

HP Assessment Management Platform

for the Windows[®] operating system

Software Version: 9.00

User Guide

Document Release Date: March 2011

Software Release Date: March 2011



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Copyright 2011 Hewlett-Packard Development Company, L.P.

Trademark Acknowledgements

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

Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Other Acknowledgements

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

Documentation Updates

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

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

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

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

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

Support

For information or assistance regarding AMP, contact customer support.

You can open a support case for Application Security Center products either online or by telephone.

Online (preferred)

- 1 Browse to URL <http://support.openview.hp.com/>.
- 2 Log in. If you have not registered before, you will need to do so and provide your Service Agreement ID (SAID) number. If you do not have an SAID number, there is an option on the page to declare yourself a “trusted customer” and enter a case.
- 3 Select your HP product and report the issue.

Telephone (voice recognition system)

- 1 Call 1-800-633-3600.
- 2 Say “Software.”
- 3 Say “Assessment Management Platform.”
- 4 Say or type your SAID.

You can access the HP Application Security Center customer forum and blogs at

<http://www.communities.hp.com/securitysoftware/>

You can also visit the HP software support Web site at:

<http://support.openview.hp.com/>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides an efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Contents

1	Welcome	1
	Introduction	1
	Features and Benefits	2
	New Features and Enhancements for AMP 9.0	3
	Assessments	3
	Findings	3
	Manual Findings	3
	Correlation of Dynamic Vulnerabilities	3
	Hybrid 2.0 - Correlation of Runtime Vulnerabilities (HP Fortify - Security Scope)	4
	Hybrid 2.0 - Correlation of Static Vulnerabilities (HP Fortify - Source Code Analysis)	4
	Scan Uploader	4
	Aliasing	4
	Correlation Management	5
	Risk Score	5
	Assessment Dashboards	5
	Screenshots	5
	Assessment State	5
	New Assessments from Existing Assessments	6
	False Positive Management (across Assessments)	6
	Reports	6
	Sending Findings to Quality Center	6
	New Tools	6
	New Features and Enhancements for AMP 8.10	7
	Roles and Permissions	7
	Optimal Scan Settings for Oracle Sites	7
	Sending Defects to HP Quality Center	8
	Administrative Approval of Binary Updates	8
	Archiving Scan Data	8
	Scan Linkage Analyzer	8
	Integration with Fortify	9
	New Features and Enhancements for AMP 8.0	9
	Web Console Login/Logout	9
	Tagging	9
	Tagging on Objects	9
	Discovery Site Tags	9
	Grouping	9
	Reporting	9
	Scan Visualization	10
	Vulnerability Details	10

Enhancements	10
2 Installation	7
Introduction	7
System Requirements	8
Upgrading from Previous Versions	10
Server/Manager Installation	11
Quality Center Service Installation	18
AMP Services Configuration Utility	19
Reporting Service	20
Service Status	20
Database Configuration	20
Logging Configuration	20
Reporting Queue Poll Interval	21
Quality Center Service	21
Service Status	21
Service Configuration	21
Logging Configuration	22
Scan Uploader Service	23
Service Status	23
AMP Configuration	23
Dropbox Configuration	23
Task Service	24
Service Status	24
Database Configuration	24
Logging Configuration	25
Scheduler Service	25
Service Status	25
Console Installation	26
If You Are Not Connected to the Internet	26
Sensor Installation	28
Time Stamping and Scheduling	29
Installations Lacking Internet Connection	29
3 Preparing Your System for Audit	31
Introduction	31
Helpful Hints	31
Using Web Forms	31
4 Getting Started	33
Introduction	33
Log On to AMP Console	33
Configure the Console	34
Assign Administrators and Create Roles	34
5 AMP Console	37
User Interface	37

Scans/Compliance Group	40
Scan Queue	40
Scan Policies	40
Compliance Templates	41
Sensors	47
Administration	48
Activity Log	49
Connected Users	49
Licensing	50
Smart Update	51
Smart Update Approval	51
Export Paths	52
E-Mail Alerts	52
SMTP Settings	53
Commands	53
SNMP Alerts	53
SNMP Settings	54
Commands	54
Sensor Users	54
Roles and Permissions	55
Roles	55
System Roles and Permissions	57
Creating an Organization	57
Administrators Tab	57
Roles Tab	57
Organization Roles and Permissions	59
Administrators Tab	59
Configuration Tab	59
Roles Tab	60
Resources Tab	61
Move/Copy Objects Tab	62
Project Roles and Permissions	63
Creating a Project	63
Administrators Tab	63
Configuration Tab	64
Roles Tab	64
Resources Tab	66
Move/Copy Objects Tab	66
Proxy Server Settings	67
QC Services	67
Certificates	69
Common AMP Console Tasks	69
Configure the Console	69
Suspend a Scan	69
Resume a Suspended Scan	70
Stop a Scan	70
Pause a Sensor	70

Continue a Sensor	71
Perform a Smart Update	71
Schedule a Smart Update.	71
View Activity Log	72
Create E-Mail Alerts.	72
Create SNMP Alerts	72
Create Export Paths	73
6 AMP Web Console	75
Toolbar	76
Options	76
General.	76
Quality Center	77
Site Filters.	78
Navigation Pane.	78
Actions	79
New Site	79
New Assessment	79
New Scan	79
New Report	79
Filtered Views	79
Dashboard	80
Sites	81
Assessments	84
Scans	87
Scan Schedules	93
Reports	93
QC Defects	95
Views	95
Discoveries	95
Resources.	96
Report Resources	96
Report Templates.	97
Scan Templates	98
Discovery Templates	99
Discovery Schedules	99
Blackouts	100
Dependencies	101
Editing the Layout	103
Columns.	103
Grouping	104
Sorting.	106
Paging	106
Simple Scan Settings	106
Advanced Scan Settings	107
Scan	108
General.	108

Tags	110
Scan Settings.....	110
Method	110
General.....	112
Content Analyzers.....	114
Requestor	115
Session Storage	116
Session Exclusions.....	117
Allowed Hosts	118
HTTP Parsing	119
Filters.....	120
Cookies/Headers	121
Proxy.....	122
Authentication	122
File Not Found.....	123
Policy	124
Crawl Settings.....	124
Link Parsing.....	124
Session Exclusions.....	125
Audit Settings.....	126
Session Exclusions.....	126
Attack Exclusions	127
Attack Expressions	128
Vulnerability Filters	128
Smart Scan.....	128
Scan Behavior	129
Blackout Action	129
Reports	129
General.....	129
Options.....	130
E-mail.....	130
Export	130
General.....	130
Enterprise Report Settings.....	130
General	131
Options	131
Tags	131
Report Template Settings	132
Template	132
Master Report	132
Report Definitions.....	132
Tags	133
Scan Template Settings.....	133
Scan	133
General.....	133
Tags	134
Sensors	134

Scan URLs	134
List-Driven Scan	134
Workflow-Driven Scan	135
Web Service Scan	135
Reports	135
Templates	135
Compliance Templates	135
Resources	136
Export Paths	136
Export	136
Export Paths	136
Site Settings	137
General	137
Information	138
Tags	138
Scheduled Scan Settings	138
Schedule	138
General	138
Recurrence	139
Tags	139
Discovery Scan Settings	139
Schedule	139
General	139
Recurrence	140
Tags	141
Discovery	141
General	141
Settings	141
Discovered Site Tags	142
Discovery Template Settings	142
Discovery	142
General	142
Tags	143
Sensors	143
IP Ranges	143
Port Ranges	144
Scan Discovered	144
General	144
Sensors	145
Discovery Schedule Settings	145
Schedule	145
General	145
Recurrence	146
Tags	146
Discovery	147
General	147
Settings	147

Discovered Site Tags	148
Blackout Settings	148
General	148
Recurrence	149
Tags	150
7 Reporting	151
Introduction	151
Generating a Scan Report	151
Manual Report	151
Scheduled Report	152
Generating an Assessment Report	153
Generating an Enterprise Report	154
Creating a Report Template	155
Viewing a Report	156
A AMP Tools	159
Introduction	159
Options	160
Policy Manager	160
Views	160
Standard View	160
Search View	161
Creating or Editing a Policy	162
Creating a Custom Check	162
Disabling a Custom Check	169
Deleting a Custom Check	169
Editing a Custom Check	169
Searching for Attack Agents	170
Policy Manager Icons	171
Audit Inputs Editor	172
Engine Inputs	172
Check Inputs	173
4719: IIS Mapping	173
4721: Admin Section Must Require Authentication	173
4722: Logins Sent Over Unencrypted Connection	174
4723: Logins Sent Over Query	174
4724: Password Field Masked	174
4726: Secure Section Only Accessible Via SSL	174
4728: Persistent Cookies	174
4729: User supplied data without POST	174
4731: Script Directory Check	175
4732: Script File Extension Disclosure	175
5151: Arbitrary Remote File Include	175
5546: Privacy Policy Not Present	177
10183: Allowed Top-Level Domain	177
10274: Proxy CONNECT Access	177

