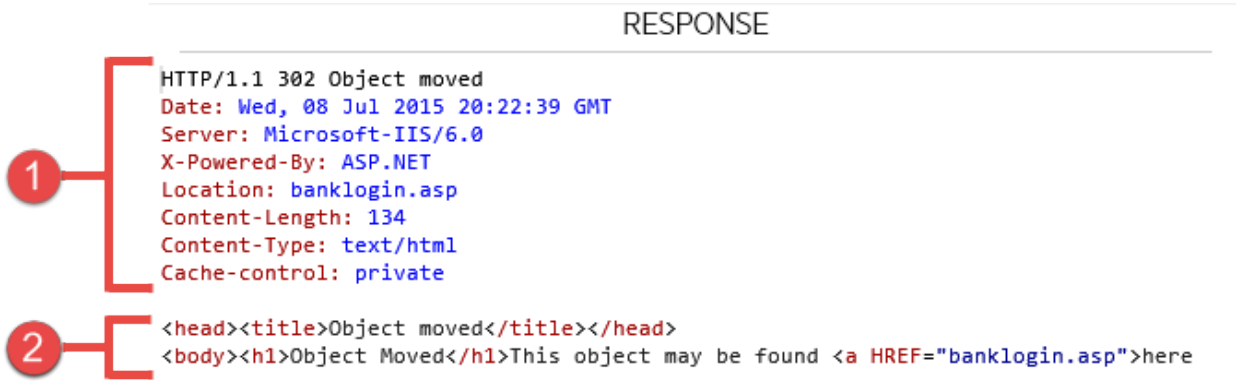
To find and replace text in requests or responses:

1. Click **ADD**.

   A default entry is added to the table.
2. Double-click the **Search On** column of the entry.
3. Click the drop-down arrow and select the message area you want to search. Options are:
   - RequestFull - Search and replace in the entire request message.
   - RequestHeader - Search and replace in the request header only.
   - RequestBody - Search and replace in the request body only.
   - ResponseFull - Search and replace in the entire response message.

- ResponseHeader - Search and replace in the response header only.
- ResponseBody - Search and replace in the response body only.

  The following diagram identifies the parts of a response message:



Item	Description
1	Response Header
2	Response Body

4. In the **For** column, type the data (or a regular expression representing the data) you want to find.
5. In the **Replace With** column, type the data you want to substitute for the found data.

   Note: To use a regular expression in the **For** and/or **Replace With** columns, select the **Regex** check box. See "Using regular expressions in rules" below.
6. Repeat steps 1-5 to create additional search rules.
7. Click **SAVE**.

Using regular expressions in rules

Caution! This section should be used only by advanced users with experience in constructing regular expression syntax.

Advanced users can configure search and replace rules using regular expressions in both the **For** column and the **Replace With** column. For example, if you enable a rule using regular expressions to search on the ResponseBody for `(<return>)([^<]+)(</return>)` and replace the findings with `$1<![CDATA[$2]]>$3`, the search rule would make the following changes:

This Response Value...	Is Replaced With this Value...
HTTP/1.1 200 OK Date: Fri, 31 Jul 2015 14:22:40 GMT Server: Apache/2.0.63 (Win32) DAV/2 mod_auth_sspi/1.0.4 PHP/5.2.5 mod_ssl/2.0.63 OpenSSL/0.9.7m X-Frame-Options: SAMEORIGIN X-Powered-By: PHP/5.2.5 X-Token: CX45865478 Content-Length: 207 Keep-Alive: timeout=15, max=98 Connection: Keep-Alive Content-Type: application/xml <?xml version="1.0" encoding="UTF-8"?> <Data xmlns="http://scanme/serv001"> <Body> <testResponse> <result>return</result> <return>2222</return> </testResponse> </Body> </Data>	HTTP/1.1 200 OK Date: Fri, 31 Jul 2015 14:22:40 GMT Server: Apache/2.0.63 (Win32) DAV/2 mod_auth_sspi/1.0.4 PHP/5.2.5 mod_ssl/2.0.63 OpenSSL/0.9.7m X-Frame-Options: SAMEORIGIN X-Powered-By: PHP/5.2.5 X-Token: CX45865478 Content-Length: 207 Keep-Alive: timeout=15, max=98 Connection: Keep-Alive Content-Type: application/xml <?xml version="1.0" encoding="UTF-8"?> <Data xmlns="http://scanme/serv001"> <Body> <testResponse> <result>return</result> <return><![CDATA[2222]]></return> </testResponse> </Body> </Data>

For more information, see "Using regular expressions" on page 139.

How rules are applied

The request/response rules are applied sequentially, in the order in which they appear. For example, if a rule changes HTTPS to SSL, and if a subsequent rule then changes SSL to SECURE, the result will be that HTTPS is changed to SECURE.

Enabling a rule

To enable a rule:

1. Select the **Enabled** check box for the rule you want to enable.
2. Click **SAVE**.

Disabling a rule

To disable a rule without deleting it:

1. Clear the **Enabled** check box for the rule you want to disable.
2. Click **SAVE**.

Deleting a rule

To delete a rule:

1. Select the rule you want to delete.
2. Click **REMOVE**.
3. Click **SAVE**.

Editing a rule

To edit a rule:

1. Click an entry in the **Search On**, **For**, or **Replace With** column.
2. Change the data.
3. Click **SAVE**.

Chapter 14: Web Discovery

Use Web Discovery to find all open hosts in your enterprise environment.

How it works

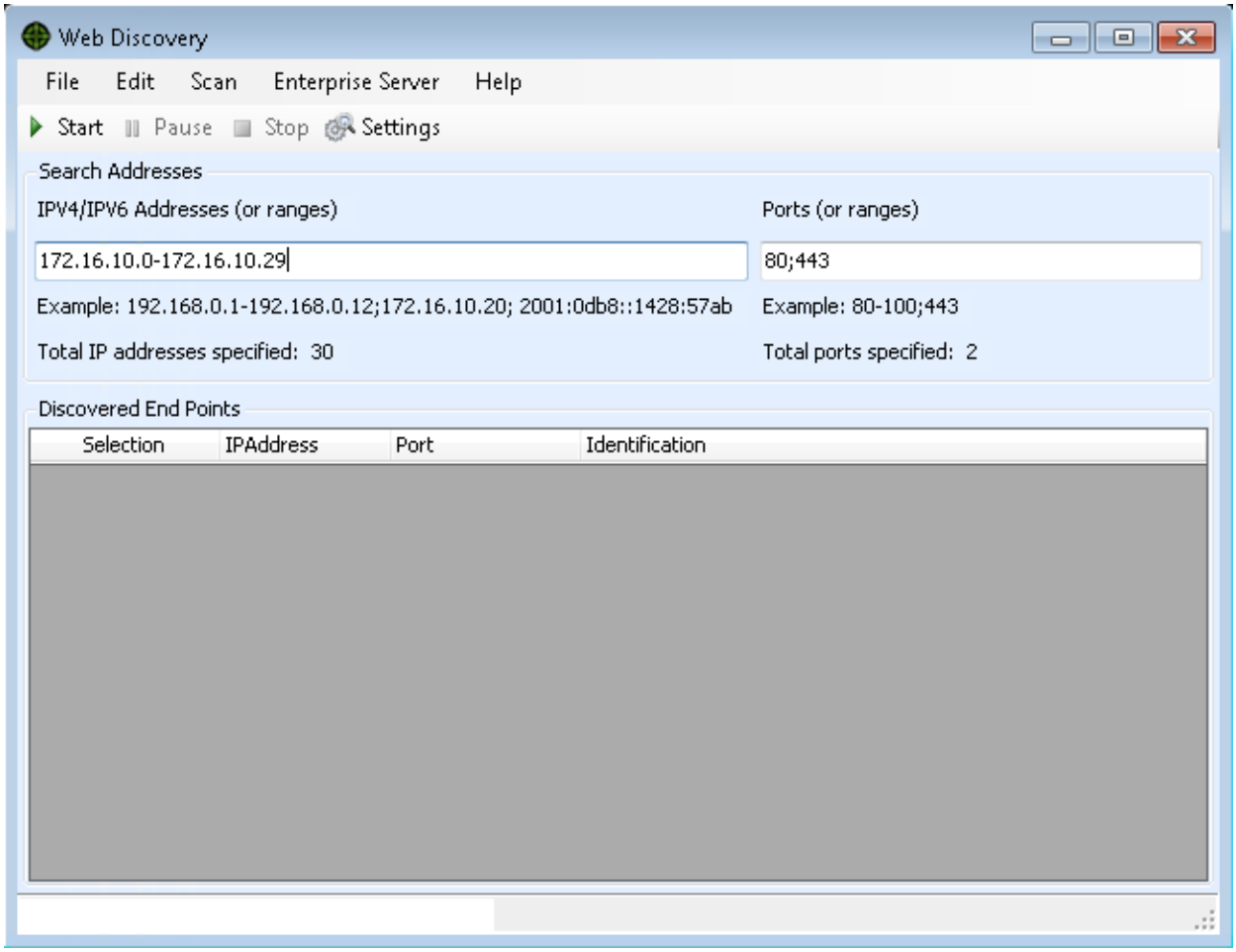
Web Discovery sends packets to all the open ports (in a range of IP addresses and ports that you specify), searches the server's response for specific information, and then displays the results. There are two predefined packets included with Web Discovery: Web Server and SSL Web Server. They both contain the following HTTP request:

```
GET / HTTP/1.0
```

Web Discovery searches the HTTP response for the string "HTTP"; if it finds the string, it displays the IP address, port number, and the text "WebServer," followed by the results of a regular expression search designed to reveal the server's name and version number.

You can save the list of discovered servers in a text file.

Web Discovery tool image



Discovering sites

To run Web Discovery to discover sites:

1. In the **IPV4/IPV6 Addresses (or ranges)** box, type one or more IP addresses (or a range of IP addresses).
   - Use a semicolon to separate multiple addresses.
     Example: 172.16.10.3;172.16.10.44;188.23.102.5
   - Use a dash or hyphen to separate the starting and ending IP addresses in a range.
     Example: 10.2.1.70-10.2.1.90

   Note: IPV6 addresses must be enclosed in brackets. For example:

   - For http://[::1]
     OpenText DAST scans "localhost."

- For http://[fe80::20c:29ff:fe32:bae1]/subfolder/

  OpenText DAST scans the host at the specified address starting in the "subfolder" directory.
- For http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/

  OpenText DAST scans a server running on port 8080 starting in "subfolder."

2. In the **Ports (or ranges)** box, type the ports you want to scan.
   - Use a semicolon to separate multiple ports.

     Example: 80;8080;443
   - Use a dash or hyphen to separate the starting and ending ports in a range.

     Example: 80-8080.
3. To modify Web Discovery settings, click **Settings**. See Web Discovery Settings for more information.
4. Click **Start** to initiate the discovery process.

   Results display in the Discovered EndPoints area.
5. Click an entry in the **IP Address** column to view that site in a browser.
6. Click an entry in the **Identification** column to open the Session Properties window and view the raw request and response.

Saving discovered sites

To save the list of discovered servers:

1. Click **File > Export**.

   If you export the data to a .csv file, the IP addresses become default OpenText™ Fortify Software Security Center applications. You can edit those applications and their associated data in Excel. In Fortify WebInspect Enterprise, you can then import the applications into Fortify Software Security Center. For more information, see the Fortify WebInspect Enterprise online Help.
2. Use the standard file-selection window to name and save the file.

Settings

To change the Web Discovery tool settings:

1. Click **Edit > Settings**.
2. In the **Select Protocols** group, choose the packets you want to send by selecting or clearing the check box next to the protocol name.

3. In the **Logging** group, select the elements you want to log:
   - **Log Open Ports**: Logs all available ports found open on the host; saves only Web server information in log file.
   - **Log Services**: Logs all services identified during the discovery.
   - **Log Web Servers**: Logs Web servers identified.
4. Enter the file location in the **Log To** box, or click the ellipsis button and use the standard file-selection window to specify the file in which the log entries should be recorded.
5. In the **Connectivity** group, set the following timeouts (in milliseconds):
   - **Connection Time Out**: The period of time that Web Discovery will wait before stopping a port scan when no information has been returned from an IP address.
   - **Send Time Out**: When sending a message to the remote IP endpoint[1], the transmission is divided into smaller packets. If the IP endpoint does not acknowledge receipt of a sent packet within the specified period of time, the socket is closed and the discovery for that endpoint reports no services.
   - **Receive Time Out**: When sending a message to the remote IP endpoint, the transmission is divided into smaller packets. If the Web Discovery tool does not receive the sent packet within the specified period of time, the socket is closed and the discovery for that endpoint reports no services.
6. Adjust the number of open sockets using the **Sockets** box. A higher number of open sockets results in a faster scan. However, a setting that exceeds a server's threshold may result in false positives.
7. Click **OK** to save the updated information and return to the Web Discovery window.

[1] (The name for the entity on one end of a transport layer connection; the point at which a service connects to the network. In a service-oriented architecture, any single network interaction involves two endpoints: one to provide a service and the other to consume it. In Web services, an endpoint is specified by a URI.)

Chapter 15: Web Form Editor

Most web applications contain forms composed of 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.

For the scanner to navigate through all possible links in the application, it must be able to submit appropriate data for each form.

With the Web Form Editor, you can create or modify a file containing the names of all input controls and the associated values that need to be submitted during a scan of your web site. These entries are categorized by URL, so even if different controls on different pages have the same name, the Web Form Editor can discriminate between them. Alternatively, you can designate a form entry as "global," meaning that its value will be submitted for any input control having the same name attribute, regardless of the URL at which it occurs.

During a scan, if the scanner encounters an input control whose name attribute is not matched in the file you create, it will submit a default value (12345).

There are two ways to create a list of form values:

- Create the list manually.
- Record the values as you navigate through the application.

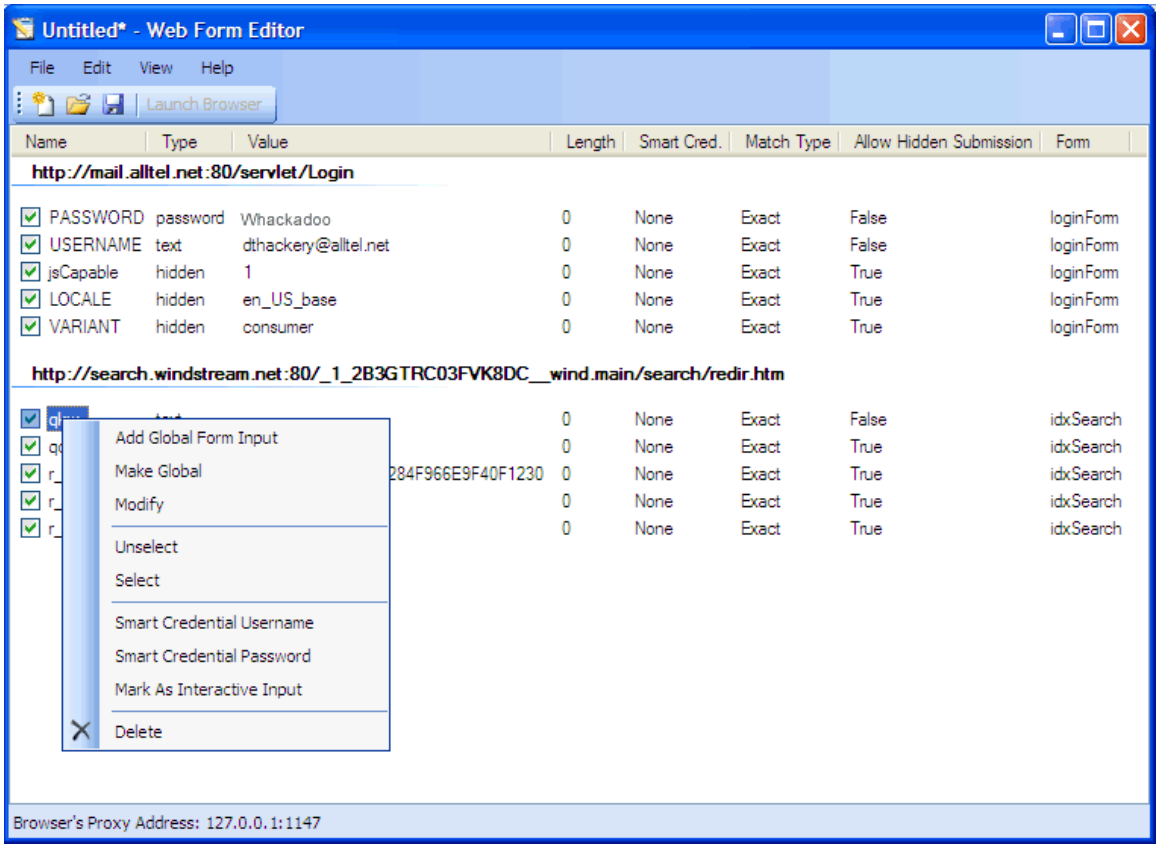
Recording Web Form values

The Web Form Editor serves as a proxy that handles HTTP traffic between a browser and a target web site. By default, it uses the local IP address 127.0.0.1 and any available port. However, you can specify a different IP address and port by selecting **Settings** from the **Edit** menu.

Use the following procedure to capture names and values of input controls on a web site.

1. To create a list of form values, select **New** from the **File** menu (or click the New icon on the toolbar).
2. To add form values to an existing list, select **Open** from the **File** menu (or click the Open icon on the toolbar) and choose a file using the standard file-selection dialog box.
3. Using the browser's Address bar, enter or select a URL and navigate to a page containing a form.
4. Complete the form and submit it (usually by clicking a button such as **Log In**, **Submit**, **Go**, etc.).

5. Navigate to additional pages and submit forms until you have traversed all the links you wish to follow.



For example, the last two entries in the list illustrated above were derived from the following HTML fragment ...

```
<form name="loginForm" action="/servlet/Login" method="POST">
<input type="password" size="16" name="PASSWORD">
<input type="text" size="16" name="USERNAME" value="">
<input type="SUBMIT" value="Submit"></form>
```

... and the user entered his name and password.

6. If necessary, you can modify items by right-clicking an entry and using the shortcut (pop-up) menu.
   - To edit an entry, select **Modify**.
   - To add an entry, select **Add Global Form Input**. A Global entry is one not associated with a specific URL.
   - To remove an entry, choose **Unselect**. This removes the entry from processing, but does not delete it from the file.
   - To delete an entry, choose **Delete**.

- To designate an entry as a smart credential, select either **Smart Credential Username** or **Smart Credential Password.** See "Smart credentials" on page 164 for more information.
- To force scanner to pause the scan and display a window prompting the user to enter a value for this entry, select **Mark As Interactive Input**.

  When a scanner encounters an HTTP or JavaScript form, it pauses the scan and displays a window that enables you to enter values for input controls within the form, provided that the scanner's option to "Prompt For Web Form Values" is selected. However, if the scanner's option to "Only Prompt Tagged Inputs" is also selected, the scanner does not pause for user input unless a specific input control has been designated **Mark As Interactive Input** (except for passwords, which always cause the scanner to pause for input).

7. From the **File** menu, select **Save** or **Save As**.

Manually adding or modifying web form values

To add or modify web form values:

1. Do one of the following:
   - To add a web form value, right-click anywhere in the Web Form Editor's work area and select **Add Global Form Input** from the shortcut (pop-up) menu.
   - To modify a web form value, right-click an entry and select **Modify** from the shortcut (pop-up) menu.

   The Add User-Defined Input or the Modify Input window appears.
2. In the **Name** box, type (or modify) the name attribute of the input element.
3. In the **Length** box, enter either:
   - the value that must be specified by the size attribute, or
   - zero, for input elements that do not specify a size attribute.

   For example, to submit data for the following HTML fragment . . .

   ```
   <INPUT TYPE="password" NAME="accessID" MAXLENGTH="6">
   ```

   . . . you must create an entry consisting of accessID (Name) and specify a size of "6" (Length).
4. In the **Value** box, type the data that should be associated with the input element (for example, a password).
5. Use the **Match** list to specify how the scanner should determine if this entry qualifies to be submitted for a particular input control. The options are:
   - **Exact** - The name attribute of the input control must match exactly the name assigned to this entry.
   - **Starts with** - The name attribute of the input control must begin with the name assigned to this entry.

- **Contains** - The name attribute of the input control must contain the name assigned to this entry.

6. Programmers sometimes use input controls with type="hidden" to store information between client/server exchanges that would otherwise be lost due to the stateless nature of HTTP. Although the Web Form Editor will collect and display the attributes for hidden controls, the scanner will not submit values for hidden controls unless you select **Allow Hidden Submission**.
7. Click **Add** (or **Modify**).
8. If necessary, you can assign additional attributes by right-clicking an entry and using the shortcut (pop-up) menu.
   - To remove an entry, choose **Unselect**. This clears the check mark and removes the entry from processing, but does not delete it from the file.
   - To activate an entry, choose **Select**. This creates a check mark and includes the entry for processing.
   - To delete an entry, choose **Delete**.
   - To designate an entry as a smart credential, select either **Smart Credential Username** or **Smart Credential Password.** See "Smart credentials" on page 164 for more information.
   - If you select **Mark As Interactive Input**, then the scanner will pause the scan and display a window prompting the user to enter a value for this entry (if the scan options include the settings **Prompt For Web Form Values During Scan** and **Only Prompt Tagged Inputs**).

     Note: It is not necessary to tag passwords with **Mark As Interactive Input**.

Import a File

You can import a file that was designed and created for earlier versions of Fortify WebInspect and convert it to a file that can be used by the current Web Form Editor.

1. From the **File** menu, select **Import**.

   The Convert Web Form Values window appears.
2. Click the browse button ... next to **Select File To Import**.
3. Using a standard file-selection window, locate the XML file created by an earlier version of the Web Form Editor.
4. Click the browse button ... next to **Select Target File**.
5. Using a standard file-selection window, specify a file name and location for the converted file.
6. Click **OK**.

Shortcut menu

The following commands are available from the pop-up menu that appears when you right-click in the work area of the Web Form Editor.

Command	Description
Add Global Form Input	Displays the Add User-Defined Input window, allowing you to specify the name, length, and value of an input control. For more information, see "Manually adding or modifying web form values" on page 157.
Make Global	Disassociates the selected entry from a specific URL. This means that the scanner will submit the value whenever it encounters an input control having this entry's name attribute, regardless of the control's location.
Modify	Enables you to change the name, length, value, and match type attributes of an entry.
Unselect	Clears the check box associated with an entry. The entry will not be saved and will not be added again to the list if you revisit this page on which it occurred.
Select	Enables the check box associated with an entry, assuring that the entry will be included in the saved list.
Smart Credential Username	If you designate an entry as a Smart Credential Username, the Web Form Editor will not save the value you entered. When the scanner scans the page containing the input element associated with this entry, it will substitute the user name specified in its Authentication options (or, if no user name is specified, the string "FormFillText").
Smart Credential Password	If you designate an entry as a Smart Credential Password, the Web Form Editor will not save the value you entered. When the scanner scans the page containing the input element associated with this entry, it will substitute the password specified in its Authentication options (or, if no password is specified, the string "FormFillText").
Mark As Interactive Input	For OpenText DAST only: Tags this entry as one requiring user input if OpenText DAST's options are set to **Prompt For Web Form Values During Scan** AND **Only Prompt Tagged Inputs**. When OpenText DAST scans the page containing the input element associated with this entry, it

Command	Description
	will pause the scan until the user enters a value for this input. This is especially useful for forms that require a unique value. Examples include an order-processing system (where a duplicate number would elicit a response such as, "That order has already been processed") and a CAPTCHA (which is a type of challenge-response test to ensure that the response is not generated by a computer).
Delete	Removes the selected entry from the list. The entry will not be saved; it will be added again to the list if you revisit this page on which it appeared, however.

Scanning with a web form file

If you designate a web form file in the default scan settings, the scanner automatically selects that file each time you start a web site assessment. You can override that selection, however, by choosing a different file for that specific scan.

Use the following procedure to scan a site using the list of web form values you created.

1. Click the OpenText DAST **Edit** menu and select **Default Scan Settings**. The Default Settings window opens.
2. In the **Scan Settings** section, select **Method**.
3. In the **Scan Behavior** group, select **Auto-fill Web Forms During Crawl**.
4. To select a previously recorded file:
   a. Click the browse button  .
   b. Using the standard file-selection window, select a file containing the web form value you want to use and click **Open**.
   c. (Optional) You can edit the contents by right-clicking an entry and selecting an option from the context menu.
5. To record web form values:
   a. Click **Create New Web Form Values**  .
   b. Click the **File** menu and select **New**.
   c. Click **Launch Browser**.
   d. See "Recording Web Form values" on page 155 for further instructions.
6. To edit web form values for the selected file:
   a. Click **Edit Current Web Form Values**  .
   b. See "Recording Web Form values" on page 155 for further instructions.

Matching web form list to input controls

When crawling a web application and submitting web form values, the OpenText scanner analyzes the entries in the web form values file to determine if a value should be submitted. The logic for determining a match is represented in the following table, ordered from "most preferred" to "least preferred."

Rules for matching web form values

Values	Match Case	Description
Page-specific form values	**Exact Match** Name exact match Length exact match	The specific web page, web form name, and value length detected on the crawled web page exactly match a single record in the webformvalues.xml selected for the scan.
	Partial Match Name-only match Length allows wildcard	The specific web page and web form name detected on the crawled web page match a single record in the webformvalues.xml selected for the scan. The field length associated with that form value allows for submission to any field input length (wildcard field length match).
Global form values	**Exact Match** Name exact match Length exact match	The web form name and value length detected on the crawled web page match a single record in the global web form values section of the webformvalues.xml selected for the scan.
	Partial Match 1 Name exact match Length allows wildcard	The web form name detected on the crawled web page exactly matches a form name found in the global values section of the webformvalues.xml selected for the scan. The field length associated with that form value allows for submission to any field input length (wildcard field length match).
	Partial Match 2 Field name starts with Name value Length exact match	A web form value in the file partially matches the field name found. All characters in the web form value match the beginning of the web page field name and the field length detected

Values	Match Case	Description
		on the crawled web page match the record in the global web form values section of the webformvalues.xml selected for the scan.
	Partial Match 3 Field name starts with Name value Length allows wildcard	A web form value in the file partially matches the field name found. All characters in the web form value match the beginning of the web page field name and the field length for the record allows for submission to any field length (wildcard field length match).
	Partial Match 4 Name value included in field name Length exact match	A web form value in the file partially matches the field name found. All characters in the web form value match a portion of the web page field name and the field length detected on the crawled web page match the record in the global web form values section of the webformvalues.xml selected for the scan.
	Partial Match 5 Name value included in field name Length allows wildcard	A web form value in the file partially matches the field name found. All characters in the web form value match a portion of the web page field name and the field length for the record allows for submission to any field length (wildcard field length match).
No match	Field name has no exact or partial matches to Web form values	No web form value match was found. Submit the specified default value (Default).
No default value	The web form values file has no default value specified	No web form value match was made and the default value is not in the webform values file. Submit "not found."

Settings: General

Use these settings to configure how the browser will interact with the target web site. To access these settings, select **Edit > Settings > General**.

Setting	Description
Proxy Listener	The Web Form Editor serves as a proxy that handles HTTP traffic between a browser and a target web site. By default, it uses the local IP address 127.0.0.1 and any available port. However, you can specify a different **Local IP Address** and **Port**. To avoid the possibility of specifying a port that is already in use, select **Automatically Assign Port**.
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 the Web Form Editor should use in the **Assumed 'charset' Encoding** list.

Settings: Proxy

Use these settings to access the Web Form Editor through a proxy server. To access these settings, select **Edit > Settings > Proxy**.

Setting	Description
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 Protocol (WPAD) protocol to locate a proxy autoconfig file and configure the browser's web proxy settings.
Use Firefox proxy settings	Select this option to import your proxy server information from Firefox.
Use System proxy settings	Select this option to import your proxy server information from the local machine.
Configure a 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** box.
Explicitly configure proxy	Select this option to access the Internet through a proxy server, and then enter the requested information:

Setting	Description
	1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080). 2. Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard. 3. If authentication is required, select a type from the **Authentication** list: • **Automatic** **Note:** Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved. • **Basic** • **Digest** • **Kerberos** • **Negotiate** • **NT LAN Manager (NTLM)** 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** box. Use commas to separate entries.
Specify Alternative Proxy for HTTPS	For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.

Smart credentials

When recording web form values, you will often encounter a log-on form requiring you to enter a user name and password. You can safely use your own user name and password, provided that you designate those entries as "Smart Credentials" before saving the file. Your actual password and user name are not saved.

When scanning the page containing the input control associated with this entry, the scanner will substitute the password specified in the product's Authentication options. This would be a known user name and password that does not require security. Alternatively, if no user name or password is specified, the scanner will submit the string "FormFillText."

Chapter 16: Web Fuzzer

The Web Fuzzer tool lets you run several automated tests for common classes of web application security vulnerabilities such as:

- SQL injection
- Format strings
- Cross-site scripting
- Path traversal
- Odd characters
- Buffer overflows
- Protocol implementation problems

What is fuzzing?

"Fuzzing" is an automated software-testing technique that generates and submits random or sequential data to various areas of an application in an attempt to uncover security vulnerabilities. For example, when searching for buffer overflows, a tester can generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

Accessing Web Fuzzer

To access the Web Fuzzer tool, do one of the following:

- On the OpenText DAST toolbar, click **Tools > Web Fuzzer**.
- Using the Security Toolkit, click **Start > OpenText > Web Fuzzer**.

Understanding the Fuzzer menu

This topic describes the various options on the Web Fuzzer menu bar.

File menu

The following table describes the File menu options.

Option	Description
Import	Imports previously saved sessions in the **Sessions** area.

Option	Description
Export	Exports sessions in the **Sessions** area to a file.
Clear Sessions	Clears the session view list.
Exit	Closes the application.

Edit menu

The following table describes the Edit menu options.

Option	Description
Server	Enables you to specify the target server and select authentication settings.
Settings	Enables you to specify general, proxy, sockets, and protocol settings.

Session menu

The following table describes the Session menu options.

Option	Description
Import	Imports an XML file containing a session that you previously saved.
Export	Exports a session to an XML file.
Create	Opens the **Session Editor**, providing a structured approach to creating requests.
Raw Create	Opens the **Raw Editor**, allowing you to edit a standard request.
Edit	Available after selecting a session; opens the **Session Editor**.
Raw Edit	Available after selecting a session; opens the **Raw Editor**.

Filters menu

The following table describes the Filters menu options.

Option	Description
Edit	Opens the **Filters** dialog, allowing you to create a regular expression that selects only those responses that you specify.
Enable	Applies filters to sessions.

Using Web Fuzzer

The following table describes how to use the Web Fuzzer.

Stage	
1.	Configure the server information. For more information, see "Configuring the server" on the next page.
2.	Configure the settings. For more information, see "Configuring Fuzzer settings" on page 176.
3.	Do one of the following: • Create a session. • Import a previously saved session and (optionally) edit it. For more information, see "Using the Session Editor" on the next page or "Using the Raw Editor" on page 172.
4.	Click **Start**. The Sessions area lists each session (request and response) generated by the tool.
5.	To examine the results, click an entry in the **Sessions** list. The HTTP request for the selected session appears in the **Request** area. The server's response appears on both the **Browser View** and **Raw Response** tabs.
6.	To edit the request that you constructed, select a session in the **Sessions** list, then click the **Session** menu and choose either **Edit** or **Raw Edit**. For more information, see "Using the Session Editor" on the next page or "Using the Raw Editor" on page 172.

Configuring the server

Use the Server Configuration dialog to identify the target web site and configure communication settings.

To configure the server settings:

1. Click **Edit**, and then select **Server**.
   The Server Configuration dialog opens.
2. In the **Host Name/IP** box, enter the fully qualified domain name (FQDN) or the IP address of the web site.
3. In the **Port** box, enter the server's port number.
4. If the server uses Secure Sockets Layer protocol, select the **SSL** check box.
5. If authentication is required, select a method from the **Type** list, and then enter a user name and password in the appropriate boxes.
6. Click **OK**.

Using the Session Editor

Use the Session Editor to create an HTTP request or to change specific sections of an HTTP request. You can replace an HTTP element with text that you type or paste into a text box, or you can insert a generator that will create multiple requests containing generated data.

Creating a session

To create a session:

- Select **Session > Create**.
  The Session Editor opens. Continue with "Configuring the session" on the next page.

Editing a session

To edit a session:

1. Select a session in the **Sessions** list.
2. Select **Session > Edit**.
   The Session Editor opens. Continue with "Configuring the session" on the next page.

Configuring the session

To configure the session in the Session Editor:

1. Click a tab.
2. See the following sections for detailed descriptions of each tab:
   - "Method tab" below
   - "Path tab" below
   - "Query tab" on the next page
   - "Version tab" on the next page
   - "Headers tab" on the next page
   - "Cookies tab" on page 171
   - "Post data tab" on page 172
3. Do one of the following:
   - Edit the data appearing in text boxes.
   - Select the **Use Generator** check box and then click **Generator** to insert a generator. For more information, see "Understanding Fuzzer generators" on page 173.
4. To change other areas, click a different tab.
5. After configuring the areas you want to change, click **OK**.
6. When you return to the Web Fuzzer window, click **Start**.

Method tab

The GET method is specified by default. You can replace it with any text, or you can insert the Method generator.

Path tab

You can fuzz three elements related to the path:

- The name of the file
- The file extension
- The character that designates a directory level (usually the forward slash /)

You can replace these elements with any text, or you can insert generators.

Query tab

Some HTTP requests include a query string, with each parameter formatted as parameter=value and separated by an ampersand (&). The resource is separated from the query by a delimiter character (usually a question mark, although other characters can be used depending on the application). For example:

```
http://www.website.com/category.cfm?model_ID=0&category_ID=12
```

To create a query string:

1. Click **Add**.

   `name=value` appears in the list, representing the query string you are creating.
2. Click the **Name** tab.

   You can edit the parameter named "`name`" or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
3. Click the **Value** tab.

   You can edit the "`value`" in the equation or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
4. Click the **Separator** tab.

   You can edit the character that separates the name from the value (usually an equals sign) or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
5. Click the **Format** tab.

   You can edit the order in which the equation elements appear, or you can introduce characters between them.
6. In the **Name Value Separator** area, you can edit the character that separates parameters (usually an ampersand) or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
7. To add another parameter, click **Add** and repeat Steps 2-6.

Version tab

The version indicates to the server which HTTP version to use for interpreting the request. Valid versions are 0.9, 1.0 and 1.1. The version information is formatted as "HTTP/version," which is a name-value pair separated by a forward slash (/). You can fuzz all three sections: Protocol, Separator, and Version. You can also fuzz the format by rearranging the order or introducing extraneous characters.

Headers tab

Headers contain basic information issued by the client to help the server or application handle the request. Common headers are Host and User-Agent. Each header is defined by using the "name: value" syntax. This name-value structure can also be separated into four fuzzing opportunities.

To create headers:

1. Click **Add**.

   `name:value` appears in the list, representing the header you are creating.
2. Click the **Name** tab.

   You can edit the parameter named "`name`" or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
3. Click the **Value** tab.

   You can edit the "`value`" text or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
4. Click the **Separator** tab.

   You can edit the character that separates the name from the value (usually a colon) or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
5. Click the **Format** tab.

   You can edit the order in which the header elements appear, or you can introduce characters between them.
6. In the **Name Value Separator** area, you can edit the character that separates headers or you can substitute a generator for it (select the **Use Generator** check box ,and then click **Generator**).
7. To add another header, click **Add** and repeat Steps 2-6.

Cookies tab

Cookies are special headers that contain parameters used by the application to manage users and states. The format of a cookie definition is:

```
Cookie: name=value;name=value
```

Each parameter is a name-value pair that can be independently fuzzed.

To create cookies:

1. Under the **Cookies** list, click **Add**.

   `Cookie:` appears in the Cookies list, representing the cookie you are creating.
2. Under the **Cookie Detail** list, click **Add**.

   `name=value` appears in the Cookie Detail list.
3. Click the **Cookie Name** tab to the right of the **Cookie Detail** list.

   You can edit the name or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
4. Click the **Value** tab.

   You can edit the "`value`" text or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
5. Click the **Separator** tab.

You can edit the character that separates the name from the value (usually an equals sign) or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).

6. Click the **Format** tab.

   You can edit the order in which the header elements appear, or you can introduce characters between them.

7. In the **Name Value Separator** area, you can edit the character that separates headers or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
8. To add another cookie, repeat Steps 1-7.

Post data tab

While a query can be appended to the Request-URI, post data is added to the end of the request. The format is similar to the URI query and is mostly used with the POST method. When post data are used, the request must contain a Content-Length header that indicates the size of the post data. You can fuzz not only the post data, but also the Content-Length value to test how the server or application handles the differences.

When fuzzing the HTTP request message, you affect two main layers of the application environment: server protocol implementation and Web application.

To create post data:

1. Click **Add**.

   `name=value` appears in the list, representing the post data you are creating.

2. Click the **Name** tab.

   You can edit the parameter named "`name`" or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).

3. Click the **Value** tab.

   You can edit the "`value`" text or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).

4. Click the **Separator** tab.

   You can edit the character that separates the name from the value (usually a colon) or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).

5. Click the **Format** tab.

   You can edit the order in which the header elements appear, or you can introduce characters between them.

6. In the **Name Value Separator** area, you can edit the character that separates headers or you can substitute a generator for it (select the **Use Generator** check box, and then click **Generator**).
7. To add another post data element, click **Add** and repeat Steps 2-6.

Using the Raw Editor

Use the Raw Editor to create an HTTP request message.

You can change any portion of the request using the tool's text-editing capabilities, or you can insert a generator.

To insert a generator:

1. Do one of the following:
   - Place the cursor anywhere in the request.
   - Highlight any portion of the request.
2. Right-click and select **Generator** from the shortcut menu.
   The Generators dialog opens.
3. On the **Generators** dialog, select a generator and click **Configure**.
   The Options dialog opens.
4. On the **Options** dialog, enter the configuration information and then click **OK**.
5. On the **Generators** dialog, click **OK**.
6. The generator you created is inserted at the cursor position (or in place of any portion highlighted during Step 1).

After editing the request or inserting a generator or both, click **OK** to return to the Web Fuzzer window. Then click **Start**.

Understanding Fuzzer generators

You can use generators to help create sessions to use for fuzzing. The following table describes the generators available in Web Fuzzer.

Generator	Description
ASCII	Inserts one ASCII character, within the range you specify, in each request. Specify the starting and ending character, and the number of times to loop through the series.
Character	Generates the character you specify and inserts multiple numbers of the character into each request. Specify the minimum and maximum number of characters, and an increment.
Decimal Number	Inserts a fractional number, within the range you specify, in each request. Specify the **Minimum** and **Maximum** number, the **Increment**, and the number of times to loop through the series.
GUID	Inserts a random Globally Unique Identifier (a 128-bit number) in each request.

Generator	Description
	Specify the number of requests.
HTTP Method	Inserts a method (GET, POST, PUT, etc.) in the request. Specify the protocol version (0.9, 1.0, 1.1, or all).
Number	Inserts a number, within the range you specify, in each request. Specify the **Minimum** and **Maximum** number, the **Increment**, and the number of times to loop through the series.

SQL Injection	Inserts a string from a text file you specify. The number of requests is determined by the number of paragraphs in the file. All `characters` in the paragraph are inserted.
	The default file (`sqlinjections.txt`) contains the following two entries:
	`' or 1=1`
	`' or like '%`

Text	Inserts the text you specify in a single request.
WordList Reader	Inserts a string from a text file you specify. The number of requests is determined by the number of paragraphs in the file. All characters in the paragraph are inserted.
XSS Injection	Inserts a string from a text file you specify. The number of requests is determined by the number of paragraphs in the file. All characters in the paragraph are inserted. The default file (`xssinjections.txt`) contains the following entry: `<script>alert('test')</script>`

Working with filters

A filter consists of a name, description, and rule. The "rule" is a regular expression that defines the text you want to locate in a particular section of the server's response. For example, if you want to display only those responses that contain the word "error" in the response body and where the response also specifies a status code between 500 and 599, then use the following rule:

```
[STATUSCODE]5\d\d AND [BODY]\serror\s
```

Use the following notation to specify a response section:

```
[HEADERS]
```

```
[STATUSLINE]
[STATUSCODE]
[STATUSDESCRIPTION]
[ALL]
[SETCOOKIES]
[BODY]
```

Accessing the Filters dialog

To access the Filters dialog:

- Select **Filters > Edit**.
  The Filters dialog opens.

Creating a filter

To create a filter:

1. In the **Filters** dialog, click **Add**.
   The tool creates a rule named Default Rule.
2. Modify the **Name**, **Description**, and **Rule**.
3. Click **Apply** to save the filter.

Editing a filter

To edit a filter:

1. In the **Filters** dialog, select a filter in the **Filters** list.
2. Modify the **Name**, **Description**, or **Rule**.
3. Click **Apply** to save the modifications.

Using a filter

To use a filter in a session:

1. In the **Filters** dialog, select a filter in the **Filters** list.
2. Select the **Enable** check box.

Important! In addition to enabling a specific rule, you must also enable the use of rules in general. To do so, select **Filters > Enable**.

Deleting a filter

To delete a filter:

1. In the **Filters** dialog, select a filter in the **Filters** list.
2. Click **Delete**.

Configuring Fuzzer settings

You can configure Web Fuzzer settings in the Settings dialog.

To configure Web Fuzzer settings:

1. Click **Edit**, and then select **Settings**.

   The Settings dialog opens.
2. Do one of the following:
   - To configure application settings, select **General** in the left pane. For more information about the available settings, see "General settings" below.
   - To configure proxy settings, select **Proxy** in the left pane. For more information about the available settings, see "Proxy settings" on the next page.
3. When finished, click **OK**.

General settings

The following table describes the General settings.

Setting	Description
Enable Filters	Enables filter support. When enabled, you can add, edit, and delete filters in the **Filters** dialog. For more information, see "Working with filters" on page 174. **Note:** You can also select **Filters > Enable** on the menu bar to enable filters.
Auto Scroll View	Enables automatic scrolling in the **Sessions** list view. When enabled, this will force the view to scroll down to the latest session automatically.
Show ToolTips	Enables the display of tool tips when you hover your mouse pointer over certain elements in the user interface (UI).

Setting	Description
Max Sockets	Specifies the maximum number of sockets to be used.
Timeout/Seconds	Specifies the socket send timeout (in seconds).
Enforce Content-Length	Web Fuzzer automatically adjusts the Content-Length value in the request when needed. If this option is enabled, you cannot fuzz the content-length header.
Enforce Host Header	Web Fuzzer includes the Host header in all requests. If this feature is enabled, you cannot fuzz the host header.