10275: Proxy GET Access	177
10280: Price-Related Form Fields	178
10287: Local File Include	178
Web Form Editor	180
Manually Creating a Web Form List	180
Recording Web Form Values	182
Importing a Web Form File	184
Scanning with a Web Form File	184
Web Form Editor Settings	185
General	185
Proxy	185
Web Form Logic	186
Web Brute	187
Mounting a Brute Force Attack	188
Creating and Importing Lists	190
Exporting Dictionaries	190
Web Brute Settings	191
Options	191
Authentication	192
Proxy	192
Web Discovery	194
Discovering Sites	194
Web Discovery Settings	195
Select Protocols	195
Logging	195
Connectivity	195
Encoders/Decoders	197
Encoding a String	197
Decoding a String	197
Manipulating Encoded Strings	198
Encoding Types	198
Prefixed	199
Regular Expression Editor	200
Testing a Regular Expression	200
Regular Expressions	201
Regular Expression Extensions	202
Regular Expression Tags	202
Regular Expression Operators	203
Examples	203
HTTP Editor	204
Request Viewer	204
Response Viewer	204
HTTP Editor Menus	205
File Menu	205
Edit Menu	205
View Menu	205
Help Menu	205

Request Actions	206
PUT File Upload	206
Change Content-Length	206
URL Encode/Decode Param Values	206
Unicode Encode/Decode Request	207
Create MultiPart Post	207
Remove MultiPart Post	207
Response Actions	207
Chunked	207
Content Codings	208
Editing and Sending Requests	208
Searching for Text	208
HTTP Editor Settings	208
Options	209
Authentication	211
Proxy	211
Web Proxy	213
Using Web Proxy	213
Creating a Web Macro	215
Web Proxy Tabs	216
Web Proxy Settings	217
Web Proxy Interactive Mode	222
Smart Update	224
Cookie Cruncher	225
Background	225
Using the Cookie Cruncher	225
Subcookies	226
Cookie Cruncher Tabs	227
Cookies Tab	227
Character Sets Tab	227
Char Freq Tab	228
Randomness Tab	228
Predictability Tab	228
Disk Plot Tab	229
Cookie Cruncher Settings	230
General	230
Authentication	231
Proxy	231
Web Fuzzer	233
Using the Web Fuzzer	233
Filters	234
Creating a Filter	235
Using a Filter	235
Deleting a Filter	235
Editing a Filter	235
Using the Session Editor	236
Creating a Query String	236

Session Editor Tabs	237
Method Tab	237
Path Tab	237
Query Tab	237
Version Tab	237
Headers Tab	237
Cookies Tab	238
Post Data Tab	238
Web Fuzzer Settings	239
General	239
Proxy	239
SQL Injector	241
Using the SQL Injector	241
SQL Injector Tabs	243
SQL Injector Settings	243
Options Tab	243
Authentication Tab	245
Proxy Tab	245
Compliance Manager	247
How It Works	247
Creating/Editing a Compliance Template	247
Testing for Compliance	251
Web Macro Recorder (Session-Based)	253
Creating a Macro	253
Editing the Logout Condition	255
URL Rewriting and Request Parameters	257
Inspecting and Editing a Macro	258
Session-Based Web Macro Recorder Settings	260
General	260
Proxy	261
Web Macro Recorder Menus	262
File	262
Edit	262
View	262
Help	263
Web Macro Recorder (Event-Based)	264
Recording a Log-In Macro	264
Specifying a Logout Condition	265
Specifying a Confirmation Element	265
Troubleshooting a Macro	265
Dynamic Challenge/Response Authentication	266
Editing a macro	266
Dynamic Challenge-Response Authentication	268
Logout Elements	270
Using a Regular Expression for Logout Detection	271
Confirmation Elements (Hints)	272
Unsupported Elements	272

Event-Based Web Macro Recorder Settings	273
Application Settings	273
Macro Settings	275
Web Service Test Designer	276
Global Values Editor	280
Importing and Exporting Operations	280
Using Autovalues	281
Web Service Test Designer Settings	281
Network Proxy	281
Network Authentication	282
Server Analyzer	283
Analyzing a Server	283
Server Analyzer Settings	283
Authentication Method	283
Authentication Credentials	284
Proxy	284
Exporting Results	285
Report Designer	286
User Interface	286
Toolbar	286
Menus	287
Designer Tabs	289
Toolbox	289
Design Surface	290
Report Explorer	290
Properties Grid	291
Creating a Report	292
Report Script Editor	292
Parameter Designer	293
Toolbar	294
Canvas	294
Properties Grid Pane	295
Controls Toolbox	295
Report Parameters Pane	295
Report Styles Editor	295
Report Structure	296
Report Structure	296
Report Header	296
Report Footer	296
Page Header	296
Page Footer	297
Group Header/Footer	297
Detail	297
Report Settings	297
Charts	297
Chart Types	297
Chart Data	308

Chart Effects	312
Chart Control Items	315
Chart Axes and Walls	317
Chart-Specific Properties	320
Chart Wizard	321
Walk-Through: Creating a Report	321
B Policies and Components	327
Introduction	327
Policies	327
Policy Components	329
Audit Engines	329
General Application Testing	331
General Text Searching	331
Third-Party Web Applications	332
Web Frameworks/Languages	332
Web Servers	332
Web Site Discovery	332
Custom Checks	332
Index	333

1 Welcome

Introduction

The Assessment Management Platform (AMP) from Hewlett-Packard is based on the industry's most successful and accurate Web application assessment tools: WebInspect and QAIInspect.

As the leader in Web application security, HP delivers the most thorough and dependable tools for evaluating Web application vulnerabilities. Since their introduction, HP scanners have quickly become the most important tools used by developers throughout the entire software development life cycle.

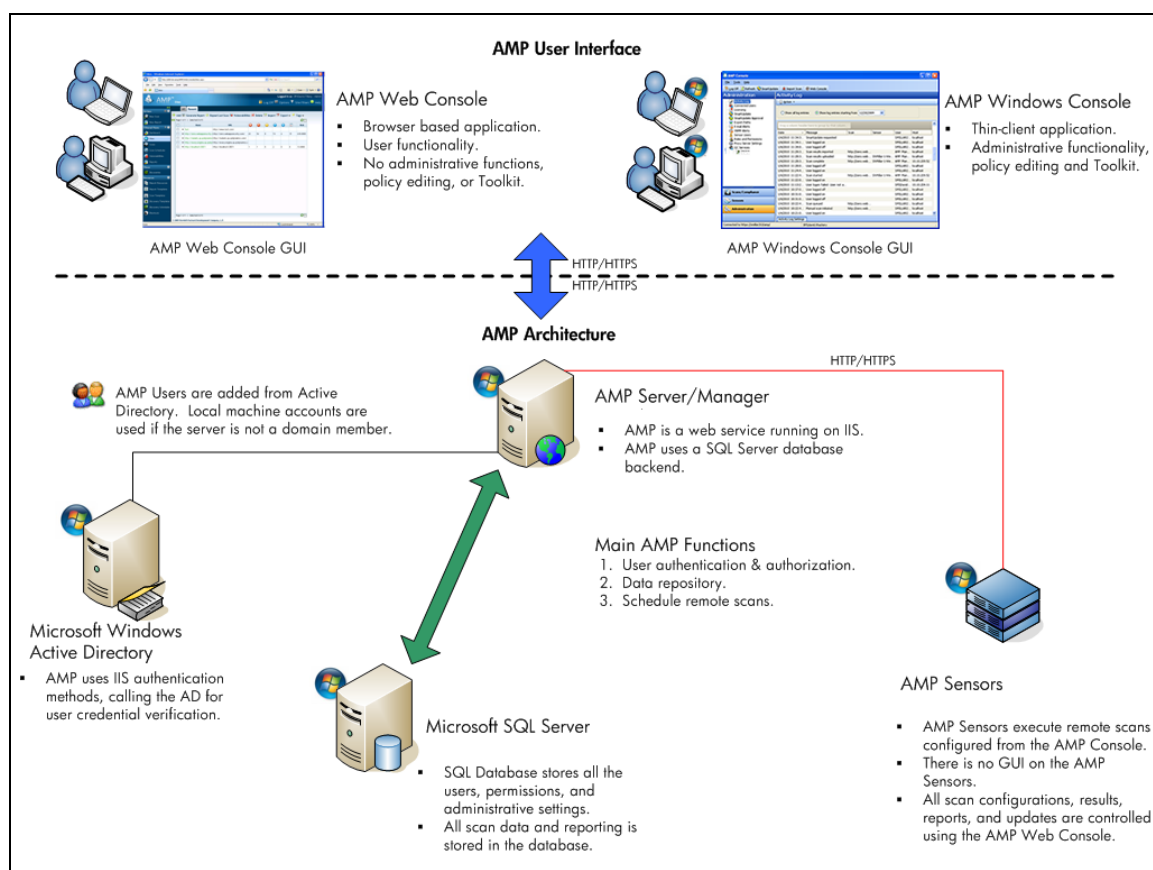
Yet despite our scanners' impressive ability to detect security flaws in Web-based applications, developers of large, intricate Web sites could not easily integrate their assessment results into a centralized repository that would provide an accurate view of the overall enterprise susceptibility.