Proxy settings

The following table describes the Proxy settings.

Setting	Description
Direct Connection (proxy disabled)	Select this option if you are not using a proxy server.
Auto detect proxy settings	Use the Web Proxy Autodiscovery (WPAD) protocol to locate a proxy autoconfig file and configure the browser's Web proxy settings.
Use System Proxy Settings	Import your proxy server information from the local machine.
Use Firefox proxy settings	Import your proxy server information from Firefox.
Configure a proxy using a PAC file	Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the **URL** box.
Explicitly configure proxy	Configure a proxy by entering the requested information. See "Configuring a proxy" on the next page.
Specify Alternative Proxy for HTTPS	For proxy servers accepting HTTPS connections, select this option and configure a proxy by entering the requested information. See "Configuring a proxy" on the next page.

Configuring a proxy

To configure a proxy:

1. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
2. From the **Type** list, select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
3. If authentication is required, select a type from the **Authentication** list:
   - **Automatic**

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

   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NT LAN Manager (NTLM)**
4. If your proxy server requires authentication, enter the qualifying user name and password.

Chapter 17: Session-based Web Macro Recorder

OpenText DAST and Fortify WebInspect Enterprise include Session-based Web Macro Recorder tools: one for login macros and one for workflow macros. In this document, these two tools are referred to generally as "Session-based Web Macro Recorder" except for specific login-related and workflow-related content.

The Session-based Web Macro Recorder can be launched in several ways. For more information, see "Accessing the Session-based Web Macro Recorder" on the next page.

About Macros

A login macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct the OpenText DAST scanner to begin a scan using this recording. A workflow macro is a recording of login steps (as needed) and specific URLs on a site.

Note: The term "scanner" is often used instead of "OpenText DAST and Fortify WebInspect Enterprise" where the information applies to both products.

IE technology

By default, the Session-based Web Macro Recorder uses Internet Explorer browser technology (also referred to here as IE technology) to record and play macros.

Login macros

A login macro is a recording of the activity that is required to access and log in to a website or web application, typically by entering a user name and password and clicking a button such as Log In or Log On. When you configure a scan, you usually specify a previously recorded login macro or record a new one at the time for the scan to use.

To prevent the scanner from terminating prematurely if it gets logged out of your application, a login macro should also specify at least one logout condition that definitively indicates that a logout has occurred. During a scan, the scanner can get logged out for a variety of reasons, including:

- Normal logout driven by the target site
- An error condition in the target site such as a timeout
- An error in the macro itself, such as an invalid parameter

Specifying a logout condition as part of the login macro makes it unnecessary for users to manually log back in, perhaps repeatedly, when unexpected logouts occur during a scan. When scanning a site, the scanner analyzes every target site response to determine the state. If the scanner determines at any time that it is logged out, it runs the login macro to log back in, and then it resumes crawling or auditing the site at the point where the logout occurred.

As the final step in recording a login macro, the Session-based Login Macro Recorder uses sophisticated analysis to try to *automatically* detect a logout condition and specify it in the login macro. In most cases you do not have to identify a logout condition manually. However, you can add or edit logout conditions.

Workflow macros

A workflow macro is a recording of the login steps (as needed) and the specific URLs to which you manually navigate on a site. OpenText DAST or Fortify WebInspect Enterprise audits only the URLs that are recorded in the workflow macro and does not take any hyperlinks encountered during the audit. This type of macro is used most often to focus on a particular subsection of an application. In terms of the macro recording process, the essential differences from login macros are that:

- Workflow macros include only the specific URLs to which a user navigated while recording them. Workflow macros access only those URLs upon replay.
- Workflow macros do not require logout conditions, so the Session-based Workflow Macro Recorder user interface excludes logout condition functionality when recording workflow macros.

Note: If your website requires authentication, do not record login steps in a workflow macro. Instead, record a separate login macro to log in to your website.

Accessing the Session-based Web Macro Recorder

The following paragraphs describe the various ways to launch the Session-based Web Macro Recorder.

Login macros

You can record a new session-based login macro or select (and optionally edit) an existing session-based login macro that was recorded in OpenText DAST or Fortify WebInspect Enterprise in the following ways:

- When configuring a Guided Scan with Internet Explorer as the rendering engine, specify that the target site requires a login macro, and click **Create** to record a new login macro or select (and optionally edit) an existing login macro.
- When configuring a Basic Scan in OpenText DAST or a Web Site Scan in Fortify WebInspect Enterprise with Internet Explorer as the rendering engine, in Step 2 select **Site Authentication** and record a new login macro or select (and optionally edit) an existing login macro.

- On the OpenText DAST toolbar, click **Tools > Login Macro Recorder > Session-based** to run the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- In Fortify WebInspect Enterprise, on the Administrative Console toolbar, click **Tools > Login Macro Recorder > Session-based** to open the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- Using the Security Toolkit, click **Start > OpenText > Login Macro Recorder (Session)** to run the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- From Windows Explorer, navigate to an existing login macro that was recorded using the Session-based Login Macro Recorder, and double-click to open it. The Session-based Login Macro Recorder opens in stand-alone mode.

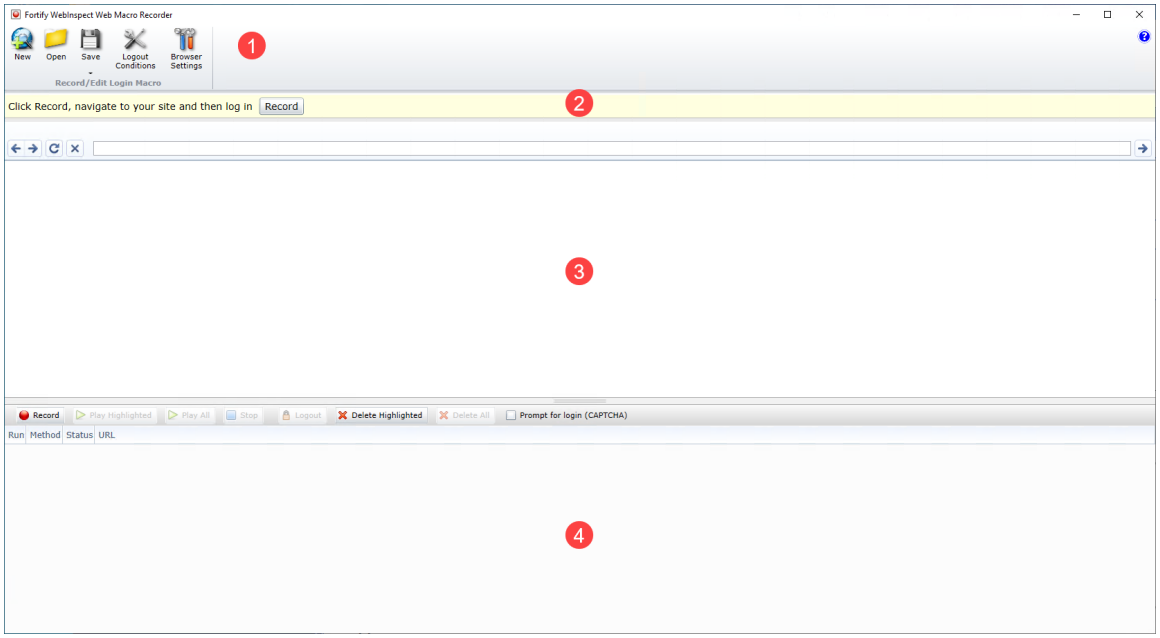
Workflow macros

You can record a new workflow macro or select (and optionally edit) an existing workflow macro that was recorded in OpenText DAST or Fortify WebInspect Enterprise in the following ways:

- When configuring a Guided Scan with Internet Explorer as the rendering engine, specify that the **Scan Type** is **Workflows** and later, in the **Workflows > 1. Manage Workflows** step, record a new workflow macro or import (and optionally edit) an existing workflow macro.
- When configuring a Basic Scan in OpenText DAST with Internet Explorer as the rendering engine, in Step 1 select **Workflow-Driven Scan** and click **Record** or **Manage** to record a new workflow macro or select (and optionally edit an existing workflow macro.
- On the OpenText DAST toolbar, click **Tools > Workflow Macro Recorder > Session-based** to run the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- In Fortify WebInspect Enterprise, on the Administrative Console toolbar, click **Tools > Workflow Macro Recorder > Session-based** to open the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- Using the Security Toolkit, click **Start > OpenText > Workflow Macro Recorder (Session)** to run the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.

Understanding the Session-based Web Macro Recorder interface

This topic describes the Session-based Web Macro Recorder user interface.



The following table describes the components of the Session-based Web Macro Recorder user interface.

Item	Description
1	Toolbar. For more information, see "Toolbar" below.
2	Yellow instruction bar that provides step-by-step guidance.
3	Target site pane.
4	Locations pane. For more information, see "Locations pane" on the next page. **Tip:** You can adjust the height of the locations pane relative to the target site pane.

Toolbar

The toolbar includes the options described in the following table.

Option	Description
New	Creates a new macro.
Open	Opens (or imports) a previously recorded macro to play or edit. You can open the following file types: • Web Macro (`*.webmacro`)

Option	Description
	• Burp Proxies (`*.*`) • HTTP Archive (HAR) files (`*.har`)
Save / Save As	Saves the macro that is currently open.
Logout Conditions	(Login Macros only) Opens the Logout Conditions Editor. For more information, see "Logout Conditions Editor" on page 186.
Browser Settings	Opens the Browser Settings dialog. For more information, see "Browser settings" on page 188.

Locations pane

The locations pane has a button bar with the buttons and check box described in the following table.

Button / Check Box	Description
Play Highlighted	Plays the single request (row) you highlighted by clicking it. Plays the highlighted request if the associated check box in the Run column is selected. Other check boxes in the Run column do not matter.
Play All	Plays only the requests that are selected (checked) in the Run column. **Note:** All steps are stored in the macro when you save it, but only the steps selected in the Run column are run whenever the macro is played.
Stop	Available during playback after you have clicked the **Play All** button. Aborts playback upon completion of the current request.
Logout	(Does not appear for workflow macros.) Logs you out of the site so that you can determine how the site responds to a subsequent request you play when logged out.
Delete Highlighted	Deletes the single request (row) you highlighted by clicking it.
Delete All	Deletes all the requests, regardless of whether they are selected in the Run column.

Button / Check Box	Description
Prompt for login (CAPTCHA)	(Does not appear for workflow macros.) CAPTCHA is a challenge-and-response test designed to ensure that a login response is provided by a person, not generated by a computer. If your target site uses CAPTCHA, select this check box. The macro still detects a logout condition, but OpenText DAST or Fortify WebInspect Enterprise users will need to log in manually at the beginning of a scan and whenever a logout occurs. Selecting this option disables selection of any of the listed requests and closes the right pane that displays HTTP traffic.

Below the button bar, the locations pane lists location and has the columns described in the following table.

Column	Description
Run	Steps that are selected (checked) are played when you click **Play All**. All steps are stored in the macro when you save it, but only the selected steps are run whenever the macro is played.
Excluded	Select **Url**, **Directory**, or **Page** to add that type of exclusion rule. The exclusion rule will apply to any requests made by a scan that uses this scan configuration. This column also displays, read only, the causes of any existing exclusions for requests—Custom, Disallowed Host, or, if **Restrict to folder** was selected at the start of configuring the scan, Outside Root.
Method	The method of the request, for example, GET or POST.
Status	The status of the response to the request, for example, 302 or 200.
Actual	The actual status returned in the response. Appears during playback if status is different than expected.
URL	The URL of the request.

The bottom right pane includes the tabs described in the following table.

Tab	Description
Details	For the selected (highlighted) request in the left pane, shows request data in the top right pane and associated response data in the bottom right pane.

Tab	Description
State	A collection of all the items that represent state or could represent state, that have been seen across all the locations that the macro has accessed. You can select them in any combination to characterize them as representing a state and you can manually add various types of items. Web applications can require that certain parameters be marked as “stateful.”
Parameters	(Does not appear for workflow macros.) For login macros, enables you to designate form input fields as being user name or password input so that the macro using IE technology can have user name and password parameters that can be specified at scan time.

Recording a macro

The Session-based Web Macro Recorder uses IE technology to record macros. This topic describes the tasks involved in interactively recording login macros and workflow macros using the Session-based Web Macro Recorder.

Note: These procedures provide general instructions for recording a macro. For best results, follow the guidance in the yellow instruction bar to record the macro.

For information about accessing the Session-based Web Macro Recorder, see "Accessing the Session-based Web Macro Recorder" on page 180.

Recording a login macro

In the Session-based Login Macro Recorder, do the following:

1. Click **Record**.
2. Type the target URL in the address field and click  .
3. Log in to your application.

   Note: IE technology does not support websites that require users to answer a variable set of questions in order to log in.

   As you access and log in to your application, a table of request data is added to the locations pane.
4. After you have logged in, click **Stop**.

   Important! Do not log out.

   The macro is saved.
5. Click **Play**.

The macro plays from the beginning, accessing your application and logging in.

6. Did the macro play correctly? In other words, indicate whether the login macro successfully logged in to the target site.
   - If you successfully accessed and logged into your application, click **Yes**.

     The macro recorder attempts to automatically detect a logout condition. When a logout condition is detected, the macro is complete. If a logout condition is not detected, you may need to identify one manually. For more information, see "Logout Conditions Editor" below.
   - If you did not successfully access and log into your application, click **No**. Click **Create** to start a new macro or see "Debugging macros" on page 189.

When you close the Login Macro Recorder, if the macro has changed since being saved, you are prompted to save changes before continuing.

Recording a workflow macro

In the Session-based Workflow Macro Recorder, do the following:

1. Type the start URL of your workflow in the address field and click  .
2. Click **Record**.
3. Navigate to the pages you want to record in the macro.

   As you navigate your application, a table of request data is added to the locations pane.
4. When you have recorded all of the steps in your workflow, click **Stop**.

   The macro is saved.
5. Click **Play**.

   The macro plays from the beginning, accessing the parts of your application recorded in the workflow.
6. Did the macro play correctly?
   - If you successfully accessed the parts of your application recorded in the workflow, click **Yes**. The macro is complete.
   - If you did not successfully access the parts of your application recorded in the workflow click **No**. Click **Create** to start a new macro or see "Debugging macros" on page 189.

When you close the Workflow Macro Recorder, if the macro has changed since being saved, you are prompted to save changes before continuing.

Logout Conditions Editor

The Logout Conditions Editor enables you to create or edit logout conditions for login macros. You can specify as many different logout conditions as you need, and if any of them is met, OpenText DAST or Fortify WebInspect Enterprise invokes the login macro to log back in and resume a scan

where it left off. The final set of all logout conditions should cover all the cases of becoming logged out during a scan of the target site.

When the Session-based Login Macro Recorder successfully detects a logout condition automatically, it categorizes the logout condition as one of the following types:

- **Automatic Redirect**. This type of logout condition is created when the Session-based Login Macro Recorder detects that the target site responds with a 302 redirect. It takes the form of a regular expression (regex).
- **Automatic**. This type of logout condition is created when the Session-based Login Macro Recorder detects that the target site responds with anything other than a 302 redirect, for example, with a 200.

Adding a logout condition

To add a new logout condition:

1. Click the **Logout Conditions** button in the toolbar.
2. Click  in the Logout Conditions pane.

   A new logout condition is added.
3. In the Properties pane, construct a regular expression (regex) to identify a logout for this logout condition.

   A regular expression is a pattern that describes a set of strings. Regular expressions are constructed much like mathematical expressions by using various operators to combine smaller expressions. Only users with a working knowledge of regular expressions should use this feature.

   The regex must reflect the difference between a) the response to a logged-in user's request to access a protected page, and b) the response to the same request from the user, while *not* logged in, to access the same protected page. The general steps to construct the regex are as follows:
   a. Start the Web Proxy tool to record web traffic. See the Web Proxy Help or the Web Proxy chapter in the *OpenText™ Dynamic Application Security Testing Tools Guide*.
   b. Log in to the target site legitimately and copy the URL of a protected page.
   c. Log out and use the copied URL to try to access the protected page without logging in.
   d. Compare the responses and identify a unique aspect of the response to the attempt to access the protected page without logging in.
   e. Open the Regular Expression Editor tool. See the Regular Expression Editor Help or the Regular Expression Editor chapter in the *OpenText™ Dynamic Application Security Testing Tools Guide*.
   f. Construct a regex that reflects the unique aspect of the response to the attempt to access the protected page without logging in.
   g. Copy the regex into the **Regex** field in the Logout Conditions Editor.
4. Click **OK** to save the logout condition and close the Logout Conditions Editor.

Deleting a logout condition

To delete a logout condition:

1. In the Logout Conditions pane, select logout condition to delete.
2. Click .

Browser settings

When using the Session-based Web Macro Recorder in stand-alone mode in OpenText DAST or in the Fortify WebInspect Enterprise Administrative Console, click the **Browser Settings** button in the toolbar to display the **Proxy Settings** and **Network Authentication** tabs.

Note: Browser settings are not saved in macros.

Proxy Settings tab

Select one of the options described in the following table.

Option	Description
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 locate a proxy autoconfig file and configure the browser's web proxy settings.
Use System proxy settings	Select this option to import the proxy server information from the local machine.
Use Firefox proxy settings	Select this option to import the proxy server information from Firefox.
Configure proxy settings using a PAC file	Select this option to load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the URL box.
Explicitly configure proxy settings	Select this option to configure a proxy by entering the requested information, as follows: • **Server:** Enter the URL or IP address of your proxy server.

Option	Description
	• **Port:** Enter the port number (for example, 8080). • **Type:** Select a protocol for handling TCP traffic through a proxy server—Standard, SOCKS4, or SOCKS5. • **Authentication:** Select an authentication method. For a description of authentication methods, see the Help or the User Guide for the product. • **User Name:** Specify a user name. • **Password:** Specify a password. • **Bypass proxy for:** If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), select this option and enter the addresses or URLs in the box. Use commas to separate entries.

Network Authentication tab

If network authentication is required:

1. Click **Network Authentication**.
2. Select one of the methods from the **Method** list. Methods are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **Negotiate**
   - **NT LAN Manager (NTLM)**
3. Specify a **User Name** and **Password** for network authentication.
4. Select or clear the **Client Certificate** check box. If selected, complete the Certificate Store fields and select a certificate.

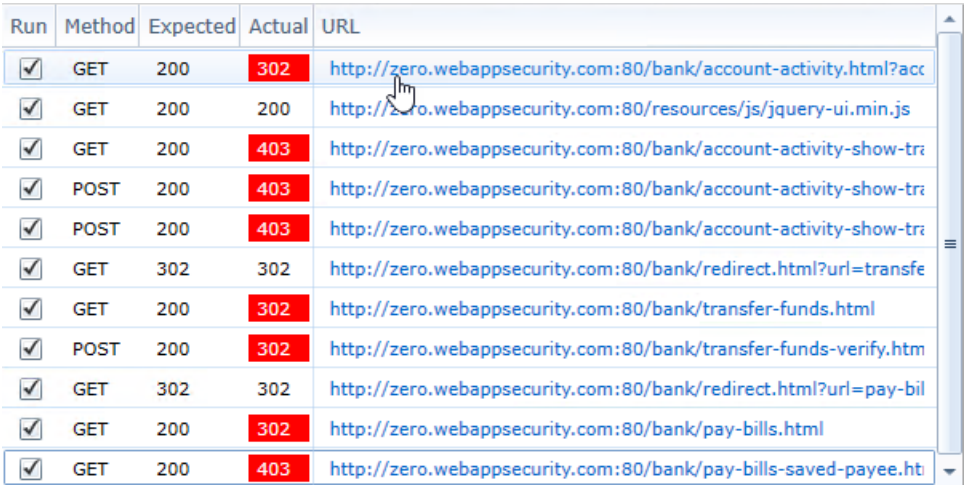
Debugging macros

This topic describes the basic steps involved in interactively debugging a macro, mainly in the locations pane.

Viewing details and state for locations in locations pane

To view details and state for recorded locations:

1. In the table in the locations pane, select a location that failed in the macro.



2. By default, the Details tab shows the Request and Response data. Verify that the **Scheme**, **Host**, and **Port** are correct.
3. Click the **State** tab to determine if state was lost during macro replay.
4. If necessary, you can add a new method for keeping state. To do so:
   a. Select a type from the **Type** drop-down list. Options for Type are:
      - Regex
      - Query
      - Post
      - Cookie
      - Custom
   b. Type a name for the new method in the **Name** field.
   c. Click **Add**.

Playing a step (location)

To play one step or location:

1. In the table in the locations pane, select a location that failed in the macro.
2. Click **Play Highlighted**.

Disabling/enabling a step (location) during replay

Disabled steps or locations remain in the macro and can be re-enabled in the future, but are not played.

To disable a macro step or location during replay:

- In the table in the locations pane, clear the check box in the **Run** column for the location.

To re-enable a macro step during replay:

- In the table in the locations pane, select the check box in the **Run** column for the location.

Deleting a step (location)

To permanently remove a location from the macro:

1. In the table in the locations pane, select a location that failed in the macro.
2. Click **Delete Highlighted**.

Chapter 18: Event-based Web Macro Recorder

OpenText™ Dynamic Application Security Testing (DAST), OpenText™ Fortify WebInspect Enterprise, and OpenText™ ScanCentral DAST include two Event-based Web Macro Recorder tools: one for login macros and one for workflow macros. In this chapter, these two tools are referred to generally as "Web Macro Recorder" except for specific login-related and workflow-related content.

Versions Available

The Event-based Web Macro Recorder is available for both Microsoft Windows® and Mac® operating systems. Most of the images in this chapter show the Windows version of the Web Macro Recorder. However, the Mac version functionality is identical unless otherwise noted.

About the Term “Sensor”

An OpenText DAST sensor is the OpenText DAST application when connected to Fortify WebInspect Enterprise or OpenText ScanCentral DAST for the purpose of performing remotely scheduled or requested scans with no direct user interaction through the OpenText DAST user interface. When content in this document applies to OpenText DAST, Fortify WebInspect Enterprise, and OpenText ScanCentral DAST, the term “sensor” is used.

About Macros

A login macro is a recording of the events that occur when you access and log in to a website. You can subsequently instruct the sensor to begin a scan using this recording. A workflow macro is a recording of specific URLs on a site. For more information, see "Login macros" on page 196 and "Workflow macros" on page 197.

TruClient Technology

The Event-based Web Macro Recorder tool was designed with TruClient technology. It uses event-based functionality and TruClient browser technology to record and play macros.

Web Macro Recorder Limitations

The Web Macro Recorder does not support the recording of Flash or Silverlight applications.

The TruClient technology used in the Web Macro Recorder is an adaptation of the Ajax TruClient technology originally developed for use with OpenText LoadRunner and OpenText Performance Center. It does not incorporate or support all the capabilities of the fully-featured version in those products.

Cookie Headers in Macros

When you play a macro, the sensor does not send any cookie headers that may have been incorporated in the recorded macro.

URLs in Macros

If a URL is in a macro, the request is always sent when the macro is played, regardless of any exclusion rules in scan settings.

Installing the Event-based Web Macro Recorder

The Event-based Web Macro Recorder is installed as part of the OpenText DAST toolkit when OpenText DAST is installed on Windows. You can install the standalone version on both Windows and Mac operating systems.

Installing the Standalone Web Macro Recorder on Windows

To install the Windows version:

1. Double-click the **MacroRecorder.msi** file.
   The Fortify Macro Recorder Setup opens.

   Note: When the file is downloaded from the ScanCentral DAST API container, the filename is `MacroRecorderWindowsX64Setup.exe`.
2. Select the checkbox to accept the terms in the License Agreement.
3. Click **Install**.
4. Click **Finish**.

Installing the Standalone Web Macro Recorder on Mac

Important! If the macOS® Gatekeeper quarantines the downloaded Web Macro Recorder DMG file, then download the file from a trusted source, such as the ScanCentral DAST API container.

To install the Mac version:

1. Double click on the **MacroRecorder<*version*>.dmg** disk image file.

   The program is mounted to the file system.

   Note: When the file is downloaded from the ScanCentral DAST API container, the filename is `MacroRecorderMacOSArm64Setup.dmg`.

2. Under **Locations** in the left pane, click **MacroRecorder** to open the installer.
3. Drag the **MacroRecorder** icon to the **Applications** icon.

Accessing the Event-based Web Macro Recorder

The following paragraphs describe the various ways to launch the Event-based Web Macro Recorder in OpenText DAST, Fortify WebInspect Enterprise, and OpenText ScanCentral DAST.

Login Macros in OpenText DAST or Fortify WebInspect Enterprise

You can record a new login macro or select (and optionally edit) an existing login macro that was recorded using TruClient browser technology in OpenText DAST or Fortify WebInspect Enterprise in the following ways:

- When configuring a Guided Scan with Firefox as the rendering engine, specify that the target site requires a login macro, and click **Create** to record a new login macro or select (and optionally edit) an existing login macro.
- When configuring a Basic Scan in OpenText DAST or a Web Site Scan in Fortify WebInspect Enterprise with Firefox as the rendering engine, in Step 2 select **Site Authentication** and record a new login macro or select (and optionally edit) an existing login macro.
- On the OpenText DAST toolbar, click **Tools > Login Macro Recorder > Macro Engine > Event-based (preferred)** to run the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- In Fortify WebInspect Enterprise, on the Administrative Console toolbar, click **Tools > Login Macro Recorder > Macro Engine > Event-based (preferred)** to open the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- Using the Security Toolkit, click **Start > Fortify > Login Macro Recorder (Event)** to run the Login Macro Recorder in stand-alone mode, and record a new login macro or open (and optionally edit) an existing login macro.
- Double-click an existing macro to open the macro in the TruClient sidebar and browser.

Workflow Macros in OpenText DAST or Fortify WebInspect Enterprise

You can record a new workflow macro or select (and optionally edit) an existing workflow macro that was recorded using TruClient browser technology in OpenText DAST or Fortify WebInspect Enterprise in the following ways:

- When configuring a Guided Scan with Firefox as the rendering engine, specify that the **Scan Type** is **Workflows** and later, in the **Workflows > 1. Manage Workflows** step, record a new workflow macro or import (and optionally edit) an existing workflow macro.
- When configuring a Basic Scan in OpenText DAST with Firefox as the rendering engine, in Step 1 select **Workflow-Driven Scan** and click **Record** or **Manage** to record a new workflow macro or select (and optionally edit an existing workflow macro.
- On the OpenText DAST toolbar, click **Tools > Workflow Macro Recorder > Macro Engine > Event-based (preferred)** to run the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- In Fortify WebInspect Enterprise, on the Administrative Console toolbar, click **Tools > Workflow Macro Recorder > Macro Engine > Event-based (preferred)** to open the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- Using the Security Toolkit, click **Start > Fortify > Workflow Macro Recorder (Event)** to run the Workflow Macro Recorder in stand-alone mode, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- Double-click an existing macro to open the macro in the TruClient sidebar and browser.

Login Macros in OpenText ScanCentral DAST

After you have downloaded the Web Macro Recorder tool to your local machine from the ScanCentral DAST API container, you can open the Login Macro Recorder in the following ways:

- When configuring a standard scan in the ScanCentral DAST Settings Configuration wizard, on the **Authentication** page, click **Open Macro Recorder 25.2**.

  Important! You cannot open the Web Macro Recorder if it has not been downloaded and installed on your local machine.

- To run the Login Macro Recorder in stand-alone mode, click **Start > Fortify ScanCentral DAST > Login Macro Recorder**, and record a new login macro or open (and optionally edit) an existing login macro.
- Double-click an existing macro to open the macro in the TruClient sidebar and browser.

For more information about downloading the Web Macro Recorder, see the *OpenText™ ScanCentral DAST Configuration and Usage Guide*.

Workflow Macros in OpenText ScanCentral DAST

After you have downloaded the Web Macro Recorder tool to your local machine from the ScanCentral DAST API container, you can open the Workflow Macro Recorder as follows:

- When configuring a workflow-driven scan in the ScanCentral DAST Settings Configuration wizard, on the **Target** page, click **Open Workflow Macro Recorder 25.2**.

  Important! You cannot open the Web Macro Recorder if it has not been downloaded and installed on your local machine.

- To run the Workflow Macro Recorder in stand-alone mode, click **Start > Fortify ScanCentral DAST > Workflow Macro Recorder**, and record a new workflow macro or open (and optionally edit) an existing workflow macro.
- Double-click an existing macro to open the macro in the TruClient sidebar and browser.

For more information about downloading the Web Macro Recorder, see the *OpenText™ ScanCentral DAST Configuration and Usage Guide*.

Standalone Web Macro Recorder on macOS

After you have installed the standalone Web Macro Recorder on the macOS, you can launch the application in the following ways:

- In **Applications**, double click the **MacroRecorder.app** icon.
- Using **Launchpad**, type `MacroRecorder` in the search field, and click the Web Macro Recorder  icon.
- Click the Web Macro Recorder  icon in the menu bar, and select **Open Web Macro Recorder**.
- Double-click an existing macro to open the macro in the TruClient sidebar and browser.

Login macros

A login macro is a recording of the activity that is required to access and log in to a website or web application, typically by entering a user name and password and clicking a button such as Log In or Log On. When you configure a scan, you usually specify a previously recorded login macro or record a new one at the time for the scan to use.

Logout conditions

To prevent the scan from terminating prematurely if the sensor gets logged out of your application, a login macro should also specify at least one logout condition that definitively indicates that a logout has occurred. During a scan, the sensor can get logged out for a variety of reasons, including:

- Normal logout driven by the target site
- An error condition in the target site such as a timeout
- An error in the macro itself, such as an invalid parameter

Specifying a logout condition as part of the login macro makes it unnecessary for users to manually log back in, perhaps repeatedly, when unexpected logouts occur during a scan. When scanning a site, the sensor analyzes every target site response to determine the state. If the sensor determines at any time that it is logged out, it runs the login macro to log back in, and then it resumes crawling or auditing the site at the point where the logout occurred.

You can specify multiple logout conditions, and if any of them are met, the sensor plays the login macro to log back in and resume the scan where it left off.

See also

"Working with logout conditions" on page 248

Workflow macros

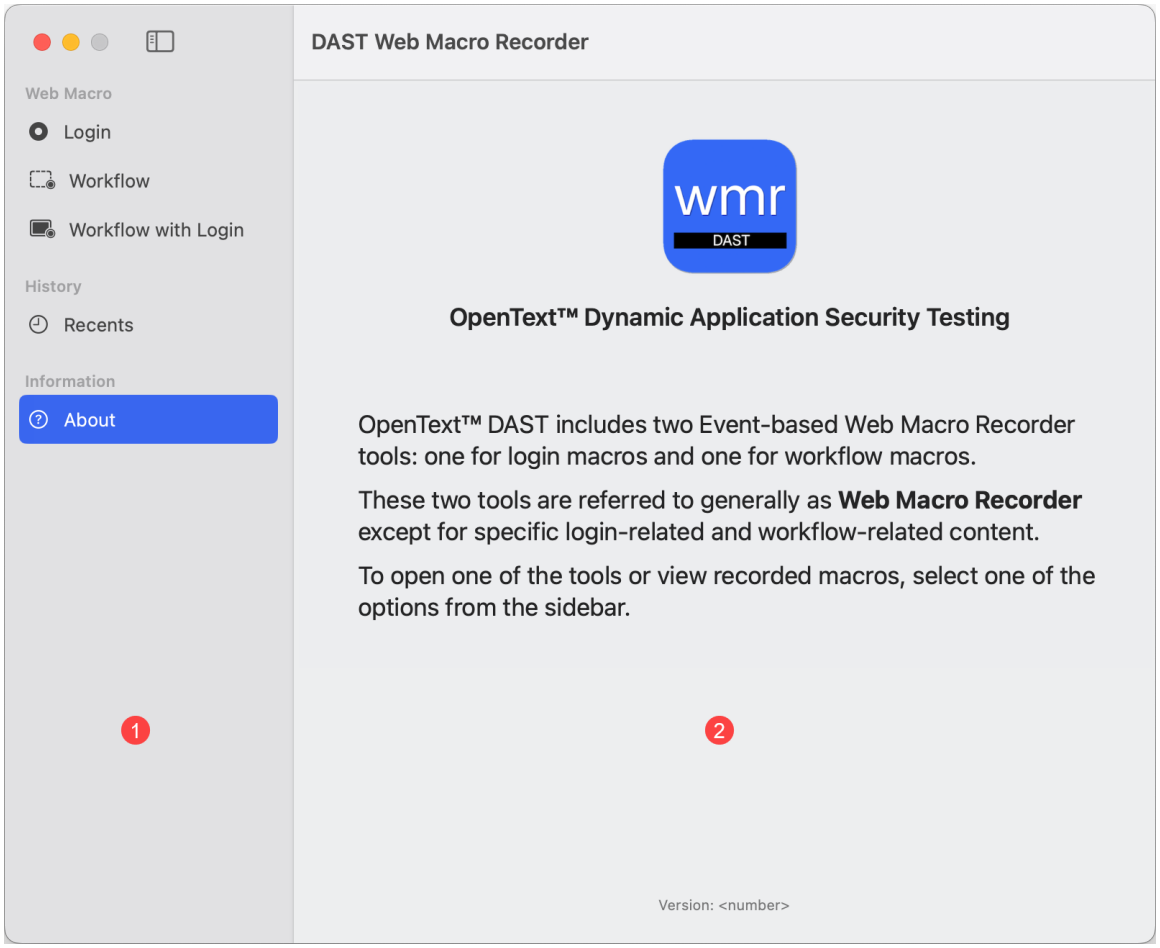
A workflow macro is a recording of the specific URLs to which you manually navigate on a site. When you configure a Basic Scan in OpenText DAST or a scan in OpenText ScanCentral DAST, you specify a previously recorded workflow macro or record a new one at the time for the scan to use. The sensor audits only the URLs that are recorded in the workflow macro and does not follow any hyperlinks encountered during the audit. This type of macro is used most often to focus on a particular subsection of an application. In terms of the macro recording process, the essential differences from login macros are that:

- Workflow macros include only the specific URLs to which a user navigated while recording them. Workflow macros access only those URLs upon replay.
- Workflow macros do not require logout conditions.

Note: If your website requires authentication, do not record login steps in a workflow macro. Instead, record a separate login macro to log in to your website. For more information, see "Login macros" on the previous page.

Working with the main application window (Mac only)

When you launch the Web Macro Recorder on the macOS, the main application window opens.



The following table describes the parts of the main application window.

Item	Description
1	The navigation sidebar provides options for recording Login, Workflow, and Workflow with Login macros, and for accessing recently edited macros. For more information about using the Login, Workflow, and Workflow with Login buttons in the navigation sidebar, see "Using the record buttons (Mac only)" on page 218.
2	The detail view provides various details or instructions for the option selected in the navigation sidebar.

Understanding the macro icons

The following table describes the icons used to indicate the different types of macros.

Icon	Type
	Login macro
	Workflow macro
	Workflow with login macro

Using the recents list

The recents list enables quick access to view or edit a recent macro.

To view or edit a recent macro:

1. In the navigation sidebar, click **Recents**.
   A list of the five most-recently edited macros appears in the detail view.

   Tip: When you hover over a macro, a tooltip displays the directory path to the file.

2. Double-click a macro in the recents list.
   The macro opens in the TruClient sidebar and browser.

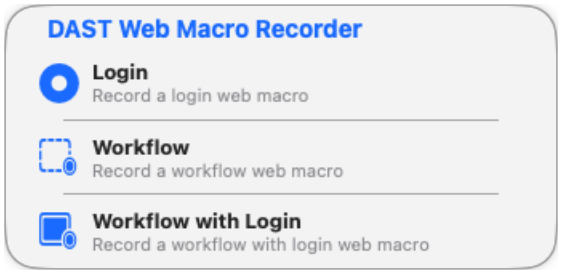
Using the recents list options

When you click the options  icon for a macro in the recents list, the following options are available:

- **Open** – Opens the macro in the TruClient sidebar and browser.
- **Open file location** – Opens the directory where the macro is saved.
- **Quick look** – Displays information about the macro without opening the Web Macro Recorder.
- **Remove** – Removes the macro from the recents list.

Using the Web Macro Recorder widget (Mac only)

The Web Macro Recorder widget provides a quick launch method to record a web macro. By default, the widget displays the Login, Workflow, and Workflow with Login macro recording options.



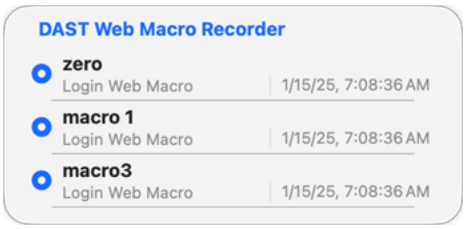
Refer to Apple® documentation for instructions on adding widgets to your desktop.

Editing the widget

After you have added the Web Macro Recorder widget to your desktop, you can configure it to display a recents list of macros.

1. On your Mac, control-click the Web Macro Recorder widget and select **Edit "DAST Web Macro Recorder"...**.
2. Slide the **Show Recent Macros** to the enabled position.
3. Click **Done**.

   The Web Macro Recorder widget now displays the three most-recently edited macros. You can select a macro from the list to open it in the Web Macro Recorder.



Using QuickLook (Mac only)

You can use the macOS QuickLook feature to view information about a web macro file without actually opening the Web Macro Recorder. Because web macros can be encrypted, only information that does not expose personally identifiable information (PII) is displayed.

For all macros, the following information is displayed:

- Macro Type - Indicates either a Login, Workflow, or Workflow with Login macro.
- Friendly Name - Identifies the user-supplied macro name.
- Engine Version - Indicates the TruClient engine version.
- Browser Version - Indicates the TruClient browser version being used, such as 110.0.
- Macro Modification Date - Indicates the date the macro was last modified.

Note: This date might be different than the system file modification date. For example, macros

that are copied from a different machine might show the date the file was copied rather than the last file modification date.

For login macros, the following additional information is displayed:

- Start Url - Specifies the start URL for the macro.
- Username - Identifies the user name whose credentials are used to login to the application.
- Has MFA - Indicates whether the macro includes multi-factor authentication.
- Has Event-Based LC - Indicates whether the macro includes an event-based logout condition.
- Has Verification Step - Indicates whether the macro includes a login verification step.

Tip: To view information about the macro, you must have permissions to access the file. If necessary, you can adjust permissions. Refer to Apple documentation for instructions on adjusting permissions.

To use QuickLook:

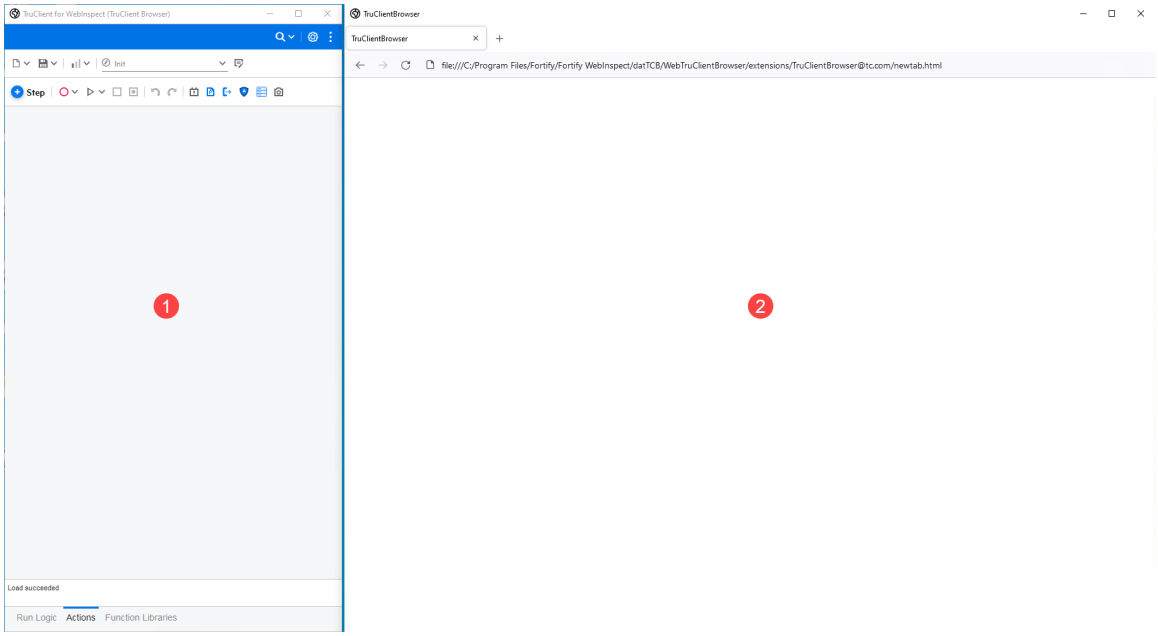
- With a web macro file selected, press the space bar.

  QuickLook displays details about the macro.

  From the QuickLook view, you can click **Open with MacroRecorder** to open the macro in the Web Macro Recorder.

Understanding the user interface

The Web Macro Recorder on Windows opens with two windows side by side as shown in the following image.



The following table describes the two windows.

Window	Description
1	The TruClient sidebar window. Use this window to control the recording and editing functions.
2	The TruClient browser window. Use this window to access your website.

The Web Macro Recorder on macOS opens the TruClient sidebar and browser upon recording or playback of a macro.

TruClient sidebar masthead

The following table describes the icons that are available in the masthead of the TruClient sidebar.

Icon	Name	Description
	**Search**	Opens the search panel. The drop-down menu provides options to search the macro or go to a specific step number. For more information, see "Searching the macro" on page 222.
	**General Settings**	Opens the General Settings dialog box. For more information, see "Configuring settings" on page 298.
	**More...**	Displays the following options: **Help** - Opens the Event-based Web Macro Recorder help. **About** - Opens a dialog box that provides version information for the Event-based Web Macro Recorder.

TruClient sidebar toolbars

The following table describes the toolbars, which are available at the top of the TruClient sidebar.

Icon	Name	Description
	**Open / New**	Opens an existing macro or script file, or creates a new one.
	**Save / Save As**	Saves a new macro or script file, or a copy of an existing file.
	**Step Level**	Modifies the script levels that are visible and replayed in the script.

Icon	Name	Description
		• - Displays and replays level 1 steps only. Level 1 steps are necessary for interacting with the application. • - Displays and replays level 1 and 2 steps. Level 2 steps affect the application in a way that is probably not important to the macro. • - Displays and replays level 1, 2 and 3 steps. Level 3 steps have no apparent effect on the application. For more information, see "Modifying the macro replay level" on page 242.
	**Action List**	Displays the actions (a set of steps) that are recorded in the macro. **Note:** Options are **Init**, **Action**, and **End**. However, the Init and End options do not apply. The Web Macro Recorder records actions in the Run Logic Action block only.
	**Manage Actions**	Opens the Actions dialog box. For more information, see "Working with actions" on page 255.
	**Add Step**	Opens the TruClient Steps box so that you can add steps to your macro. For more information, see "Using the Steps box" on page 214.
	**Record**	Starts recording the macro. Additionally, you can use the arrow to specify whether to record before, into, or after the selected step.
	**Replay**	Replays (or resumes replay of) the macro. Additionally, you can use the arrow to specify whether to play the selected step only, or to run the script step by step. Running the script step by step pauses the replay after each step.
	**Pause**	Pauses the replay of the macro.
	**Stop**	Stops recording or replaying the macro.
	**Toggle Breakpoint**	Toggles a breakpoint on the selected step. For more information, see "Using breakpoints" on page 289.

Icon	Name	Description
	**Undo / Redo**	Reverses your last action or restores your original change.
	**Event Handler Editor**	Opens the Event Handler Editor dialog box. For more information, see "Working with event handlers" on page 243.
	**Edit Parameters**	Set parameter values. For more information, see "Working with parameters" on page 259.
	**Edit logout conditions**	Opens the Logout Condition Editor. For more information, see "Working with logout conditions" on page 248.
	**Edit authenticators**	Opens the Authenticator Dialog. For more information, see "Using TOTP authentication" on page 234.
	**Edit Web Storage keys**	Opens the Manage Web Storage Keys dialog box. For more information, see "Working with web storage keys" on page 257. This icon is visible only if the **Support Web Storage** setting is enabled. For more information, see "Interactive Options" on page 303.
	**Snapshot view**	Not supported.

Context menu

Select a step in the TruClient sidebar and right click to display the context menu. The following table describes the context menu options.

Menu Option	Description
Play This Step	Replays the selected step only.
Play From This Step	Replays from the selected step. You cannot use **Play From This Step** if the target step: • Is located in an action that is not part of the run logic • Is inside a For loop or If block • Is a Catch Error step • Acts on a Web object that is not available on the current Web page
Play Until This	Replays from the beginning and stops before the selected step.

Menu Option	Description
Step	
Record > Before step	Inserts the next set of recorded steps before the selected step.
Record > Into step	Inserts the next set of recorded steps into the selected step.
Record > After step	Inserts the next set of recorded steps after the selected step.
Toggle Breakpoint	Inserts or removes a breakpoint on the selected step.
Group Steps	Groups multiple steps together as a single step.
Group Into	Groups multiple steps into: • **Action** - A group of steps that you define as a new or existing action. • **If Clause** - A logical structure that controls the flow of your script. • **For Loop Clause** - A logical structure that repeats the steps contained in the loop a specified number of times. • **New Function** - A group of steps, such as a login, that you define as a function. • **Two-factor authentication** - A group of steps that includes a request to the two-factor authentication control center and a step that waits for a two-factor authentication response.
Ungroup Steps	Reverts grouped step into multiple steps.
Cut	Cuts the selected step from the macro.
Copy	Copies the selected step in the macro.
Paste	Pastes the copied step into the macro.
Export Steps	Copies the selected steps in a macro to paste into another macro.
Import Steps	Pastes the steps that have been exported into a second script.
Delete	Deletes a step from the macro.

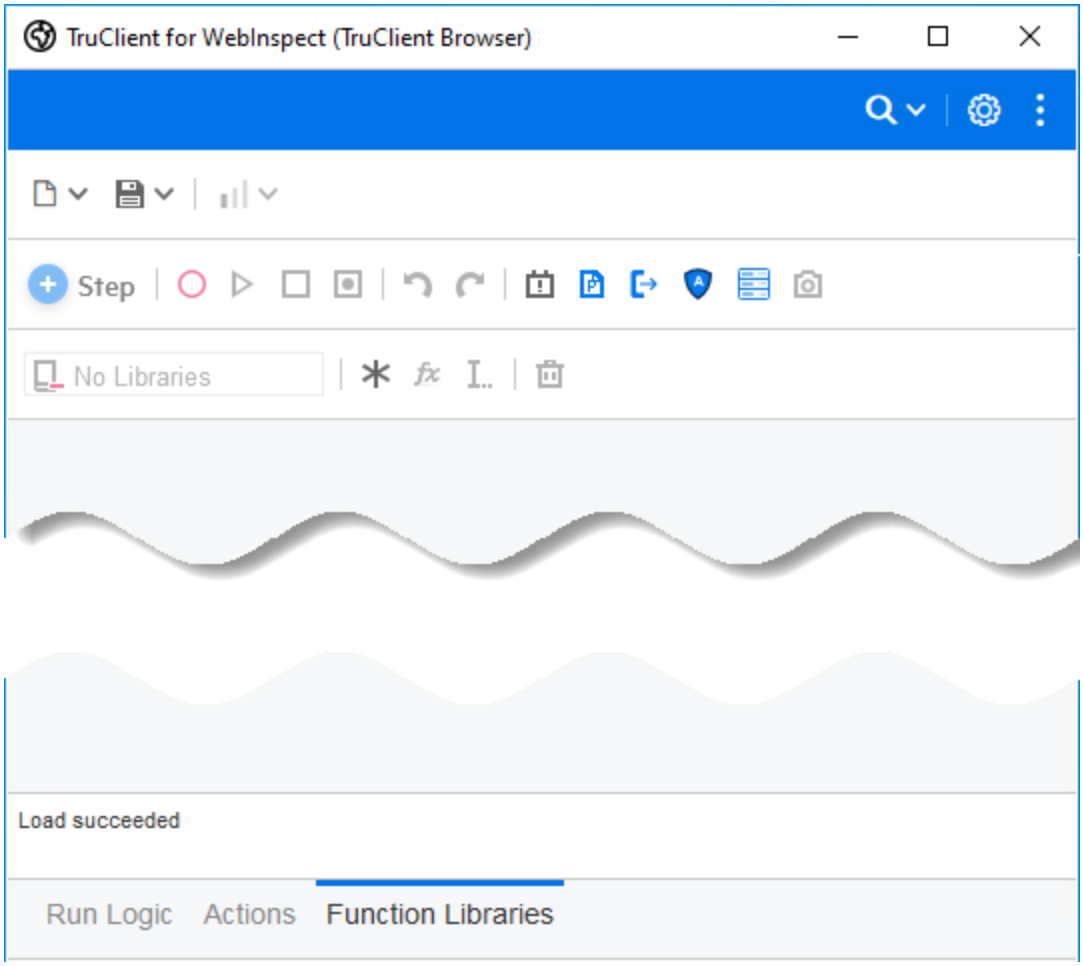
Menu Option	Description
Enable/Disable	Toggles between disabling or enabling a step during replay.
Edit Step	Expands the step to display the step, argument, and transaction properties.
Fold All Steps	Minimizes all steps and groups.
Unfold All Steps	Displays all steps and groups.
Reset Auto End Event	Enables you to reset the selected step or steps to **Automatic: Not Yet Set**.
Change Object Identification Method	Enables you to change the object identification method to: • Automatic • XPath • JavaScript • Descriptors

TruClientBrowser menu (Mac only)

The Mac version includes the TruClientBrowser menu, which is a Mac-specific menu with functions for managing the TruClient Browser window.

Understanding the Function Libraries tab

The Function Libraries tab includes a toolbar with icons for creating and managing TruClient function libraries.



Function Libraries toolbar

The following table describes the toolbar, which is available at the top of the TruClient sidebar when the Function Libraries tab is selected.

Icon	Name	Description
✳	**New Library**	Opens the New library dialog box and enables you to create a new library.
fx	**New Function**	Creates a new function. For more information, see "Working with function libraries" on page 245.
I	**Rename Library**	Renames an existing library. **Important!** If you rename a library, modify all references to it.
🗑	**Delete Library**	Deletes a local function library from the script.

Using shortcut keys

You can use shortcut keys to access most of the functionality in the Web Macro Recorder. While some of the shortcut keys are the same on both Windows and Mac keyboards, there are many differences. The following tables describe how to access the various functions using shortcut keys.

Basic functionality

The following table describes shortcut keys for basic functions, such as opening existing macros, creating new ones, and accessing certain product features.

Function	Windows	Mac
Open	Alt + O	⌥ + O
New	Alt + N	⌥ + N
Save	Ctrl + Alt + S	⌘ + ⌥ + S
Save As	Ctrl + Alt + A	⌘ + ⌥ + A
Record	Ctrl + Alt + R	⌘ + ⌥ + R
Play / Pause	Ctrl + Alt + 5	⌘ + ⌥ + 5
Replay selected step	F7	F7
Replay step by step	F8	F8
Stop	Ctrl + Alt + X	⌘ + ⌥ + X
Toggle breakpoint	F9	F9
Go To	Ctrl + G	⌘ + G
Undo	Ctrl + Z	⌘ + Z
Redo	Ctrl + Y	⌘ + Y
Snapshot viewer	Ctrl + Alt + V	⌘ + ⌥ + V
Open / Close Steps Box	Ctrl + Alt + K	⌘ + ⌥ + K

Recents list functionality (Mac only)

The following table describes shortcut keys that are available for a macro that is selected in the recents list.

Function	Mac
Open	⌘ + O Enter
Open file location	Shift + ⌘ + O
Quick look	⌘ + P Spacebar

Login and workflow functionality (Mac only)

The following table describes shortcut keys that are available for the login or workflow sections of the application.

Function	Mac
Start the TruClient sidebar and browser for login macro recording (from the login section)	⌘ + S
Start the TruClient sidebar and browser for workflow macro recording (from the workflow section)	

Search functionality

The following table describes shortcut keys for searching.

Function	Windows	Mac	Notes
Search in Current View	Ctrl + F	⌘ + F	Opens the search view if it is closed
	/ (forward slash)	/ (forward slash)	
	' (single quote)	' (single quote)	
Find Next	F3	F3	
Find Prev	Shift + F3	Shift + F3	
	Ctrl + Shift + G	⌘ + Shift + G	
Hide Search	Esc	Esc	Closes the search view if it is open
Search Whole Script	Ctrl + Shift + F	⌘ + Shift + F	

Step-related functionality

The following table describes shortcut keys for functions related to steps inside recorded macros, such as playing a step, moving a step, and grouping steps.

Function	Windows	Mac	Notes
Play Step-by-Step	F8	F8	
Play This Step	F7	F7	
	l (lowercase L)	l (lowercase L)	If the Step context menu is open
Play From This Step	F	F	If the Step context menu is open
Play Until This Step	U	U	
Open "Record" Sub Menu	R	R	

Function	Windows	Mac	Notes
Record Before Step	B	B	If the Record sub menu is open
Record After Step	A	A	
Record Into Step	I	I	If the Record sub menu is open and the step is a group step
Toggle Breakpoint	F9	F9	
	B	B	If the Step context menu is open
Group Steps	G	G	If the Step context menu is open
Open "Group Into" Sub Menu	u	u	
Group Into Action	A	A	If the Group Into sub menu is open
Group Into If Clause	I	I	
Group Into For Loop	F	F	
Group Into New Function	N	N	
Group Into Two-factor authentication	T	T	
Cut	Ctrl + X	⌘ + X	
	t	t	If the Step context menu is open
Copy	Ctrl + C	⌘ + C	
	C	C	If the Step context menu is open
Paste	Ctrl + V	⌘ + V	
Open "Paste" Sub	P	P	If the Step context menu is open

Function	Windows	Mac	Notes
Menu			
Paste Before	Alt + P	⌥ + P	
	B	B	If the Paste sub menu is open
Paste Into	Alt + I	⌥ + I	
	I	I	If the Paste sub menu is open
Paste Into Else	Alt + E	⌥ + E	
Paste After	Alt + A	⌥ + A	
	A	A	If the Paste sub menu is open
Export Steps	Ctrl + Alt + Q	⌘ + ⌥ + Q	
	x	x	If the Step context menu is open
Import Steps	Ctrl + Alt + I	⌘ + ⌥ + I	Step must be selected to import after
	m	m	If the Step context menu is open
Delete	Delete (⌦)	Backspace (⌫)	
	D	D	If the Step context menu is open
Enable/Disable	Ctrl + /	⌘ + /	
Enable	Shift + /	Shift + /	
Disable	Alt + /	⌥ + /	
Edit Step	Ctrl + Alt + O	⌘ + ⌥ + O	Expand the step to display step argument properties
	E	E	If the Step context menu is open
Fold All Steps	Alt + 0	⌥ + 0	
Unfold All Steps	Alt + Shift + 0	⌥ + Shift + 0	
Reset Auto End Event	Alt + B	⌥ + B	

Function	Windows	Mac	Notes
Change Object Identification Method	I	I	If the Step context menu is open
Open Step Context Menu	Context Menu key	⌥ + Enter	
Set Step Object Identification Method to "Descriptors"	Ctrl + Alt + 3	⌘ + ⌥ + 3	
Select All Steps	Ctrl + A	⌘ + A	
Expand Group Step	Right Arrow (▸)	Right Arrow (▸)	Group step must be selected
Collapse Group Step	Left Arrow (◂)	Left Arrow (◂)	
Move to Last Step	Page Down	Page Down	
Move to First Step	Page Up	Page Up	
Move Between Steps	Up / Down Arrows (▲ | ▼)	Up / Down Arrows (▲ | ▼)	
Select All Steps Above Current Step	Shift + Home	Shift + ⌘ + Up Arrow (▲)	
Select All Steps Below Current Step	Shift + End	Shift + ⌘ + Down Arrow (▼)	

Object selection functionality

The following table describes shortcut keys for functions related to object selection in the TruClient browser window.

Function	Windows	Mac	Notes
Suspend Object Selection	Ctrl + Alt + F6	⌘ + ⌥ + F6	Object Selection dialog must be open. Allows access to the application elements while remaining in Object Selection mode.
Highlight Object in Application	Ctrl + Alt + H	⌘ + ⌥ + H	Step must be selected

Using the Steps box

The Steps box (previously called the Toolbox) contains all of the steps that you can add to a macro.

Adding a step

To add a step to a macro:

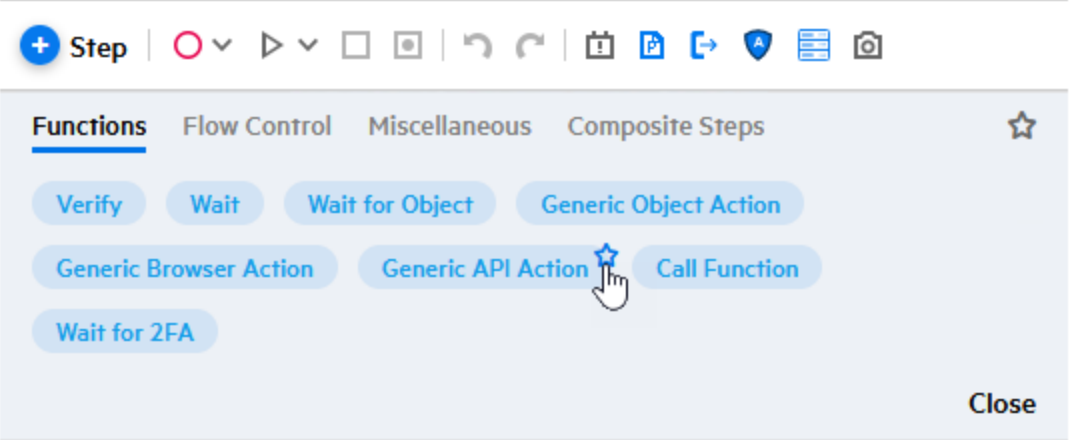
1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Select the tab for the type of step to add. For more information about the tabs, see the following:
   - "Functions tab" on the next page
   - "Flow Control tab" on page 216
   - "Miscellaneous tab" on page 217
   - "Composite Steps tab" on page 218
3. Select a step in the tabs and drag it to the desired location in the macro.

Marking a step as favorite

You can mark a step as a favorite and then quickly access it in the favorites view.

To mark a step as a favorite:

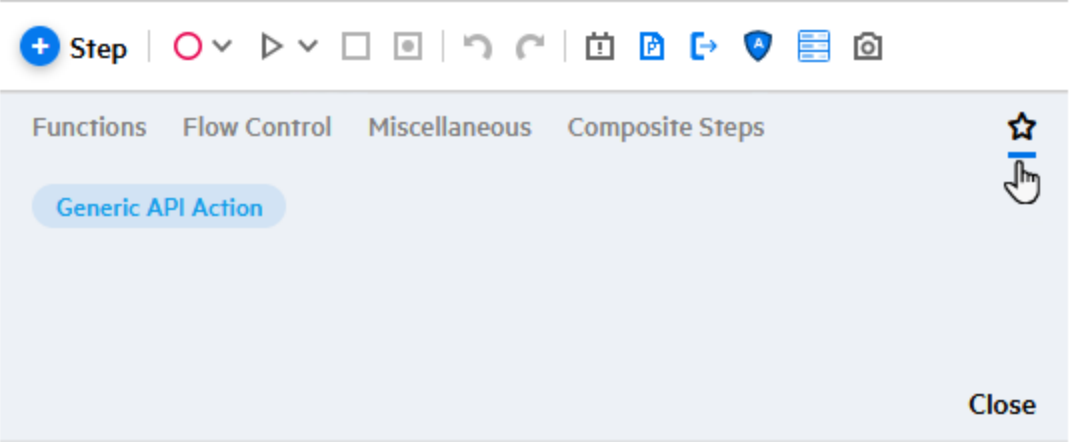
- Click the star icon for the desired step.



Viewing favorite steps

To view your favorite steps:

- Click the star icon in the Steps box.



Functions tab

The following table describes functions steps.

Step	Description
Verify	Verify that an object exists in the application.
Wait	Wait for a specified number of seconds before continuing with the next step.

Step	Description
Wait for Object	Wait for an object to load before continuing with the next step.
Generic Object Action, **Generic Browser Action**, or **Generic API Action**	Blank steps that can be inserted and manually configured. For API argument details, refer to the API Help in the TruClient Help Center at https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/TC_Functions.htm. **Note:** The Web Macro Recorder supports a subset of the API arguments documented in the TruClient Help Center.
Call Function	Not supported.
Wait for 2FA	Wait for a two-factor authentication response to be forwarded from the two-factor authentication control center. The two-factor authentication control center processes the SMS and email responses coming from your application server. For more information, see "Using two-factor authentication" on page 228. **Note:** This step is included in the **Two-factor Authentication** group step.

Flow Control tab

The following table describes flow control steps.

Step	Description
For Loop	A logical structure that repeats the steps contained in the loop a specified number of times. For more information, see "Inserting loops and loop modifiers" on page 284.
If Block	A logical structure that runs the steps contained in the block if the condition is met. • **Add else** – Click the **Add else** link to add an **Else** section to your **If** block. If the condition is not met, the steps included in the **Else** section run. • **Remove else** – Removes the **Else** section from the **If** block. **Note:** The else sections apply to all If types (If Block, If Exists, If Verify, and If Browser). If the **Else** section contains steps and you click **Remove else**, the steps are deleted. Copy and paste them into the main

Step	Description
	body of your macro to save them. For more information, see "Inserting If blocks, If-else blocks, and Exit steps" on page 285.
If Verify	A combination of “If Block” and “Verify,” a logical structure that runs the steps contained in the block if the condition on a property of the selected object is met.
If Exists	A logical structure that runs the steps contained in the block if the selected object exists in the application.
Break	Causes the loop to end immediately without completing the current or remaining iterations.
Continue	Causes the current loop iteration to end immediately. The macro continues with the next iteration.
Catch Error	Catches an error in the step immediately preceding and runs the contents of the catch error step. For more information, see "Inserting Catch Error steps" on page 287.
Exit	Exits the iteration or the entire macro, depending on the specified setting.
Two-factor Authentication	Sends a request to the two-factor authentication control center to begin the authentication flow. This group step includes basic instructions on how to configure two-factor authentication components. For more information, see "Using two-factor authentication" on page 228. **Note:** This is a group step that includes the **Wait for 2FA** step.

Miscellaneous tab

The following table describes miscellaneous steps.

Option	Description
Evaluate JavaScript	Runs the JavaScript code contained in the step.
Evaluate JS on	Runs the JavaScript code contained in the step after the specified object is

Option	Description
Object	loaded in the application.
Comment	A blank step that enables you to write comments in your macro.

Composite Steps tab

The **Answer Security Questions** step enables you to select the interface object (usually a label) that asks a security question and the interface object (usually a text box) where the user provides the answer. Then you specify the text of the question and the answer.

Using the record buttons (Mac only)

The Mac version of the Web Macro Recorder enables you to record three types of macros:

- Login – a traditional login web macro. See "Login macros" on page 196.
- Workflow – a traditional workflow web macro. See "Workflow macros" on page 197.
- Workflow with Login – a workflow web macro with login credentials. This option enables you to select an existing login macro which is loaded into the TruClient sidebar. You can then play the login steps, navigate to your first workflow step, and start recording.

Starting a login macro

To begin recording a login macro:

1. On the main application window or the Web Macro Recorder widget, click **Login**.
2. Click **Start**.
3. Continue with "Recording a login macro" on the next page.

Starting a workflow macro

To begin recording a workflow macro:

1. On the main application window or the Web Macro Recorder widget, click **Workflow**.
2. Click **Start**.
3. Continue with "Recording a workflow macro" on page 220.

Starting a workflow with login macro

To begin recording a workflow with login macro:

1. On the main application window or the Web Macro Recorder widget, click **Workflow with Login**.
2. Select or drag and drop the login macro to use for authentication.
3. Click **Start**.

   The login macro is loaded into the TruClient sidebar and played automatically. After successful login, the login macro is closed. You are now logged in and can record your workflow macro.
4. Continue with "Recording a workflow macro" on the next page.

Recording a macro

When recording a macro, use the TruClient sidebar to control the recording functions and the TruClient browser to access your website.

Recording a login macro

This procedure describes how to record a basic login macro. For information about challenge-response login macros, see "Challenge-response authentication" on page 224 and "Recording a macro for challenge-response logins" on page 225.

To record a login macro:

1. In the TruClient browser, navigate to the start URL for your website.
2. In the TruClient sidebar, click the **Record** icon ( ).
3. In the TruClient browser, navigate to the login form and log in to the application.
4. After you log in, click the **Stop** icon ( ) in the TruClient sidebar, but do not log out.
5. In the TruClient sidebar, click the **Play** icon ( ) to verify that your macro logs in correctly.
6. Did the macro log in correctly?
   - If *yes*, the TruClient sidebar prompts you to select an object to indicate a successful login. Proceed to the next step.

     Note: If the **Force last step to be a validation step** setting on the **Interactive Options** tab is disabled, you will not be prompted to select an object. Proceed to Step 8. For more information, see "Configuring settings" on page 298.
   - If *no*, click **File > New**. If prompted, do not save the macro. Return to Step 1.
7. In the TruClient browser, identify an object that appears only after successful login.

Important! If the **Force last step to be a validation step** setting on the **Interactive Options** tab is enabled, the last step must be a “wait for object” step.

A wait action for the selected object is added to the recorded steps.

The Web Macro Recorder attempts to automatically detect a logout condition. For information about how to add or edit logout conditions later, see "Working with logout conditions" on page 248.

8. Click the **Save** icon ( ) to save the macro.

To add options to the login macro, see "Enhancing macros" on page 283.

Recording a workflow macro

To record a workflow macro:

1. In the TruClient browser, navigate to the start URL for your workflow.
2. In the TruClient sidebar, click the **Record** icon ( ).
3. In the TruClient browser, navigate to the pages you want to record in the macro.
4. After you record your navigation, click the **Stop** icon ( ) in the TruClient sidebar.
5. Do one of the following:
   - To verify that your navigation was recorded correctly, click the **Play** icon ( ) in the TruClient sidebar.
   - To add steps from the Steps box to your recorded navigation, click the **Add Step** (Step) icon. For more information, see "Using the Steps box" on page 214.
6. When you have finished, click the **Save** icon ( ) to save the macro.

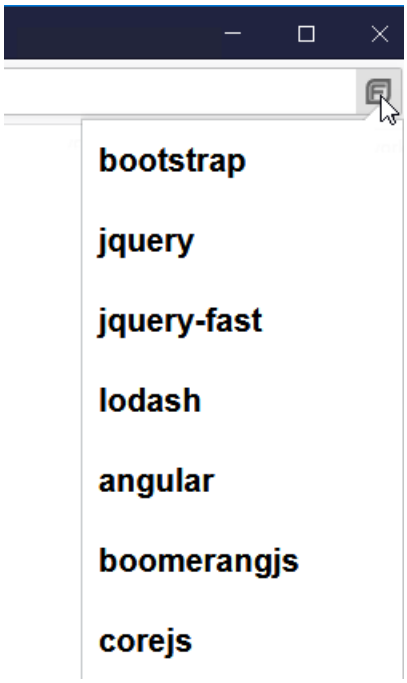
Automatic detection of client-side frameworks

When accessing an application, the Web Macro Recorder attempts to detect client-side frameworks that are used in the target application. If the Web Macro Recorder detects such frameworks, an icon with a Fortify logo appears to the right of the URL address box in the TruClient browser window.

Viewing detected frameworks

To view the detected client-side frameworks:

1. Click the Fortify logo to the right of the URL address.
   The list of detected frameworks appears.



Tip: If you notice a framework in the list that indicates a single-page application (SPA), you can enable the SPA Support option in your scan settings. For more information, refer to the *OpenText™ Dynamic Application Security Testing User Guide* or the *OpenText™ ScanCentral DAST Configuration and Usage Guide*.

2. (Optional) Hover over a framework in the list to view its version.

Note: The Web Macro Recorder cannot determine all versions of frameworks. In such cases, it indicates "unknown version."

Editing a macro

As you edit a macro, you use the TruClient sidebar to add or edit the recorded steps and the TruClient browser to access your website. For more information, see "Understanding the user interface" on page 201.

To edit a macro:

1. In the TruClient sidebar, click the drop-down arrow in the **File** icon ( ) and select **Open**.
2. Add or edit steps in the macro. For more information, see "Enhancing macros" on page 283 and "Debugging macros" on page 288.
3. Click the save icon ( ) to save the macro.

Searching the macro

You can search the macro or go to a specific step number in the macro.

Searching the steps

To search the macro:

1. In the TruClient sidebar, click the search icon ( ).
   The search panel opens.
2. Optionally, specify what to search in the drop-down lists. Options for the search scope are:
   - **Current View** - searches only steps that are visible
   - **Whole Script** - searches all steps, even those that are not expanded

   Options for the entity type are:
   - **All** - searches in steps and transactions
   - **Steps** - searches steps only

   Note: Transactions are not used in the Web Macro Recorder, so the **Transactions** entity type does not apply.
3. Type a search string in the search box.
   For a Current View search, the search string is highlighted in the visible steps and/or transactions as you type.
   For a Whole Script search, a list of the steps and/or transactions in which the search string is found appears as you type.
4. Press the **Enter** key to navigate through the search results.

   Tip: You may also use the **Go to the next result** and **Go to the previous result** icons beside the result count to navigate through the search results.

Going to a specific step number

To go to a specific step number in the macro:

1. In the TruClient sidebar, click the search icon drop-down arrow ( ), and then select **Go To**.
   The Go To dialog box appears.
2. In the **Step number** box, type a number.
3. Click **Go To**.
   The step is highlighted in the macro.

Using the CLI (Windows only)

You can perform some common tasks using the Event-based Web Macro Recorder by way of the command-line interface (CLI).

Launching the CLI

To launch the CLI:

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

  The Administrator: Command Prompt window appears.

Important! At the command prompt, use the `cd` command to change the current working directory to the directory where the Web Macro Recorder application is installed.

The Web Macro Recorder is installed in the same directory as OpenText DAST. By default, the installation directory is:

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

CLI options

The following table describes the options that are available for the Web Macro Recorder tool in the CLI.

To...	Type the following at the command prompt...
Record a login macro	`macrorecorder.exe`
Load an existing login macro for editing	`macrorecorder.exe --fileToLoad 'PathToFile'`
Record a workflow macro	`macrorecorder.exe --workflow`
Load an existing workflow macro for editing	`macrorecorder.exe --fileToLoad 'PathToFile' --workflow`
Load and automatically play an existing login macro so that a workflow macro can be recorded	`macrorecorder.exe --pre-workflow-login 'PathToLoginFile' --workflow`
Load and automatically play an	`macrorecorder.exe --fileToLoad 'PathToFile' --pre-workflow-login 'PathToLoginFile' --`

To...	Type the following at the command prompt...
existing login macro followed by an existing workflow macro for editing	`workflow`
Display the CLI help	`macrorecorder.exe --help`

Challenge-response authentication

Challenge-response authentication is a family of protocols in which the server presents a question (the challenge) and the client must provide a valid answer (the response). In the simplest example, the challenge asks for a password and the valid response is the correct password.

Multiple challenges

Some websites present multiple challenges to the user. Typically, when a user first registers with a website, the site presents a list of questions to which the user provides answers that will be used for subsequent authentication. For example:

- What is your favorite color?
- What was the name of your first pet?
- In what town or city were your born?
- What was the make of your first automobile?

When the user later attempts to log in, the website presents two or more of these challenges.

Groups of challenges

Some sites also create groups of challenges, and present questions from the groups on each new login attempt, as demonstrated in the following example.

When registering for the example website, the user is asked to provide answers to nine questions, which are arranged into three groups of three questions each, as follows.

Group 1

Q: What is your quest? A: happiness
Q: What is your name? A: Smith
Q: What is your favorite color A: blue

Group 2

Q: What is the name of your favorite pet? A: Rusty
Q: What is your mother's maiden name? A: Jones
Q: In what state were you born? A: Delaware

Group 3

Q: What is the capital of Mongolia? A: Ulaanbaatar
Q: What is the name of a sea bird? A: Albatross
Q: What is your paternal grandmother's first name? A: Esther

The login page might look like this (using the first question from each group):

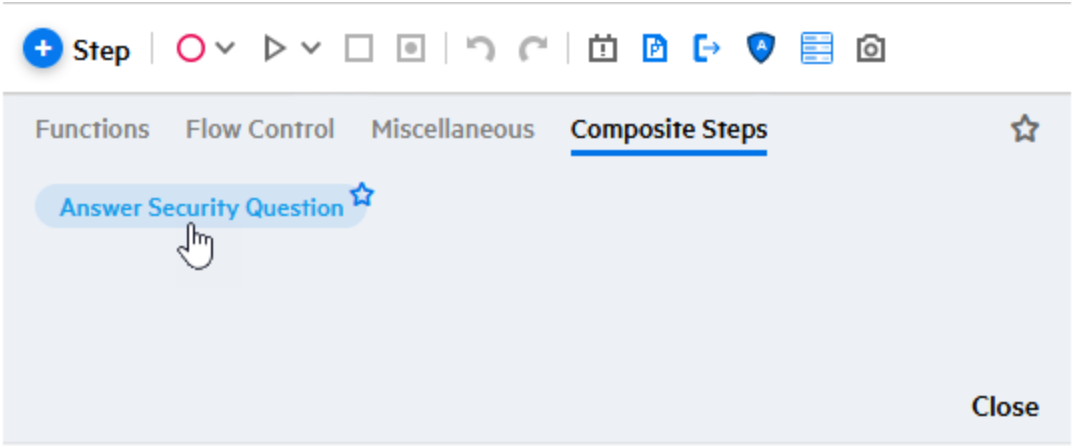
Recording a macro for challenge-response logins

When recording a macro for a challenge-response type of login, you must know all possible question-and-answer combinations, even if only a subset of those combinations might be presented during any one login. You enter these combinations manually, as special steps as you record a macro.

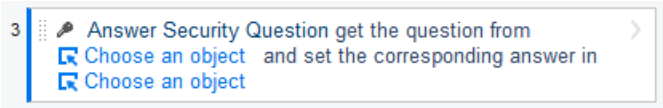
At the point where the target site asks the challenge questions, usually after logging in with username and password credentials, use the following procedure to manually create the required steps for the set of questions:

1. While recording the macro, click the **Stop** icon (☐) in the TruClient sidebar.
2. Click the **Add Step** icon (Step).

3. Click **Composite Steps**, and then click and drag the **Answer Security Question** step into the recorded steps.

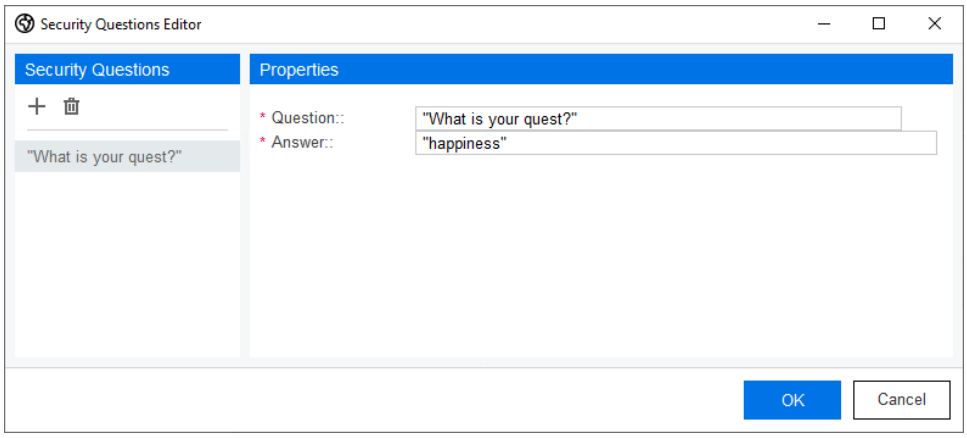


A new step is created.



4. Click the first **Click to choose an object** link in the new step and then, in the TruClient browser window, click the object representing the question (usually a label).
5. Click the second **Click to choose an object** link in the new step and then, in the TruClient browser window, click the object representing the answer (usually a text box).
6. In the TruClient sidebar, click the **Step Editor** icon ( ) for the Answer Security Question step.
   The Step Editor opens.
7. Click (expand) the **Security Questions** section.
8. Click + to open the Security Questions editor.
9. In Security Questions Editor, click the **Add a new question** icon (+).
   A new question appears with the default name "Question1." Its properties include the text box labeled Question (also shown with a default value of "Question1") and the text box labeled Answer, with a default value of "Answer1."
10. In the **Question** text box, type over the default text with the actual question exactly as it appears on the login page, including capitalization and punctuation. The question in the left pane is simultaneously updated.

Important! Be sure to enclose the text in quotation marks.



11. In the **Answer** box, enter the correct response in quotation marks.
12. Repeat Steps 9 through 11 to add the information for the second question that might appear in the same location on the web page. In this example, the question is "What is the name of your favorite pet?"
13. Repeat Steps 9 through 11 to add the information for the third question that might appear in the same location on the web page. In this example, the question is "What is the capital of Mongolia?"
14. Click **OK**.

    The questions and answers are added to the table in the Security Questions section in the macro step.

Tip: If you later need to edit a question or answer, reopen the Security Questions Editor.

This completes the macro step for this particular location on the web page. To create more questions and answers for additional challenges, continue with "Adding questions and answers for additional challenges" below.

Adding questions and answers for additional challenges

To add questions and answers for additional challenges:

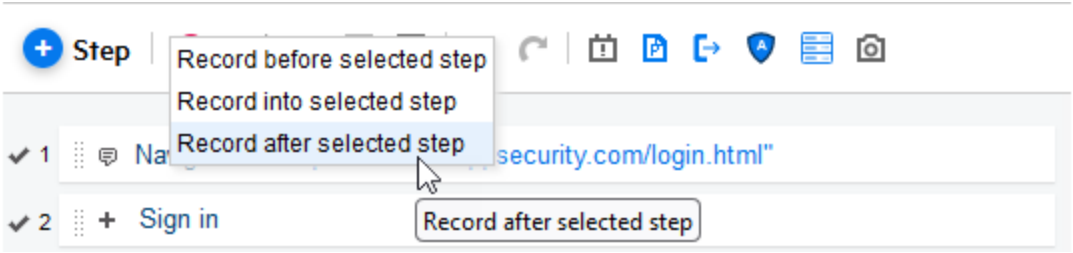
1. Do one of the following to refresh the web page until the second set of questions appears:
   - Click in the TruClient browser window and press **F5**.
   - Right-click in the TruClient browser window and select the **Reload** icon.
2. Repeat Steps 2 through 14 of "Recording a macro for challenge-response logins" on page 225 to add another macro step for the second set of three questions and answers at the second location on the web page.

3. Do one of the following to refresh the web page until the third set of questions appears:
   - Click in the TruClient browser window and press **F5**.
   - Right-click in the TruClient browser window and select the **Reload** icon.
4. Repeat Steps 2 through 14 of "Recording a macro for challenge-response logins" on page 225 to add another macro step for the third set of three questions and answers at the third location on the web page.

Recording additional steps

If you need to record additional steps after creating steps for all possible question-and-answer combinations, then do the following:

1. In the TruClient sidebar, select the last step you created.
2. Click the drop-down arrow in the **Record** icon (○ ⌄) and select **Record after selected step**.



3. Continue recording as usual.
4. Click the **Stop** icon (□).
5. Replay and save the macro.

Using two-factor authentication

After recording your login macro, you can add a **Two-factor Authentication** group step to the macro to use two-factor authentication in a scan in OpenText DAST or OpenText ScanCentral DAST.

Note: Two-factor authentication is not supported in Fortify WebInspect Enterprise.

Important! If testing locally prior to using two-factor authentication in a scan, then you must first configure the two-factor authentication control center and the **Fortify2FA** mobile application.
For more information, see "Configuring settings" on page 298.

Recommendation

For privacy concerns, OpenText does not recommend using personal phones or email addresses. OpenText strongly recommends using test phones or test email addresses only.

Known limitations

The following known limitations apply to the two-factor authentication feature:

- IMAP and POP3 servers are supported. However, only POP3 servers that support unique ID listing (UIDL) are supported.
- Currently, only Android mobile phones are supported.
- The mobile phone requires a Wi-Fi connection on the same subnet where OpenText DAST is installed.

Facts about Gmail accounts

Be aware of the following facts related to Gmail accounts:

- Gmail account settings include normal mode and recent mode. If you use a Gmail account and experience issues with new incoming emails, using recent mode might resolve this issue. To enable recent mode, configure the account name in your POP3 account settings using the following format:

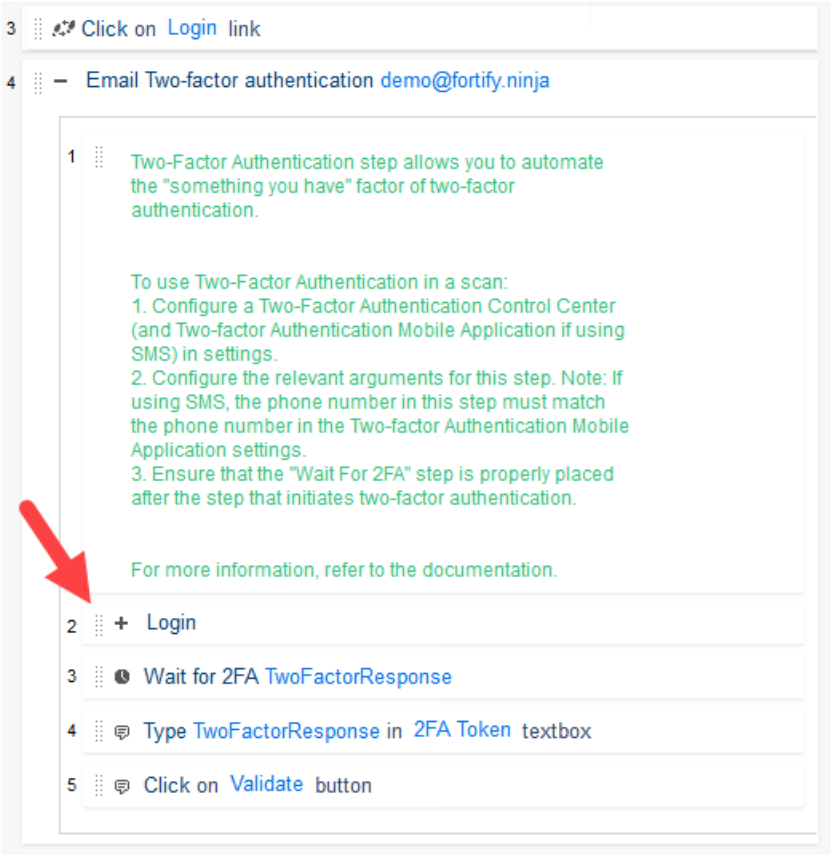
  `recent:<email_address@gmail.com>`
- For security, Google uses "Sign in with Google" to connect Gmail to a user's Google account and does not accept user-created passwords. When using a Gmail account, you must create and use a Google app password. For more information, refer to Google account documentation for creating and using app passwords.

Guidelines

Follow these guidelines when configuring Two-factor Authentication:

- You cannot have a **Two-factor Authentication** group step inside another **Two-factor Authentication** group step.
- You cannot have two **Wait for 2FA** steps inside a **Two-factor Authentication** group step.
- You must configure a **Type** step and a **Click** step after the **Wait for 2FA** step to complete the log in process.

- When configuring a login macro for Two-factor Authentication, the login step must be inside the **Two-factor Authentication** group step as shown in the following image.



Adding a Two-factor Authentication group step

The **Two-factor Authentication** group step sends a request to the two-factor authentication control center to begin the authentication flow.

Important! The **Two-factor Authentication** group step includes a **Wait for 2FA** step that you must also configure. Otherwise, the **Two-factor Authentication** group step will fail.

To add a **Two-factor Authentication** group step:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **Two-factor Authentication** group step to the recorded steps, and drop it after the username and password have been entered.
   By default, an SMS Two-factor authentication step is added.
4. Continue according to the following table.

For...	Do this...
SMS Responses	Expand the **Arguments** and configure the following: • In the **Phone Number** box, enter the phone number that will receive SMS responses. **Tip:** You can enter JavaScript, but the result of the JavaScript execution must be the phone number. You can also use a Parameter Name. For more information, see "Creating parameters for two-factor authentication" on page 265. • In the **Regular Expression** box, construct a regular expression that will extract only the token from the SMS response. **Tip:** Click the drop-down arrow for a sample regular expression.
Email Responses	a. Expand the **Step**. b. In the **Action** list, select either **IMAP Email Two-factor authentication** or **POP3 Email Two-factor authentication**. c. Expand the **Arguments** and configure the following: ◦ In the **Email** box, enter the email address that will receive the email response. **Tip:** You can enter JavaScript, but the result of the JavaScript execution must be the email address. You can also use a Parameter Name. For more information, see "Creating parameters for two-factor authentication" on page 265. ◦ In the **Server** box, enter the IP address or URL for the email server. ◦ In the **Server Port** box, enter the port used for email messages. ◦ In the **TLS** box, select whether the email server uses the TLS protocol. **Note:** The default setting is true. ◦ In the **Password** box, enter the password for the email

For...	Do this...
	account. ○ In the **Regular Expression** box, construct a regular expression that will extract only the token from the email response. **Tip:** Click the drop-down arrow for a sample regular expression.