That's why we developed AMP.

Features and Benefits

AMP is a distributed network of HP scanners controlled by a system manager with a centralized database. This innovative architecture allows you to:

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



New Features and Enhancements for AMP 9.0

Assessments

The most notable development for version 9 is the introduction of assessments. An assessment is a virtual workspace for your scans and vulnerability information, allowing you to bring together all the results of your web application investigation into one centralized location. Within an assessment, you can combine data from multiple scans, remove duplicate vulnerabilities, add manually found vulnerabilities, and attach documentation such as notes and screenshots. This new concept in AMP v.9 shifts the Quality Assurance focus from individual scans to a repository of findings that are accumulated during the entire testing phase and throughout the life cycle development process.

Once an assessment is created for a site, you can add scans from different or overlapping areas of the application, scans acquired with different scan settings, or scans that are “application snapshots” taken at different stages of development. You can even import static analysis results from HP Fortify SCA and Security Scope.

Once a scan is associated with an assessment, the results of the scan are automatically updated whenever a change is made within the assessment. For example, if an assessment “finding” is marked as a false positive, then the associated vulnerability in the scan is automatically designated a false positive. For this reason, operations that may potentially change assessment data are disabled; all modifications to the scan must occur in the assessment, not in the scan.

Findings

A finding typically represents a single vulnerability or a group of “correlated” vulnerabilities. For example, if there are two dynamic scans of a web site with different configurations, and both scans have some overlap and report the same vulnerability, then when the scans are added to an assessment, the two vulnerabilities are combined into a single finding. This correlation produces a more accurate risk evaluation.

Manual Findings

For many organizations, an automated dynamic scan is just part of a larger web application examination process that typically also includes manual investigations. Until now, there was no mechanism for programmatically incorporating manual results into the AMP analysis. With this release of AMP, however, you can create a “finding” within an assessment and add the supporting documentation. This information will then be included in the dashboard and added to the assessment reports. Manual findings are available only within an assessment.

Correlation of Dynamic Vulnerabilities

AMP v9 can compare the results of several dynamic scans and determine which vulnerabilities are actually multiple occurrences of the same issue. It performs this correlation by comparing the location of the vulnerability (URL, parameters, etc.), the nature of the vulnerability (cross-site scripting, SQL injection, etc.) and other attributes. This correlation occurs automatically when a scan is added to an assessment. Matched vulnerabilities are grouped into a “finding.”

This time-saving feature can be a valuable asset when investigating issues such as false positives. For example, assume that an assessment comprises three scans and all three contain the same vulnerability. Each identical vulnerability is then combined into a single

finding. After review, the user marks the finding as a false positive, which causes the individual vulnerabilities in each scan to be updated as false positives. Subsequently, if the user conducts a fourth scan and the same vulnerability is found again, then when the scan is added to the assessment, the vulnerability would be correlated to the same finding and automatically marked as a false positive.

Hybrid 2.0 - Correlation of Runtime Vulnerabilities (HP Fortify - Security Scope)

If you use HP Fortify products and have deployed Security Scope on your Web application, you can incorporate your Security Scope “runtime analysis” results into an assessment. If Security Scope was running while an AMP Sensor (or WebInspect) was assessing the application, then the Security Scope results can be correlated with the dynamic analysis results when they are imported into an AMP assessment. Once a dynamic vulnerability and a runtime vulnerability have been correlated into a single finding, a “Runtime” tab becomes available on the finding and will display the application call stack as the dynamic attack traversed through the web application. This greatly reduces the difficulty in determining what code changes are needed to fix a vulnerability.

Hybrid 2.0 - Correlation of Static Vulnerabilities (HP Fortify - Source Code Analysis)

If you use HP Fortify products and have performed a Source Code Analysis (SCA) scan of your application, you can import these results into AMP. If Security Scope results are also available and Security Scope was running when the dynamic analysis scan occurred, you can correlate static analysis results to the dynamic analysis results. For example, if you have an assessment that contains a dynamic analysis scan (WebInspect/AMP sensor), a runtime analysis scan (Security Scope), and a source analysis scan (SCA), the results can be combined into findings. A single finding may contain multiple dynamic vulnerabilities combined with a single source location as the system determines that many dynamic vulnerabilities are caused by a single source code problem.

When SCA results have been imported into an assessment, the **Source Code** tab will be enabled for findings that are found by static analysis or have been correlated to static analysis vulnerabilities.

Scan Uploader

The Scan Uploader is a new utility that allows you to upload WebInspect or QAIInspect scan files (*filename.scan*) or Fortify scan files (*filename.fpr*) to AMP. You can specify the site (and optionally the assessment) to which the data should be uploaded, and you can even create a site. The Scan Uploader replaces the Fortify2AMP utility that was distributed with AMP 8.10.

Note that scans can also be uploaded through the Scan Uploader service provided by the AMP Services Manager. If you scan a Web site with WebInspect, QAIInspect, or Fortify, you can copy the results to a location called a “dropbox.” The AMP Scan Uploader service (which is separate from the Scan Uploader utility) can access each dropbox periodically and, if files exist, upload those files to the AMP Manager. You can configure this feature through the AMP Services Configuration utility.

Aliasing

Some web sites have may have different names, but are in actuality identical sites. For example, a site named QA.testsite.com may be exactly the same as a site named Staging.testsite.com. This becomes problematic when performing a dynamic analysis scan because correlation uses the URL as a key component to match multiple vulnerabilities. Both

scans would be added to an assessment, but all the results would be disjointed and uncorrelated, making the vulnerability counts incorrect and much harder to manage and remediate. To overcome this problem, AMP v.9 includes a new feature known as aliasing, which allows you to define all the equivalent URLs and hostnames for the web application, allowing correlation to occur for all active and future assessments (see managing status for more information).

Correlation Management

When reviewing findings within an assessment, users can modify the relationship between vulnerabilities and findings. If two findings are, in fact, duplicates, then users can merge these multiple findings into one. The opposite capability also exists; if users feel that multiple vulnerabilities were incorrectly grouped together as a single finding, they can select one or more of those vulnerabilities and separate them, producing a new finding for the selected vulnerabilities.

Risk Score

In previous versions of AMP, the risk score (a numerical representation of the security posture of a site) was determined by calculating the number of vulnerabilities from the most recent scan. If that happened to be a low-quality or crawl-only scan, the resulting low risk score would incorrectly indicate that the site was more secure than it actually was. In AMP v9, with the addition of assessments, the user can now specify the source of data from which the risk score is calculated. A site risk score can be either the last completed assessment, a specifically selected completed assessment, or the last completed scan (if there are no completed assessments).

Assessment Dashboards

Along with the new assessment capabilities of correlation, aliasing, and manual findings, new dashboards have been added to provide summary information including what the vulnerability counts would be without correlation as well as information about the number of findings by source (static/runtime/dynamic).

Screenshots

Screenshots are a principal method for proving and documenting a vulnerability. In AMP v9, you can attach screenshots to specific findings and later view them when generating certain reports or include them as attachments when sending findings to Quality Center (ALM) as defects.

Assessment State

To help differentiate between assessments, each assessment can be in one of the following states: Completed, Abandoned, or In Progress. By default, once a user marks an assessment as complete, the site's risk score is updated to match the risk score of the assessment. The last completed assessment represents the current security posture of the site. Assessments are also presented in the central dashboard by their state as well: Active Assessments and Recently Completed Assessments.

New Assessments from Existing Assessments

Frequently, certain compliance rules require certain sites to be reassessed on a regular basis: monthly, quarterly, or semi-annually. The “Create [Assessment] From Existing Assessment” functionality has been designed with this in mind and enables you to quickly create a new assessment and copy content from an existing assessment. For example, if as part of the “June Assessment” for site “HR Portal” three scans are needed in a variety of configurations, then users can automatically copy the scan configurations into a new assessment and immediately start the scans. In addition, users can copy the status of ignored and false positives for specific vulnerabilities into the new assessment (more information below).

False Positive Management (across Assessments)

A number of customers have reported that it is troublesome to continually mark a vulnerability as False Positive (or Ignored) each time they encounter the same vulnerability from scan to scan. As part of the new “Create [Assessment] From Existing Assessment” feature, there is an option to copy False Positive and Ignored vulnerabilities. When this option is selected, all of those items are internally copied from the old assessment into the new assessment. Once new scans are created or added to the new assessment, each vulnerability (location + check) is compared to the copied list of False Positives and Ignored vulnerabilities and the status is automatically updated if a match occurs.

Reports

Three new reports have been specifically created for assessments:

- The Assessment Summary report provides a high-level perspective to the results of the assessment. This report includes charts that summarize the results of the assessment by severity, analysis type, and scan.
- The Assessment Compliance report is similar to the scan compliance report in that it measures results against specific compliance criteria. However, since it uses an assessment as its source, it includes static analysis findings as well.
- The Assessment Findings report is designed for persons who remediate the results of an assessment and optionally includes HTTP requests and responses, runtime call-stack, and source code (depending on the vulnerability type).

Sending Findings to Quality Center

In previous releases of AMP, users had the option to send vulnerabilities to Quality Center as defects. With the introduction of the AMP findings, there is an additional concept that represents a logical defect for Quality Center. When sending a finding to Quality Center, additional information above sending a vulnerability is included: attached screenshots, stack traces (Runtime Findings), and source code (Static Analysis Findings).

New Tools

Version 9 of AMP includes two new tools that enhance and improve the accuracy of your scans.

- **Web Service Test Designer** - This new tool, which replaces the SOAP Designer, allows you to create a file containing verified data for submission to a Web service.

- **Event-Based Web Macro Recorder** - This tool was devised specifically to create reliable log-in macros, especially for sites that employ Web 2.0 technology, including dynamic challenge/response authentication.

New Features and Enhancements for AMP 8.10

Roles and Permissions

Security provisions for allowing access to various AMP objects has changed radically in response to suggestions from our customers. In previous releases, a user's role specified various permissions for each securable object (such as individual sites, scans, templates, etc.). While initial configuration was tedious, changing permissions on existing objects was even more difficult. The new security architecture for AMP distributes roles and permissions across three levels, configurable in the AMP Console. The levels are system, organization, and project.

The delineation of permissions by organization and project reflects the way in which AMP now categorizes all scanning activity. You can create multiple organizations, and each organization can contain one or more projects. Each site is associated with one (and only one) project. At a minimum, there must be at least one organization and one project.

System permissions determine which users can perform various functions in the AMP Console. The system administrator can also create administrators for each security level. A system administrator is not, by default, an administrator of an organization or project.

Organization permissions pertain to objects that are not common across projects, such as templates, report definitions, and a subset of AMP Console functions. Organization administrators may also limit the priority that may be assigned to a scan conducted by this organization, specify vulnerability weights for calculating organization risk levels, and restrict the organization to a subset of objects (for example, making only five of the 17 scanning policies available to the organization).

Project permissions include sites, scans, templates, reports, console functions (alerts and blackouts), and restrictions on using tools in the HP Toolkit. The important change from previous releases of AMP is that permissions are no longer assigned to individual objects, such as scans and sites. For example, if a user in a given project role has permission to view scans, that user may view all scans in the project. A site inherits its permissions from the project with which it is associated; if you move a site from one project to another, the site acquires its permissions from the new site.

For complete information, see [Roles and Permissions](#) on page 55.

Optimal Scan Settings for Oracle Sites

Users may create a scan template containing sensor settings that are optimized for Oracle sites. To do so:

- 1 Click **Scan Templates** in the Navigation pane of the Web Console.
- 2 Hover the mouse pointer over the **Add from** icon.
- 3 Select **Oracle Settings**.

The *Configure Scan Template* window opens prepopulated with settings optimized for Oracle sites.

Sending Defects to HP Quality Center

AMP users can now select a vulnerability detected by HP scanners and submit it as a defect to a project in a Quality Center application. You must first install the Quality Center service on a resource that is accessible from both the AMP Console and the AMP Web Console. Next, a system administrator, using the AMP Console, must specify the URL of the Quality Center application and the path to the Quality Center service. Finally, the AMP Web Console user must create at least one Quality Center profile using the Options feature.

After properly configuring these requirements, users can send a defect to Quality Center using either the Site Details, Scan Details, or Vulnerabilities forms. You can also view a list of defects sent to Quality Center by accessing the QC Defects form.



Beginning with version 11, HP Quality Center has been renamed HP Application Lifecycle Management (ALM). All references to Quality Center also apply to ALM, except where specifically noted. If you are integrating ALM with AMP, you must also install the HP Application Lifecycle Management Connectivity Add-in; select Add-Ins Page from the ALM main window.

Administrative Approval of Binary Updates

When the HP server downloads updates for AMP client applications, a notification appears in the AMP Console's Smart Update Approval module. A system administrator must approve the update before the AMP manager makes it available to the client applications. This feature applies only to binary updates. Updates to the AMP database (checks, policies, etc.) are applied automatically.

Archiving Scan Data

Scan data consumes considerable storage space on AMP servers. Additionally, a large scan database can adversely affect performance when loading or viewing scan data. You can now archive a scan, which extracts the data, compresses it, and stores it in a separate database. Archived scans can be deleted or restored.

With the exception of "General" reports, archived scans cannot be used for reports. High-level metrics are available, but not the scan details.

Scan Linkage Analyzer

A new tool, the Scan Linkage Analyzer, presents a graphic visualization of the relationships between page connections on the target site. Each node represents a page or folder. A plus sign (+) on the periphery of a node indicates the existence of at least one child node. You can double-click (or Ctrl-click) a node, thus drilling down through the site to investigate vulnerabilities. The Scan Linkage Analyzer is available from the Scan Details module. To use this feature, you must install Microsoft Silverlight.

Integration with Fortify

[Note: The Fortify2AMP utility has been replaced in release 9.00 with the Scan Uploader] A new utility distributed with AMP 8.10 allows Fortify 360 users to integrate scan results from Fortify's static source code analyzer into AMP. The Fortify2AMP utility converts the Fortify file to an HP proprietary format before uploading to AMP. This can be a manual process or it can be set up as a service to automatically upload on a file basis.

New Features and Enhancements for AMP 8.0

Web Console Login/Logout

The user must now log in to the Web Console (and also has the ability to log out). This functionality was added so that users logging in and out would appear in the Activity log. In addition, the user can now see all users logged into Web consoles (by clicking the Administration group and selecting Connected Users).

Tagging

AMP 8.0 introduced the concept of tagging to allow data to be grouped and categorized as appropriate for the enterprise. These tags are name/value pairs (such as. "project=AMP" or "region=North America").

Tagging on Objects

An object can be assigned multiple tags, but each tag must have a different name. The AMP system will then allow these custom field values to be displayed as columns in object grids or used in reporting for sorting and grouping the data.

Discovery Site Tags

When configuring a Discovery Scan, you can specify a tag name that will be assigned to all sites found during the scan.

Grouping

AMP 8.0 also allows the user to group data so that all objects sharing a given attribute can be viewed and accessed at once. This grouping can be either on standard data fields or custom tags defined for the object. For example, if severity is selected as the grouping option for vulnerabilities, then the different severity levels would be shown in a new collapsible group pane located to the left of the Vulnerability grid. When "Critical" is selected in the grouping pane, the vulnerability grid will be updated to just show vulnerabilities with critical severity.

Reporting

A new reporting utility provides the following functionalities:

- Report Designer - From the AMP Console, you can launch a report designer to create or modify reports. This allows you to provide additional information or remove data that is not relevant to your organization.
- Session Report - You can now generate session-based reports that show the HTTP request and response, as well as an appendix of all checks found.
- Additional Enterprise Reports - Three new enterprise reports provide information about all sites in the system:
 - Average Risk by Site and Month
 - Vulnerability Counts by Severity and Site Tag
 - Vulnerability Counts by Category and Site Tag
- Reports across multiple scans - When you select multiple scans for a report, the data will be combined into one report (rather than generating the same report multiple times).

Scan Visualization

The ability to track the progress of a scan was greatly enhanced in AMP 8.0. While a scan is running, you can track the following details:

- Vulnerabilities - You no longer need to wait for the scan to complete before obtaining information about discovered vulnerabilities.
- Crawled URL information - Each URL that is crawled is displayed, along with its response time and status code. When the scan is complete, you can see the details for the session (response, request, and additional information, when applicable) and generate a session report.
- Scan log - The Scan log is now visible from the Web console.
- Scan activity - Scan activity messages (showing the time, sensor, user, and sensor host) are available from the Web console.

Vulnerability Details

Vulnerability details can now be viewed from the vulnerability list. When you click the vulnerability name, a bottom-tabbed pane is rendered showing the summary, request, response, tags, and properties associated with the vulnerability. This detail pane is updated as new vulnerabilities are selected in the grid, allowing you to compare a specific detail about multiple vulnerabilities. The vulnerability Properties tab has fields that allow you to mark a vulnerability as false positive or ignored, or to add a note concerning the vulnerability.

Enhancements

- Improved Web Console user interface - Most non-administrative functions have been moved from the AMP Console to the AMP Web Console. There is no longer any shared functionality between the two consoles. In addition, the Web Console has been improved with increased use of AJAX, a new navigation menu, and breadcrumbs.
- Multiple selection for object permissions - The administrator can select multiple objects and set their permissions in one transaction.
- Improved site filters - Sites can now be filtered on tag name values, risk scores, and scan date ranges.

- Improved international support - Input validation now handles Asian character sets.
- Large scan file upload support (Zip-64) - Large scans (greater than 2GB) can now be imported to and exported from AMP.
- Import/Export Site lists in XML - Site lists can now be imported and exported in XML format in addition to CSV format.