Configuring the Wait for 2FA step

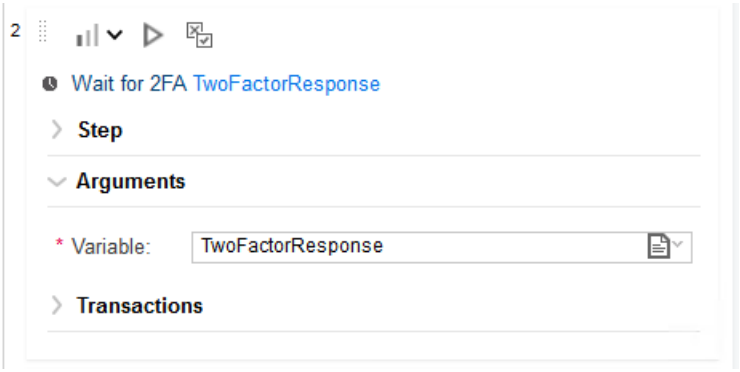
The **Two-factor Authentication** group step includes a **Wait for 2FA** step that you must also configure. The **Wait for 2FA** step waits for a two-factor authentication response to be forwarded from the two-factor authentication control center.

Important! The **Wait for 2FA** step can only be executed inside the **Two-factor Authentication** group step. It cannot be executed as a standalone step.

To configure the **Wait for 2FA** step:

1. By default, the **Step Timeout** extends the macro playback time by 180 seconds. To extend it further, such as in the case of a slow response from the application server, increase the **Step Timeout** setting.
2. Expand the **Arguments** and enter a variable name in the **Variable** box.

   The following image uses TwoFactorResponse as an example.



   The Web Macro Recorder places the response from the control center into this variable.

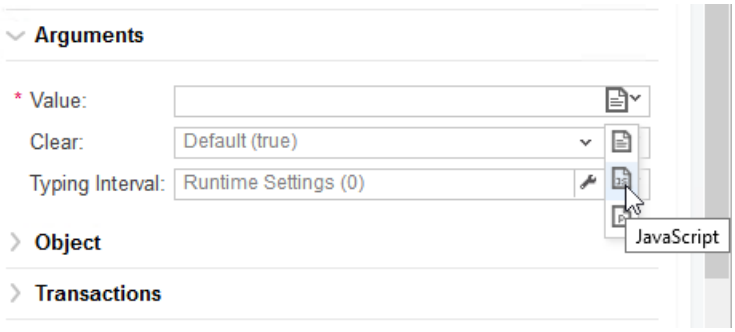
Adding type and click steps

You must also add two **Generic Object Action** steps inside the **Two-factor Authentication** group step. You must configure one as a **Type** step that types the response from the control center into the

two-factor authentication response text box. You must configure the other as a **Click** step that clicks a button, such as Sign In or Next, to gain access to the site.

To add and configure **Type** and **Click** steps:

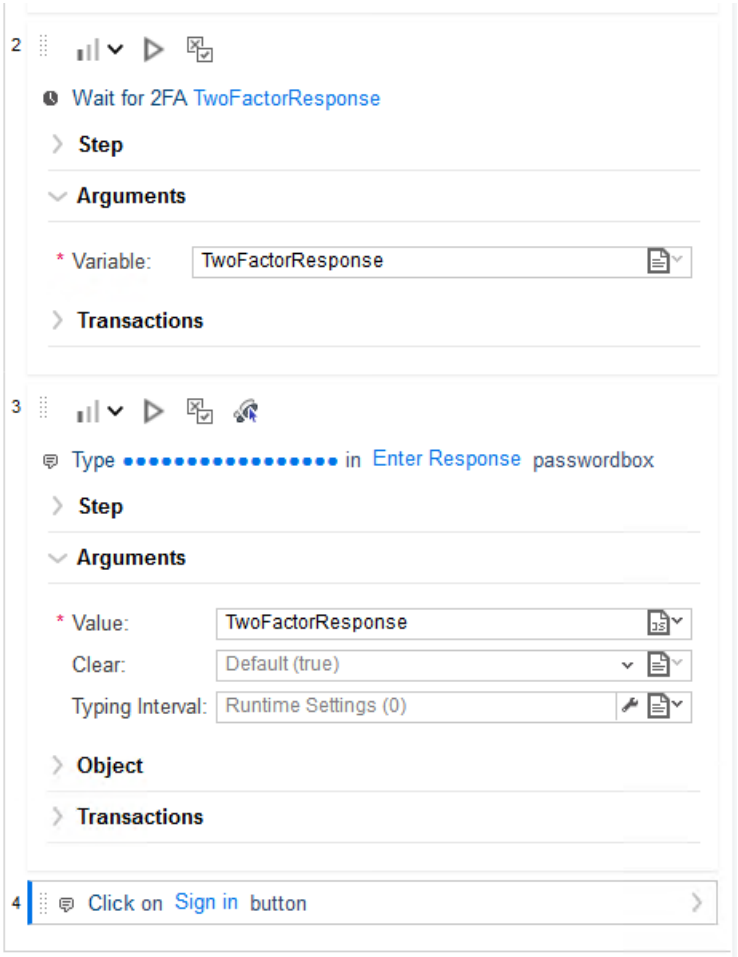
1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. In the **Functions** tab, click and drag the **Generic Object Action** step to the recorded steps, and drop it inside the **Two-factor Authentication** group step immediately following the **Wait for 2FA** step.
3. Configure the step as follows:
   a. Click **Choose an object** and follow the instructions to select the two-factor authentication response text box.
   b. Expand the **Step**, and then select **Type** from the **Action** list.
   c. Expand the **Arguments**.
   d. In the **Value** box, select **JS**.



   e. In the **Value** box, type the variable name you created in the **Wait for 2FA** step. The preceding procedure uses TwoFactorResponse as an example.

4. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
5. In the **Functions** tab, click and drag the **Generic Object Action** step to the recorded steps, and drop it inside the **Two-factor Authentication** group step immediately following the **Type** step.
6. Configure the step as follows:
   a. Click **Choose an object** and follow the instructions to select the button, such as Sign In or Next, to gain access to the site.
   b. Expand the **Step**, and then select **Click** from the **Action** list.

The completed **Type** and **Click** steps should be similar to those in the following image. Note their placement directly following the **Wait for 2FA** step.



Using TOTP authentication

Another method of two-factor authentication is time-based one-time password (TOTP) authentication. This method uses a shared secret and the system time to generate a token that a user enters rather than receiving a token by way of SMS or email. While you can enter the TOTP secret key if you have it, the Event-based Web Macro Recorder automates the process with a way to set up and manage TOTP authenticators, and then use the authenticators in a new "Type Time-based One-time Password" step.

Setting up the TOTP authenticator

The initial stage for registering an authenticator usually involves scanning a QR Code. The Event-based Web Macro Recorder can read information from a QR Code and extract the secret key for seeding the TOTP authenticator. Alternatively, if you can access the secret key, you can enter it directly into the Authenticator Dialog to seed the TOTP authenticator.

To set up a TOTP authenticator:

1. In the TruClient browser, navigate to your Web application and log in.
2. Enable two-factor authentication in your application.

   This should generate a QR code or a secret key in the user interface.
3. In the TruClient sidebar, click the **Edit authenticators** ( ) icon.

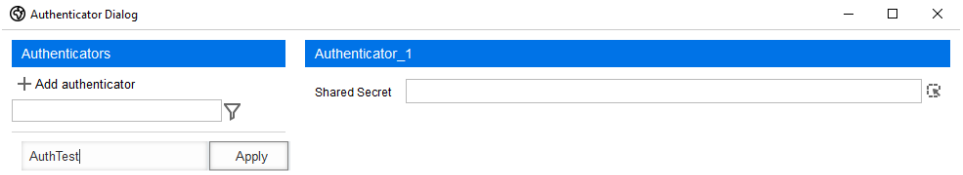
   The Authenticator Dialog opens.
4. Click **+ Add authenticator**.

   A new authenticator is added with the default name `Authenticator_1`. Each new authenticator added to a macro increments the trailing number in the default name by one.
5. Optionally, rename the authenticator as follows:

   a. Click the **Edit authenticator name** ( ) icon for the new authenticator.

   b. Type a name for the authenticator and click **Apply**.

      In this example, the authenticator name is `AuthTest`.



6. Continue according to the following table.

If...	Then...
The shared secret is provided or you know the shared secret	Type the secret in the **Shared Secret** box.
A QR code is provided	a. Click the **select object** ( ) icon to the right of the **Shared Secret** box. A Select Object dialog box opens in the TruClient sidebar window. b. Do one of the following: ◦ Click the QR code in the TruClient browser. ◦ Click an area of the page and drag the cursor to select the section of the page containing the QR code. c. Click **Select**. The shared secret is extracted, masked, and placed into the Shared Secret box.

7. Click **OK**.

Tip: You can create and manage multiple authenticator name / shared secret pairs for use in the same macro. However, each authenticator name must be unique.

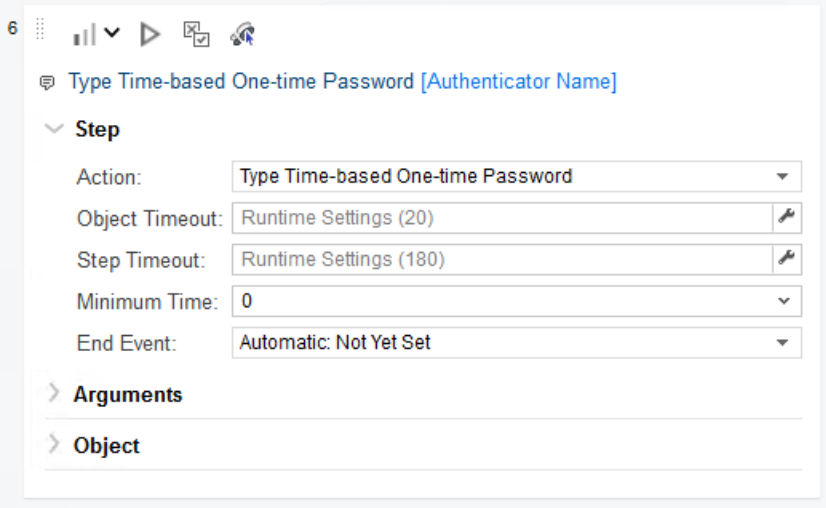
Recording a macro with TOTP

To use TOTP in a macro, you must record your login process a usual, but pausing to add a **Generic Object Action** step with **Type Time-based One-time Password** action.

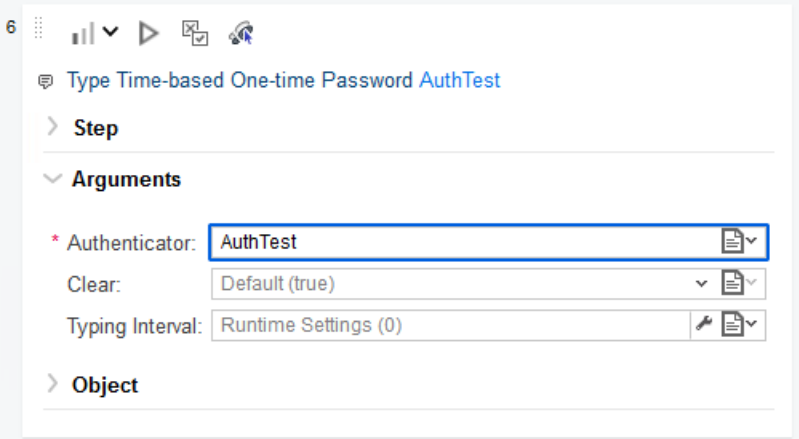
To record a macro with TOTP:

1. In the TruClient sidebar, click the **Record** icon ( ).
2. In the TruClient browser, navigate to the login form and log in to the application.
3. At the point where you would enter an authentication code, click the **Stop** icon ( ) in the TruClient sidebar.
4. In the TruClient sidebar, click the **Add Step** icon (Step).

   The Steps box opens.
5. In the **Functions** tab, click and drag the **Generic Object Action** step to the recorded steps, and drop it after the last recorded step. Configure the step as follows:
   a. In the step, click **Choose an object**.
   b. In the TruClient browser, select the TOTP text box (or field).
   c. In the Generic Object Action step, expand the **Step** and select **Type Time-based One-time Password** from the **Action** list.



   d. Expand the **Arguments**, and then type the authenticator name to use in the **Authenticator** box.



In this example, the authenticator name is `AuthTest`.

Tip: To view the available authenticators, click the Edit authenticators ( ) icon to open the Authenticator Dialog.

6. With the **Generic Object Action** step selected, click **Record after selected step** to continue recording the login process.
7. If the TruClient sidebar does not prompt you to choose an object for login verification, add a verify step after the login step and identify an object that appears only after successful login.
8. Click the **Play** icon ( ) to verify that your macro logs in correctly.

Troubleshooting TOTP

If you encounter issues when using TOTP authentication, this topic might help determine possible causes and solutions.

Troubleshooting QR code errors

The following table describes possible causes and solutions related to QR code errors.

Error	Possible Cause	Possible Solution
"Failed to extract the shared secret from the QR code"	The QR code may not contain a proper TOTP registration URL.	Ensure that the TOTP registration URL is accurate and uses proper syntax. For example, the TOTP registration URL usually starts with: `otpauth://totp/IDENTIFICATION?secret=YOUR_SECRET`
"Failed to parse the QR code"	The Web Macro Recorder could not parse the QR	The Web Macro Recorder might be able to parse the QR code if it is converted to

Error	Possible Cause	Possible Solution
	code element presented in the Web page.	an image element.

Troubleshooting macro playback failures

The following table describes possible causes and solutions related to macro playback failures.

Error or Symptom	Possible Cause	Possible Solution
"Authenticator with name <*name*> was not found"	The authenticator might have been configured incorrectly in the Authenticator Dialog.	Reconfigure the authenticator in the Authenticator Dialog. For more information, see "Setting up the TOTP authenticator" on page 234.
"Failed generating TOTP for authenticator named <*name*>"	The shared secret might be incorrect.	Re-enter the shared secret manually (if available) or by means of a QR code. For more information, see "Setting up the TOTP authenticator" on page 234.
	The system time is not configured properly.	Sync the system time in System Settings on the host where the Web Macro Recorder is running. Ensure that the time and the timezone are properly set.
The token is incorrect and login fails.	The system time is not configured properly.	Sync the system time in System Settings on the host where the Web Macro Recorder is running. Ensure that the time and the timezone are properly set.
	The token has a 30-second timeframe.	Wrap the "Type Time-based One-time Password" step in a **For Loop** step with retries. For more information, see "For Loop" on page 282 and "Inserting loops and loop modifiers" on page 284.

Using IMAP multi-factor authentication with OAuth2

If you use OAuth 2.0 authentication in the IMAP protocol, the Event-based Web Macro Recorder enables you to record a login macro that includes the prompt for the token and then modify it to add the OAuth authentication. Currently, Microsoft® Outlook® is the only supported email client for OAuth authentication.

Before you begin

Follow these guidelines before recording and modifying the macro:

- You must configure an email client that supports OAuth authentication, such as the open-source Mozilla Thunderbird email application. For configuration purposes, you will need the application client ID that is generated when you configure the application with the mail service provider.
- Provide the email application with the correct permission, which is:

  `IMAP.AccessAsUser.All POP.AccessAsUser.All offline_access`
- Configure the email client to redirect URI to `http://localhost`. For more information, refer to Microsoft documentation for authenticating an IMAP, POP, or SMTP connection using OAuth.
- When you record the login macro, you must copy a token from an email and paste it into a token textbox to authenticate. For convenience, log in to the email account that is registered to receive tokens from the target web application.

Recording a macro using OAuth 2.0

To record a macro using OAuth 2.0:

1. In the TruClient sidebar, click the **Record** icon (○ ⌄).
2. In the TruClient browser, navigate to the login form and log in to the application.
3. When prompted for the token, manually copy the token from the email sent to the registered email account, paste it into the form, and click submit (or enter or login). The action will be recorded in the macro. You will edit the step later.
4. Click the **Stop** icon (□) in the TruClient sidebar.

   Note: At this point, the login macro will fail upon replay because the hard-coded token will have expired or otherwise be invalid.
5. Proceed "Creating a function library for OAuth" on the next page.

Creating a function library for OAuth

To create a function library:

1. On the **Function Libraries** tab, click **New Library** ✳.
   The New library dialog box opens.
2. In the **Library Name** box, enter a meaningful name, such as `mfa_oauth`.
3. Click **OK**.
4. Proceed with "Adding a function to the OAuth function library" below.

Adding a function to the OAuth function library

To add a function to the library:

1. Click the **New Function** drop-down arrow *fx* ⌄, and then select **OAuth 2.0**.
   The New OAuth 2.0 function dialog box opens.
2. In the **Function Name** box, type a meaningful name, such as `outlook_login`.
3. The first time you create an OAuth 2.0 function, you must configure the client application. The client application is the public identifier that identifies the application against the mail provider. It must be preregistered and recognized by the mail provider with specific authorization to open and read emails. To configure the client application, do the following:
   a. Click **Open Client Configuration**.
      The OAuth 2.0 for Two-Factor Authentication Configuration Dialog opens.
   b. Click ✚ **Add application client**.
      A client is added with the default name `AppClient_<number>`.
   c. Replace `AppClient_<number>` in the name box with a meaningful name, such as `Thunderbird`, and then click **Apply**.
   d. In the **Service Provider** drop-down list, select **Office 365 (IMAP)**.
   e. In the **Application Client ID**, paste the client ID GUID.
   f. Click **OK**.
      The OAuth 2.0 for Two-Factor Authentication Configuration Dialog closes.
4. In the **Client Application** drop-down list on the **New OAuth 2.0 function** dialog box, select an application, such as `Thunderbird`.
5. In the **Email** box, enter the email that will receive the token. This is the account that is registered with the site under test.

   Important! Ensure that the **Create Two-Factor Autnentication step** checkbox is selected. This enables you to easily configure a Two-factor authentication step in the script that synchronizes all the browsers when they run during the scan.

6. Click **OK**.

A login page opens and prompts for the password for the specified email account.

7. Enter the password and click sign in.

   The navigation is recorded in the OAuth 2.0 function. On the Actions tab, you will see that the following steps have been added to the macro:

   - Email (IMAP XOAUTH2) Two-factor authentication
   - IMAP XOAUTH2 Connect With *<client_application>*
   - Wait for 2FA (This is the step that waits for the token.)

8. Proceed with "Configuring the Email (IMAP XOAUTH2) Two-factor authentication step" below.

Configuring the Email (IMAP XOAUTH2) Two-factor authentication step

To configure the two-factor authentication step:

1. In the Step Editor, expand the **Arguments**.
2. In the **Email** box, enter the email that will receive the token.
3. In the **Server** box, enter `outlook.office365.com`.
4. In the **Server Port** box, enter `993`.
5. In the **Regular Expression** drop-down list, select the default regular expression to find a numeric-based token in the email.

   Tip: If a non-numeric token is used, you can construct a custom regular expression and paste it into the Regular Expression box.

6. Proceed with "Configuring the Wait for 2FA step" below.

Configuring the Wait for 2FA step

The Wait for 2FA step is the step that waits for the token.

To configure the Wait for 2FA step:

1. In the Step Editor, expand the **Arguments**.
2. In the **Variable** box, enter a variable name that will be the placeholder for the token retrieved from the email. For example, `OTP`.
3. Proceed with "Reorganizing the steps" on the next page.

Reorganizing the steps

You must reorganize the original recorded login and token-textbox steps into the appropriate order among the navigation steps in the OAuth 2.0 function.

To reorganize the steps:

1. Select the login steps from the script, and then right-click and select **Cut**.
2. In the **Email (IMAP XOAUTH2) Two-factor authentication** step, select the **IMAP XOAUTH2 Connect With *<client_application>*** step, and then right-click and select **Paste > Paste After**.
3. Select the token-textbox steps (such as **Click on Token textbox** and **Type [Value] in Token textbox**), and then right-click and select **Cut**.
4. Select the **Wait for 2FA** step, and then right-click and select **Paste > Paste After**.
5. Proceed with "Configuring the Type [value] in Token textbox step" below.

Configuring the Type [value] in Token textbox step

You must delete the hard-coded value from the Type [value] in Token textbox step and configure the step to accept the value from the variable in the Wait for 2FA step.

To configure the Type [value] in Token textbox step:

1. In the Step Editor, expand the **Arguments**.
2. In the **Value** box, do the following:
   a. Delete the hard-coded value.
   b. From the drop-down list, select **JS** (JavaScript).
   c. Type the Variable name from the **Wait for 2FA** step. For example, `OTP`.
3. Save the macro.
4. Replay the macro to ensure successful login.

Modifying the macro replay level

As you record a macro, TruClient assigns a level from 1 to 3 to each step. For example, a level 1 step is essential to the macro. A click step that occurs in an area of the application that has no effect is assigned to level 2. Mouse-over steps are generally considered unnecessary for the macro and are assigned to level 3.

Macro steps are displayed and played with the granularity specified as level 1, 2, or 3 in the step level slider in the toolbar at the top of the TruClient browser. The highest granularity is level 3—setting the slider to level 3 displays and plays back all the steps at levels 1, 2, and 3. Using higher granularity might be required for successful playback, but it can cause the macro to take longer to run. By default, the Script Level is set to 1.

To modify a macro's replay level:

- In the TruClient browser, click the step-level drop-down arrow ( ) and select one of the following:
  - - Displays and replays level 1 steps only. Level 1 steps are necessary for interacting with the application.
  - - Displays and replays level 1 and 2 steps. Level 2 steps affect the application in a way that is probably not important to the macro.
  - - Displays and replays level 1, 2 and 3 steps. Level 3 steps have no apparent effect on the application.

If you select a lower level, some steps are hidden. If you select a higher level, additional steps become visible.

Working with event handlers

If you record or add a step that does not occur in every run or occurs randomly, or if elements appear on the page in random locations, your macro might fail when the behavior does not occur.

For example, during logon, the following notification occasionally appears:

“Server is busy. Please wait for 10 seconds and try again.”

Or a website might prompt visitors to register and receive a coupon. If there is no step to handle such occurrences, the macro might fail when the behavior occurs. An event handler calls a function to handle a condition only if the condition occurs.

Creating an event handler

To create an event:

1. In the TruClient sidebar window, click the **Event Handler Editor** icon ( ).
   The Event Handler Editor opens.
2. Click the **Add a new event handler** icon ( ) to add a new event handler.
   An error icon appears next to the handler name until enough information is added to define the handler.
3. Configure the **General** properties as follows:
   a. In the **Name** box, enter a name for the event handler and click **Apply**.
   b. To execute the event handler only once during the current iteration (it resets to zero when the iteration ends), select **Execute only once**.
   c. To enable other event handlers to run while this event is occurring, select **Allow other handlers to interrupt**.

d. To allow the Web Macro Recorder to listen for the event throughout the macro playback and call the event handler whenever the event occurs, select **Event can be triggered during the entire script**.

e. To allow the Web Macro Recorder to listen for the event during only part of the macro playback, clear **Event can be triggered during the entire script**.

> **Tip:** If you clear this box, the **Start** and **End** drop-down lists become visible. Select start and end steps from these lists to specify the range of steps where the event can be triggered.

f. From the **Type** drop-down list, select one of the following:

- **Object** – When an object-related event occurs. For example, a certain object appears on the page, or a certain object property gets a certain value.
- **Dialog** – When a dialog box pops up. For example, an alert or a prompt appears.

4. For **Object** type, click **Choose an object**, and then select an object in the TruClient browser window. Optionally, make changes to the following options, which may be automatically populated:

- In the **Roles** box, specify the operations that can be performed on the object. For more information, see "Step arguments related to objects" on page 268.
- In the **Name** box, enter a name for the object.
- From the **ID Method** drop-down list, select one of the following:
  - Automatic
  - XPath
  - JavaScript
  - Descriptors

    For more information on TruClient descriptors, see https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm
- In the **Related Objects** box, associate the object with another object in your application to facilitate object identification during playback. For more information, see "Relating objects to other objects" on page 297.

5. For an Object event, in the **Type** drop-down list, select one of the following:

- **Object Exists** – If the object exists during replay, the event handler is triggered.
- **Property exists on Object** – If the property of an object meets the defined criteria, the event handler is triggered.

> **Note:** For a Dialog Event, the Type is **Dialog Opened**. When the specified dialog box is opened, the event handler is triggered.

6. Optionally, configure a handler function as follows:

> **Important!** The handler function must be in a library.

a. From the **Library** drop-down list, select the library containing the function.
b. From the **Function** drop-down list, select the function.
c. If the selected Function has function parameters, enter the argument values in the **Arguments** field.

7. Click **OK** to save the changes and close the editor.

Working with function libraries

Function libraries enable you to combine repetitive step execution into a single call. They also allow you to combine a sequence of events into a logical flow, or library, to handle various tasks with functions.

For example, in a SPA that includes search, you can combine the search flow into a search library where the input is the only variable that changes while the steps remain the same. There is no need to clone the steps.

For more information about TruClient functions and function libraries, see https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/_tc_c_step_functions.htm.

Known limitation

Currently, only local libraries are supported, so a library is available only in the macro where it was created. Global libraries are not supported, so sharing libraries between macros is not possible.

Creating a function library

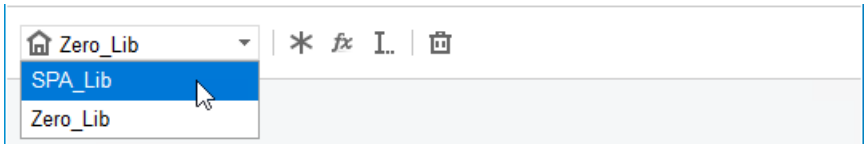
To create a function library:

1. Select the **Function Libraries** tab at the bottom of the TruClient sidebar window.
2. Click the **New Library** icon (✳) from the Function toolbar.
   The New library dialog box opens.
3. In the **Library Name** box, type a name for the library and then click **OK**.
   The new library is added to the list of libraries in the Function toolbar. Add functions to the library as described in "Creating a function" on the next page.

Creating a function

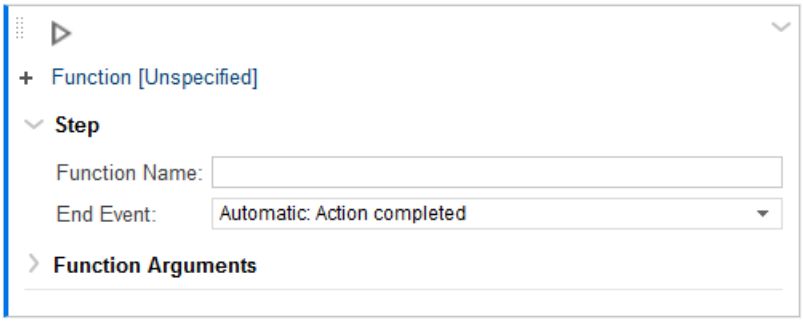
To create a function:

1. From the Function toolbar, select a library from the library list.



2. Click the **New Function** icon (fx) to create a new function.
   A new unspecified function is added to the library.

3. Click the **Open/Close the Step Editor** ( ) icon to expand the function and display the step and function arguments.

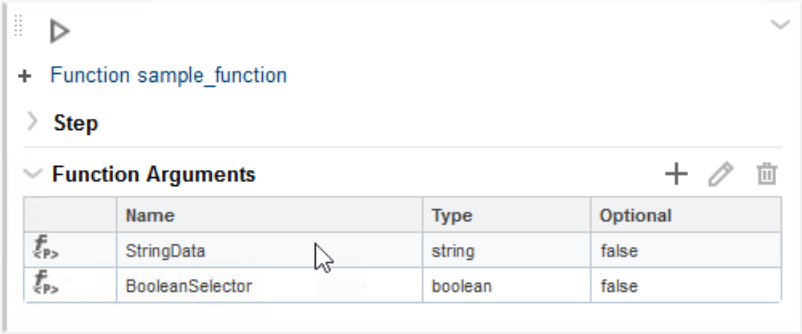


4. In the **Function Name** box, type a name for the function.
5. From the **End Event** list, select an end event. For more information, see "Understanding end events" on the next page.
6. Expand the **Function Arguments**.
7. Click the **Create a new argument** icon (+).
   The Arguments Editor opens.
8. Define the arguments as follows:
   a. In the **Name** box, type a meaningful name for the argument so that it is clear what value you need to specify when you are using the function.
   b. From the **Type** list, select a type of argument. Options are **string**, **integer**, or **boolean**.
   c. From the **Optional** list, select whether the argument is optional. Options are **true** or **false**.
   d. Click **OK**.
      The argument is added to the step.

Editing an argument

To edit the argument for a function:

1. In the **Function Arguments** table, select the argument to edit.



2. Click the **Edit argument** icon ( ).
   The Arguments Editor opens.
3. Update the argument as described in Step 8 of "Creating a function" on the previous page.

Deleting an argument

To delete an argument:

1. In the **Function Arguments** table, select the argument to delete.
2. Click the **Delete the selected argument** icon ( ).

Understanding end events

The Web Macro Recorder defines when the End Event occurs during the first script replay on each supported browser. You can use the end event that is automatically identified by Web Macro Recorder, or you can assign a different end event to the step.

The following table describes the end events that are available in the Web Macro Recorder.

End Event	Description
Action completed	The step ends when its action is completed. An example of an action is a button click.
Automatic: Action completed	The step ends whenever TruClient identifies that the action is completed.

End Event	Description
Dialog opened	The step ends when a dialog box is opened.
Document Loaded	The step ends when the process of loading a document is completed. All scripts and stylesheets have finished loading and have been executed, and all images have been downloaded and displayed.
DOM Content Loaded	The step ends when the page's Document Object Model (DOM) is ready. The API for interacting with the content, style, and structure of a page is ready to receive requests from your application's client-side code.
Step network completed	The step ends when all HTTP requests have completed including requests initiated by XMLHttpRequest.
Step synchronous network completed	The step ends when all HTTP requests have been completed, excluding requests that are associated with open connections that are not relevant to the step. Usually, these requests are triggered by using XMLHttpRequest.

Working with logout conditions

The Web Macro Recorder may be able to automatically detect a logout condition for the target website. However, you can specify as many different logout conditions as you need, and if any of them is met, the sensor will invoke the login macro to log back in and resume a scan where it left off. You can add, edit, and delete logout conditions using the Logout Condition Editor.

Important! The final set of all logout conditions should cover all the cases of becoming logged out during a scan of the target site.

Logout condition types

Logout conditions can be complicated. You must identify anything in the page that can trigger a logout. The Logout Condition Editor enables you to create and manage the following types of logout conditions:

- Session-based – uses a URL and regular expression to identify a redirect that indicates an unauthenticated user. You must view the traffic and write a regular expression or type a URL that fits the response for the request that triggers a logout.
- Event-based – uses JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout. You can choose sample JavaScript code from a list of templates, and then edit the code for logout conditions that are specific for your application. For more information about the templates, see "Understanding event-based logout templates" on page 253.

Logout conditions from earlier Web Macro Recorder versions

Conducting a scan with a macro that uses automatic logout detection and that was recorded in the Web Macro Recorder with Macro Engine 5.<*version*> may yield undesirable results. OpenText recommends that you remove the previously-detected logout condition as follows:

1. Open the existing macro in the Event-based Web Macro Recorder.
2. Click the **Edit logout conditions** icon ( ).
   The Logout Condition Editor opens and displays all logout conditions already detected or created.
3. Delete the existing automatic logout condition.
4. Play the macro.
   A new logout condition is automatically detected.

Accessing the Logout Condition Editor

To open the Logout Condition Editor:

- After recording a successful login, click the **Edit logout conditions** icon ( ).
  The Logout Condition Editor opens and displays all logout conditions already detected or created.

Adding a session-based logout condition

To add a session-based logout condition:

1. In the left pane, click the **Add new session logout condition** icon (+).
   A session-based logout condition is added.
2. In the **Name** box, type a name for the new condition.
   The name in the left column is simultaneously updated with your changes.
3. Select which type of logout condition you want to use and complete the information required for that type. The following table describes the options.

Option	Description
Regex	With this option, you construct a regular expression (regex). A regular expression is a pattern that describes a set of strings. Regular expressions are constructed much like mathematical expressions by using various operators to combine smaller expressions. Only users with a working knowledge of regular expressions should use this feature. The regex must reflect the difference between a) the response to a logged-

Option	Description
	in user's request to access a protected page, and b) the response to the same request from the user, while *not* logged in, to access the same protected page. The general steps to construct the regex are as follows: a. Start the Web Proxy tool to record web traffic. For more information, see the Web Proxy Help or the *OpenText™ Dynamic Application Security Testing Tools Guide*. b. Log in to the target site and copy the URL of a protected page. c. Log out and use the copied URL to try to access the protected page without logging in. d. Compare the responses and identify a unique aspect of the response to the attempt to access the protected page without logging in. e. Open the Regular Expression Editor. For more information, see the Regular Expression Editor Help or the *OpenText™ Dynamic Application Security Testing Tools Guide*. f. Construct a regex that reflects the unique aspect of the response to the attempt to access the protected page without logging in. g. Copy the regex into the **Regex** field of the Logout Condition Editor.
URL	When you select this option, the currently displayed web page is automatically used as the default value. You can specify a static URL to which the target site redirects users when it logs them out. Do not specify the target site's general login page.

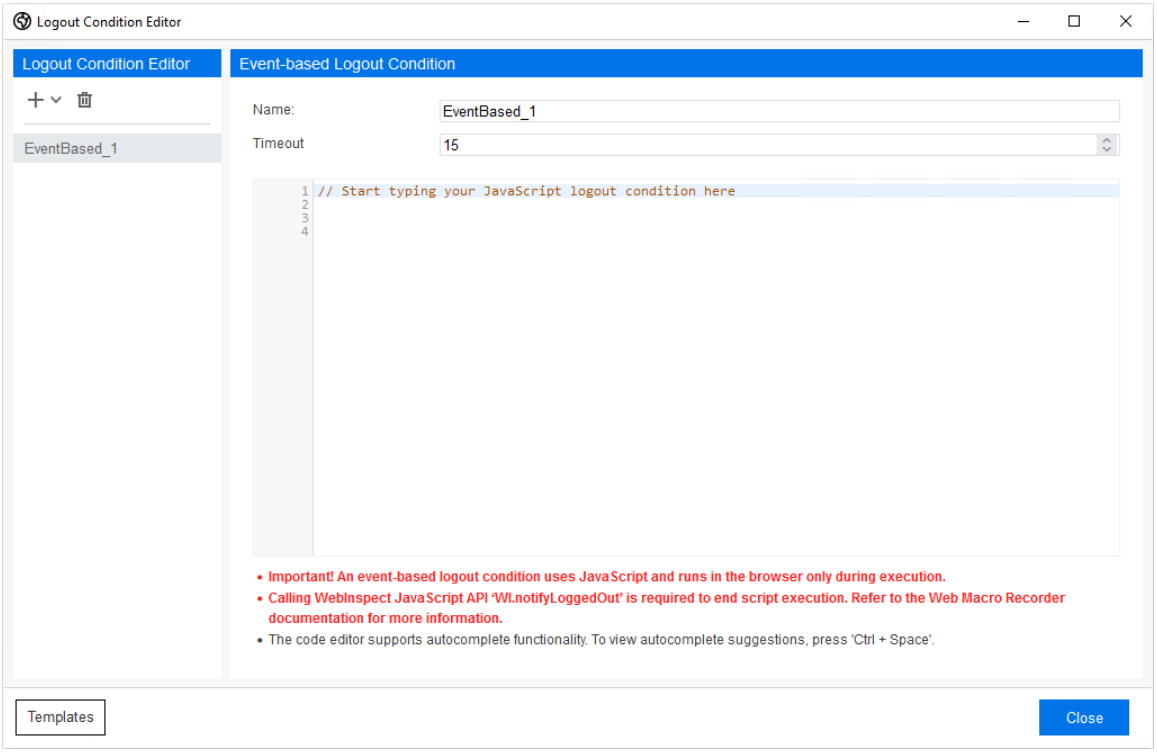
4. Click **Close** to save the logout conditions and close the Logout Condition Editor.

Adding an event-based logout condition

To add an event-based logout condition:

1. In the left pane, click the **Add logout condition** drop-down icon (⌄), and then select **Event-based**.

   An event-based logout condition is added along with a JavaScript code editor.



2. In the **Name** box, type a name for the new condition .

   The name in the left column is simultaneously updated with your changes.
3. In the **Timeout** box, enter the number of seconds for the logout condition to time out. Valid values are from 10 to 60 seconds. The default value is 15 seconds.
4. Continue according to the following table.

To...	Then...
Use a predefined template	a. Click **Templates**. The Templates List dialog box opens. For more information about the templates, see "Understanding event-based logout templates" on page 253. b. In the left pane, select a template. c. Click **Load**. A prompt warns that you are about to override the current event-based logout condition with code from the selected template. d. Click **Confirm**. e. The code is added to the code editor.

To...	Then...
	f. Edit the JavaScript as needed for event-based logout conditions in your application.
Write your own JavaScript	Type JavaScript code in the code editor. **Tip:** To view autocomplete suggestions while coding, do one of the following: • On Windows, press `CTRL` + `Space`. • On macOS, press `Ctrl+ Cmd+`.

Important! Whether you use a predefined template or write your own code, the JavaScript must end with the following code to notify the OpenText DAST sensor of a logout state to avoid a timeout:

```
WI.notifyLoggedOut(isLoggedOut);
```

5. Click **Close** to save the logout conditions and close the Logout Condition Editor.

Editing a logout condition

To edit an existing logout condition in the Logout Condition Editor:

1. Select the logout condition to edit in the left pane.
   The Properties pane lists the properties.
2. Edit the properties as needed.
3. Click **Close** to save the logout conditions and close the Logout Condition Editor.

Deleting a logout condition

To delete an existing logout condition in the Logout Condition Editor:

1. Select the logout condition to delete in the left pane.
2. Click the **Delete** icon (🗑).
   A Confirm Delete prompt appears.
3. Click **Yes**.
4. Click **Close** to save the logout conditions and close the Logout Condition Editor.

Understanding event-based logout templates

This topic describes the event-based logout templates that are available to edit with specifics for your application.

Missing Local Storage Key

This template handles logout conditions occurring when a local storage key is not found. This event-based logout condition requires that web storage detection be enabled. For more information, see "Interactive Options" on page 303.

The following table describes the JavaScript code used in the Missing Local Storage Key template.

JavaScript Code	Description
`var token = window.localStorage.getItem("<key>");`	Returns the value of the specified key that is saved in the browser and places it in the variable named `token`.
`var isLoggedOut = document.location.origin == "http(s)://<path>:<port>" && !token;`	Confirms logout condition if the `document.location.origin` property matches the specified URL, but the token is not found.
`WI.notifyLoggedOut(isLoggedOut);`	Notifies OpenText DAST that the sensor is logged out.

Missing Session Storage Key

This template handles logout conditions occurring when a session storage key is not found. This event-based logout condition requires that web storage detection be enabled. For more information, see "Interactive Options" on page 303.

The following table describes the JavaScript code used in the Missing Session Storage Key template.

JavaScript Code	Description
`var token = window.sessionStorage.getItem("<key>");`	Returns the value of the specified key that is stored for the session and places it in the variable named `token`.
`var isLoggedOut = document.location.origin == "http(s)://<path>:<port>" && !token;`	Confirms logout condition if the `document.location.origin` property matches the specified URL,

JavaScript Code	Description
	but the token is not found.
`WI.notifyLoggedOut(isLoggedOut);`	Notifies OpenText DAST that the sensor is logged out.

Object Exists

This template handles logout conditions occurring when an object exists that indicates logout.

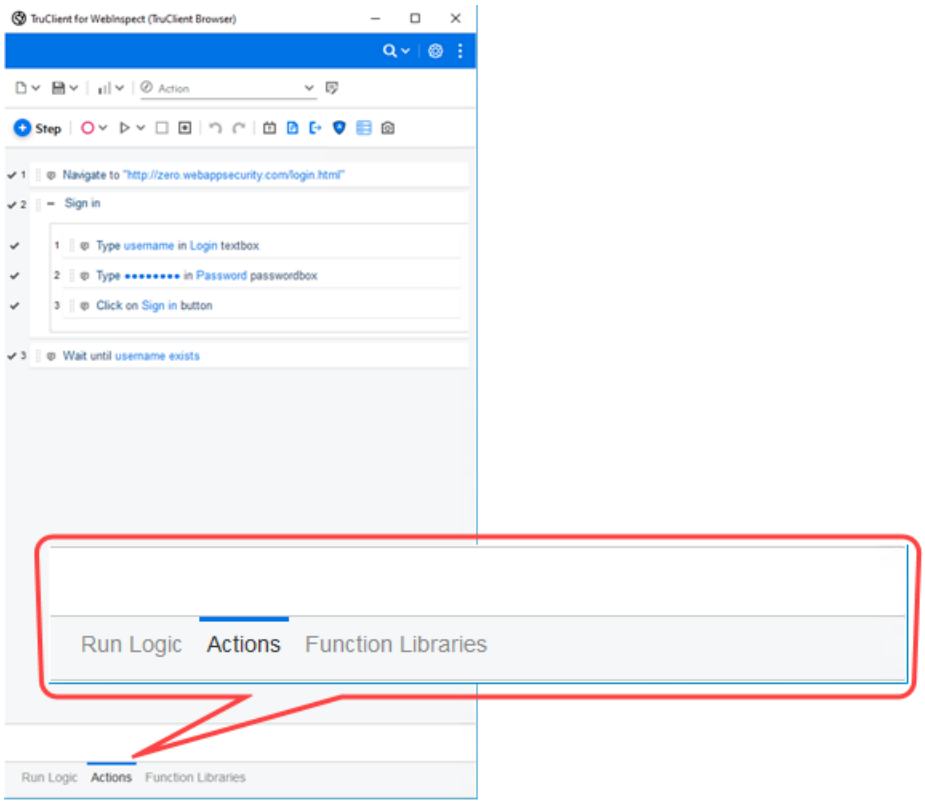
The following table describes the JavaScript code used in the Object Exists template.

JavaScript Code	Description
`const element = document.` `  getElementById("<element_id>");`	Defines a constant reference for the element with the specified ID.

`WI.notifyLoggedOut(document.location.origin`
`  == "http(s)://<path>:<port>" &&`
`  (element !== undefined && element !== null));`
	Notifies OpenText DAST that the sensor is logged out if the `document.location.origin` property matches the specified URL and the identified element exists.