2 Installation

Introduction

The Assessment Management Platform comprises the following:

- The AMP server/manager
- The AMP Console (which provides the graphical user interface to the system manager)
- The AMP Web Console (a browser-based interface to the system manager, designed specifically for non-administrative functions)
- AMP Quality Center service (if integrating with HP Quality Center)
- Scanners. Two types of scanners are supported:
 - Sensor - This is the WebInspect application when connected to AMP for the purpose of performing remotely scheduled or requested scans with no direct user interaction through its graphical user interface. It receives its instructions exclusively from the configurable connection to an AMP Manager.
 - Client - A client is any HP scanner (WebInspect, QAInspect, or DevInspect) that connects to AMP to receive license, permissions, updates or scan data, and which also presents a user interface through which scans may be conducted. AMP controls permissions for a client and also provides the policies and compliance templates used by clients. A client can be configured to upload scan results to AMP automatically at the completion of the scan or only when specifically instructed by the user.

Typical installations contain one SQL Server, one or more consoles, and multiple scanners. These components can be distributed across your network in any way you like, but you must configure at least one of each.

You cannot install this software remotely. You must run the installation program on each server or PC that you intend to integrate into the AMP system, beginning with the SQL Server. For that reason, you may prefer to save the installation program to your hard drive and copy it to a CD, or save it to a network location that can be accessed by each machine on which you expect to install a component.

System Requirements

Before installing AMP, make sure that your system meets the requirements listed below.

All Products

- Platform: Microsoft .NET 3.5 SP1
- Supported Browsers: Microsoft Internet Explorer 6 (minimum), 7 or 8 (recommended), or FireFox 3.x
- Network: An active Internet or intranet connection



Note: If you are installing software on a machine that does not have an Internet connection, see [“If You Are Not Connected to the Internet”](#) on page 26.

AMP Server

- Processor: 2.5 GHz or better
- RAM: 4 GB or more
- Hard Disk Space: 5 GB (using remote database) or 20 GB (minimum if using local database); 100+ GB recommended
- Platforms
 - Microsoft IIS 6.0 (Minimum)
 - Microsoft IIS 7.0
 - Microsoft IIS 7.5 (Recommended)
- Supported Operating Systems
 - Windows Server 2003 Standard SP2 (32-/64-bit)
 - Windows Server 2008 SP2 (32-/64-bit)
 - Windows Server 2008 R2 (32-/64-bit)
- Supported Integrations
 - HP Quality Center (QC) v9.2 or v10.0
 - HP Application Lifecycle Management (ALM) v11.0
 - HP Fortify SCA 3.0
 - HP Fortify Security Scope 3.0

AMP Console/Client

- Processor: 1.5 GHz or better
- RAM: 1 GB or more
- Hard Disk Space: 2 GB
- Supported Operating Systems
 - Windows XP Professional SP3 (32-bit),
 - Windows Server 2003 SP2 (32-bit/64-bit)
 - Windows Server 2008 SP2 (32-/64-bit)

- Windows Vista SP2 (32-bit/64-bit)
- Windows 7 (32-bit/64 bit)
- Supported Databases
 - Microsoft SQL Server Express Edition 2008 SP2 (4 GB scan database limit)
 - Microsoft SQL Server Express Edition 2005 SP3 (4 GB scan database limit).

A database is required only if you want to edit policies, compliance templates, or audit inputs.
- Platform: Silverlight Runtime v3 (required only if you want to use the Scan Link Analyzer and Screenshot Attachments)

AMP Database

- Processor: 2.5 GHz or better
- RAM: 2 GB or more
- Hard Disk Space: 20 GB minimum, 100+ GB recommended
- Supported Operating Systems
 - Windows Server 2003 SP2 (32-/64-bit)
 - Windows Server 2008 SP2 (32-/64-bit)
 - Windows Server 2008 R2 (32-/64-bit)
- Supported Databases
 - Microsoft SQL Server 2005 SP4
 - Microsoft SQL Server 2008 SP2
 - Microsoft SQL Server 2008 R2 (Recommended).

Note: Assessment Management Platform does not support SQL Server Express Edition.

AMP Sensor (WebInspect 9.0)

- Supported Operating Systems
 - Windows 7 (32-/64-bit) (Recommended)
 - Windows XP Professional SP3 (32-bit)
 - Windows Vista SP2 (32-/64-bit)
 - Windows Server 2003 SP2 (32-bit)
 - Windows Server 2008 SP2 (32-/64-bit)
 - Windows Server 2008 R2 (32-/64-bit)
- Processor: 1.5 GHz Single-Core minimum; 2.5 GHz Multi-Core recommended
- RAM: 2 GB minimum; 4 GB recommended
- Hard Disk: 10 GB minimum; 100+ GB recommended
- Display: 1024 x 768 minimum; 1280 x 1024 recommended
- Supported Databases

- Microsoft SQL Server Express Edition 2008 R2 (Minimum) (10 GB scan database limit)
- Microsoft SQL Server Express Edition 2008 SP2 (4 GB scan database limit)
- Microsoft SQL Server Express Edition 2005 SP3 (4 GB scan database limit)
- Microsoft SQL Server 2008 R2 (Recommended) (No scan database limit)
- Microsoft SQL Server 2008 SP2 (No scan database limit)
- Microsoft SQL Server 2005 SP4 (No scan database limit)
- Platform: Microsoft .NET Framework 3.5 Service Pack 1
- Supported Browsers
 - Internet Explorer 6.0 (Minimum)
 - Internet Explorer 7.0
 - Internet Explorer 8.0 (Recommended)
 - Mozilla Firefox 3.6 (Proxy Settings Only)

For an AMP environment to support Internet Protocol version 6 (IPv6), the IPv6 protocol must be deployed on each AMP Console, AMP Sensor, and the AMP Manager.

Upgrading from Previous Versions

Observe the following guidelines if you are upgrading from AMP 8.10.

- You cannot upgrade to AMP 9.0 from versions previous to 8.10.
- AMP 9.0 does not support versions of WebInspect prior to 7.0 and requires WebInspect 8.0, 8.10, or 9.0 to support AMP's new scan visualization feature.
- Make a back-up copy of your database.
- The AMP 9.0 database must be installed on the same database server used by AMP 8.10.
- Before upgrading, use your SQL Server configuration tools to confirm that the hard drive on your database server contains free space equal to at least 3-4 times the size of your existing database. This is because you need to have room for the new database and about 2-3 times the database size for the SQL Server transaction log. For example, if you have a 30 GB AMP 8.10 database, then you will need at least 90-120 GB of free disk space for the upgrade to succeed. Once the upgrade has succeeded, you should be able to shrink your new database's transaction log to a more reasonable size.

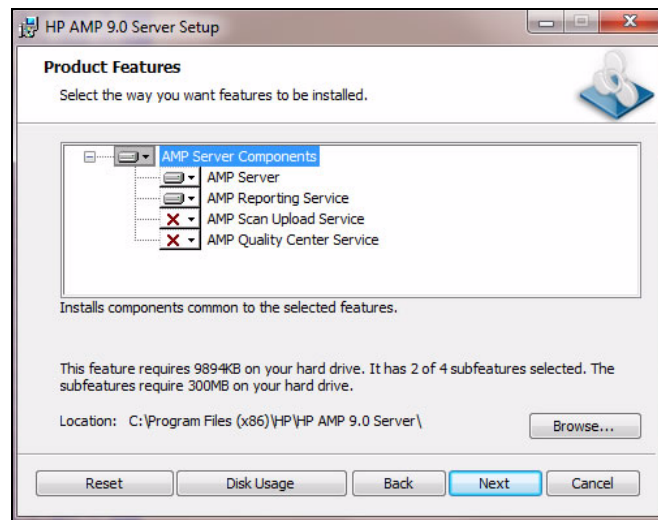
Server/Manager Installation

When installing components on different machines, begin with the machine on which the server/manager will be installed.



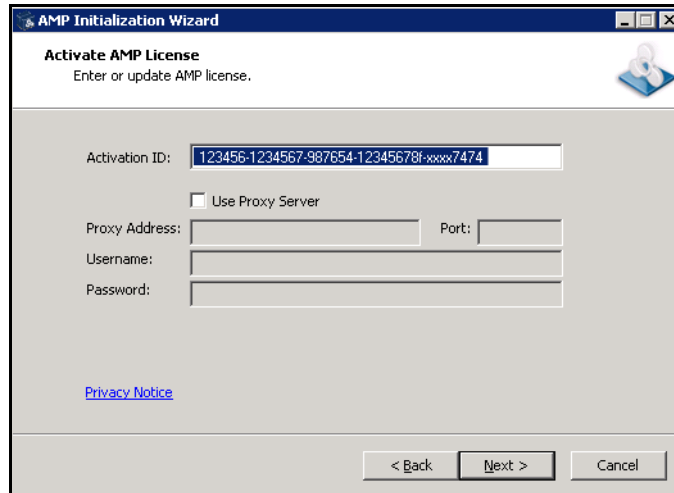
Install the server on one machine only.

- 1 Start the installation program.
- 2 On the *Welcome* page, click **Next**.
- 3 Review the license agreement. If you accept, select the check box and click **Next**; otherwise click **Exit**.
- 4 On the *Server Setup* window, select the components you want to install.



- 5 Select the location in which you want to install the software and click **Next**.
- 6 When ready to install, click **Install**.
- 7 After installation, click **Finish**.
- 8 When the Initialization Wizard appears, click **Next**.

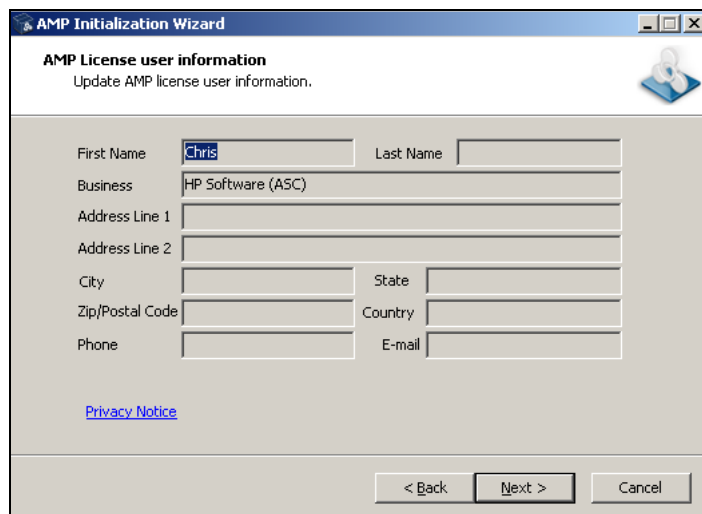
- 9 Enter the Activation ID sent to you by HP.



The screenshot shows the 'AMP Initialization Wizard' window with the title 'Activate AMP License'. Below the title is the instruction 'Enter or update AMP license.' There is a text field for 'Activation ID' containing the value '123456-1234567-987654-12345678f-xxxx7474'. Below this is a checkbox labeled 'Use Proxy Server' which is currently unchecked. Underneath the checkbox are four text fields: 'Proxy Address:', 'Port:', 'Username:', and 'Password:'. At the bottom left is a link for 'Privacy Notice'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

- 10 If using a proxy server, select **Use Proxy Server** and provide the requested information and click **Next**.

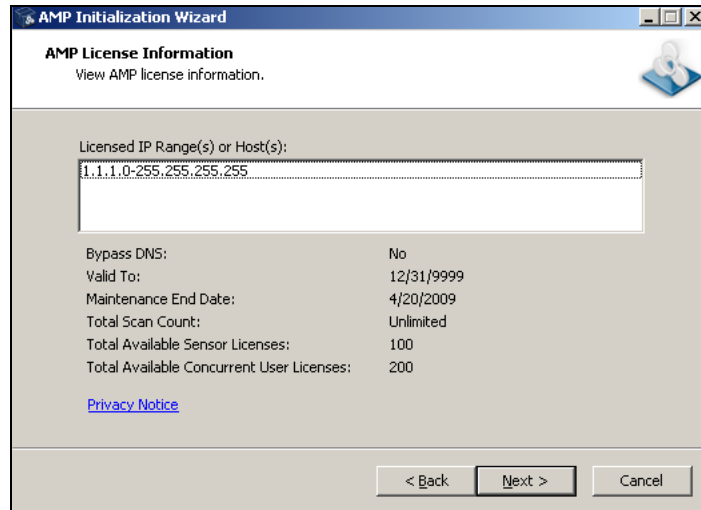
The *AMP License User Information* window displays user information as submitted to HP.



The screenshot shows the 'AMP Initialization Wizard' window with the title 'AMP License user information'. Below the title is the instruction 'Update AMP license user information.' There are several text fields for user information: 'First Name' (containing 'Chris'), 'Last Name', 'Business' (containing 'HP Software (ASC)'), 'Address Line 1', 'Address Line 2', 'City', 'State', 'Zip/Postal Code', 'Country', 'Phone', and 'E-mail'. At the bottom left is a link for 'Privacy Notice'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

- 11 Click **Next**.

The *AMP License Information* window displays information about the license token.

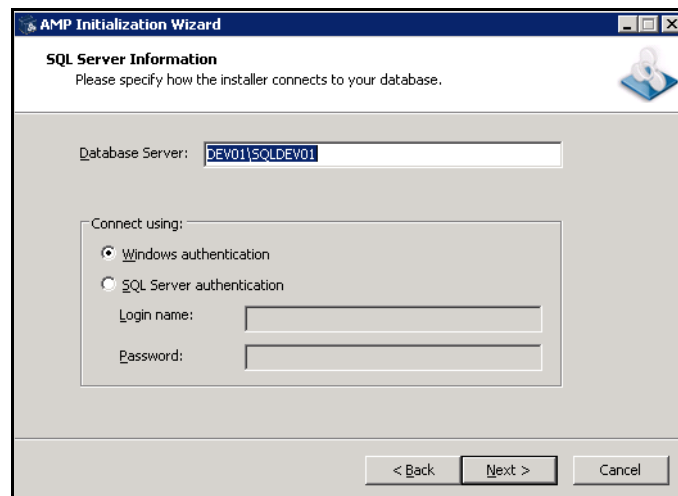


The screenshot shows the 'AMP License Information' window within the 'AMP Initialization Wizard'. The window title is 'AMP Initialization Wizard' and the subtitle is 'AMP License Information'. Below the subtitle, it says 'View AMP license information.' The main content area displays the 'Licensed IP Range(s) or Host(s):' as '1.1.1.0-255.255.255.255'. Below this, a table lists license details: 'Bypass DNS: No', 'Valid To: 12/31/9999', 'Maintenance End Date: 4/20/2009', 'Total Scan Count: Unlimited', 'Total Available Sensor Licenses: 100', and 'Total Available Concurrent User Licenses: 200'. A blue link for 'Privacy Notice' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

AMP License Information	
View AMP license information.	
Licensed IP Range(s) or Host(s): 1.1.1.0-255.255.255.255	
Bypass DNS:	No
Valid To:	12/31/9999
Maintenance End Date:	4/20/2009
Total Scan Count:	Unlimited
Total Available Sensor Licenses:	100
Total Available Concurrent User Licenses:	200
Privacy Notice	

12 Click **Next**.

13 On the *SQL Server Information* panel, enter the name of the SQL Server and select the authentication method that will be used. If you are upgrading from an AMP 8.0 database, you must have at least “read access” to the database. If you are installing AMP 9.0 for the first time, then you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).



The screenshot shows the 'SQL Server Information' window within the 'AMP Initialization Wizard'. The window title is 'AMP Initialization Wizard' and the subtitle is 'SQL Server Information'. Below the subtitle, it says 'Please specify how the installer connects to your database.' The main content area has a 'Database Server:' label followed by a text box containing 'DEV01\SQLEDEV01'. Below this, a 'Connect using:' section has two radio buttons: 'Windows authentication' (selected) and 'SQL Server authentication'. Under 'SQL Server authentication', there are 'Login name:' and 'Password:' labels followed by empty text boxes. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

Database Server: DEV01\SQLEDEV01

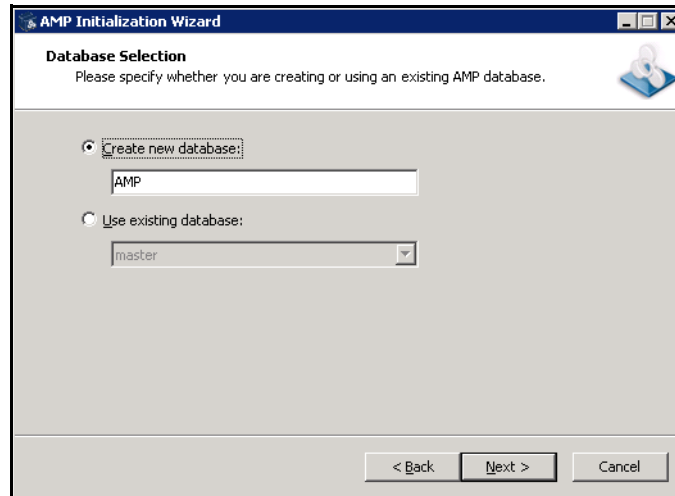
Connect using:

- ☒ Windows authentication
- ☐ SQL Server authentication

Login name:

Password:

- 14 Click **Next**.