Working with actions

You create and run actions in the **Actions** tab, which you access from the bottom of the TruClient sidebar window.



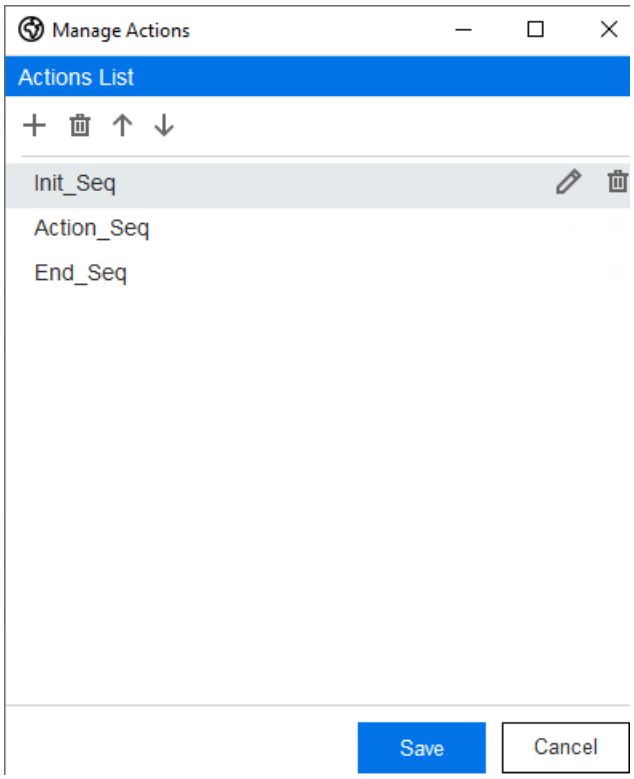
From this tab, you record, edit, and replay your macros.

Adding an action to your macro

To add an action to your macro:

1. Click the **Manage Actions** icon (💬) at the upper right hand corner of the TruClient sidebar window.

   The Manage Actions dialog box appears.



2. Click the **Add action** icon (+). Give the action a meaningful name.

Rearranging the order of actions

To rearrange the order of actions:

1. Click the **Manage Actions** icon () at the upper right hand corner of the TruClient sidebar window.

   The Manage Actions dialog box appears.
2. Select an action.
3. Click the **Move up** or **Move down** icons (↑ ↓) to move the action up or down in the list.

Deleting an action

To delete an action:

1. Click the **Manage Actions** icon () at the upper right hand corner of the TruClient sidebar window.

   The Manage Actions dialog box appears.
2. Select the action to delete.
3. Click the **Delete** icon (🗑).

Working with web storage keys

During the login process, an application that uses web storage for state management might set relevant keys in local storage. Those keys must be synchronized in the Web Macro Recorder to enable the application to determine and maintain state. Otherwise, during macro playback the application may fail to find the state in web storage and result in either an unauthenticated scan or redirection.

You can add, edit, and delete web storage keys, as well as load keys from playback, using the Web Storage Key Editor.

Accessing the Web Storage Key Editor

To open the Web Storage Key Editor:

- After enabling the **Support Web Storage** setting, click the **Edit Web Storage keys** icon ( ).
  The Web Storage Key Editor opens.

  Note: This icon is visible only if the **Support Web Storage** setting is enabled. For more information, see "Interactive Options" on page 303.

Loading keys from playback

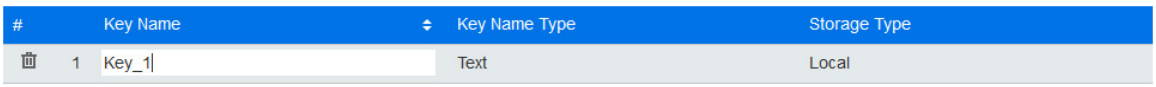
If the macro was played before opening the Web Storage Key Editor, you can load the keys that were found in the recent playback. To load keys from playback:

- Click **Load from playback**.
  The keys are displayed in the list of web storage keys.

Adding a web storage key

To add a web storage key in the Web Storage Key Editor:

1. Click the **Add** icon ( ).
   A web storage key is added with default values.
2. Double-click the default name in the **Key Name** column.
   The field becomes available to edit.



3. Type a string or regular expression in the field.
4. To change the key name type, double-click the **Key Name Type** column, and then select the type from the drop-down list. Options are:

- **Text** – For a key name that consists of plain text.
- **Regex** – For a key name that consists of a regular expression.

  Note: Syntax validation is performed for regular expressions.

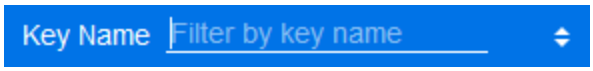
5. To change the storage type, double-click the **Storage Type** column, and then select the type from the drop-down list. Options are:
   - **Local** – For data in localStorage that does not expire and is available when the user revisits the web page.
   - **Session** – For data in sessionStorage that is cleared when the browser is closed.
6. Click **Save**.

Filtering web storage keys

You can filter web storage keys based on any of the columns of data.

To filter keys in the list by **Key Name**:

1. Double-click in the **Key Name** column heading.
   An input box appears in the heading.

2. Type the search criteria in the box.
   The list is filtered as you type.

To filter keys by **RegEx** or **Text**:

1. Double-click in the **Key Name Type** column heading.
   A drop-down list box appears in the heading.

2. Select the filter criteria.
   The list is filtered.

To filter by **Local** or **Session**:

1. Double-click in the **Storage Type** column heading.
   A drop-down list box appears in the heading.
2. Select the filter criteria.
   The list is filtered.

Clearing filters

To clear a filter by **Key Name**:

- Click the in the heading filter box.

To clear a filter by **Key Name Type** or **Storage Type**:

- Select **All** from the drop-down list box in the heading.

Editing a web storage key

To edit an existing web storage key:

Note: If keys were loaded from macro playback, you can edit these keys. However, unless you change the **Key Name** to a regular expression and **Key Name Type** to **RegEx**, the edits will not help with state management.

1. Double-click a row in the column you want to change.
2. Do one of the following:
   - For the **Key Name**, edit the text as needed.
   - For the **Key Name Type** or **Storage Type**, select the desired value from the drop-down lists.

Deleting a web storage key

To delete an existing web storage key:

- Select the key to delete, and then click the **Delete** icon ( ).
  The key is removed from the list.

Working with parameters

When recording a macro, you can use parameters to do the following:

- Create parameters for the user name and password to allow testers to use their own authentication credentials when starting a scan or to use multiple credentials for a multi-user login scan. For more information, see "Using username and password parameters" on the next page.
- Create a parameter for the URL to allow testers to designate an alternate URL when the macro runs. This method may be useful if your application resides in multiple environments and you want to run scans as part of a continuous integration and continuous delivery (CI/CD) pipeline. For more information, see "Using a URL parameter" on page 263.
- Create parameters for phone number, email, and email password to allow testers to conduct multi-user login scans that require two-factor authentication. For more information, see "Creating parameters for two-factor authentication" on page 265.

Case-sensitive parameter names

Parameter names are case sensitive and must contain lowercase letters only.

Using username and password parameters

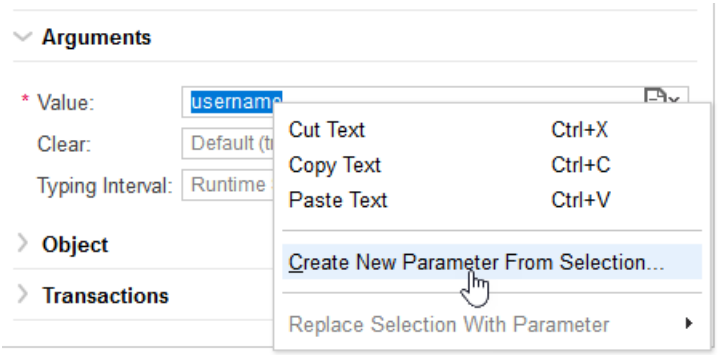
After creating and testing your login macro, you can create username and password parameters that replace the recorded values with parameter names. You can then create a list of values to substitute for the username and password parameters during playback.

Creating parameters in steps

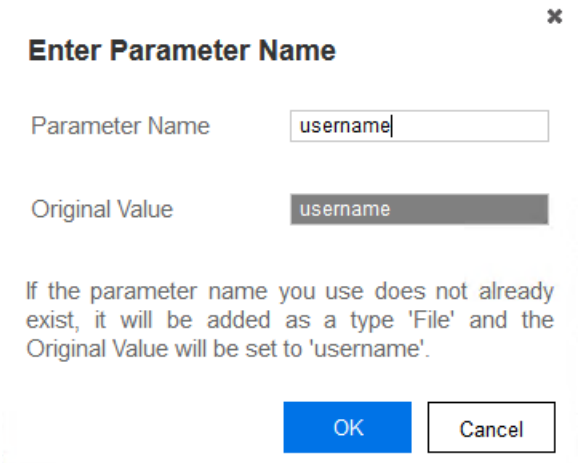
You can create username and password parameters directly in steps using the context menu.

To create parameters in steps:

1. In the step that contains the username, click the **Step Editor** icon ( ).
   The Step Editor opens.
2. Click (expand) **Arguments**.
3. In the **Value** box, select the value and then right-click.



4. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.
5. In the **Parameter Name** box, type `username`, and then click **OK**.



Important! Parameter names are case sensitive and must contain lowercase letters only.

6. In the step that contains the password, click the **Step Editor** icon ( ).
   The Step Editor opens.
7. Click (expand) **Arguments**.
8. In the **Value** box, select the value and then right-click.
9. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.
10. In the **Parameter Name** box, type `password`, and then click **OK**.

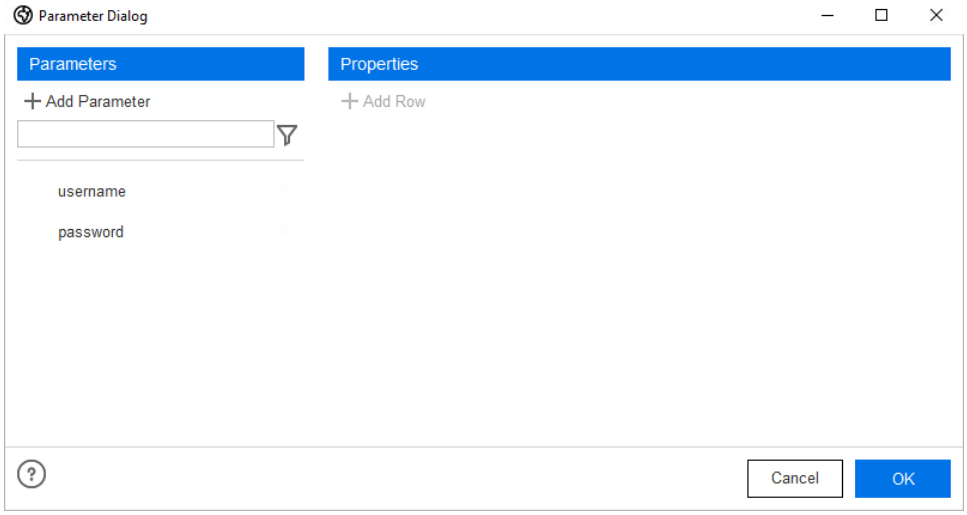
The username and password parameters have been created directly in steps where they will be used during playback. You must now use the Parameters Dialog to create the lists of values for the username and password parameters.

Creating list of values in the Parameters Dialog

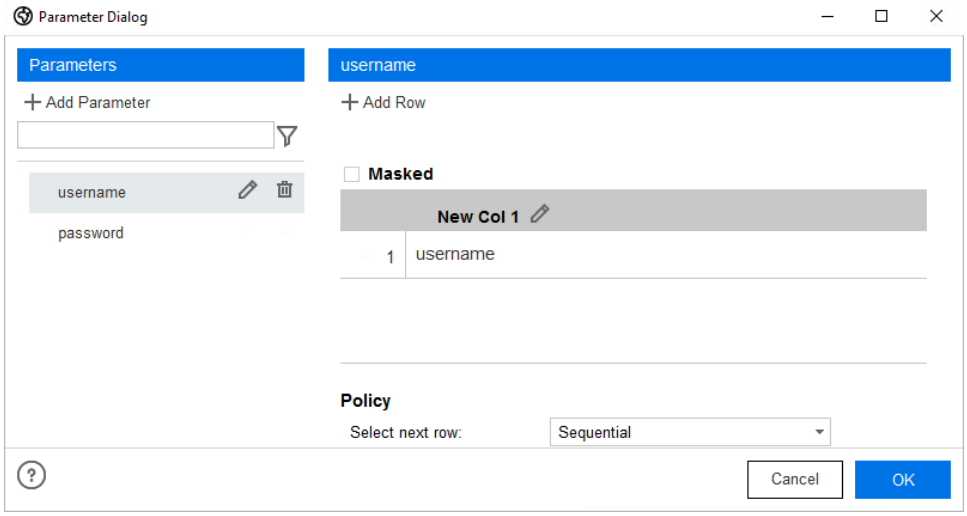
Use the Parameters Dialog to create the lists of values to substitute for the username and password parameters.

To create a list of values:

1. In the TruClient sidebar, click the **Edit Parameters** icon ( ).
   The Parameter Dialog opens with the parameters listed.



2. Click the **username** parameter.
   The list of username values appears. The original value recorded in the macro is listed as the first value to use during macro replay.



Tip: To edit the column name, click the edit icon in the column heading and type a new column name, such as `User Names`.

3. (Optional) To mask the value entered, select **Masked**.

   Note: Values that are masked in the Web Macro Recorder are also masked when configuring a Guided Scan in OpenText DAST and Fortify WebInspect Enterprise.

4. (Optional) To add another value (for example, to create a list of usernames for a multi-user login scan):
   a. Click **Add Row**.
   b. Place your cursor in the new row.
   c. Type the next value to use during macro replay.
   d. Repeat Steps a through c for each additional value to add.
5. Click the **password** parameter.

   The list of password values appears. The original value recorded in the macro is listed as the first value to use during macro replay.
6. (Optional) To mask the value entered, select **Masked**.

   Note: Values that are masked in the Web Macro Recorder are also masked when configuring a Guided Scan in OpenText DAST and Fortify WebInspect Enterprise.

7. (Optional) To add another value (for example, to create a list of passwords for a multi-user login scan):
   a. Click **Add Row**.
   b. Place your cursor in the new row.
   c. Type the next value to use during macro replay.
   d. Repeat Steps a through c for each additional value to add.
8. Click **OK** to save the parameters to the macro and close the Parameters Dialog.

9. Play the macro to verify that it logs in correctly.
10. Save the macro.

Policy

The Policy settings that are visible in the Parameters Dialog are not applicable to OpenText DAST.

Using a URL parameter

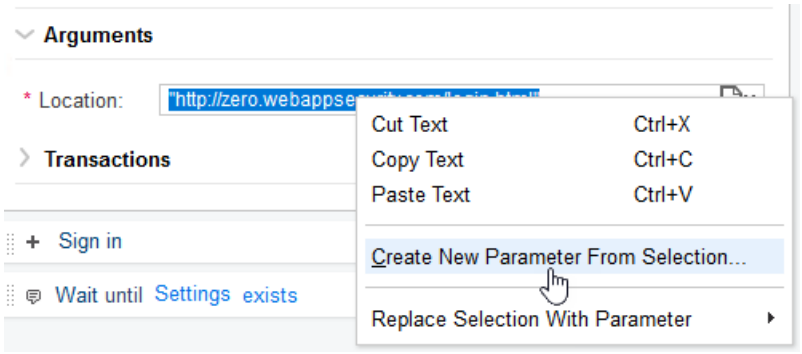
After creating and testing your login macro, you can create a URL parameter that replaces the recorded value with a parameter name.

Creating the parameter in a step

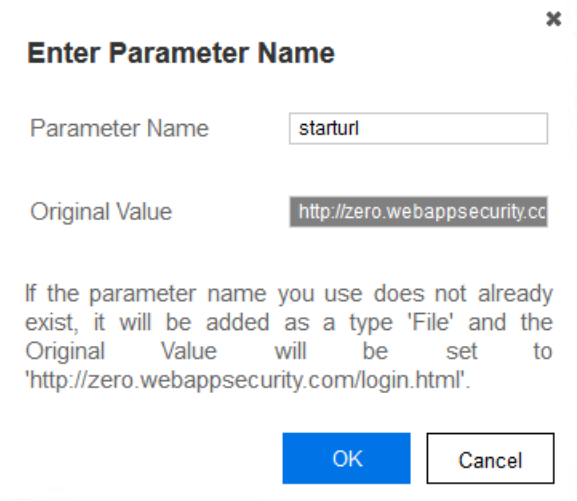
You can create a URL parameter directly in a step using the context menu.

To create a parameter in a step:

1. In the step that contains the URL ("Navigate to..."), click the **Step Editor** icon ( ).
   The Step Editor opens.
2. Click (expand) **Arguments**.
3. In the **Location** box, select the value and then right-click.



4. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.



Important! Parameter names are case sensitive and must contain lowercase letters only.

5. In the **Parameter Name** box, type a name, such as `starturl`, and then click **OK**.

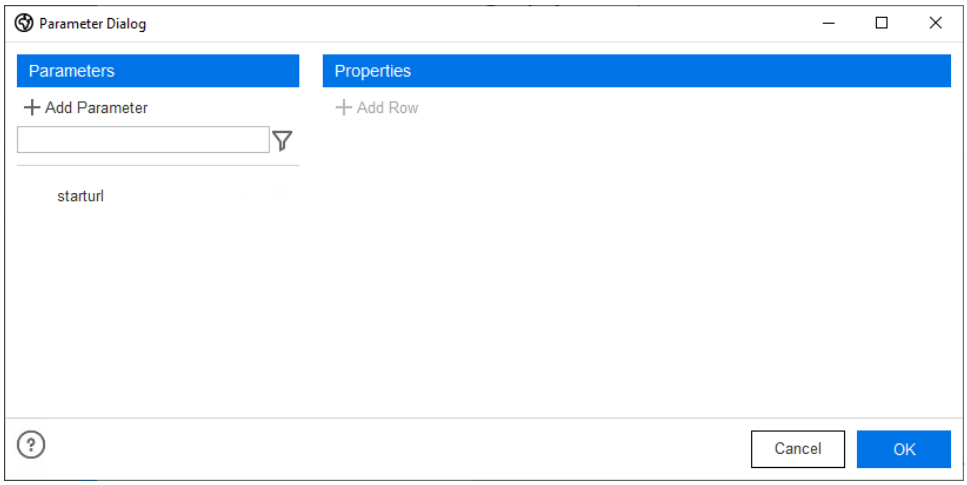
The starturl parameter has been created directly in the step where it will be used during playback. You must now use the Parameters Dialog to create the list of values for the starturl parameter.

Creating list of values in the Parameters Dialog

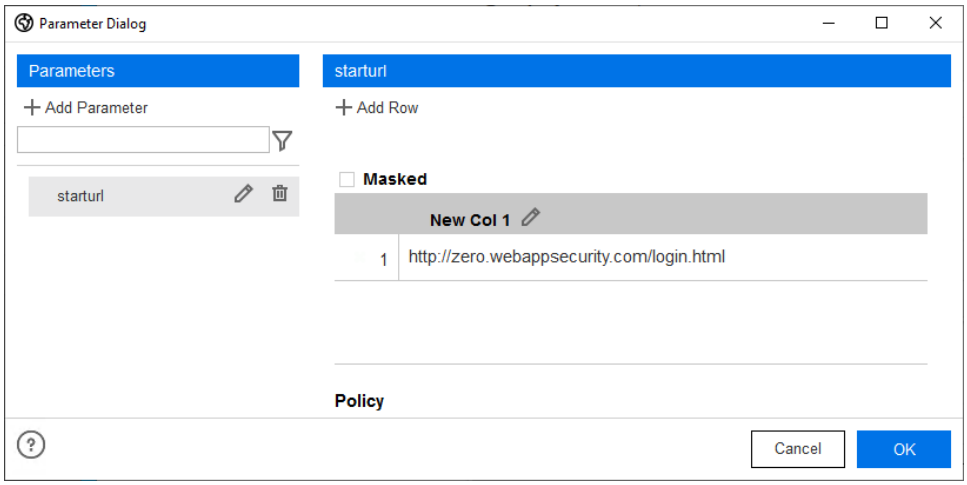
Use the Parameters Dialog to create the list of values to substitute for the starturl parameter.

To create a list of values:

1. In the TruClient sidebar, click the **Edit Parameters** icon ( ).
   The Parameter Dialog opens with the parameter listed.



2. Click the URL parameter, which is **starturl** in this example.
   The list of URL values appears. The original value recorded in the macro is listed as the first value to use during macro replay.



Tip: To edit the column name, click the edit icon in the column heading and type a new column name, such as `URLs List`.

3. (Optional) To add another value:
   a. Click **Add Row**.
   b. Place your cursor in the new row.
   c. Type the next value to use during macro replay.
   d. Repeat Steps a through c for each additional value to add.
4. Click **OK** to save the parameters to the macro and close the Parameters Dialog.
5. Play the macro to verify that it logs in correctly.
6. Save the macro.

Policy

The Policy settings that are visible in the Parameters Dialog are not applicable to OpenText DAST.

Creating parameters for two-factor authentication

After creating and testing your login macro, you can create phone number, email, and email password parameters. You can then create a list of values to substitute for these parameters during playback. Using parameters for two-factor authentication enables you to conduct a multi-user login scan.

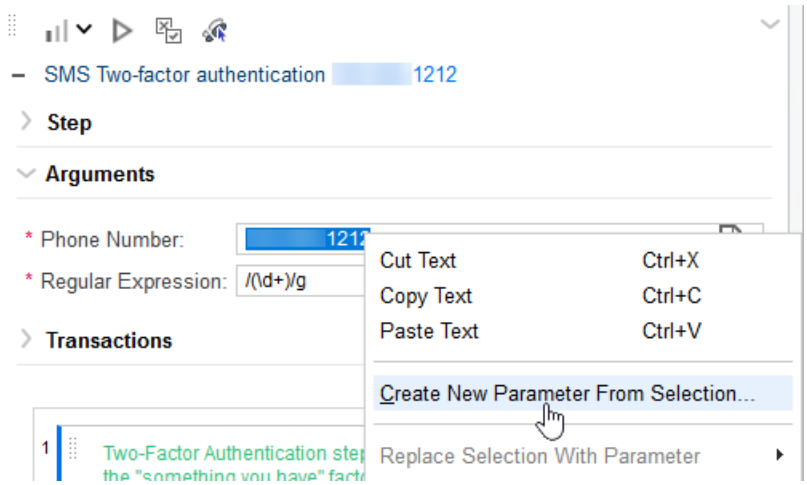
Tip: After creating parameters in the Event-based Web Macro Recorder, you can configure a multi-user login scan and enter additional phone numbers, email addresses, and email passwords in the Scan Settings: Authentication dialog box in OpenText DAST.

Creating a phone number parameter

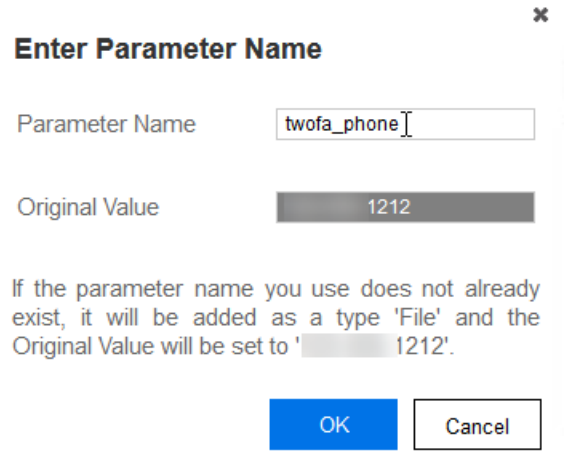
You can create a phone number parameter directly in the **Two-factor Authentication** group step using the context menu.

To create a phone number parameter:

1. In the **Two-factor Authentication** group step, click the **Step Editor** icon ( ).
   The Step Editor opens.
2. Click (expand) **Arguments**.
3. In the **Phone Number** box, select the number and then right-click.



4. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.
5. In the **Parameter Name** box, type `twofa_phone`, and then click **OK**.



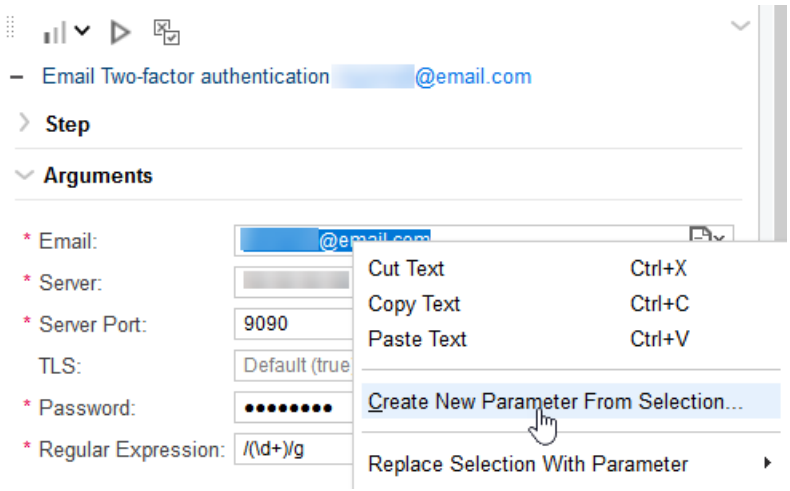
Important! Parameter names are case sensitive and must contain lowercase letters only.

Creating email and email password parameters

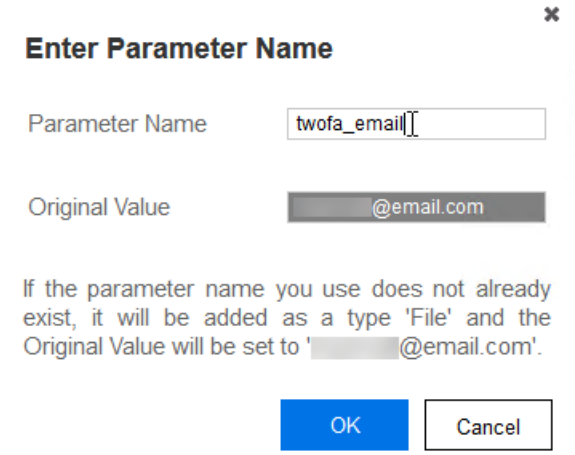
You can create email and email password parameters directly in the **Two-factor Authentication** group step using the context menu.

To create email and email password parameters:

1. In the **Two-factor Authentication** group step, click the **Step Editor** icon ( ).
   The Step Editor opens.
2. Click (expand) **Arguments**.
3. In the **Email** box, select the email address and then right-click.



4. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.
5. In the **Parameter Name** box, type `twofa_email`, and then click **OK**.



Important! Parameter names are case sensitive and must contain lowercase letters only.

6. In the **Password** box, select the password and then right-click.
7. Select **Create New Parameter From Selection...**.
   The Enter Parameter Name dialog box opens.
8. In the **Parameter Name** box, type `twofa_emailpassword`, and then click **OK**.

Step arguments related to objects

The following step arguments related to objects, categorized by role, are available in TruClient:

Audio role

The following table describes the step argument for the **Seek** action of the audio role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Time	Sets or returns the current position (in seconds) of the audio playback.

Browser role

The following tables describe the step arguments related to browser role objects.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Activate

The following table describes the step arguments for the Activate action.

Argument	Description
Ordinal	Defined as an integer.
Title	Defined as a string. **Note:** The title is automatically updated during recording and can be set as an alternative step.

Activate Tab

The following table describes the step arguments for the Activate Tab action.

Argument	Description
Ordinal	Specifies which tab (integer) to activate.
Title	Defined as a string. **Note:** The title is automatically updated during recording and can be set as an alternative step.

Close Tab

The following table describes the step arguments for the Close Tab action.

Argument	Description
Ordinal	Specifies which tab (integer) to close.
Title	Moves the specified browser window to the foreground. Defined as a string. **Note:** The title is automatically updated during recording and can be set as an alternative step.

Add Tab

The following table describes the step arguments for the Add Tab action.

Argument	Description
Location	Specifies the URL to navigate to in the newly opened tab.
Window	Points to the global window object of the application. **Note:** The `window.location` object cannot be used with Internet Explorer. Use the `document.URL` object instead.

Navigate

The following table describes the step argument for the Navigate action.

Argument	Description
Location.	Specifies the URL to navigate to.

Go Back

The following table describes the step argument for the Go Back action.

Argument	Description
Count	Specifies the number of pages to go back.

Go Forward

The following table describes the step argument for the Go Forward action.

Argument	Description
Count	Specifies the number of pages to go forward.

Resize

The following table describes the step arguments for the Resize action.

Argument	Description
Width	Specifies the new width. Leaving this blank means do not resize the

Argument	Description
	width.
Height	Specifies the new height. Leaving this blank means do not resize the height.

Scroll

The following table describes the step arguments for the Scroll action.

Argument	Description
X Coordinate	Indicates the new x coordinate. Leaving this blank means do not scroll along the x axis.
Y Coordinate	Indicates the new y coordinate. Leaving this blank means do not scroll along the y axis.

Dialog - Confirm

The following table describes the step argument for the Dialog - Confirm action.

Argument	Description
Button	Indicates OK or Cancel.

Dialog Prompt

The following table describes the step arguments for the Dialog Prompt action.

Argument	Description
Value	Indicates the string to enter.
Button	Indicates OK or Cancel.

Dialog - Authenticate

The following table describes the step arguments for the Dialog - Authenticate action.

Argument	Description
Username	Specifies the username to enter.

Argument	Description
Password	Specifies the password to enter.
Domain	Specifies the domain to enter.
Button	Indicates OK or Cancel.

Dialog - Prompt Password

The following table describes the step arguments for the Dialog - Prompt Password action.

Argument	Description
Password	Specifies the password to enter.
Button	Indicates OK or Cancel.

Verify

The following table describes the step arguments for the Verify action.

Argument	Description
Value	Indicates the value of the property to verify.
Property	Identifies the property to verify. You can verify the following properties of a browser object: • **Title** - Specifies the title of the browser window. • **Location** - Specifies the location of the browser window.
Condition	Specifies the relationship between the value and property arguments.

Checkbox role

The following table describes the step argument for the **Set** action of the checkbox role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Checked	Sets the check box to either checked (true) or unchecked (false).

Datepicker role

The following table describes the step argument for the **Set Day** action of the datepicker role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Day	Represents the day of the month. Value is an integer between 1-31.

Element role

The following tables describe the step arguments related to element role objects.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Mouse actions

The following table describes the step arguments for the Mouse Down, Mouse Up, Mouse Over, Click, and Double Click mouse actions.

Note: Mouse Over does not have the X/Y Coordinate arguments.

Argument	Description
Button	Identifies the mouse button that is clicked.
X Coordinate	Identifies the offset location of the action relative to the upper left corner of the object. If not specified, the default is the center of the object.
Y Coordinate	Identifies the offset location of the action relative to the upper left corner of the object. If not specified, the default is the center of the object.
Ctrl Key	Indicates whether this key is pressed during the action.
Alt Key	Indicates whether this key is pressed during the action.
Shift Key	Indicates whether this key is pressed during the action.

Drag

The following table describes the step arguments for the Drag action.

Argument	Description
Button	Identifies the mouse button that is clicked.
X Offset	Indicates the amount of pixels to drag the object on the x axis. A positive number indicates a drag to the right.
Y Offset	Indicates the amount of pixels to drag the object on the y axis. A positive number indicates a drag down.
Path	Identifies the list of coordinates representing the user drag path. Do not modify this argument.
Ctrl Key	Indicates whether this key is pressed during the action.
Alt Key	Indicates whether this key is pressed during the action.
Shift Key	Indicates whether this key is pressed during the action.

Note: The **X Offset**, **Y Offset**, and **Path** arguments are mutually exclusive.

Drag To

The following table describes the step arguments for the Drag To action.

Argument	Description
Target Object	Indicates that the step object is dragged to this target object.
HTML 5	Provides drag and drop support to the browser making it easier to code. When this argument is "true", only the "Target Object" and "HTML5" arguments are visible. When it is "false", the other arguments are also visible.
Button	Identifies the mouse button that is clicked.
X Offset	Identifies the offset from the top left of the target object in the x axis. This number must be positive.
Y Offset	Identifies the offset from the top left of the target object in the y axis.

Argument	Description
	This number must be positive.
Ctrl Key	Indicates whether this key is pressed during the action.
Alt Key	Indicates whether this key is pressed during the action.
Shift Key	Indicates whether this key is pressed during the action.

Get Property

The following table describes the step arguments for the Get Property action.

Argument	Description
Property	Indicates the property whose value will be stored in the specified variable. The list of properties available depends on all the roles of the object. The following are the default properties available for all objects: • **Visible text** - Indicates the visible text of the item, corresponding to the DOM textContent property. • **All text** - Indicates the entire text of the item, corresponding to the DOM textContent property. • **Inner HTML** - Indicates the inner html markup of the object, corresponding to the DOM innerHTML property.
Variable	Indicates the name of the variable in which to store the specified property value.

Scroll

The following table describes the step arguments for the Scroll action.

Argument	Description
Horizontally	Specifies the distance (in pixels) to scroll horizontally.
Vertically	Specifies the distance (in pixels) to scroll vertically.

Note: Both arguments must be integers, with a minimum and default value of 0. The scrolling is done on the containing document rather than on the element itself.

Upload

The following table describes the step arguments for the Upload action.

Argument	Description
Path	Specifies the selected path.

Verify

The following table describes the step arguments for the Verify action.

Argument	Description
Value	Indicates the string or number to verify.
Property	Indicates the object property whose value will be verified. The list of properties available to verify depends on all the roles of the object. The following are the default properties available for verification on all objects: • **Visible text** - Identifies items that are visible in the application. • **All text** - Identifies items that are in the application but are not necessarily visible. Items in this category are contained in DOM property textContent. • **Inner HTML** - Identifies items that are contained in the DOM property innerHTML.
Condition	Indicates the relationship between the value and property arguments.

Wait for Property

The following table describes the step arguments for the Wait for Property action.

Argument	Description
Value	Indicates the value of the specified property that the step will wait for, before the step passes.
Property	Indicates the object property whose value the script will wait for. The list of properties available for which to wait, depends on all the roles of the object. The following are the default properties available for all objects:

Argument	Description
	• **Visible text** - Identifies items that are visible in the application. • **All text** - Identifies items that are in the application but are not necessarily visible. Items in this category are contained in DOM property textContent. • **Inner HTML** - Identifies items that are contained in the DOM property innerHTML.
Condition	Indicates the relationship between the value and property arguments.

Filebox role

The following table describes the step argument for the **Set** action of the filebox role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Path	Specifies the selected path.

Flash object role

The following table describes the step argument for the **Type** action of the flash object role.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Value	Specifies what is typed.

Focusable role

The following table describes the step arguments for the **Press Key** action of the focusable role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Key Name	Specifies Enter, Space, Backspace, Tab, Escape, Delete, Up, Down, Left, or Right.
Ctrl Key	Indicates whether this key is pressed during the action.
Alt Key	Indicates whether this key is pressed during the action.
Shift Key	Indicates whether this key is pressed during the action.

Listbox role

The following table describes the step arguments for the **Select** action of the listbox role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Text	Indicates the selected string or a regular expression. This value is optional.
Ordinal	Specifies the order of the selected item in the list. If the text argument is also specified, then this argument refers to the instance of the specified text value in the listbox. An ordinal of 0 generates a random value. If both text and ordinal are left empty, then the default ordinal (1) is automatically filled.
Inner Object	Allows selecting an option based on TruClient's object identification mechanism for the option element itself, rather than identifying its container object and specifying an Ordinal.

Multi_listbox role

The following tables describe the step arguments related to multi_listbox role objects.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Select

The following table describes the step arguments for the Select action.

Argument	Description
Text	Indicates the selected string or a regular expression.
Ordinal	Specifies the order of the selected item in the list. If the text argument is also specified, then this argument refers to the instance of the specified text value in the listbox. An ordinal of 0 generates a random value.

Multi Select

The following table describes the step arguments for the Multi Select action.

Argument	Description
Text	The option's text.
By Ordinal	Specifies the ordinals of the item's Delimiter.
Delimiter	Specifies the characters used to separate the selected values.

Radiogroup role

The following table describes the step arguments for the **Select** action of the radiogroup role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Text	Indicates the selected string or regular expression.
Ordinal	Specifies the order of the selected item in the list. If the text argument is also specified, then this argument refers to the instance of the specified text value in the listbox. An ordinal of 0 generates a random value.

Slider role

The following table describes the step argument for the **Set** action of the slider role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Value	Specifies the value to which the slider is set.

Textbox role

The following table describes the step arguments for the **Type** action of the textbox role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Value	Indicates what is typed.
Clear	Clears the text box before typing. The default is true.
Typing Interval	Indicates the average time in milliseconds between keystrokes.

Video role

The following table describes the step argument for the **Seek** action of the video role object.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Argument	Description
Time	Sets or returns the current position (in seconds) of the video playback.

Step arguments not related to objects

The following tables describe the step arguments not related to objects. The actions in these step arguments do not operate on objects. Therefore, they do not have a role.

Tip: Mandatory arguments are marked with a red star to the left of the argument name in the user interface. All arguments can accept JavaScript code and TruClient functions as values.

Evaluate JavaScript

The Evaluate JavaScript action runs the JavaScript code contained in the step. The following table describes the step argument for the Evaluate JavaScript action.

Argument	Description
Code	Specifies the JavaScript code to run.

Evaluate JS on Object

The Evaluate JS on Object action runs the JavaScript code contained in the step after the specified object is loaded in the application. It also enables you to interact with the object by using the "object" keyword. For example, you can execute `object.click();` to initiate a click on the object.

The following table describes the step argument for the Evaluate JS on Object action.

Argument	Description
Code	Specifies the JavaScript code to run.

Catch Error

The Catch Error action catches an error in the step immediately preceding and runs the contents of the catch error step. The following table describes the step argument for the Evaluate C action.

Argument	Description
Error Type.	Specifies the error type you want to catch: • **Any** • **Object identification** - Indicates that the object the action is performed on cannot be found. • **Step arguments** - Indicates that one or more of the arguments to the preceding step is invalid. For example, the data type is wrong. • **Step Action** - Indicates that the user action failed. For example, a navigation step did not find the page. For an action on a UI element, this error is triggered if the object was found and the action failed anyway.

For Loop

The For Loop is a logical structure that repeats the steps contained in the loop a specified number of times. The following table describes the step arguments for the For Loop action.

Argument	Description
Init	Specifies the condition for the initialization operation, which must be met before testing the condition of the first iteration.
Condition	Specifies the condition for continuing to the next iteration. Options are: • **true** - Indicates that the specified condition is met. • **false** - Indicates that the specified condition is not met. • **Regular expression** - Defines a regular expression as the condition.
Increment	Increments a counter in the condition.

Generic API Action

The Generic API Action are blank steps that can be inserted and manually configured. The arguments vary according to the API selected. For API argument details, refer to the API Help in the TruClient Help Center at https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/TC_Functions.htm.

Note: The Web Macro Recorder supports a subset of the API arguments documented in the TruClient Help Center.

The following table describes the step argument for the Generic API Action.

Argument	Description
Variable	Specifies the name of the JavaScript variable in which the returned value is stored.

If Block

The If Block action is a logical structure that runs the steps contained in the block if the condition is met. The following table describes the step argument for the If Block action.

Argument	Description
Condition	Specifies the condition for continuing to the next iteration. Options are:

Argument	Description
	• **true** - Indicates that the specified condition is met (this is the default setting). • **false** - Indicates that the specified condition is not met. • **Regular expression** - Defines a regular expression as the condition.

Wait

The Wait action waits for a specified number of seconds (or milliseconds), before continuing with the next step. The following table describes the step arguments for the Verify PDF Content action.

Argument	Description
Interval	Specifies the time value that the step will wait for, before the step passes. The default value is 3.
Unit	Specifies the interval value. The unit properties available are Seconds (this is the default setting) and Milliseconds.
Think Time	Specifies whether to include the wait time in the think time calculation. The default setting is true.

Enhancing macros

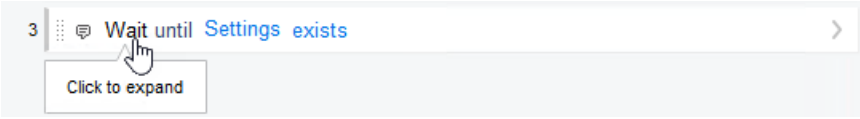
You can incorporate the following optional enhancements to recorded macros:

- "Modifying steps" below
- "Inserting loops and loop modifiers" on the next page
- "Inserting If blocks, If-else blocks, and Exit steps" on page 285
- "Inserting comments " on page 286
- "Inserting Catch Error steps" on page 287
- "Verifying that an object exists" on page 287
- "Inserting generic steps" on page 287

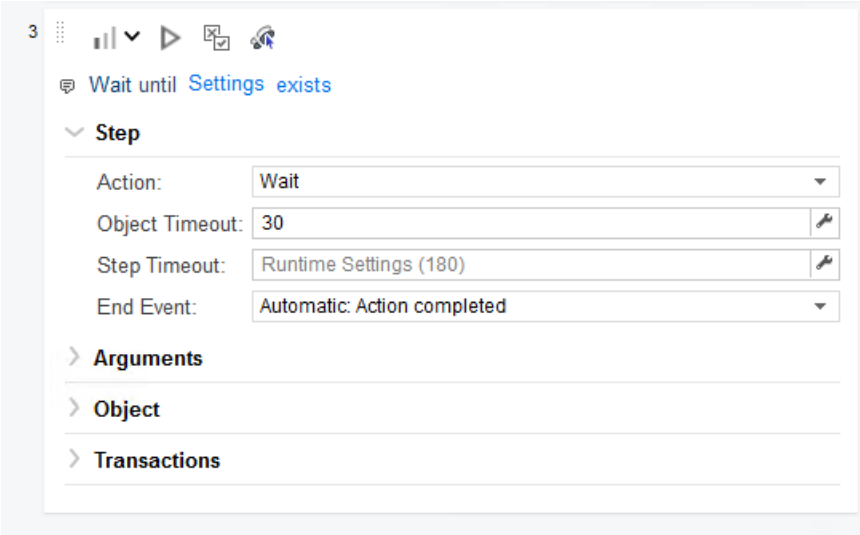
Modifying steps

To modify step arguments and objects:

- Select the desired step and expand the options.



This expands the step and enables you to modify the objects and properties.