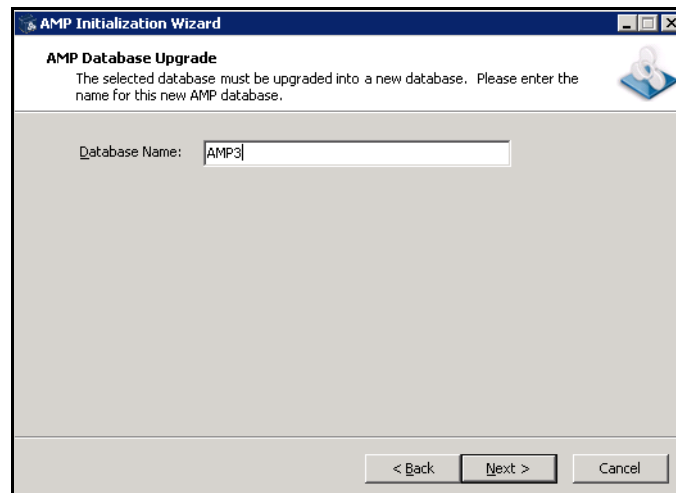
The screenshot shows the 'AMP Initialization Wizard' window with the 'Database Selection' tab selected. The window title is 'AMP Initialization Wizard'. Below the title bar, the text reads 'Database Selection' and 'Please specify whether you are creating or using an existing AMP database.' There are two radio buttons: 'Create new database:' (selected) and 'Use existing database:'. The 'Create new database:' option has a text box next to it containing the text 'AMP'. The 'Use existing database:' option has a dropdown menu next to it showing 'master'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

- 15 On the *Database Selection* window:

- a Choose one of the following:
- To use a new database, select **Create new database** and enter the database name. You must have privileges to create this database.
 - To upgrade from an AMP 8.0 or 8.10 database, or to replace a previous installation of AMP 9.0, select **Use existing database** and select one from the list. You must have owner privileges for that database.

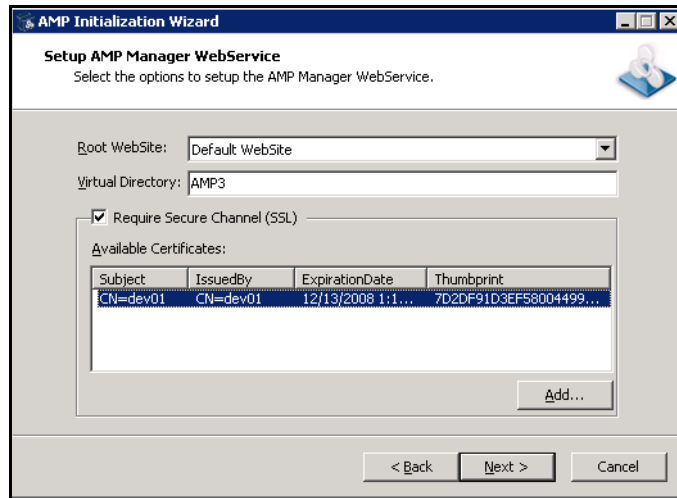
- b Click **Next**.

- 16 For an existing database only, the *AMP Database Upgrade* window appears. Enter a name for the new database and click **Next**.



The screenshot shows the 'AMP Initialization Wizard' window with the 'AMP Database Upgrade' tab selected. The window title is 'AMP Initialization Wizard'. Below the title bar, the text reads 'AMP Database Upgrade' and 'The selected database must be upgraded into a new database. Please enter the name for this new AMP database.' There is a text box labeled 'Database Name:' containing the text 'AMP3'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

- 17 On the *Setup AMP Manager WebService* window, enter the root Web site and the name of the IIS virtual directory.



Caution: If you are upgrading, do not choose the same IIS Virtual Directory name used for previous AMP installations.

If you select **Require Secure Channel (SSL)**, add and/or select an SSL certificate. For security reasons, HP recommends that you use SSL.

These entries create the URLs for the following components.

AMP Console:

`http(s)://<AMP server computer name>/<virtual directory name>/`

AMP Web Console:

`http(s)://<AMP server computer name>/<virtual directory name>/WebConsole`

- 18 Click **Next**.
- 19 On the *Setup the AMP Manager User* window, enter the local or domain user account that you want to associate with the AMP Manager Web Service. For AMP to work properly, this account must be a local administrator. This enables the AMP Manager to install service packs and patches released by HP.

20 Click **Next**.

21 On the *Setup AMP Database User* window, specify how the AMP Manager should connect to the AMP database.

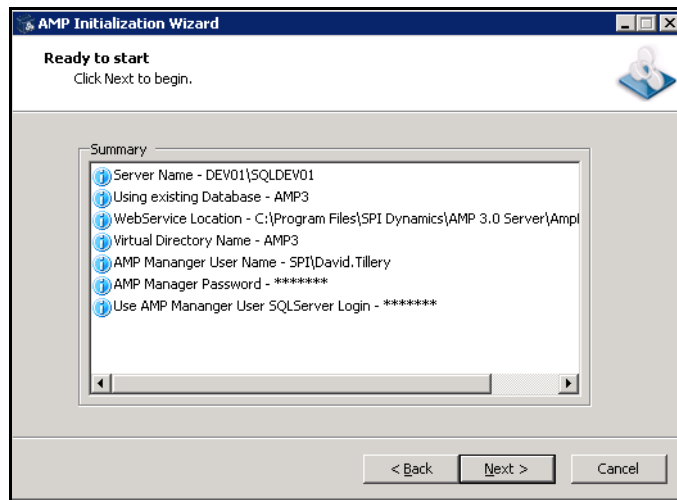
- **Windows Authentication** - The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same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

22 Click **Next**.

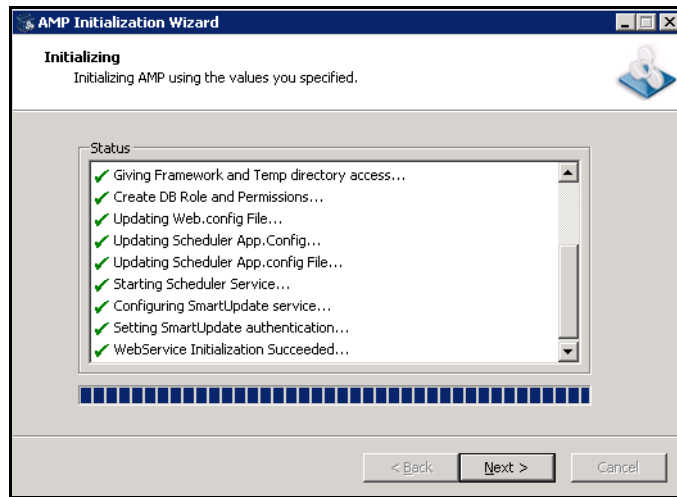
23 On the *Ready To Start* window, verify your previous choices.

- To change settings, click **Back**.

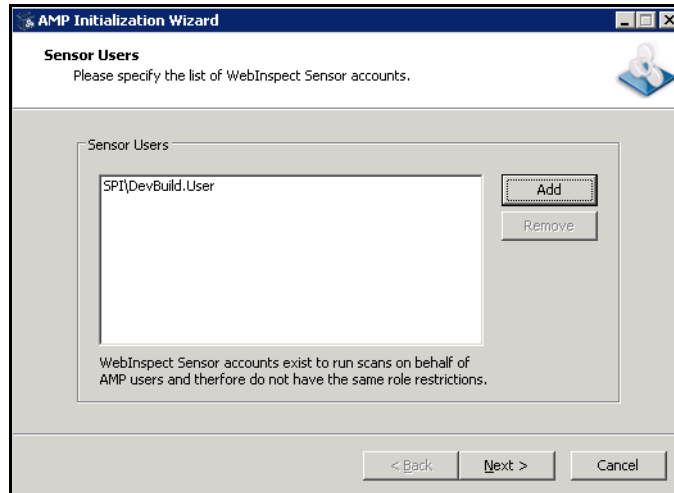
- To begin configuration, click **Next**. The program creates and populates the database, and initializes other database and system components.



- 24 The program displays the initialization results. Click **Next**.

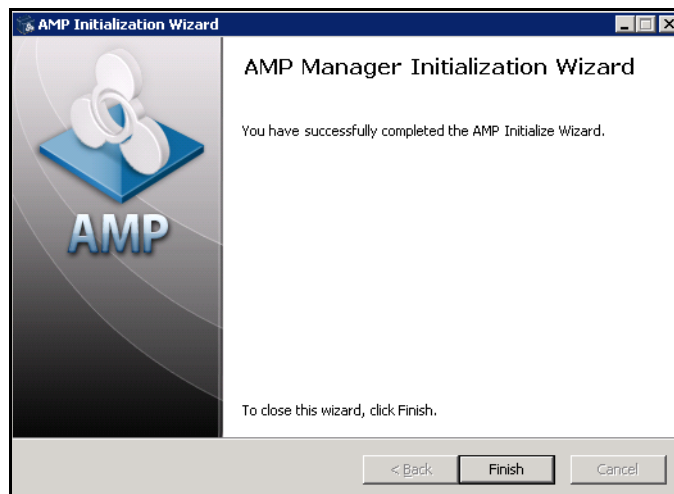


- 25 On the *Sensor Users* window, click **Add** and enter the user accounts that will be associated with the sensors (WebInspect installations).



26 Click **Next**.

27 When installation is complete, the following window appears. Click **Finish**.



Quality Center Service Installation

If you plan to integrate AMP with an HP Quality Center installation (which would allow you to submit vulnerabilities to Quality Center as defects), you must install the Quality Center service. The AMP QC service must be installed on a machine that also has the Quality Center client application installed.

Note: AMP's "Send to Quality Center" feature supports only Quality Center versions 9.2, 10, and 11 (with all applicable service packs installed). Also, these versions support only the following operating systems: Windows XP SP2 and SP3, Windows 7 32-bit, and Vista (32-bit).