Inserting loops and loop modifiers

Loops repeat selected portions of the macro until certain criteria are met or for a specified number of iterations. You can insert loops and break/continue loop modifiers from the Flow Control section of the Steps box.

Inserting "For" loops

"For" loops perform the steps surrounded by the loop until the end condition is met or the code reaches a break statement. Loop arguments use JavaScript syntax.

To insert a For loop:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **For loop** step to the desired location in the recorded steps.

Inserting "Break" statements

Break statements indicate that the current loop should end immediately. For example, if a Break statement is encountered in the second of five iterations in a For loop, the loop will end immediately without completing the remaining iterations.

To insert a Break statement:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **Break** step to the desired location in the recorded steps.

Inserting "Continue" statements

Continue statements indicate that the current loop iteration should end immediately. The loop condition is then checked to see if the entire loop should end as well. For example, if a Continue statement is encountered in the second of five iterations in a For loop, the second iteration will end immediately and the third iteration will begin.

To insert a Continue statement:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **Continue** step to the desired location in the recorded steps.

Inserting If blocks, If-else blocks, and Exit steps

To conditionalize a portion of the macro, you can insert If or If-else blocks. Exit steps cause a macro to exit the iteration or the entire macro. These can be used with If statements to exit a macro or iteration when a specified condition occurs.

For information about specific actions and arguments for each of these, see "Step arguments not related to objects" on page 280.

Inserting an If block

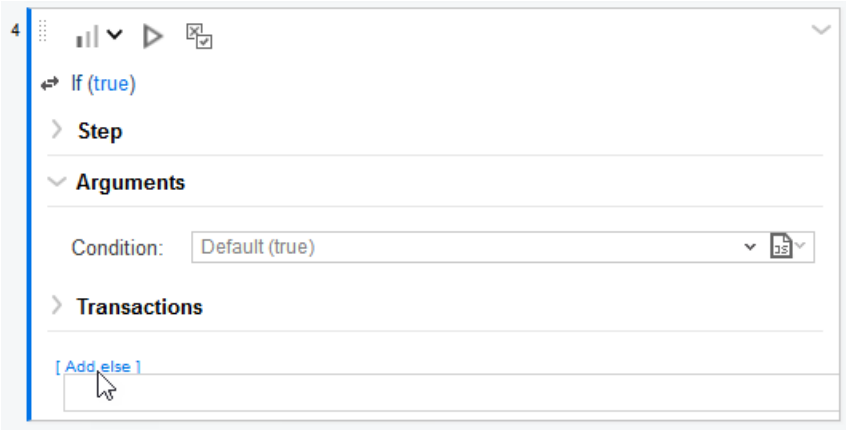
To insert an If block:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **If block** step to the desired location in the recorded steps.

Adding an Else condition

To add an Else condition:

1. Click the **Add else** link in the expanded step.



2. In the **Else** field, type the else condition.

Inserting an Exit step

To insert an Exit step:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **Exit** step to the desired location in the recorded steps.

Inserting comments

You can add comments to your macro so that others can understand what specific steps in the macro accomplish.

To insert comments into your macro:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Miscellaneous**.
3. Click and drag the **Comment** step to the desired location in the recorded steps.
4. Type the comment in the space provided.

Inserting Catch Error steps

"Catch Error" steps are group steps that run their contents if the previous step contains an error. Additionally, the error is "caught" and is not returned. You can define catch error steps to catch any error, or a specific type of error. If there are two catch error steps in a row, they both apply to the same step.

Tip: To group steps, use **Ctrl** + click to select multiple steps, right-click any of them, and click **Group Steps**.

To insert a catch error step:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Flow Control**.
3. Click and drag the **Catch Error** step to the desired location in the recorded steps.
4. Expand the catch error step and configure the argument. For more information, see "Step arguments not related to objects" on page 280.

Verifying that an object exists

You can insert a verify step to verify that a string or object exists in the application.

To insert a verify step:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Functions**.
3. Click and drag the **Verify** step to the desired location in the recorded steps.
4. In the verify step, click the **Click to choose an object** link.
5. In the TruClient browser, select the object you want to verify.

Inserting generic steps

You can insert a blank or generic step and manually configure it.

To insert a generic step:

1. In the TruClient sidebar, click the **Add Step** icon (Step).
   The Steps box opens.
2. Click **Functions**.

3. Click and drag the **Generic Object Action** step or the **Generic Browser Action** step to the desired location among the macro steps.

   Tip: Generic Object Actions perform an unspecified action on an object. Generic Browser Actions perform an unspecified action on the browser such as go back, reload, switch tabs, and so on.

4. Expand the step, and configure the step properties. For more information, see "Step arguments not related to objects" on page 280.

Inserting a Wait step

Wait steps cause the macro to pause for a specified amount of time before continuing with the next step. Wait for Object steps cause the macro to wait for a specified object to appear in the application before continuing with the next step. Wait steps begin after the End Event of the previous step is reached. This means that the previous step may continue to run after the wait step has been reached.

To insert a wait step:

1. In the TruClient sidebar, click the **Add Step** icon ().

   The Steps box opens.
2. Click **Functions**.
3. Click and drag the **Wait** step or the **Wait for Object** step to the location you want in the recorded steps.
4. If you inserted a Wait for Object step, select the **Click to choose an object** link to select the target object in the application.

Debugging macros

You can try these tasks to interactively debug a macro:

- "Viewing replay errors" on the next page
- "Running the macro step by step" on the next page
- "Using breakpoints" on the next page
- "Modifying step levels" on page 290
- "Inserting a Wait step" above
- "Disabling/enabling steps" on page 291
- "Making a step optional" on page 291
- "Playing a step" on page 291
- "Playing from a step to end of macro" on page 292

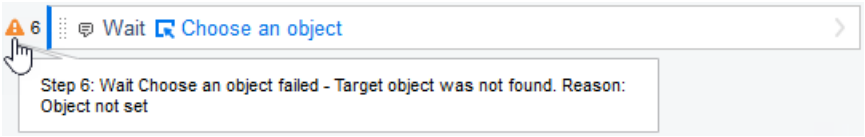
Viewing replay errors

If any steps failed during replay, they are marked with an error icon (⚠).

To view details about the error:

- Hover the mouse pointer over the error icon.

  A description of the error appears.



Running the macro step by step

The step-by-step replay pauses the replay after each step, which enables you to view the sequence more slowly and in a controlled manner.

To run the macro step by step:

- In the TruClient sidebar, select the drop-down arrow in the **Replay** icon (▷ ⌄) and select **Replay step by step**.

  The first (or next) step plays and the replay stops.

Repeat this procedure after each step to continue the step-by-step replay.

Using breakpoints

Breakpoints instruct the macro to stop running during a replay. You can insert (or toggle on) breakpoints to help debug a macro. After inserting a breakpoint on a step, the macro plays to the breakpoint and pauses. At this point, the Inspector Panel opens at the bottom of the TruClient browser. You can then continue playing the macro from the breakpoint.

Note: The Web Macro Recorder adds a breakpoint automatically if the macro fails during playback.

Inserting a breakpoint

To insert a breakpoint:

1. In the TruClient browser, select the step where you want to insert the breakpoint.
2. Click the toggle breakpoint icon (⊡).

A breakpoint is added to the step.

Deleting a breakpoint

To delete a breakpoint:

1. In the TruClient browser, select the step where the breakpoint has been inserted.
2. Click the toggle breakpoint icon ( ).

The breakpoint is removed from the step.

Modifying step levels

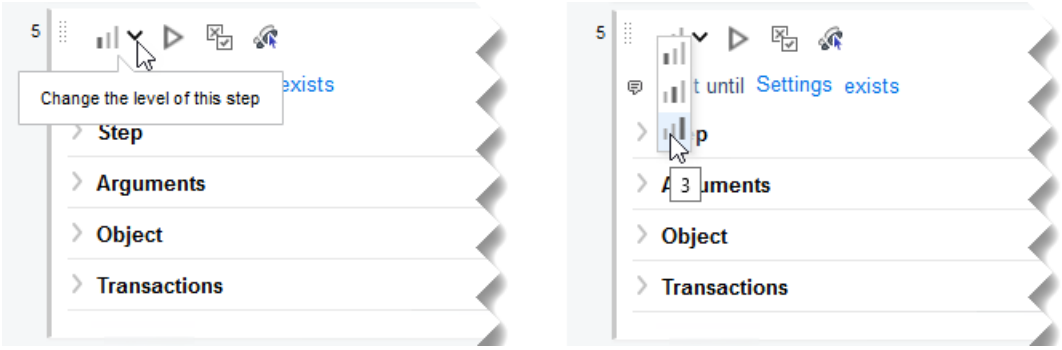
As you record a macro, TruClient assigns a level from 1 to 3 to each step. For example, a level 1 step is essential to the macro. A click step that occurs in an area of the application that has no effect is assigned to level 2. Mouse-over steps are generally considered unnecessary for the macro and are assigned to level 3.

Macro steps are displayed and played with the granularity specified as level 1, 2, or 3 in the step level slider in the toolbar at the top of the TruClient browser. The highest granularity is level 3—setting the slider to level 3 displays and plays back all the steps at levels 1, 2, and 3. Using higher granularity might be required for successful playback, but it can cause the macro to take longer to run. By default, the Script Level is set to 1.

In certain cases, you may want to manually change the level of a particular step, not the entire macro. For example, you may want to display and play a particular mouse-over step.

To change the level of a step:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click the **Step Level** drop-down arrow and select the desired level.



Important! If the step is part of a group step, both the group step and the individual step must be modified.

Tip: To group steps, use **Ctrl** + click to select multiple steps, right-click any of them, and click **Group Steps**.

See also

"Modifying the macro replay level" on page 242

Disabling/enabling steps

You can disable recorded steps so that they remain in the macro and can be re-enabled in the future, but are not played.

To disable/enable a macro step during replay:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click the **Disable/Enable during replay** icon ( ) in the toolbar for the step.

Tip: Alternatively, to disable or re-enable one or more steps, use Ctrl + click to select them, right-click one of the steps, and click **Disable Steps** or **Enable Steps** on the context menu.

Making a step optional

You can make some steps optional. An optional step is skipped during replay if its object is not found.

To make a step optional:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click the **Set step as optional** icon ( ) in the step toolbar.

Tip: To make a step non-optional again, click the icon again.

Playing a step

You can play a specific step to inspect the activity recorded in the step.

To play one step:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click the **Play this step only** icon ( ) in the step toolbar.

Playing from a step to end of macro

To start playback at a particular step and continue until the end of the macro:

1. Select the step where you want to start playback.
2. Right-click the step, and then select **Play From This Step** on the context menu.

Resolving object identification issues

In dynamic websites, objects that have been recorded can often move or change content. Object identification presents one of the biggest challenges with recording and replaying Web 2.0 applications. The dynamic nature of these sites can cause the macro to fail to locate the object.

The Web Macro Recorder includes sophisticated mechanisms to overcome this challenge, including the **Highlight**, **Improve Object Identification**, **Replace**, and **Related Object** options within steps that have objects. Using these options requires that you select an object in the application. For cases where various actions are required in the application to make the object visible, such as mouse over and mouse click, use the Ctrl+Alt+F4 option to suspend the object-selection mode until you bring the object into view and press Ctrl+Alt+F4 again to select the object.

When identifying objects for applications recorded in windows, use the **Windows** tab to make sure that the correct window is selected.

After you perform any of the changes, first replay the single failed step in question, and then replay the entire macro. This will help verify whether the change has solved the issue you encountered.

The following topics describe ways to resolve object identification issues:

- "Highlighting an object" below
- "Improving object identification" on the next page
- "Using alternative steps" on the next page
- "Modifying the object identification method" on page 295
- "Modifying the macro timing" on page 296
- "Relating objects to other objects" on page 297
- "Replacing an object" on page 298

Highlighting an object

For help in identifying an object previously selected in a step:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click (expand) **Object**.
3. Click **Highlight** to identify the object in the application.

If the object is found, it is temporarily highlighted by a blinking box.

If the object is not found, an error message is displayed. For more information, see "Improving object identification" below.

Tip: The error could be an issue of pacing and timing, or it might indicate that the correct page to find the object is not currently displayed.

Improving object identification

If highlighting an object fails, you can use the improve object identification function to re-select the target object.

To re-select the object:

1. In the Step Editor for the failed step, click the **Improve object identification** icon ( ) next to the **ID Method** field.

   The Web Macro Recorder relearns the properties of the object and compares them to the properties learned during recording. Based on the detected differences, you can make the necessary adjustments. Depending on how dynamic the application is, you may need to use the improve object identification function more than once.
2. Replay the step to see whether the problem was solved.

Using alternative steps

Alternative steps allow you to view multiple ways to perform the same action in a step, where it is possible. You can modify the step for the best or most consistent macro performance, or for debugging purposes.

For example, you may click on an option in a list in which the text changes based on some value. If you try to click based on the text, the step may fail. If you use an alternative step that selects the item in the list based on the ordinal value of the option within the list, the click succeeds regardless of the text.

Steps that have alternative options are labeled with an alternative step icon ( ) on the left.

Viewing and selecting alternative steps

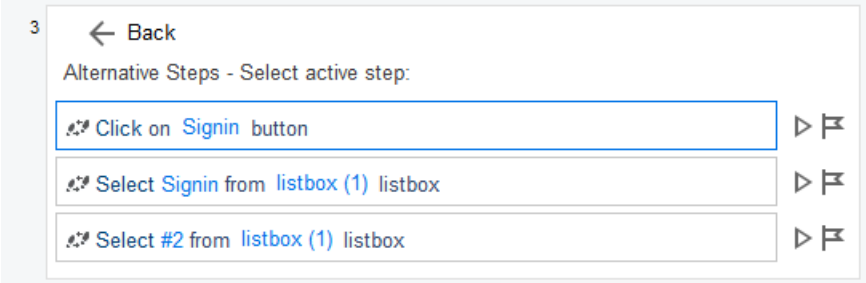
To view and select alternative steps:

1. Click the alternative step icon ( ) to view the alternative options for that step.

   Tip: If the Step Editor is open, the same icon appears in the step's toolbar and performs the same function.

   The alternative steps are shown.

2. Do one of the following:
   - To view an alternative step in the application, click the **Highlight the object in the AUT** icon ( ) to the right of the alternative.

     Tip: AUT means application under test.

     This performs the same highlighting function as described in "Highlighting an object" on page 292, with the convenience of allowing you to highlight each alternative one at a time within the macro step.

   - To play an alternative step in the application, click the **Play** icon ( ) to the right of the alternative.
3. Click an alternative to make it active.
4. Click **Back** to return to the Step Editor.

   The alternative that you selected is displayed for the step.
5. Replay the macro to test it.

Modifying the object identification method

You can modify the way the Web Macro Recorder identifies the object by modifying the object identification method (ID method) in the Object section of the Step Editor.

Available methods

The following table describes the available methods of object identification.

Method	Description
Automatic	The Automatic method is the default and recommended object identification method. This method allows the Web Macro Recorder to use its internal advanced algorithms to locate the object. **Tip:** If this method does not successfully find the object during replay, click the **Improve object identification** icon ( ) and replay the macro again.
XPath	If Automatic identification fails, even after using improve object identification or related objects, try using the XPath identification method. This method identifies the object based on an XPath expression that defines the object in the DOM tree. For example, if you need to select the first search result, regardless of the term being searched for, using XPath identification may help. **Tip:** For the XPath ID method, the icon function changes to **Regenerate expression**. When you click the icon, you can select an object in the interface and create its associated XPath.
JavaScript	This method uses JavaScript code that returns an object. For example: `document.getElementById("SearchButton")` returns an element that has a DOM ID attribute of "SearchButton." This method enables you to write JavaScript code that references the returned document. You can use CSS selectors and other standard functions. For example, the page returned by the server contains multiple links with the same "title" attribute (search results) and we want the script to randomly click on one of the available links. Object identification for this case, using the JavaScript identification method, may look similar to the following:

Method	Description
	`var my_results = document.querySelectorAll('a [title="SearchResult"]'); random(my_results);`
Descriptors	Enables you to identify an object by its properties in an editor. For more information, see TruClient Descriptors at https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm.

Selecting the object identification method

To select a different object identification method:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click (expand) **Object**.
3. Select a different method from the **ID Method** drop-down list.
4. Continue as follows:
   - If you selected **Automatic**, the procedure is complete.
   - If you selected **XPath**, a code snippet appears in an XPath text box below the ID Method list. Optionally, click the drop-down arrow next to the **XPath** text box and select a suggested XPath code for the object.

     Tip: You can click the Edit icon ( ) at the right end of the XPath text box to open the XPath Editor and edit the suggested XPath code.
   - If you selected **JavaScript**, a code snippet appears in a JavaScript text box below the ID Method list. Optionally, click the Edit icon ( ) at the right end of the **JavaScript** text box to open the JavaScript Editor and edit the suggested JavaScript code.
   - If you selected **Descriptors**, an empty Descriptors text box appears below the ID Method list. Click the Edit icon ( ) to create descriptor conditions for the object. For more information, see TruClient Descriptors at https://admhelp.microfocus.com/tc/en/2022-2022-r1/Content/TruClient/descriptors.htm.

Modifying the macro timing

Sometimes objects may not be found because of timing and synchronization issues. For example, the macro may be looking for an object that was in the application, but the macro replayed too quickly and already progressed to another page. If you suspect that the object is not being found because of

a timing or synchronization issue, you can insert Wait steps. For more information, see "Inserting a Wait step" on page 288.

Relating objects to other objects

If other options do not solve the issue with object identification, you can try using the **Related Objects** option.

If an object becomes difficult to identify on its own, you can label the object based on a different, more stable object. For example, you can select an object that is not dynamic and "relate it" to the target object. Relations are defined visually, relating objects according to their distance in pixels from other objects. Relations are defined per ID method, per object. If more than one relation is defined for an ID method of a given object, both relations must locate the same object for the step to pass.

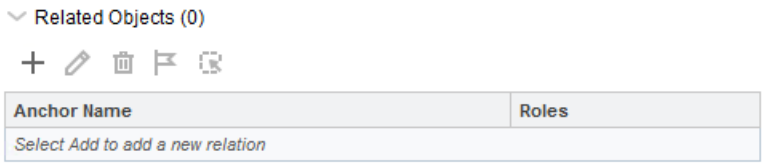
To use this function:

1. In the Step Editor for the failed step, click (expand) **Object**.

   Note: You can also find the **Related Objects** option in the Object area of the Event Handler Editor.

2. Click (expand) **Related Objects**.

   A relation table appears.



3. Click the **Add a new relation** icon (+).
   The Add related object window appears.
4. Follow the onscreen instructions to create a relation.
   The anchor object is added to the Related Objects table.

Tips

Follow these tips when using the Related Objects option:

- Use this feature only if other identification methods have failed, as it may be more resource intensive.
- Use the minimum search area to improve performance.

- Related Objects are sensitive to window sizing. Resizing may alter object positions and relationships. Take this into account.
- Each identification method (Automatic, XPath, JavaScript, and Descriptors) has its own set of related objects. These related objects are not shared among identification methods.
- If several relations exist, they must all be found in order for the identification to succeed.

Replacing an object

If you selected the wrong object during recording, or an object has permanently changed, you can replace it with a different object without replacing the step. This effectively resets the step, deleting changes (such as relations) made to the original step.

Using the Replace option tells the macro recorder that the object currently referenced in the step is incorrect. The macro recorder removes all current knowledge of the object and learns the object you select. Therefore, you must use the Replace option only if you used the wrong object during recording.

To replace an object:

1. In the TruClient sidebar, click the **Step Editor** icon ( ) for the step to change.
   The Step Editor opens.
2. Click (expand) **Object**.
3. Click **Replace**.
4. Select the new object.
5. Replay the macro.

Configuring settings

You can configure browser settings and interactive settings in the TruClient General Settings.

Accessing the TruClient General Settings

To access the General Settings:

1. In the TruClient sidebar, click the **General Settings** icon ( ).
   The TruClient General Settings window appears.
2. Configure settings as described in the following topics:
   - "Browser Settings" on the next page
   - "Interactive Options" on page 303
   - "Two-factor authentication" on page 304

- "Configuring certificates" on page 312

3. Click **Done** to save the settings and close the TruClient General Settings window.

Browser Settings

The following table describes the options on the **Browser Settings** tab.

Setting	Description

User Agent
 	
- HTTP Header
	Specifies the user agent string for the browser. You can configure user agent settings that will synchronize in both OpenText DAST and the Event-based Web Macro Recorder.
	
	Note: If you open the Event-based Web Macro Recorder from within a scan wizard, the user agent is populated from the application settings in OpenText DAST. If you open the Event-based Web Macro Recorder as a standalone tool, either from the OpenText DAST Tools menu or the Windows Start menu, the user agent field might be empty. In this case, the default browser value is used.
	
	The following list shows sample values, but is not complete:
	
	Default
	
	`Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:110.0) Gecko/20100101 Firefox/110.0`
	
	Internet Explorer 6
	
	`Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)`
	
	Internet Explorer 7
	
	`Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)`
	
	Internet Explorer 8
	
	`Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB5; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)`
	
	Googlebot 2.1

Setting	Description

	`Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)`
	Bingbot
	`Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)`
	Yahoo! Slurp
	`Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)`
	iPhone, iOS 14.3
	`Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.1`
	Important! You may also use a custom user agent string. However, OpenText recommends that only advanced users use a custom user agent string.

User Agent **- Navigator Interface**	These settings provide information that legacy web applications use to facilitate browser detection. You can customize these settings if you require browser-specific behavior. • **appName** - All browsers return "Netscape" as the value of this property. • **appVersion** - The browser returns either "4.0" or a string representing version information about the browser. • **platform** - The browser returns an empty string or a string representing the platform on which the browser is running. **Examples:** `MacIntel`, `Win32`, `Win64`, `iPhone`
Customize Keep-Alive timeout value	If you select the checkbox to enable this setting, configure the following: • **Keep-Alive timeout (milliseconds)** - Specifies the timeout (in milliseconds) for keeping idle connections open. This setting applies to both direct and proxied connections.

Setting	Description
Temporary Internet Files	The browser stores copies of web pages, images, and media for faster viewing later. Configure the **check for newer versions of stored pages** to determine when the browser is to compare the local copy of resource (cache) to the Web server. The options are: • **Every time I visit the webpage** - The browser checks the resource on every request to see whether the page changed since you last viewed it. If the page has changed, the browser displays the new page and stores it in the Temporary Internet Files folder. • **Every time I start browser** - The browser checks the resource on browser start. When you view a website that you have visited before in the same browser session, the browser uses the cached temporary Internet files instead of downloading the page. • **Automatically** - The browser checks for new content only when you return to a page that you viewed in an earlier session or on an earlier date. Over time, if the browser determines that images on the page are changing infrequently, it checks for newer images less frequently. • **Never** - The browser does not check the Web server for newer content.
Proxy	Specifies the proxy settings. The options are: • **Direct connection (proxy disabled)** - Make requests without a proxy connection. • **Auto detect proxy settings** - Use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the browser's web proxy settings. • **Use System proxy settings** - Import your proxy server information from the local machine. **Note:** System proxy settings are not supported on the Mac version. • **Configure proxy settings using a PAC file** - Load proxy settings from a Proxy Automatic Configuration (PAC) file in the location you specify in the **URL** field. • **Explicitly configure proxy settings** - Access the Internet through a proxy server. Provide the following server information:

Setting	Description
	• **Server** - Enter the URL or IP address of your proxy server. • **Port** - Enter the port number (for example, 8080). • **Type** - Select the protocol type for handling TCP traffic through the proxy server. The options are: **Standard**, **SOCKS4**, or **SOCKS5**. • **Authentication** - If authentication is required, select a type from the Authentication list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, or **Negotiate**. **Note:** Kerberos is supported on the Windows version only. • **User Name** - If your proxy server requires authentication, enter the qualifying user name. • **Password** - If your proxy server requires authentication, enter the qualifying password. • **Bypass proxy for** - 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.
Network Authentication	Specifies the authentication details to use when a server or form requires authentication. The settings are: • **Authentication** - Select a type from the Authentication list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, **Negotiate**, or **ADFS CBT**. **Note:** Kerberos is supported on the Windows version only. • **Username** - Enter the qualifying user name. • **Password** - Enter the qualifying password.

Interactive Options

The following table describes the settings on the **Interactive Options** tab.

Setting	Description
Enable webmacro file encryption	Encrypts the entire macro file upon saving. Otherwise, the file is saved in plain text, which exposes user names and passwords. This option is selected (ON) by default. **Note:** You can open encrypted macros even if this option is not selected. You can also open encrypted macros that were recorded using Web Macro Recorder with Firefox 30.
Force last step to be a validation step	Forces the last step in a login macro to be a validation step. After successful playback of a recorded macro, you are prompted to select an object to use for login validation. If you do not select an object, a prompt enforces this setting by asking you to select an object or discard the macro. This option is selected (ON) by default. If your application does not use an object for login validation, then disable this setting.
Support Web Storage	Enables web storage detection. When enabled, you can create and manage custom keys for web storage. Additionally, predefined event-based logout condition templates become available in the Logout Condition Editor. For more information, see "Working with web storage keys" on page 257 and "Working with logout conditions" on page 248.
Action on error	Specifies the action that TruClient takes when an error occurs during replay. The options are: • **Abort script** - Abort the script on error. • **Continue to the next iteration** - Stop iteration on error and continue to the next iteration. • **Continue to the next step** - Continue to the next step on error.
Snapshot generation	Not supported.
Steps generation	Configures settings for step generation. The **Default identification method** setting options are:

Setting	Description
	• **Replace server with parameter** - Replace the server name with a parameter in navigation steps. • **Create alternative steps when applicable** - Indicate whether or not to create alternative steps (when applicable). • **Create level 2 or level 3 steps during recording** - Indicate whether or not to create steps in level 2 or level 3.
Debug	The debug settings do not apply to replay outside of debugging. The options are: • **Enable Object Identification Assistant** - Enable object identification assistant. • **Ignore wait steps** - Accelerate script debugging by ignoring wait steps. • **Hide inspector panel** - If the script hits a breakpoint, hide the inspector panel. • **Automatically populate inspector pane** - Automatically load user defined data to the inspector panel. This option does not apply to coded-action debugging.

Two-factor authentication

Important! Configuring the two-factor authentication control center and mobile application applies only to standalone instances of the Event-based Web Macro Recorder. It is intended for testing locally prior to using in a scan.

"Something you have" two-factor authentication involves an application server sending an SMS or email response to the user upon login to the web application. To use two-factor authentication in a scan, you must configure a Node.js server as a control center to process the SMS and email responses coming from your application server.

Note: Only POP3 servers that support unique ID listing (UIDL) are supported.

Two-factor authentication control center

To configure the two-factor authentication control center:

1. In the **Local IP Address** drop-down list, select an IP address.

   Note: These IP addresses are available on the machine where the Event-based Web Macro Recorder is installed.

2. Do one of the following:
   - To use a specific port, select the port from the **Port** list.
   - To have the Web Macro Recorder choose the port, select the **Automatically Assign Port** check box.

     Important! The port for the control center must be exposed in the firewall so that the mobile application can access the server.
3. Click **Initialize**.

   The control center is started.

Mobile application

If your application server sends SMS responses, then you must install the **Fortify2FA** mobile application and download your two-factor authentication settings to it. After configuration, the mobile application receives the SMS response and forwards it to the control center.

Note: Currently, the mobile application is available only for Android operating systems.

To configure the mobile application:

1. In the **Phone Number** box, enter the phone number that will receive SMS responses.
2. Click **Generate QR Code**.

   The control center generates a quick response (QR) code that includes the two-factor authentication settings and a link to download the mobile application.
3. Install and configure the mobile application. For more information, see "Installing and configuring the Fortify2FA mobile app" below.

   Tip: If you use multiple threads in the scan, you might want to use more than one phone. Using the same phone number for multi-user scans can affect the scan time.
4. (Optional) To configure the mobile application for another phone, repeat steps 1-3.

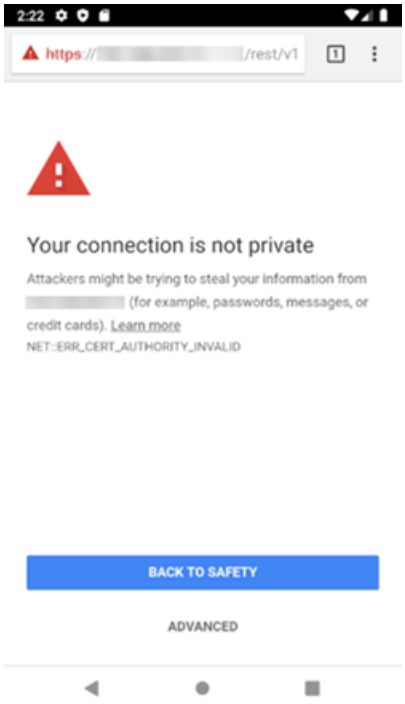
Installing and configuring the Fortify2FA mobile app

To install and configure the mobile application on the phone that will receive SMS responses:

1. Use the mobile phone's camera or QR code scanner to scan the QR code in the **Two-factor Authentication Mobile Application** settings.

   A link appears.
2. Click the link (or **Open** button) to access the site for downloading the app.

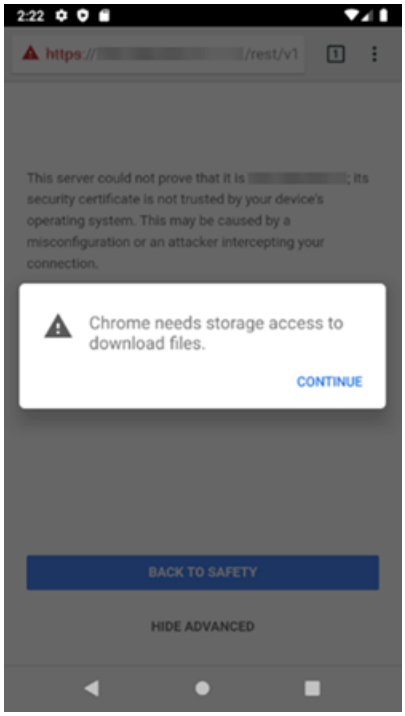
A warning about the self-signed certificate appears.



3. Click **ADVANCED**.
   Additional information is provided along with a link to proceed.

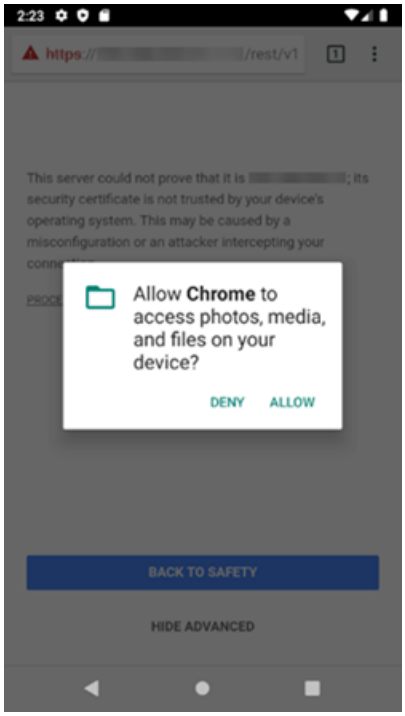
4. Click **PROCEED TO *<ip_address>* (UNSAFE)**.

A prompt requests storage access to download files.



5. Click **CONTINUE**.

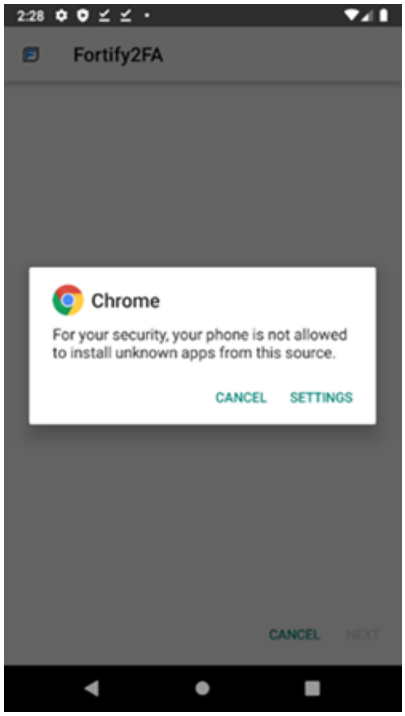
   A prompt requests access to photos, media, and files on the device.



6. Click **ALLOW**.

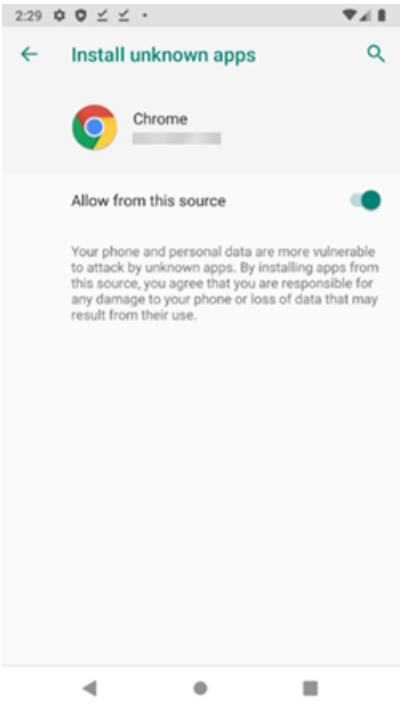
The fortify-2fa.apk file is downloaded.

7. Click **OPEN**.
   A prompt advises about installing unknown apps.

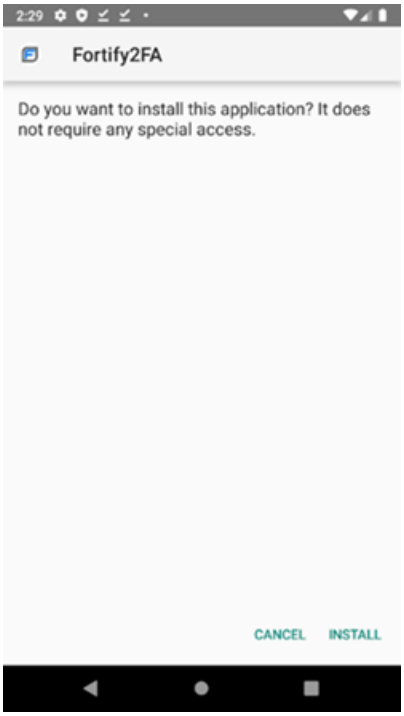


8. Click **SETTINGS**.

The Install unknown apps setting appears.

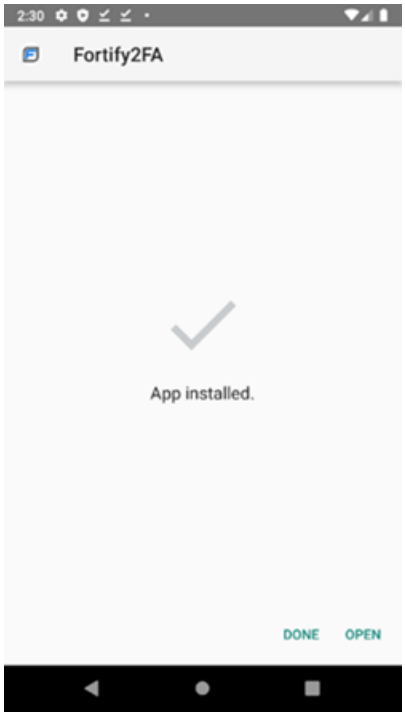


9. Enable **Allow from this source**.
   A prompt asks if you want to install the application.



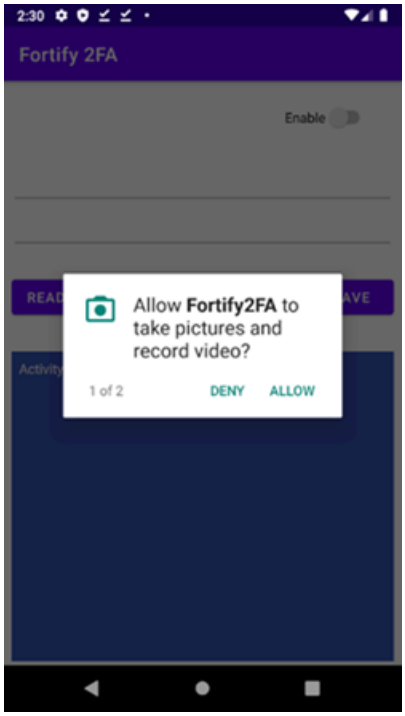
10. Click **INSTALL**.

A message indicates that the app is installed.



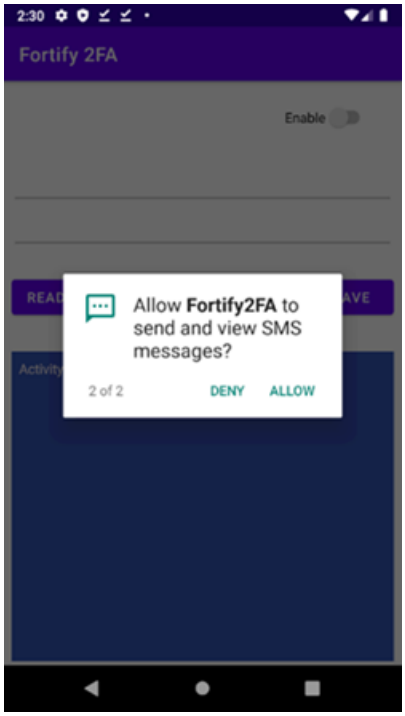
11. Click **OPEN**.

    A prompt requests permission to take pictures and record video.



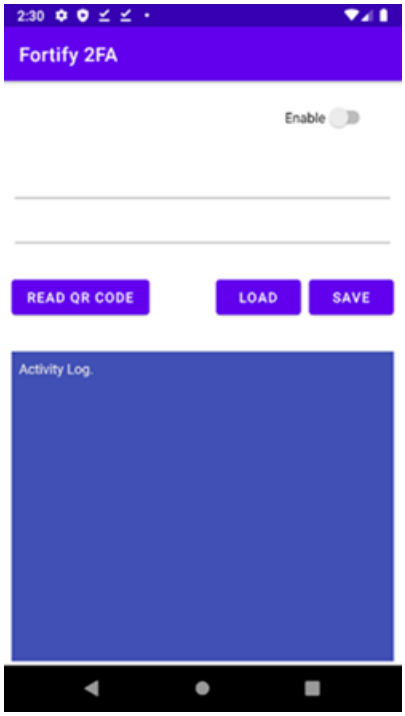
12. Click **ALLOW**.

A prompt requests permission to send and view SMS messages.



13. Click **ALLOW**.

    The app is ready to be configured.



14. Click **READ QR CODE** to scan the QR code in the **Two-factor Authentication Mobile Application** settings.

The two-factor authentication settings are configured in the **Fortify2FA** mobile application.

Configuring certificates

The **Browser Settings** and **Interactive Options** tabs (and the **Custom Keychains** tab in the Mac version) include a **Certificates** button that enables you to import a certificate from the local store into the Web Macro Recorder settings for use during a scan. For example, if the target application is a QA environment that uses a non-trusted certificate, you can add the non-trusted certificate to the local store, and then import it into the Web Macro Recorder settings.

When you configure certificates in the Web Macro Recorder settings, the certificates will be packaged as part of the macro and provided when the server requests client certificates during the scan.

Important! If, while recording, you navigate to a server that requires a client certificate, a dialog opens in the TruClient sidebar window with the following prompt:

"The site <*host*> is requesting a client certificate. Would you like to configure one now?"

OpenText recommends that you click **Yes** to configure a certificate. The prompt appears only once, and clicking **No** will require that you manually configure the certificate the next time you work with the macro. In some cases, macro playback during a scan might fail if a certificate has not been configured.

Adding a custom keychain on Mac

On macOS, you can add a custom keychain as a certificate store name.

To add a custom keychain:

1. On the **Custom Keychains** tab, click +.
2. Type the keychain name in the empty field.
3. Click **Done**.

   You can now configure certificates from this store name as described in "Configuring certificates" below.

Configuring certificates

To configure certificates:

1. On the **TruClient General Settings**, click **Certificates**.

   The Certificates Configuration dialog opens.
2. In the **Certificate Store** area, select one of the following:
   - **Local Machine** – This certificate store is local to the computer and is global to all users on the computer.
   - **Current User** – This certificate store is local to a user account on the computer.

3. In the **Certificate** area, select a certificate to add to the macro.
4. Click **OK**.

Uninstalling the Event-based Web Macro Recorder on Windows

When you uninstall OpenText DAST on Windows, you automatically uninstall the Event-based Web Macro Recorder that was installed as part of the OpenText DAST toolkit. You can also uninstall the standalone version on Windows operating systems.

To uninstall the Windows version:

1. In the **Control Panel**, go to **Programs** > **Programs and Features**.
2. In the list of programs, select **OpenText DAST Macro Recorder *<version>***.
3. Click **Uninstall**.

   A message prompts to confirm the uninstall.
4. Click **Yes** to confirm.

Cleaning up or uninstalling the Web Macro Recorder on Mac

In some cases, there might be a corrupted file or confirmation that interferes with the Web Macro Recorder operations. You can use the Troubleshoot menu options on the macOS menu bar to cleanup and refresh the Web Macro Recorder installation. You can also uninstall the Web Macro Recorder.

Using the Troubleshoot menu

To use the Troubleshoot menu:

1. In macOS menu bar, click **Troubleshoot**.
2. Choose one of the following menu options:
   - **Clean Application State** - Cleans the application state for the Web Macro Recorder launcher and its widget.
   - **Erase All Settings** - Erases all settings to correct configuration issues.
   - **Erase TruClientBrowser Executable** - Erases the TruClientBrowser executable and reinstalls it to correct installation issues.
   - **Uninstall** - Removes the Web Macro Recorder and all of its data from the system.

3. If uninstalling the Web Macro Recorder, continue as follows to completely remove the application and its files and containers:
   a. On the DAST Web Macro Recorder Uninstall Main Screen, click **Configure All Files Access**.
      The Full Disk Access dialog opens.
   b. Click **+** and enter your password.
   c. From the **Applications** list, select **MacroRecorder.app** and then click **Open**.
      A message prompt appears.
   d. Click **Quit & Reopen**.
      The Web Macro Recorder closes and reopens.
   e. In macOS menu bar, click **Troubleshoot** > **Uninstall**.
   f. Click **Continue**.
   g. Enter your password and click **OK**.
      The DAST Web Macro Recorder Uninstall Main Screen shows the progress.
   h. Upon completion, click **Done**.

Chapter 19: Web Proxy

Web Proxy is a stand-alone, self-contained proxy server that you can configure and run on your desktop. With it, you can monitor traffic from a scanner, a browser, or any other tool that submits HTTP requests and receives responses from a server. It is a tool for debugging and penetration assessment; you can see every request and server response while browsing a site.

You can also create a workflow macro or a login macro that you can use with OpenText DAST.

Tip: You can create a workflow macro from a set of Burp proxy files or an HTTP Archive (HAR) file. For more information, see "Creating a web macro" on page 331.

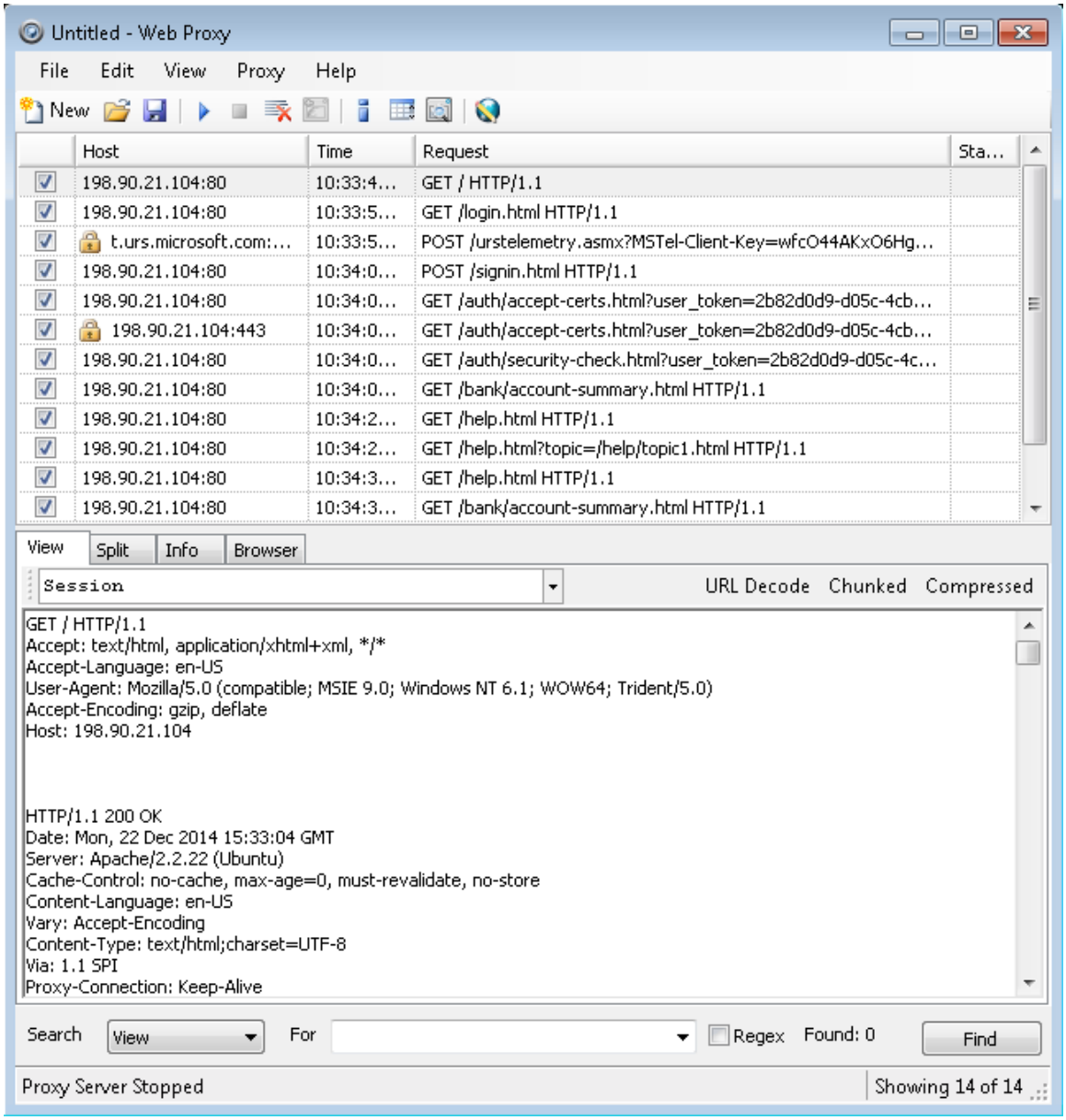
Using Web Proxy

To use Web Proxy with a browser:

1. Click **Tools > Web Proxy**.
   The Web Proxy window opens.
2. Click **Start** (or select **Start** from the **Proxy** menu).
   "Listening on <server:port number>" appears in the Web Proxy status bar.
3. Click **Launch Browser**.
   This starts a web browser and configures it to communicate through Web Proxy. Alternatively, if you prefer to use a different browser, see "Manual configuration of browser" on page 336 for configuration instructions.
4. Manually navigate the site for which you want capture requests/responses.
5. If Web Proxy receives a request for a certificate from a web server, it displays a dialog box asking you to locate the certificate. The program then caches your selection on a "per server" basis. Therefore, if you subsequently want to use a different certificate for a particular server, you must clear the cache by stopping and then restarting Web Proxy.
6. When you have browsed to all necessary pages, return to Web Proxy and click (or select **Stop** from the **Proxy** menu).

Image of Web Proxy

The following image shows the Web Proxy after it has been stopped.



7. To change the format in which the message is displayed, select one of the tabs (**View**, **Split**, **Info**, or **Browser**).

   When using the **View** or **Split** tabs, you can enable or disable URL decoding of requests and responses by selecting the **URL Decode** button. Since most OpenText DAST attack traffic is URL encoded, this feature makes it easier to analyze HTTP messages. To illustrate, compare the following URL encoded and decoded versions of the same GET request:

   - GET

```
/notes.asp?noteid=1%20union%20%20select%200%2c1%2c2%20from%20informatio
n_schema.tables%20order%20by%204%20desc%20limit%201 HTTP/1.1
```

- `GET /notes.asp?noteid=1 union select 0,1,2 from information_ schema.tables order by 4 desc limit 1 HTTP/1.1`

The **Chunked** and **Compressed** buttons are enabled if a response is either chunked-encoded or compressed. This feature enables you to view the original response received by Web Proxy as well as the de-chunked or decompressed response.

8. To resend a request (with or without editing), select it from the list of displayed sessions and click the HTTP Editor icon (or right-click the request and select **HTTP Editor** from the context menu).
9. To clear sessions from the list, select one or more sessions and press the Delete key (or click **Edit > Clear Selected**). To clear all sessions, click **Edit > Clear All**.

Note: When you clear a session from the Web Proxy list, you also remove it from the captured data. For example, if you have 100 sessions in the list and clear 98 of them, and then save the sessions to a file, only the two remaining sessions will be included. When clearing sessions, ignore the check boxes.

Use the File menu to save selected requests to a traffic session file (`.tsf`) and later load them for analysis (using the **File > Open** command). You can also save a sequence of requests as a Web Macro that you can use when conducting an OpenText DAST scan. All **File** menu commands apply to "check-marked" requests.

Saving sessions

To save one or more sessions for later analysis:

1. Select the sessions you want to save by placing a check mark in the left column.
2. Click the **File** menu and select **Save** or **Save As**.
3. Enter a name in the **File name** box and click **Save**.

Clearing sessions

When you clear a session from the Web Proxy list, you also remove it from the captured data. For example, if you have 100 sessions in the list and clear 98 of them, and then save the sessions to a file, only the two remaining sessions will be included.

To clear one or more sessions:

1. Select a session. For multiple sessions, use the CTRL or SHIFT keys.

Note: Note: When clearing sessions, ignore the check boxes.

2. Do one of the following:
   - Press the **Delete** key
   - Click **Edit > Clear Selected**.

To clear all sessions, click  (or click **Edit > Clear All**).

Searching a message

You can locate information in the message displayed on the View, Split, or Info tabs using the controls at the bottom of the Web Proxy window.

To search a message:

1. From the **Search** list, select a tab to search.
2. In the **For** box, enter the text (or a regular expression representing the text) you want to locate.
3. If you entered a regular expression in step 2, select the **Regex** check box.
4. Click **Find**.

Note: You can also create rules that will locate information during each session, without requiring you to manually search using the above procedure. See "Settings: Search-and-Replace" on page 326 and "Settings: Flag" on page 327.

Searching all messages

You can search all sessions for specific information.

To search all messages:

1. Click the **Toggle Search View** button  on the toolbar (or select **Search** from the **View** menu).
2. Use the **Search Area** list to specify whether you want to search the entire contents of all sessions or limit the search to a particular segment.
3. In the **Search For** box, enter a regular expression representing the text you want to locate.
4. Click **Search**.

Note: You can also create rules that will locate information during each session, without requiring you to manually search using the above procedure. See "Settings: Search-and-Replace" on page 326 and "Settings: Flag" on page 327.

Changing options

To change Web Proxy options:

1. If Web Proxy is listening, do one of the following:
   - Click the **Proxy** menu and select **Stop**
   - Click  on the toolbar.
2. Click **Edit > Settings**, and select **Proxy Servers** tab.

See "Settings: Proxy Servers" on page 323 for more information.

Web Proxy tabs

Each HTTP session (a single request and the associated response) is listed in the top pane of Web Proxy. When you select a session, Web Proxy displays information about the session in the lower pane. The information displayed depends on which tab you select.

You can search these tabs for specific content using the controls immediately above the status bar.

View

Use the **View** tab to select which HTTP messages you want to inspect. Options available from the drop-down list immediately below the tab are:

- Session: view the complete session (both request and response)
- Request from browser to Web Proxy: view only the request made by the browser to Web Proxy
- Request to server from Web Proxy: view only the Web Proxy request to the server
- Response from server to Web Proxy: view only the server response to Web Proxy
- Response to browser from Web Proxy: view only the Web Proxy response to the browser

Split

Click the **Split** tab to create two information areas for a single session. For example, you could show the HTTP request message created by the browser (in one area) and the HTTP response generated by the server (in the second area).

Info

Use the **Info** tab to view detailed information about the requests. Information includes the number of forms found, header information, and the properties of the page.

Browser

Click the **Browser** tab to view the response as formatted in a browser.

Web Proxy interactive mode

Use Interactive mode to view each browser request and each server response as the messages arrive at Web Proxy. The message will not continue toward its destination until you click **Send**. This permits you to modify the message before it is delivered.

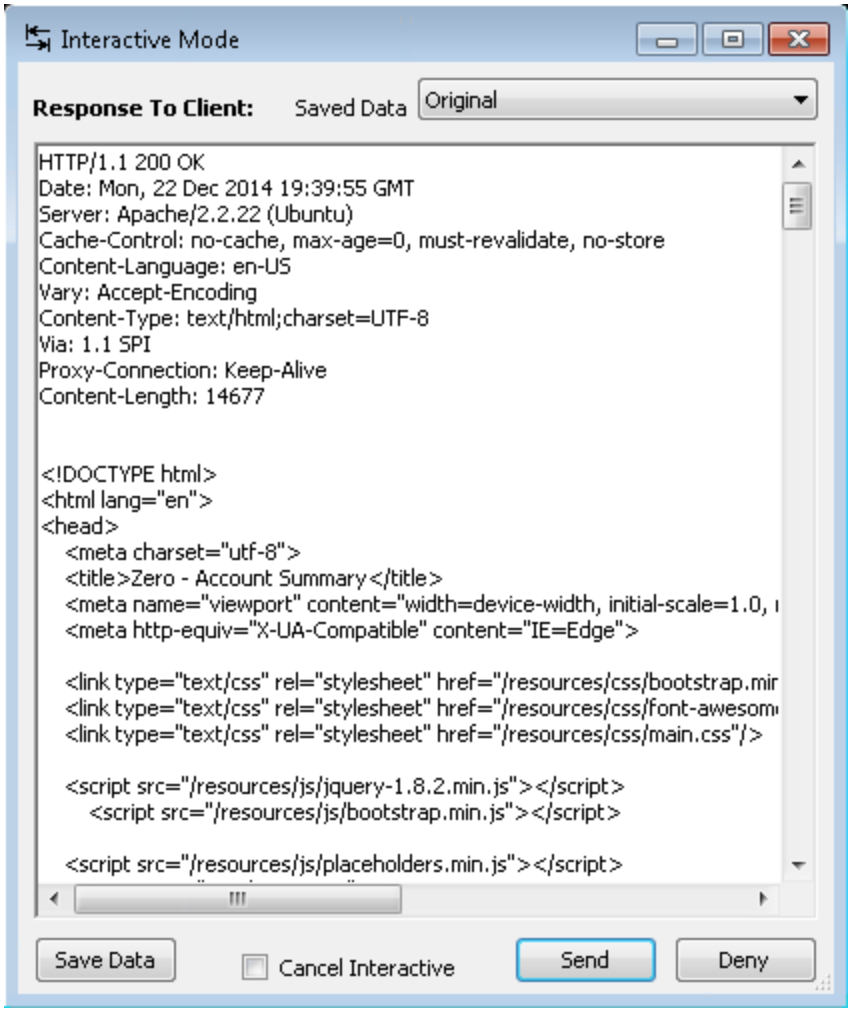
You can also prevent the message from being sent to the server by clicking **Deny**.

Using the **General** tab in the Web Proxy Settings window, you can force Web Proxy to pause as follows:

- After each request
- After each response
- After locating specific text in either the request or response (using search rules)

Image of Web Proxy interactive mode

The following image shows the Web Proxy in interactive mode.



Enabling interactive mode

To enable interactive mode:

1. Click the **Proxy** menu and select **Stop**.
2. Do one of the following:
   - Click the **Proxy** menu and select **Interactive**.
   - Click  on the toolbar.
3. Click the **Proxy** menu and select **Start**.

Note: When Web Proxy is in Interactive mode, a check mark appears next to the **Interactive** command on the **Proxy** menu and the Interactive icon is backlit  . Clicking the icon or selecting the command will toggle the Interactive mode on or off.

Settings

Use this property sheet to configure Web Proxy's interface, add proxy servers, and create regular expressions for locating specific information in the request or response.

Note: You cannot change settings while Web Proxy is running. Select **Stop** from the **Proxy** menu, change the settings, and then restart Web Proxy.

The Web Proxy Settings property sheet has the following tabs:

- General (see "Settings: General" below)
- Proxy Servers (see "Settings: Proxy Servers" on the next page)
- Search and Replace (see "Settings: Search-and-Replace" on page 326)
- Flag (see "Settings: Flag" on page 327)
- Evasions (see "Settings: Evasions" on page 327)
- Network Authentication (see "Settings: Network Authentication" on page 330)

Settings: General

The **General** tab contains the following options.

Proxy listener configuration

Enter an IP address and port number. By default, Web Proxy uses address 127.0.0.1 and port 8080, but you can change this if necessary.

Note: Both Web Proxy and your Web browser must use the same IP address and port.

To configure Web Proxy on your host to be used by another host, you will need to change the value of the Local IP Address. The default address of 127.0.0.1 is not available to outside hosts. If you change this value to your workstation's current IP address, remote stations can use your workstation as a proxy.

Do not record

Use this option to create a regular expression filter that keeps files of specific types from being handled by Web Proxy. The most common types are already excluded as defaults, but other types (MPEG, PDF, etc.) can also be excluded. The purpose is to allow you to focus on HTTP request/response lines and headers by removing clutter from the message body.

Interactive

When using the interactive mode, you can force Web Proxy to pause when it:

- Receives a request from the client
- Receives a response from the server
- Finds text that satisfies the search rules you create (using the **Flag** tab)

If you select any of these options, Web Proxy will continue only after you click the **Allow** button.

Logging

Select the type of items you want to record in the log file and specify the directory in which the log file should be maintained.

If you elect to record requests and/or responses, you can also choose to convert and log the data using Base 64 encoding. This can be useful when responses contain binary data (such as images or flash files) that you want to examine.

- Raw Request refers to the HTTP message sent from the client to Web Proxy.
- Modified Request refers to the HTTP message sent from Web Proxy to the server.
- Raw Response refers to the HTTP message sent from the server to Web Proxy.
- Modified Response refers to the HTTP message sent from Web Proxy to the client.

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 Web Proxy should use.

Settings: Proxy Servers

Use this area to add one or more proxy servers through which Web Proxy will route all its requests. Distributing the attack across multiple servers makes detection and counter-measures more difficult, thus mimicking how a hacker might attempt to avoid an intrusion detection system.

If you use multiple proxy servers, Web Proxy will "round-robin" the requests (i.e., Web Proxy will sequence through the list of proxy servers, sending the first request to the first server, the second request to the second server, and so on).

You can also specify IP addresses that should be accessed without using a proxy server.

Adding a proxy server

To add a proxy server through which Web Proxy requests will be routed:

1. In the **Proxy Address** box, type the IP address of the server through which you want to route Web Proxy requests.
2. Specify the port number in the **Proxy Port** box.
3. Select the type of proxy (standard, SOCKS4, or SOCKS5) from the **Proxy Type** list.
4. Select an authentication type: **None**, **Auto**, **Kerberos**, **NTLM**, or **Basic**.

   If you are unsure of which type to use, select **Auto**; Web Proxy will attempt both NTLM and Basic authentication.
5. If this server requires authentication, type your authentication credentials in the **Username** and **Password** boxes.
6. Click **Add** to add that server and display its IP address in the **Available Proxy Servers** list.

Importing a proxy server

To import a list of proxy servers:

1. Click **Import**.
2. Using the standard file-selection dialog box, select a delimited text file that contains the list of proxy servers.
3. Click **Open**.

The file containing proxy information must be formatted as follows:

- Each line contains one record followed by a carriage return and line feed.
- Each field in the record is separated by a semicolon.
- The fields appear in the following order:
  address;port;proxytype;username;password;authenticationtype
- The username and the password are optional. However, if authorization is not used, you must include two semicolons as placeholders.

Examples:

```
128.121.4.5;8080;Standard;magician;abracadabra;NTLM
127.153.0.3;80;socks4;;None
128.121.6.9;443;socks5;myname;mypassword;None
```

Editing proxy servers

To edit the list of proxy servers:

1. Select a server from the **Available Proxy Servers** list.
2. Change the information displayed in any of the controls: Proxy Address, Proxy Port, Proxy Type,

Username, or Password.

3. Click **Update**.

Removing a proxy server

To remove a proxy server from the list:

1. Select a server from the **Available Proxy Servers** list.
2. Click **Remove**.
3. Click **Yes** to confirm the deletion.

Bypassing proxy servers

If you do not need to use a proxy server to access certain URLs (such as internal testing sites), you can specify one or more hosts in the **Bypass Proxy List** area. To bypass proxy servers when accessing certain sites:

1. Click **Add**.

   The Bypass Proxy dialog box appears.
2. Enter the host portion of the HTTP URL that should be bypassed.

   Do not include the protocol (such as http://).
   For example, to bypass a proxy server for this URL

   ```
   http://zero.webappsecurity.com/Page.html
   ```

   enter this string

   ```
   zero.webappsecurity.com
   ```

   or this string

   ```
   zero.*
   ```

   Note: You can also enter an IP address. Note that Web Proxy will not resolve host names to IP addresses. That is, if you specify an IP address and the HTTP request actually contains that numeric IP address, then Web Proxy will bypass a proxy server for that host. However, if the HTTP request contains a host name that normally resolves to the IP address you specify, Web Proxy will still send the request to a proxy server (unless you also specify the host name).
3. Click **OK**.

Deleting an address

To delete an address from the **Bypass Proxy List**, select the address and click **Remove**.

Settings: Search-and-Replace

Use this tab to create rules for locating and replacing text or values in HTTP messages. This feature provides a highly flexible tool for automating your simulated attacks. Some suggested uses include:

- Masking sensitive data, such as user names and passwords
- Appending a cookie to each request
- Modifying the Accept request-header field to add or delete media types that are acceptable for the response
- Replacing a variable in the Request-URI with a cross-site scripting attack

Finding and replacing text

To find and replace text in requests or responses:

1. Click **Add**.

   Web Proxy creates a default entry in the table.
2. Click the **Search Field** column of the entry.
3. Click the drop-down arrow and select the message area you want to search.
4. In the **Search For** column, type the data (or a regular expression representing the data) you want to find.
5. In the **Replace With** column, type the data you want to substitute for the found data.
6. Repeat steps 1-5 to create additional search rules.

The request/response rules are applied sequentially, in the order in which they appear. For example, if a rule changes HTTPS to SSL, and if a subsequent rule then changes SSL to SECURE, the result will be that HTTPS is changed to SECURE.

Note: Search-and-replace rules are executed on request messages sent from Web Proxy to the server and on response messages sent from Web Proxy to the browser. You can observe the altered messages by choosing the **Info** tab, or by selecting either the **View** or **Split** tab and then choosing one of the following from the drop-down list immediately below the tab:

- Request: WebProxy -> Server
- Response: Browser <- WebProxy
- Session

Deleting a rule

To delete a rule:

1. Select the rule you want to delete.
2. Click **Remove**.

Editing a rule

To edit a rule:

1. Click an entry in the **Search Field**, **Search for**, or **Replace with** column.
2. Change the data

Deactivating a rule

To deactivate a rule without deleting it:

1. Clear the **On** check box.
2. Click **OK**.

Settings: Flag

You can search areas of request and response messages to find and highlight the data you specify.

1. Click **Add**.

   Web Proxy creates a default entry in the table.
2. Click the **Search Field** column of the entry.
3. Click the drop-down arrow and select the message area you want to search.
4. In the **Search** column, type the data (or a regular expression representing the data) you want to find.
5. Click the **Flag** column of the entry.
6. Click the drop-down arrow and select a color with which to highlight the data, if found.
7. Repeat steps 1-6 to create additional search rules.

Settings: Evasions

Evasions are techniques that Web Proxy uses to circumvent intrusion detection systems, monitors, sniffers, firewalls, log parsers, or any device that attempts to shield systems from attack by filtering HTTP requests. Typically, these filters examine portions of the request, searching for "signatures" that indicate malicious threats or potential breeches of system security. If they detect these signatures, they reject the request.

To evade detection, Web Proxy modifies the HTTP request to obscure the signature for which the filter is searching, while retaining integrity sufficient for the message to be processed by the server. Of course, the techniques used by Web Proxy are not always successful. As developers become aware of methods that compromise their product's effectiveness, they incorporate procedures to combat them.

Caution! This feature is intended for use as a penetration testing tool. Do not use it or enable it when conducting vulnerability assessment scans with OpenText DAST.

Use the following procedure to enable evasions:

1. Select **Enable Evasions**.
2. Choose one or more evasion techniques, as described in the following sections.

Method Matching

Web Proxy replaces the GET method with HEAD. This is an attempt to defeat a filter that searches for a signature that begins with GET.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.microsoft.com/secretfile.txt HTTP/1.1
```

Web Proxy sends the following message to the server:

```
HEAD http://www.microsoft.com/secretfile.txt HTTP/1.1
```

URL Encoding

Web Proxy converts characters in the URL to a "%" followed by two hexadecimal digits corresponding to the character values in the ISO-8859-1 character set.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/cgi-bin/filename.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET %2f%63%67%69%2d%62%69%6e%2f%66%69%6c%65%6e%61%6d%65%2e%63%67%69
HTTP/1.1
Host: zero.webappsecurity.com
```

If the device is looking for "cgi-bin" as the signature, it does not match the string "%63%67%69%2d%62%69%6e" and so the request is not rejected.

Double Slashes

Web proxy converts each forward slash (/) into a double forward slash (//).

For example, the browser sends the following message to Web Proxy:

```
GET http://www.microsoft.com/en/us/secrets.aspx HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET //en//us//secrets.aspx HTTP/1.1
Host: www.microsoft.com
```

If the device is looking for "/secrets.aspx" as the signature, it does not match the string "//secrets.aspx" and so the request is not rejected.

Reverse Traversal

This technique attempts to disguise a request for a certain resource by interjecting references to relative directories, which equates to the original request.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.TargetSite.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /d/../cgi-bin/d/../some.cgi HTTP/1.1 [which equates to GET/cgi-bin/some.cgi]
Host: www.TargetSite.com
```

Self-Reference Directories

Web Proxy uses the notation for parent directory (../) and current directory (./) to obfuscate the request.

For example, the browser sends the following message to Web Proxy:

```
GET http://www.TargetSite.com/cgi-bin/phf HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /./cgi-bin/./phf HTTP/1.1  [which equates to GET /cgi-bin/phf]
Host: www.TargetSite.com
```

Parameter Hiding

A request can contain parameters that are used to build dynamic page content. These parameters are typically used when search requests or selections are made and take this form:

```
/anypage.php?attack=paramhiding&evasion=blackhat&success...
```

This technique is effective against a device that does not examine that portion of the request following the question mark (?). However, the parameter indicator can be used to potentially mask further relevant data.

For example, the browser sends the following message to Web Proxy:

```
GET /index.htm%3fparam=/../cgi -bin/test.cgi
```

Web Proxy sends the following message to the server:

```
GET /index.htm?param=/../cgi -bin/test.cgi
```

HTTP Misformatting

An HTTP request has a clearly defined structure:

```
Method<space>URI<space>HTTP/Version<CR><LF>
```

However, some web servers will accept a request that contains a tab character instead of a space, as in the following:

```
Method<tab>URI<tab>HTTP/Version<CR><LF>
```

Any filter that incorporates the space (between the three components) as part of the signature for which it searches will fail to reject the request.

Long URLs

This technique is directed toward devices that do not examine the entire request string, but concentrate only on a subset of a programmable length (such as the first 50 characters). Web

Proxy inserts a large number of random characters at the beginning of the request so that the operative portion of the request is pushed beyond the area normally examined by the filter.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/ HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /YPVIFAHD[hundreds of characters]NIWCJBXZPXMP/../ HTTP/1.1
Host: zero.webappsecurity.com
```

DOS/Win Directory Syntax

A Windows-based filter that attempts to detect a specific signature (such as /cgi-bin/some.cgi) might be fooled if a backward slash is substituted for a forward slash (such as /cgi-bin\some.cgi). Windows-based web servers convert a forward slash to a backward slash when interpreting directory structures, so the notation is valid. However, HTTP rules require the first character of a URI to be a forward slash.

NULL Method Processing

This technique injects a URL-encoded NULL character immediately after the METHOD (such as GET%00). It is designed for a filter that attempts to apply string operations on the request, and those string libraries use the NULL character to denote the end of a string. If this ploy is successful, detection of the NULL character prevents the device from examining the remainder of the message.

Case Sensitivity

This technique is designed to evade a filter that searches for a case-specific string.

For example, the browser sends the following message to Web Proxy:

```
GET http://zero.webappsecurity.com/cgi-bin/some.cgi HTTP/1.1
```

Web Proxy sends the following message to the server:

```
GET /CGI-BIN/SOME.CGI HTTP/1.1
Host: zero.webappsecurity.com
```

Settings: Network Authentication

If your proxy server requires network authentication, you can configure it on the **Network Authentication** tab in the Web Proxy Settings.

To configure network authentication:

1. Select **Enable Network Authentication**.
2. Choose an authentication type from the **Authentication Type** list. Available types are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**

- **Digest**
- **Kerberos**
- **Negotiate**
- **NT LAN Manager (NTLM)**

3. Type a user ID in the **Username** box and the user's password in the **Password** box.

Creating a web macro

You can use either the Web Macro Recorder or Web Proxy to create a workflow macro or a login macro.

A workflow macro is used most often to focus on a particular subsection of an application. It specifies URLs that an OpenText scanner will use to navigate to the area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application. You can use sessions captured by Web Proxy or a set of Burp proxy files or an HTTP Archive (HAR) file.

A login macro is used for web form authentication, allowing the scanner to log in to an application. You can also incorporate logic that will prevent the scanner from inadvertently logging out of your application.

Using Burp proxy or HAR Files

To create a workflow macro from a set of Burp proxy files or an HTTP Archive (HAR) file:

1. Click **File > Open**.
   A standard Windows Open dialog box opens.
2. In the drop-down list, select either **Burp proxy (*.*)** or **Har File (*.har)**.
3. Navigate to and open the Burp proxy or .Har files.
   The sessions are populated in the Web Proxy.
4. Continue with "Creating a web macro from selected sessions" below.

Creating a web macro from selected sessions

To create a web macro using sessions displayed in or captured by Web Proxy:

1. Select the sessions you want to include in the macro by placing a check mark in the left column.
2. Click the **File** menu and select **Create Web Macro**.
   The Create Web Macro dialog box opens.
3. (Optional) On the Create Web Macro dialog box, select **Enable Check for Logout** and then enter a regular expression that identifies a unique text or phrase that occurs in the server's HTTP response when a user logs out or when a user who is not logged in requests access to a protected

URL.

Example: During a normal scan, the scanner begins crawling your site at the home page. If it encounters a link to another resource (usually through an <A HREF> HTML tag), it will navigate to that URL and continue its assessment. If it follows a link to a logout page (or if the server automatically "logs out" a client after a certain number of minutes), the scanner will not be able to visit additional resources where the client is required to be logged in. When this inadvertent log-out occurs, the scanner must be able to log in again without user intervention. This process hinges on the scanner's ability to recognize when it is no longer logged in.

In some applications, if the user logs out (by clicking a button or some other control), the server responds with a unique message, such as "Have a nice day." If you specify this phrase as the server's logout signature, the scanner will search every response message for this phrase. Whenever it detects the phrase, the scanner will attempt to log in again by sending an HTTP request containing the user name and password.

The scanner can also detect that it has logged out if the server sends a specific message in response to the scanner's attempt to access a password-protected URL. For example, the server may respond with a status code of "302 Object moved." If the scanner knows specifically what to look for in this response, the program will recognize that it has been logged out and can re-establish a logged-in state.

Using the example above, if your server returns a message such as "Have a nice day" when a user logs out of your application, then enter "Have\sa\snice\sday" as the regular expression ("\s" is used in regular expressions to designate a space). A more likely example is where the server returns a 302 status code and references a new URL. In this case, "[STATUSCODE]302 AND [ALL]http://login.myco.com/config/mail?" might be a typical regex phrase. For tips on building a regular expression, see "Regular expression extensions" on page 334.

4. Enter a path and file name in the **Save Macro As** box, or click **Browse** to open a standard file-selection dialog box and name the file.
5. Click **OK**.

Client certificates

If Web Proxy receives a request for a certificate from a web server, it displays a dialog box asking you to locate the certificate. The program then caches your selection on a "per server" basis. Therefore, if you subsequently want to use a different certificate for a particular server, you must clear the cache by stopping and then restarting Web Proxy.

Regular expressions

Special characters and sequences are used in writing patterns for regular expressions. The following table describes some of these characters and includes short examples showing how the characters are used. Another recommended resource is the Regular Expression Library.

Also see "Regular expression extensions" on the next page for information about special tags and operators that may be used.

Character	Description
\	Marks the next character as special. /n/ matches the character " n ". The sequence /\n/ matches a linefeed or newline character.
^	Matches the beginning of input or line. Also used with character classes as a negation character. For example, to exclude everything in the content directory except /content/en and /content/ca, use: /content/[^(en|ca)].*/.* . Also see \S \D \W.
$	Matches the end of input or line.
*	Matches the preceding character zero or more times. /zo*/ matches either " z " or "zoo."
+	Matches the preceding character one or more times. /zo+/ matches "zoo" but not "z."
?	Matches the preceding character zero or one time. /a?ve?/ matches the "ve" in "never."
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. /[abc]/ matches the "a" in "plain."
\b	Matches a word boundary, such as a space. /ea*r\b/ matches the "er" in "never early."
\B	Matches a nonword boundary. /ea*r\B/ matches the "ear" in "never early."
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a nondigit character. Equivalent to [^0-9].
\f	Matches a form-feed character.
\n	Matches a linefeed character.
\r	Matches a carriage return character.
\s	Matches any white space including space, tab, form-feed, and so on. Equivalent to [\f\n\r\t\v]

Character	Description
\S	Matches any nonwhite space character. Equivalent to [^ \f\n\r\t\v]
\w	Matches any word character including underscore. Equivalent to [A-Za-z0-9_].
\W	Matches any nonword character. Equivalent to [^A-Za-z0-9_].

Regular expression extensions

OpenText engineers have developed and implemented extensions to the normal regular expression syntax, along with a set of operators.

Regular expression tags

When building a regular expression, you can use the extensions to specify in which element of the request or response to search for a match. The following table describes the extensions.

Extension	Element
[ALL]	All elements of the request or response
[BODY]	Request Body Response Body
[COOKIES]	Cookie in the Request
[HEADERS]	Request Headers Response Headers
[METHOD]	Request Method
[POSTDATA]	Post Data
[REQUESTLINE]	Request Line (the start line of an HTTP request)
[SETCOOKIES]	Set-Cookie Response Header
[STATUSCODE]	Status Code
[STATUSDESCRIPTION]	Status Description (a string that describes the status of the HTTP output returned to the client)

Extension	Element
[STATUSLINE]	Status Line (the start line of an HTTP response)
[URI]	The request target (a URI)
[VERSION]	HTTP Version

Regular expression operators

OpenText engineers have developed regular expression operators that you can use to construct complex regular expression patterns. The operators are:

- AND
- OR
- NOT
- [ ]
- ( )

Examples

The following paragraphs provide examples of how the use the extensions and operators:

- To detect a response in which (a) the status line contains a status code of "200" and (b) the phrase "logged out" appears anywhere in the message body, use the following regular expression:
  [STATUSCODE]200 AND [BODY]logged\sout
- To detect a response indicating that the requested resource resides temporarily under a different URI (redirection) and having a reference to the path "/Login.asp" anywhere in the response, use the following:

  [STATUSCODE]302 AND [ALL]Login.asp
- To detect a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response, use the following regular expression:

  ([STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired) OR ([STATUSCODE]302
  AND [ALL]Login.asp)

  Note: You must include a space before and after an "open" or "close" parenthesis. Otherwise, the parenthesis will be erroneously considered as part of the regular expression.
- To detect a redirection response where "login.aspx" appears anywhere in the redirection Location header, use the following regular expression:
  [STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx

- To detect a response containing a specific string (such as "Please Authenticate") in the Reason-Phrase portion of the status line, use the following regular expression:

  [STATUSDESCRIPTION]Please\sAuthenticate

Manual configuration of browser

If you do not start a web browser by clicking **Launch Browser**  on the Web Proxy toolbar, you can launch a browser outside the Web Proxy user interface. However, you must configure your browser's proxy settings. See your browser documentation for specific instructions.

Chapter 20: Web Service Test Designer

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

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

Use the Web Service Test Designer to create a Web Service Test Design file (<*filename*>.wsd) containing the values that should be submitted when conducting a web service scan.

Although the following procedure invokes the Web Service Test Designer from the OpenText DAST **Tools** menu, you can also open the designer through the OpenText DAST Scan Wizard by selecting **Start a Web Service Scan** from the OpenText DAST Start page and, when prompted, electing to launch the designer.

Note: When the Web Service Test Designer is launched from the OpenText DAST Scan Wizard, if the WSDL has not yet been configured, the designer will automatically import the WSDL, assign "auto values" to each parameter, and invoke all operations. This does not occur when you launch the tool from the OpenText DAST Tools menu or from the Security Toolkit.

1. Select **Tools > Web Service Test Designer**.
2. On the startup dialog box, select one of the following:
   - **New Web Service Test** - Design a new Web Service test.
   - **Open Web Service Test** - Edit a design that you previously created.

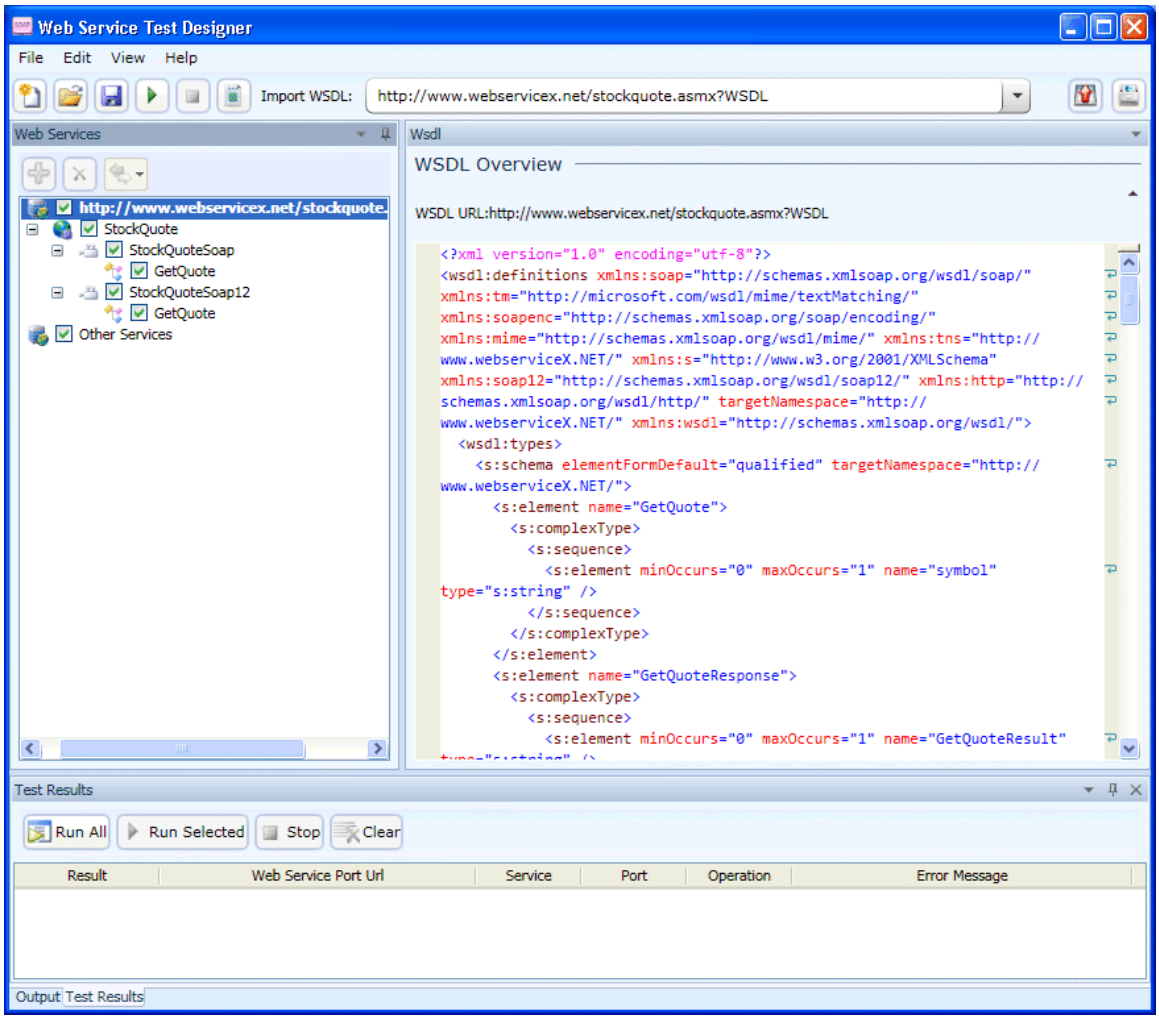
   The following procedure assumes that you are creating a design.
3. Do one of the following:
   - In the **Import WSDL** box, type or select the URL of the WSDL site (for example, http://www.webservicex.net/stockquote.asmx?WSDL) and click **Import WSDL**  .
   - Click **Browse for WSDL**  and select a WSDL file that you previously saved locally.

   Note: If authentication is required, or if SOAP requests need to be made through a proxy server, see "Settings" on page 348 for more information.

Also note that "Other Services" appears by default. This feature is used to add services manually when a service is not associated with a WSDL. See "Manually adding services" on page 343 for more information. Remove the check mark next to this item.

Image of imported WSDL

The following image shows an imported WSDL in the Web Service Test Designer.



4. Select a service transport in the left pane to display the port information in the right pane. A port defines an individual endpoint by specifying an address for a binding. Note that if the description of the WSDL includes both SOAP version 1.1 and version 1.2, and if the operations in both descriptions are the same, the versions are assumed to be identical and the services in version 1.1 only are configured. If you wish to attack both versions, then you must select the check box for each version 1.2 operation.

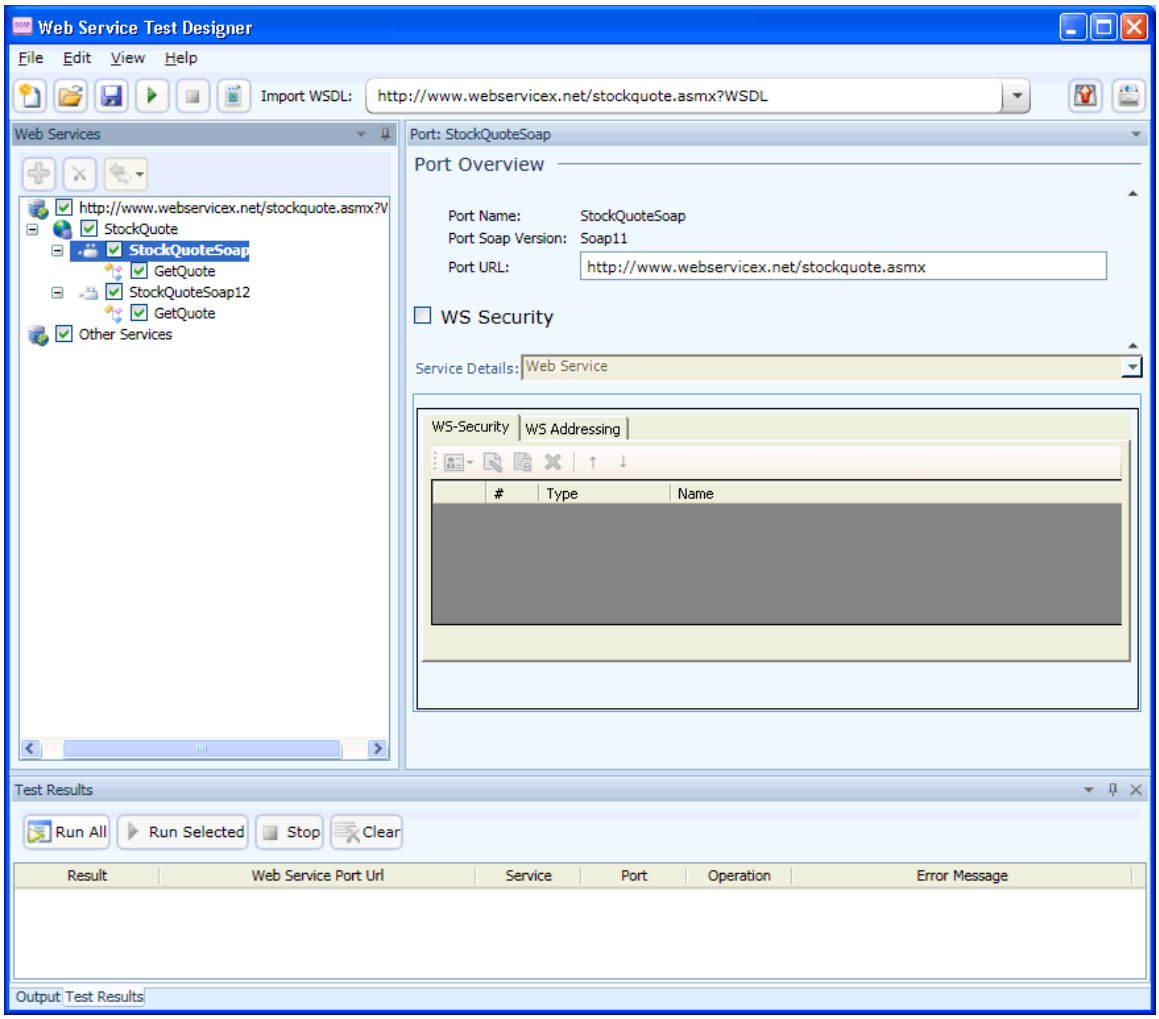
Note: The Port Overview panel for SOAP version 1.2 contains an additional option to include SOAP action in the HTTP header.

Even though the SOAP specification states that the SOAP Action is optional for SOAP version 1.2, some architectures require it and some cannot accept it. You can choose to include or exclude the SOAP action for a SOAP 1.2 binding, depending on your specific environment. The check box appears for SOAP 1.2 ports only and defaults to true.

Caution! RPC-encoded services require manual configuration. The **Schema Fields** tab is populated using a default SOAP schema. You can obtain the desired SOAP message from a developer or a proxy capture, and then paste the message into the **XML** tab (or import the saved message from a file). You can then click **Send** to test the operation.

Image of service transport/port information

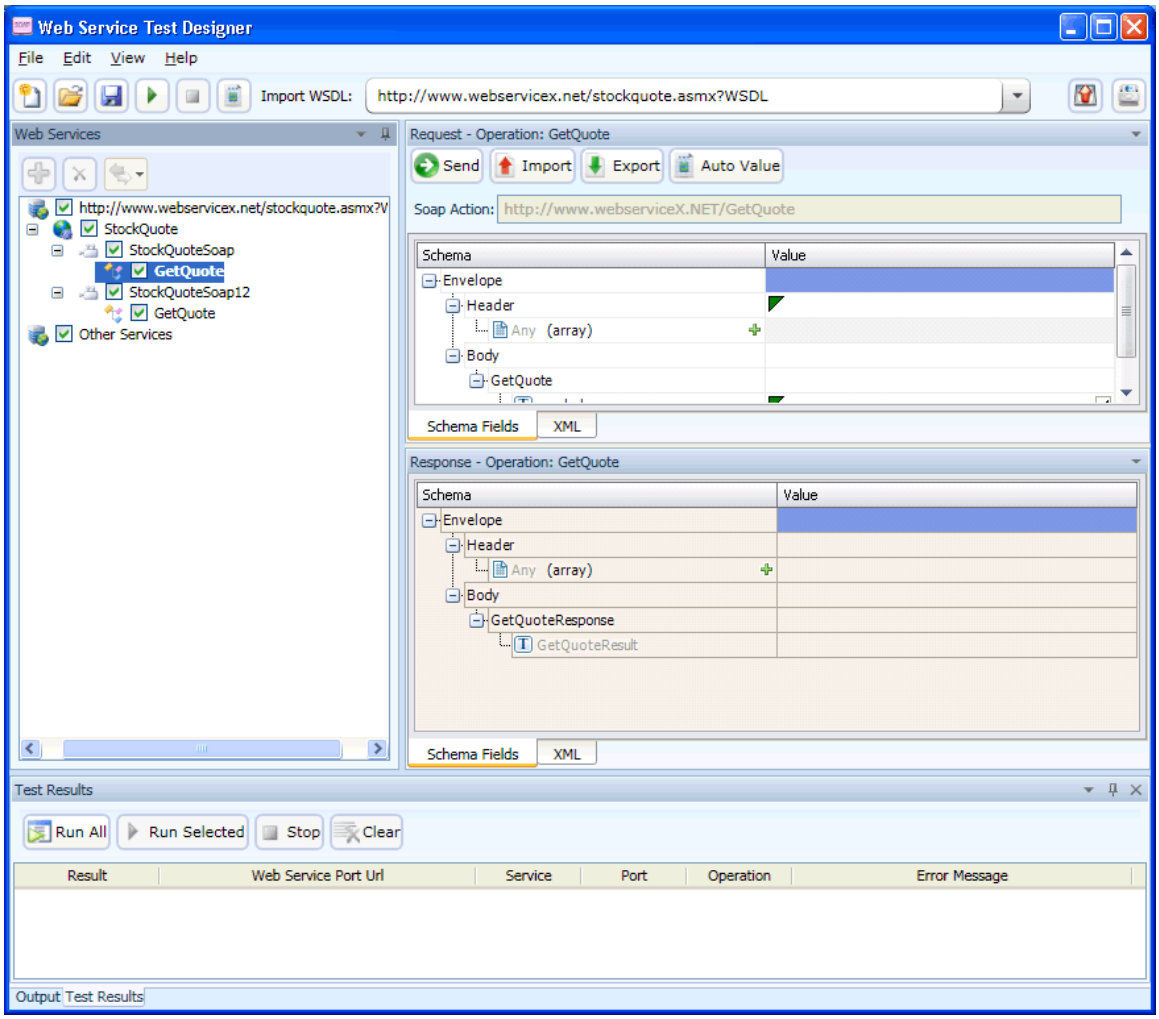
The following image shows the port information for the selected transport.



5. If security is required:
   a. Select **WS Security**.
   b. Select an option from the **Service Details** list.
   c. Provide the required information. For help with security settings, see "WS Security" on page 351.
6. Click an operation to display schema for the request (in the top half of the right pane) and the response (in the lower half).

Image of request/response schema

The following image shows the schema for the selected request.



7. Enter a value for the operation. In this example, the user entered OTEX (the stock symbol for Open Text Corporation).

   Note: If you click **Auto Value**, the designer assigns a value to the operation. This value is either:

   - Obtained from the GlobalValuesDefault.xpr file, if the file contains an entry that matches the name of the parameter; see "Global Values Editor" on page 344 for more information.
   - Created by the designer, based on the data type. In this example, the designer would populate the parameter "symbol" with the value "symbol1."

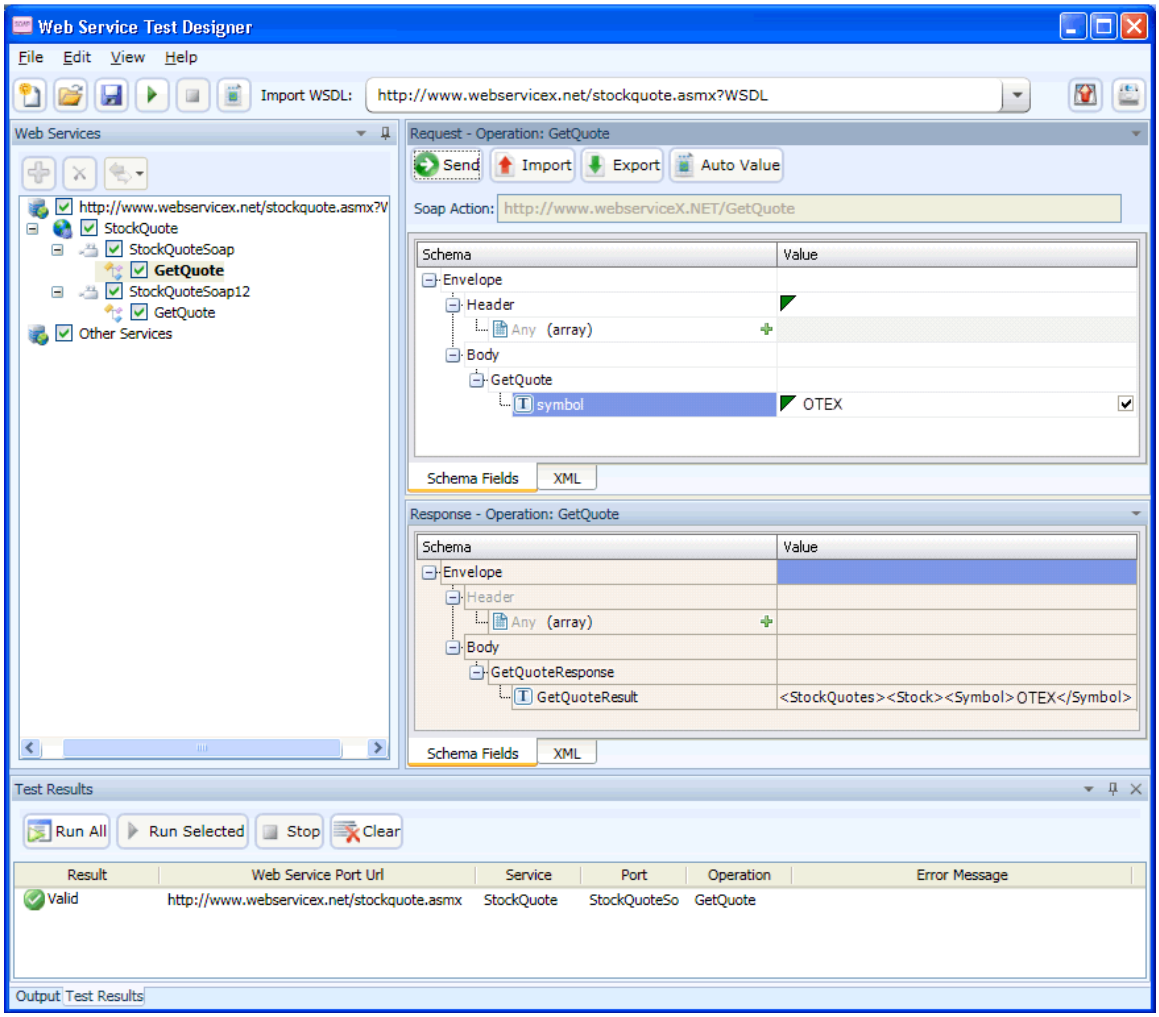
   See "Using Autovalues" on page 344 for more information.

8. Click **Send**.

Results appear in the lower response pane. You can alternate between the Schema and XML views by clicking the appropriate tabs.

Image of sending a request

The following image shows the test results of a request that was sent.



9. When you have assigned and tested values for each operation (although only one operation is depicted in this example):
   a. Click **File > Save**.
   b. Using the standard file-selection dialog box, select a name and location for the Web Service Design file (.wsd).

Note: If the WSDL contains multiple operations, data is saved for each operation regardless of whether or not the operation is checked. A check mark simply indicates that the operation will be used for auditing.

Manually adding services

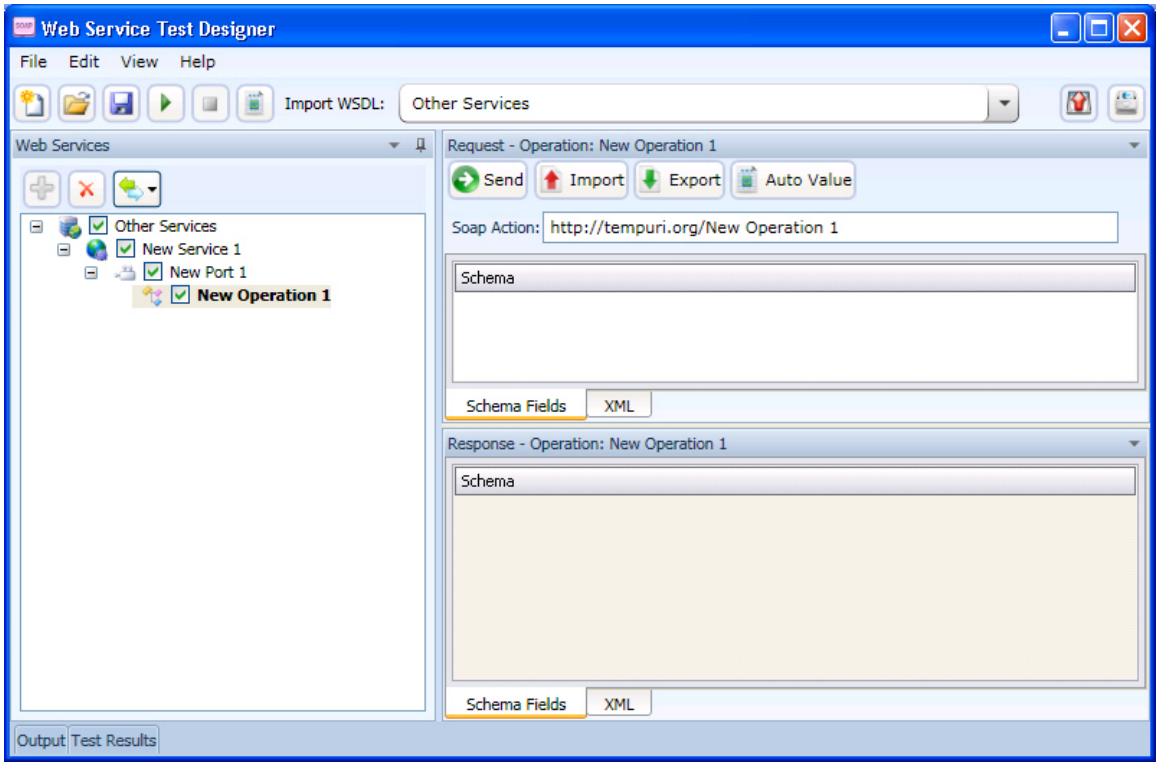
You may encounter a web service that does not have a WSDL associated with it.

For example, the OpenText DAST Recommendations module monitors scans to detect omissions, abnormalities, or anomalies that interfere with or diminish the thoroughness of a scan. If it detects SOAP requests during a web site scan, it suggests that you conduct a web service scan of that site and creates a Web Service Test Design file (*filename*.wsd) for that purpose. A WSDL file may or may not be available.

You may create a service manually, as shown in the following example.

1. Right-click the default "Other Services" service and select **Add Service**.

   New Service 1 appears in the Web Services tree in the left pane.
2. If authentication is required, select **WS Security** and provide the required credentials.
3. Right-click New Service 1, select **Add Port**. and then choose either **SOAP 1.1** or **SOAP 1.2**.
   New Port 1 appears in the Web Services tree.
4. In the **Port URL box**, enter the correct URL to the service.
5. Right-click New Port 1 and select **Add Operation**.



Note: To change service, port, or operation names, double-click the name.

6. You can import a file containing a SOAP envelope (possibly obtained using the Web Proxy tool) or you can copy and paste a SOAP envelope that you obtained from a developer onto the **XML** tab.

   If importing from a proxy capture, the SOAP action will be in the HTTP header (Soapaction=<*action_name*>).
7. If necessary, modify the values using either the **Schema Fields** tab or the **XML** tab.
8. To test the service, click either **Send** or **Run All**.

Global Values Editor

You can create a library of name/value parameters for operations that you frequently encounter.

After importing a WSDL file, if you click **Set Auto Values**  , the Web Service Test Designer searches the Global Values file for the names of parameters contained in the WSDL operations. If it finds a matching name, it inserts the associated value from the file into the parameter value field.

To add a global value:

1. Click **Edit > Global Values Editor**.

   The Global Values Editor opens and displays the contents of the default xml parameter registry (xpr) file named GlobalValuesDefault.xpr.
2. Click **Add**.

   This creates an entry with the default name of [Name] and a default value of [Value].
3. Click anywhere on the entry and substitute an actual name and value for the default.
4. Repeat steps 2-3 to create additional entries.
5. Do one of the following:
   - Click **OK** to save and close the file.
   - Click **Save As** to create and close the file using a different file name and/or location.

Using Autovalues

Use the Autovalues feature as an alternative to manually entering specific values for each parameter. The Web Service Test Designer analyzes each parameter and inserts a value that is likely to fulfill the service requirement. This can save considerable time when dealing with large web services.

After selecting a WSDL file:

1. Place a check mark next to each operation you want to autofill.
2. Click **Set Auto Values**  .

The following message appears: "Would you like the default values to be replaced with the defined global values?"

If you click **Yes**, any values you may have entered manually will be erased. Also, if any parameter name in any operation matches a parameter name in the Global Values file, the associated value in the file will be substituted for the value that would normally be generated for the operation.
If you click **No**, the function terminates.

3. Click **Yes**.
4. Click **Run All Tests**  .
   The Web Service Test Designer submits the service request, with values inserted for each operation.
5. Click the **Test Results** tab (at the bottom of the window).
6. If an operation returned an error, double-click the operation to open it in the Request pane and manually provide a value.

See also

"Global Values Editor" on the previous page

Importing and exporting operations

You can build a library of operations and their assigned values, allowing you to quickly modify other web service designs or exchange these components with other developers/testers. Each module is saved as an XML file, such as the following request used in the preceding example:

```
<Envelope xmlns="http://www.w3.org/2003/05/soap-envelope">
  <Header />
  <Body>
    <GetQuote xmlns="http://www.webserviceX.NET/">
      <symbol>MFGP</symbol>
    </GetQuote>
  </Body>
</Envelope>
```

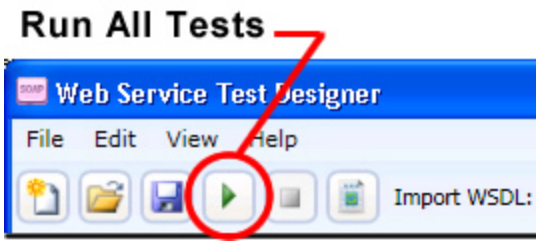
To save or import an operation:

1. Select an operation in the left pane.
2. Click **Import Request**  to load the operation.
3. Click **Export Request**  to save the operation.

Testing your design

You can, at any time, test the configuration of any or all operations.

After importing the WSDL, click **Run All Tests**.

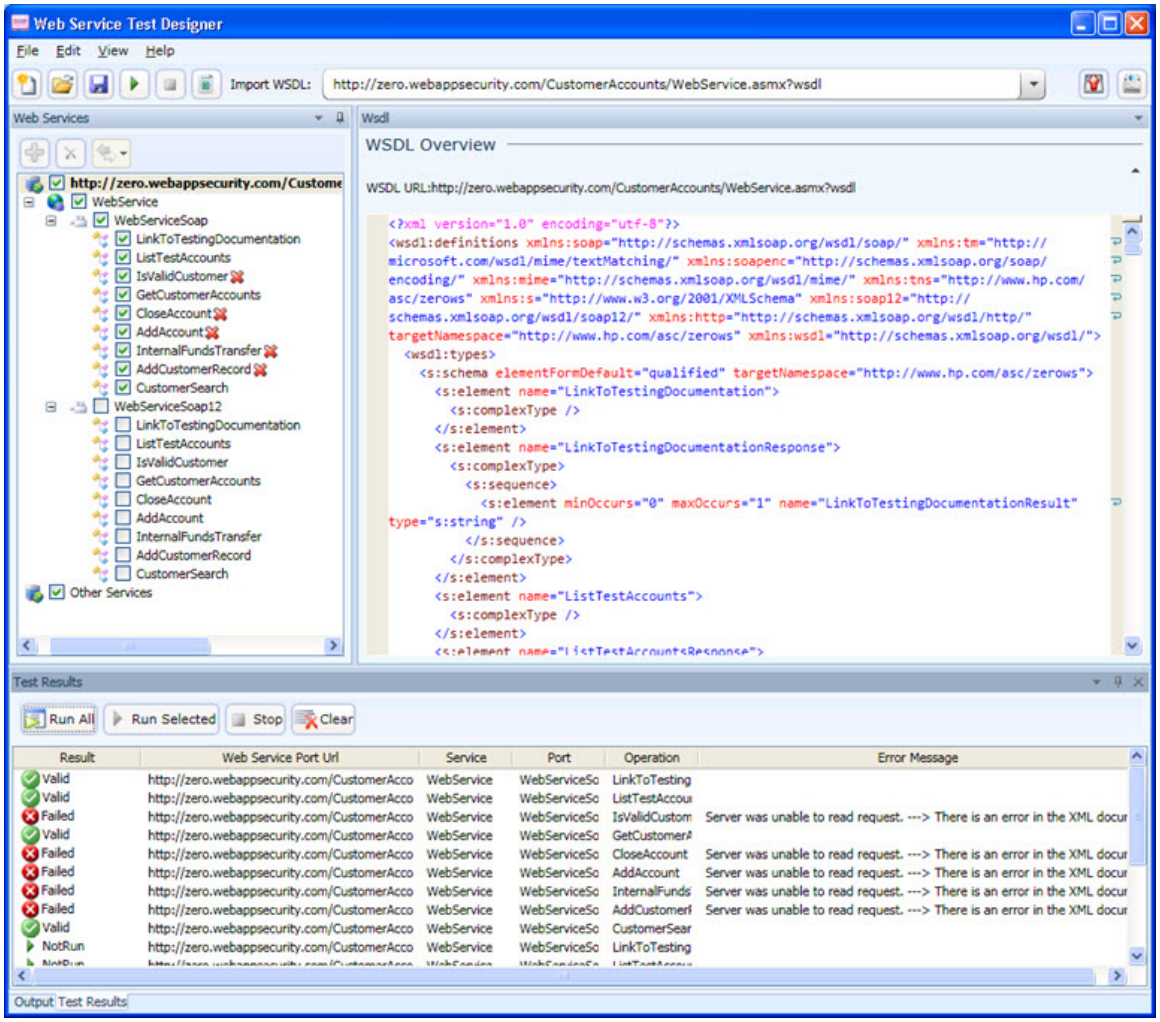


The designer attempts to submit all selected operations and displays the results.

To open the special Test Results pane, click **Test Results** on the Status bar.

Image of test results

The following image shows test results in the Web Service Test Designer.



The Test Results pane displays the following information:

- **Result** – The test outcome. Possible values are:
  - Valid: The operation succeeded without a server error or SOAP fault.
  - Not Run: The operation was not submitted because it was not selected (no check mark) or the Stop button was pressed before the operation was submitted.
  - Pending: The Run button has been pressed but the operation has not yet been submitted.
  - Failed: The request was unsuccessful, the server returned an error message, or a SOAP fault was received.
- **Web Service Port URL** – The URL associated with the item
- **Service** – The service associated with the item
- **Port** – The port associated with the item

- **Operation** – The operation the item represents
- **Error Message** – Explanation for failure

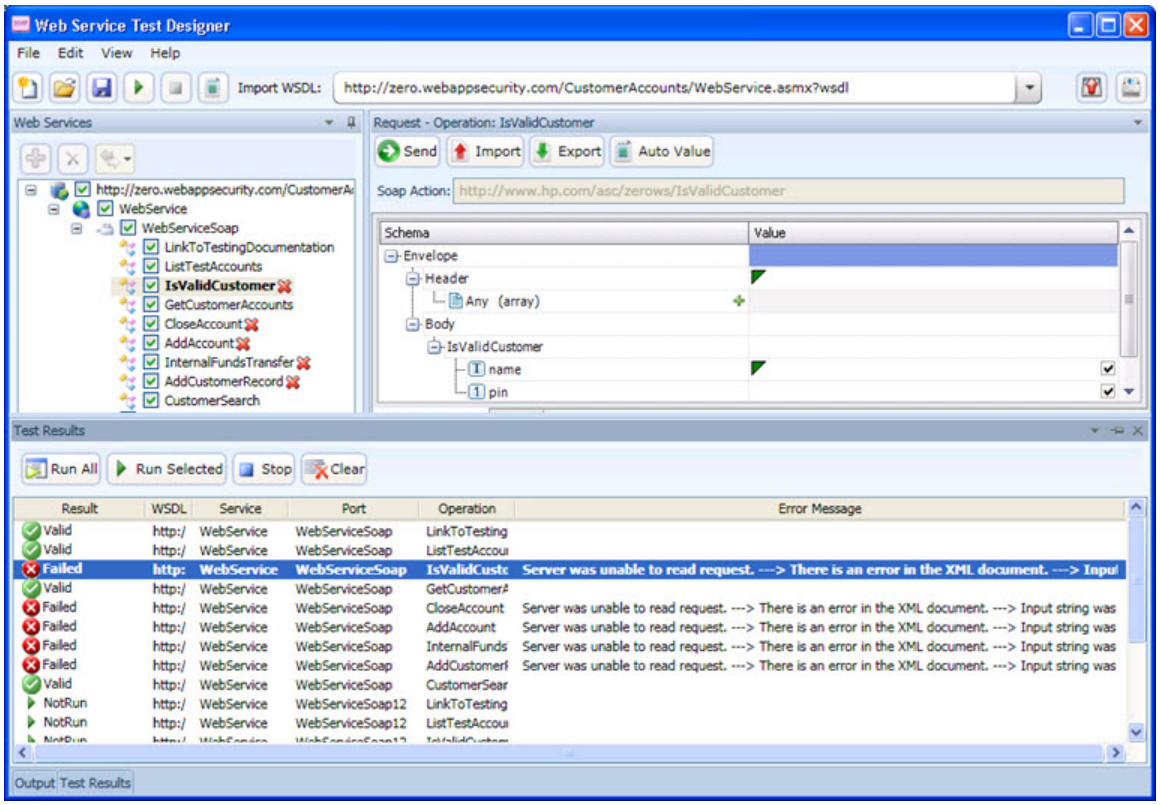
The Test Results toolbar contains the following buttons:

- **Run All** – The designer submits the service request for each checked operation.
- **Run Selected** – The designer submits the service request for operations selected in the Test Results pane.
- **Stop** – cancels the sending of service request.
- **Clear** – Removes all items from the Test Results pane.

If you double-click an item in the Test Results pane, the designer highlights the related operation in the Schema Fields pane, where you can enter values for each parameter.

Image of selected error with operation highlighted

The following image shows a selected error and its operation displayed in the Schema Fields pane.



Settings

The Web Services Designer has two categories of settings:

- "Network proxy" on the next page
- "Network authentication" on page 350

Network proxy

To configure a network proxy:

1. Select a profile from the **Proxy Profile** list:
   - **Direct**: Do not use a proxy server.
   - **Auto Detect**: Use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's web proxy settings.
   - **Use System Proxy**: Import your proxy server information from the local machine.
   - **Use PAC File**: Load proxy settings from a Proxy Automatic Configuration (PAC) file. Then specify the file location in the **URL** box.
   - **Use Explicit Proxy Settings**: Access the Internet through a proxy server using information you provide in the Explicitly Configure Proxy section.
   - **Use Mozilla Firefox**: Import proxy server information from Firefox.

     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," then a proxy will not be used.
2. If you selected **Use PAC File**, enter the location of the PAC file in the **URL** box.
3. If you selected **Use Explicit Proxy Settings**, provide the following information:
   a. In the **Server** box, type the URL or IP address of your proxy server, followed (in the **Port** box) by the port number (for example, 8080).
   b. From the **Type** list, select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
   c. If authentication is required, select a type from the **Authentication** list:
      - **Automatic**

        Note: Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
      - **Basic**
      - **Digest**
      - **Kerberos**
      - **Negotiate**
      - **NTLM (NT LAN Manager)**
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** box. Use commas to separate entries.
6. Click **Save**.

Network authentication

If server authentication is not required, select **None** from the **Method** list.

Otherwise, select an authentication method and enter your network credentials. The authentication methods are:

- **ADFS CBT**
- **Automatic**
- **Basic**
- **Digest**
- **Kerberos**
- **Negotiate**
- **NTLM (NT LAN Manager)**

Using a client certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can select a certificate from the local machine or a certificate assigned to a current user. You can also select a certificate from a mobile device, such as a common access card (CAC) reader that is connected to your computer. To use client certificates:

1. Select the **Enable client certificate on proxy** check box.
2. Click **Client Certificate**.

   The Soap Client Certificate window opens.
3. Do one of the following:
   - To use a certificate that is local to the computer and is global to all users on the computer, select **Local Machine**.
   - To use a certificate that is local to a user account on the computer, select **Current User**.

     Note: Certificates used by a common access card (CAC) reader are user certificates and are stored under Current User.
4. Do one of the following:
   - To select a certificate from the "Personal" ("My") certificate store, select **My** from the drop-down list.
   - To select a trusted root certificate, select **Root** from the drop-down list.
5. Does the website use a CAC reader?

- If *yes*, do the following:
  i. Select a certificate that is prefixed with "(SmartCard)" from the **Certificate** list.

  Information about the selected certificate and a PIN field appear in the Certificate Information area.

  ii. If a PIN is required, type the PIN for the CAC in the **PIN** field.

  > **Note:** If a PIN is required and you do not enter the PIN at this point, you must enter the PIN in the Windows Security window each time it prompts you for it during the scan.

  iii. Click **Test**.

  If you entered the correct PIN, a Success message appears.
- If *no*, select a certificate from the **Certificate** list.

  Information about the selected certificate appears in the Certificate Information area.

6. Click **OK**.

WS Security

You can configure security settings for all operations in a Web service port, using a variety of services:

- Web Service (see "Web Service settings" below)
- Windows Communication Foundation (WCF) Service (see "WCF Service (CustomBinding) settings" on page 353)
- WCF Service (Federation) (see "WCF Service (Federation) settings" on page 354)
- WWCF Service (WSHttpBinding) (see "WCF Service (WSHttpBinding) Settings" on page 355)

Select an appropriate service from the **Service Details** list and then provide the requested information.

Web Service settings

When Security credentials, known as tokens, are placed in the SOAP request, the web server can verify that the credentials are authentic before allowing the web service to execute the application. To further secure web services, it is common to use digital signatures or encryption for the SOAP messages. Digitally signing a SOAP message verifies that the message has not been altered during transmission. Encrypting a SOAP message helps secure a web service by making it difficult for anyone other than the intended recipient to read the contents of the message.

WS-Security tab

1. To add a security token, click  , select a token type, and provide the requested information.
   - **UserName**. This token specifies a user name and password. You can elect to include a nonce, specify how to send the password to the server for authentication (Text, None, or Hash) and indicate whether to include a timestamp.
   - **X509 Certificate**. This token is based on an X.509 certificate. You can purchase a certificate from a certificate authority, such as VeriSign, Inc., or set up your own certificate service to issue a certificate. Most Windows servers support the public key infrastructure (PKI), which enables you to create certificates. You can then have it signed by a certificate authority or use an unsigned certificate. Select a certificate and specify the reference type (BinaryCertificateToken or Reference).
   - **Kerberos /Kerberos2**. (For Windows 2003 or XP SP1 and later). The Kerberos protocol is used to mutually authenticate users and services on an open and unsecured network. Using shared secret keys, it encrypts and signs user credentials. A third party, known as a Kerberos Key Distribution Center (KDC), authenticates the credentials. After authentication, the user may request a service ticket to access one or more services on the network. The ticket includes the encrypted, authenticated identity of the user. The tickets are obtained using the current user's credentials. The primary difference between the Kerberos and Kerberos2 tokens is that Kerberos2 uses the Security Support Provider Interface (SSPI), so it does not require elevated privileges to impersonate the client's identity. In addition, the Kerberos2 security token can be used to secure SOAP messages sent to a web service running in a web farm. Specify the host and domain.
   - **SAML Token**. Security Assertion Markup Language (SAML) is an XML standard for exchanging security-related information, called assertions, between business partners over the Internet. The assertions can include attribute statements, authentication, decision statements, and authorization decision statements. Click Load from file to browse to a SAML certificate. Click Certificate to import a certificate. Finally, select a certificate reference type: X509 Data or RSA.

2. To add a message signature, click  and provide the requested information.
   - **Signing token.** The token to use for signing, usually an X.509 type. Select from the list of all added tokens.
   - **Canonicalization algorithm.** A URL for the algorithm to use for canonicalization. A drop-down list provides common algorithms. If you are unsure which value to use, keep the default.
   - **Transform algorithm.** A URL for the Transform algorithm to apply to the message signature. A drop-down list provides common algorithms. If you are unsure which value to use, keep the default.
   - **Inclusive namespaces list.** A list of comma-separated prefixes to be treated as inclusive (optional).
   - **What to sign.** The SOAP elements to sign: SOAP Body, Timestamp, and WS-Addressing.

- **XPath (optional).** An XPath that specifies which parts in the message to sign. If left blank, the elements selected in the **Signature options** field are signed. For example, //*[local-name (.)='Body'].
- **Token (optional).** The target token you want to sign. Select from the drop-down list of all added tokens. With most services, this field should be left empty.

3. To add message encryption, click  and provide the requested information.
   - **Encrypting token.** The token to use for encryption (usually an X.509 type). You can select from a list of all previously created tokens.
   - **Encrypting type.** Indicates whether to encrypt the whole destination Element or only its Content.
   - **Key algorithm.** The algorithm to use for the encryption of the session key: RSA15 or RSAOAEP.
   - **Session algorithm.** The algorithm to use for the encryption of the SOAP message. You can select from a list of common values.
   - **XPath (optional).** An XPath that indicates the parts of the message to encrypt. If left blank, only the SOAP body is encrypted.
   - **Token (optional).** The name of the encrypted token. A drop-down box provides a list of all added tokens. With most services, this field should be left empty.
4. Use the Up and Down arrows  to position the security elements in order of their priority.

WS Addressing tab

Use the **WS-Addressing** tab to indicate whether WS-Addressing is used by the service, and if so, its version number.

WCF Service (CustomBinding) settings

WCF Service (CustomBinding) enables the highest degree of customization. Since it is based on WCF customBinding standard, it allows you to test most WCF services, along with services on other platforms such as Java-based services that use the WS - <*spec_name*> specifications.

Transport. Select HTTP, HTTPS, or AutoSecuredHTTP. Named Pipes and TCP transport are not supported.

Encoding. Select Text, MTOM, or WCF Binary.

Security. Select an authentication mode and bootstrap policy from the appropriate list**.**

Net Security. The type of stream security: None, Windows stream security, or SSL stream security**.**

Reliable Messaging. Select **Enabled** to use reliable messaging and then select a format: either **Ordered** or **Not Ordered**.

Identities. Provide identity information for the bindings and certificate:

- **Username** and **Password**
- **Server Certificate/Client certificate**. A certificate that provides identity information for the server or client. Use the **Browse** button to open the Select Certificate dialog box.
- **Expected DNS**, **SPN**, and **UPN.** The expected identity of the server in terms of its DNS, SPN, or UPN. This can be localhost, an IP address, or a server name.

Client Windows Identity. Provide identity information for the client windows:

- **Current User**. The identity of the user logged onto the machine.
- **Custom User**. Specify the Username, Password, and Domain.

Click **Advanced** to open the Advanced Settings dialog box. See "Advanced security settings" on page 356 for additional information.

WCF Service (Federation) settings

When using WCF Service (Federation), the client authenticates against the Security Token Service (STS) to obtain a token. The client uses the token to authenticate against the application server.

Server

- **Transport.** The transport type: HTTP or HTTPS.
- **Encoding.** The server's encoding policy: Text or MTOM.

Security

- **Authentication mode.** A drop-down list of possible modes of authentication, such as AnonymousForCertificate, MutualCertificate, and so forth.
- **Bootstrap Policy.** A drop-down list of possible bootstrap policies for Secure Conversation authentication, such as SspiNegotiated, UserNameOverTransport, and so forth.

Identities

The identity information for the bindings and certificate:

- **Server certificate.** A certificate that provides identity information for the server. Use the **Browse** button to open the Select Certificate dialog box.
- **Expected DNS.** The expected identity of the server in terms of its DNS. This can be localhost, an IP address, or a server name.

STS (Security Token Service) details

- **Endpoint address.** The endpoint address of the STS. This can be localhost, an IP address, or a server name.
- **Binding.** The scenario which references the binding that contacts the STS.

Click **Advanced** to open the Advanced Settings dialog box. See "Advanced security settings" on the next page for additional information.

WCF Service (WSHttpBinding) Settings

Using WCF Service (WSHttpBinding), you can choose from several types of authentication: None, Windows, Certificate, or Username (message protection). Select an option from the Client authentication type list. Your selection determines which additional information is required, as described below.

Type	Parameters
None	• **Negotiate server credentials**. Negotiates the Web Service's certificate with the server. You can also provide the server's DNS information. • **Specify service certificate**. The location of the service's certificate. If you select this option, the **Negotiate service credentials** option is not relevant. • **Expected server DNS.** The expected identity of the server in terms of its domain name system. This can be localhost, an IP address, or a server name. It can also be the common name by which the certificate was issued. • **Enable secure session**. Allows a secure session using Certificate type authentication.

Windows	• **Expected server identity**. The service principal name (SPN) or user principal name (UPN). SPN ensures that the SPN and the specific Windows account associated with the SPN identify the service. UPN ensures that the service is running under a specific Windows user account; the user account can be either the current logged-on user or the service running under a particular user account.
	• **Client Windows identity**. The identity information for the client windows:
	  • **Current User.** Use the credentials of the user logged onto the machine.
	  • **Custom User.** Provide the user credentials (Username, Password, and Domain) and optionally select an impersonation level (which determines the operations a server can perform in the client's context). Impression levels are as follows:
	  ◦ None - No level selected.
	  ◦ Anonymous - The server cannot impersonate or identify the client.
	  ◦ Identification - The server can get the identity and privileges of the client, but cannot impersonate the client.
	  ◦ Impersonation - The server can impersonate the client's security

Type	Parameters
	context on the local system. ◦ Delegation - The server can impersonate the client's security context on remote systems. • **Enable secure session**. Allows a secure session using Windows type authentication.
Certificate	• **Client certificate**. The location of the client certificate. The **Browse** button opens the Select Certificate dialog box. • **Negotiate server credentials**. Negotiates the Web Service's certificate with the server. You can also provide the server's DNS information. • **Specify service certificate**. The location of the service's certificate. If you select this option, the **Negotiate server credentials** option is disabled. • **Expected server DNS.** The expected identity of the server in terms of its DNS. This can be localhost, an IP address, or a server name. It can also be the common name by which the certificate was issued. • **Enable secure session**. Allows a secure session using Certificate type authentication.
User Name (Message Protection)	• **Username, Password**. The authentication credentials of the client. • **Negotiate server credentials**. Negotiates the Web Service's certificate with the server. You can also provide the server's DNS information. • **Specify service certificate**. The location of the service's certificate. If you select this option, the **Negotiate server credentials** option is disabled. • **Expected server DNS**. The expected identity of the server in terms of its DNS. This can be localhost, an IP address, or a server name. It can also be the common name by which the certificate was issued. • **Enable secure session**. Allows a secure session using Username type authentication.

Advanced security settings

This dialog box enables you to customize the security settings for your test on the following tabs.

Encoding tab

The Encoding tab includes the following options:

- **Encoding**. The encoding type to use for the messages: Text, MTOM, or WCF Binary.
- **WS-Addressing version**. The version of WS-Addressing for the selected encoding: None, WSA 1.0, or WSA 04/08.

Advanced Standards tab

The Advanced Standards tab includes the following options:

- **Reliable messaging**. Enables reliable messaging for services that implement the WS-ReliableMessaging specification. The encoding type to use for the messages: Text, MTOM, or WCF Binary.
- **Reliable messaging ordered**. Indicates whether the reliable session should be ordered.
- **Reliable messaging version**. The version to apply to the messages: WSReliableMessagingFebruary2005 or WSReliableMessaging11.
- **Specify via address**. Sends a message to an intermediate service that submits it to the actual server. This may also apply when you send the message to a debugging proxy. This corresponds to the WCF clientVia behavior. This is useful to separate the physical address to which the message is actually sent, from the logical address for which the message is intended.
- **Via address**. The logical address to which to send the message. It may be the physical of the final server or any name. It appears in the SOAP message as follows:

  `<wsa:Action>http://myLogicalAddress<wsa:Action>`
  The logical address is retrieved from the user interface. By default, it is the address specified in the WSDL. You can override this address using this field.

Security tab

The Security tab includes the following options:

- **Enable secure session**. Establish a security context using the WS-SecureConversation standard.
- **Negotiate service credentials**. Allow WCF proprietary negotiations to negotiate the service's security.
- **Default algorithm suite**. The algorithm to use for symmetric/asymmetric encryption. The list of algorithms is populated from the SecurityAlgorithmSuite configuration in WCF.
- **Protection level**. Indicates whether the SOAP Body should be encrypted/signed. The possible values are: None, Sign, and Encrypt And Sign (default)
- **Message protection order**. The order for signing and encrypting. Choose from: Sign Before Encrypt, Sign Before Encrypt And Encrypt Signature, Encrypt Before Sign.
- **Message security version**. The WS-Security security version. You can also indicate whether to require derived keys for the message.

- **Security header layout**. The layout for the message header: Strict, Lax, Lax Timestamp First, or Lax Timestamp Last.
- **Key entropy mode**. The entropy mode for the security key. The possible values are: Client Entropy, Security Entropy, and Combined Entropy.
- **Require security context cancellation**. Indicates whether to require the cancellation of the security context. If you disable this option, stateful security tokens will be used in the WS-SecureConversation session, if they are enabled.
- **Include timestamp**. Includes a timestamp in the header.
- **Allow serialized signing token on reply**. Enables the reply to send a serialized signing token.
- **Require signature confirmation**. Instructs the server to send a signature confirmation in the response.

Note: The next four options apply only when using an X.509 certificate.

- **X509 Inclusion Mode**. Specifies when to include the X.509 certificate: Always to Recipient. Never, Once, Always To Initiator.
- **X509 Reference Style**. Specify how to reference the certificate: Internal or External.
- **X509 require derived keys**. Indicates whether X.509 certificates should require derived keys.
- **X509 key identifier clause type**. The type of clause used to identify the X.509 key: Any, Thumbprint, Issuer Serial, Subject Key Identifier, Raw Data Key Identifier.

HTTP & Proxy tab

The HTTP and Proxy tab includes the following options:

- **Transfer mode**. The transfer method for requests/responses. The possible values are Buffered, Streamed, Streamed Request, and Streamed Response.
- **Max response size (KB)**. The maximum size of the response before being concatenated.
- **Allow cookies**. Indicates whether to enable or disable cookies.
- **Keep-Alive enabled**. Indicates whether to enable or disable keep-alive connections.
- **Authentication scheme**. The HTTP authentication method: None, Digest, Negotiate, NTLM, Integrated Windows Authentication, Basic, or Anonymous.
- **Realm**. The realm of the authentication scheme in the form of a URL.
- **Require client certificate**. Indicates whether to require a certificate for SSL transport.
- **Use default web proxy**. Indicates whether to use machine's default proxy settings.
- **Bypass proxy on local**. Indicates whether to ignore the proxy when the service is on the local machine.
- **Proxy address**. The URL of the proxy server.
- **Proxy authentication scheme**. HTTP authentication method on Proxy: Digest, Negotiate, NTLM, Basic, or Anonymous.

Send Documentation Feedback

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

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

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

Feedback on Tools Guide (Dynamic Application Security Testing 25.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!