Beginning with version 11, HP Quality Center has been renamed HP Application Lifecycle Management (ALM). All references to Quality Center also apply to ALM, except where specifically noted. If you are integrating ALM with AMP, you must also install the Connectivity Add-in as part of the ALM installation.

AMP QC Service installation can be launched from AMP Server installation wizard.

Configuration information is maintained in a file named `QualityCenterService.conf`, which is stored on the machine on which the service is installed. The default location is `C:\Documents and Settings\All Users\Application Data\HP\AMP\8.0\QualityCenterService`.

A sample file is illustrated below:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration>
  <host>DTHACKERY2</host>
  <port>8001</port>
  <ssl>True</ssl>
  <style>tcp</style>
  <messagetimeout>60</messagetimeout>
  <connectiontimeout>10</connectiontimeout>
  <maxsize>524288</maxsize>
  <retries>1</retries>
  <certificateserialnumber>7E98ABF6E78AE359</certificateserialnumber>
  <certificatevalidationmode>Trust</certificatevalidationmode>
  <clientcredentialtype>None</clientcredentialtype>
</Configuration>
```

To change the default port number from 8001, edit the `<port>` attribute.

To use unsecured communications, change the `<ssl>` attribute from “True” to “False.”

To use your own server certificate (instead of the HP certificate created during installation), edit the `<certificateserialnumber>` attribute.

To use client certificate authentication, change the `<clientcredentialtype>` attribute from “None” to “Certificate.”

To configure the QC Service to accept untrusted certificates, change the `<certificatevalidationmode>` attribute from “Trust” to “None.”

AMP Services Configuration Utility

Use the AMP Services Configuration Utility to configure or modify services associated with the Assessment Management Platform (AMP).

After starting the utility, click one of the buttons in the left column. They are:

- **Reporting Service** - Monitors the queue dedicated to requests for report generation.
- **Quality Center Service** - Handles communication between AMP and any Quality Center servers that may be configured.
- **Scan Uploader Service** - Handles the transfer of scans from WebInspect or Fortify to AMP.
- **Task Service** - Monitors the queue for various tasks, including the archiving and restoring of scans.
- **Scheduler Service** - Handles the scheduling of scans, discovery scans, and smart updates.

Reporting Service

Service Status

This area reports the current state of the service. You can start, stop, restart, or configure the reporting service.

To configure the service:

- 1 Click **Configure**.

The Configure Service dialog appears.

- 2 Select which credentials should be used for logging on to the service:
 - **Local system account** - This option is disabled for the Reporting service.
 - **This account** - An account identified by the credentials you specify.
- 3 If you select **This account**, enter an account name and password.
- 4 Click **OK**.

Database Configuration

This area reports the database server name and database name.

To configure the database:

- 1 Click **Configure**.

The Database Configuration dialog appears.

- 2 Enter a server name.
- 3 Specify the account under which AMP will connect to the database.
 - **Windows Authentication** - The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the AMP Server and the database computers.
 - **SQL Authentication** - Enter the SQL Server user name and password.
- 4 Enter or select a database.
- 5 Click **OK**.

Logging Configuration

This area reports current settings for the logging function.

To configure settings:

- 1 Click **Configure**.

The Logging Configuration dialog appears.

- 2 The logging output is contained in the Amp9ReportingService_trace.log. To specify the location of the logs, choose one of the following:
 - **Default location**
On Windows Server 2003, the location is:

\Documents and Settings\All Users\Application
Data\HP\AMP\9.0\AmpReportingService

On Windows Server 2008, the location is:

\ProgramData\HP\AMP\9.0\AmpReportingService

- **Enter location for log file**

Type a path to the folder that will contain the logs, or click **Browse** to select a location.

- 3 For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
- 4 Specify the maximum file size of a log file (in megabytes).
- 5 Specify the number of log files that will be retained.

When a log file reaches its maximum size, AMP will close it and open another file, repeating this process until the maximum number of log files is created. When that file is full, AMP will close it, delete the oldest file, and open a new one. Files are named in sequence: AmpReportingService_trace.log, AmpReportingService_trace.log.1, etc.

Reporting Queue Poll Interval

Specify how often (in milliseconds) AMP will access the polling queue to write data to the logs; then click **Apply**.

Quality Center Service

Service Status

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

To configure the service

- 1 Click **Configure**.

The Configure Service dialog appears.

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

Service Configuration

Use this area to report and configure the Quality Center Service.

To configure the service:

- 1 Click **Configure**.

The QC Service Configuration dialog appears.

- 2 Enter a host name and port number.
- 3 To enable encrypted communication, select **Use SSL communication protocol**. If you choose this option, you may also
 - a Create or select a server certificate.
 - b Require a client certificate. If you select this option, you may also choose to allow a non-trusted client certificate.
- 4 In the **Settings** area, enter values for the following parameters:
 - Message Timeout
 - Connection Timeout
 - Max Message Size
 - Failure Re-tries

Logging Configuration

This area reports current settings for the logging function.

To configure settings:

- 1 Click **Configure**.

The Logging Configuration dialog appears.

- 2 The logging output is located in the AmpQCSservice_trace.log. To specify the location of the logs, choose one of the following:

- **Default location**

On Windows Server 2003, the location is:

\Documents and Settings\All Users\Application
Data\HP\AMP\9.0\QualityCenterService

On Windows Server 2008, the location is:

\ProgramData\HP\AMP\8.0\QualityCenterService

- **Enter location for log file**

Type a path to the folder that will contain the logs, or click **Browse** to select a location.

- 3 For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
- 4 Specify the maximum file size of a log file (in megabytes).
- 5 Specify the number of log files that will be retained.

When a log file reaches its maximum size, AMP will close it and open another file, repeating this process until the maximum number of log files is created. When that file is full, AMP will close it, delete the oldest file, and open a new one. Files are named in sequence: AmpQCSservice_trace.log, AmpQCSservice_trace.log.1, etc.

Scan Uploader Service

Certain applications (currently WebInspect, QAInspect, and Fortify) can scan a Web site and export the scan results to a location called a “dropbox.” The purpose of the AMP Uploader service is to access each dropbox periodically and, if files exist, to upload those files to the AMP Manager.

Service Status

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

To configure the service:

- 1 Click **Configure**.

The Configure Service dialog appears.

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

AMP Configuration

This area reports the AMP Manager configuration.

To configure the AMP Manager:

- 1 Click **Configure**.

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

Dropbox Configuration

Certain applications (currently WebInspect, QAInspect, and Fortify) can scan a Web site and export the scan results to a location called a “dropbox.” The purpose of the AMP Uploader service is to access each dropbox periodically and, if files exist, to upload those files to the AMP Manager.

Use the following procedure to create a dropbox.

- 1 Click **Add**.

The Configure Dropbox dialog appears.

- 2 Enter a dropbox name.
- 3 Enter the full path and name of the folder that will be used as the dropbox (or click Browse to select or create a folder).
Be sure to select or create a folder that will not be used for any other purpose.
- 4 Select a site that will be serviced by this dropbox.
- 5 Click **OK**.

Task Service

Service Status

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

To configure the service:

- 1 Click **Configure**.
The Configure Service dialog appears.
- 2 Select which credentials should be used for logging on to the service:
 - **Local system account** - This option is disabled for the Task service.
 - **This account** - An account identified by the credentials you provide.
- 3 If you select **This account**, enter an account name and password.
- 4 Click **OK**.

Database Configuration

This area reports the database server name and database name.

To configure the database:

- 1 Click **Configure**.
The Database Configuration dialog appears.
- 2 Enter a server name.
- 3 Specify the account under which AMP will connect to the database.
 - **Windows Authentication** - The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the AMP Server and the database computers.
 - **SQL Authentication** - Enter the SQL Server user name and password.
- 4 Enter or select a database.
- 5 Click **OK**.

Logging Configuration

This area reports current settings for the logging function.

To configure settings:

- 1 Click **Configure**.

The Logging Configuration dialog appears.

- 2 The logging output is contained in the AmpTaskService_trace.log. To specify the location of the logs, choose one of the following:

- **Default location**

On Windows Server 2003, the location is:

\Documents and Settings\All Users\Application Data\HP\AMP\9.0\TaskService

On Windows Server 2008, the location is:

\ProgramData\HP\AMP\9.0\TaskService

- **Enter location for log file**

Type a path to the folder that will contain the logs, or click **Browse** to select a location.

- 3 For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
- 4 Specify the maximum file size of a log file (in megabytes).
- 5 Specify the number of log files that will be retained.

When a log file reaches its maximum size, AMP will close it and open another file, repeating this process until the maximum number of log files is created. When that file is full, AMP will close it, delete the oldest file, and open a new one. Files are named in sequence: AmpTaskService_trace.log, AmpTaskService_trace.log.1, etc.

Scheduler Service

Service Status

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

To configure the service:

- 1 Click **Configure**.

The Configure Service dialog appears.

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

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

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

Console Installation

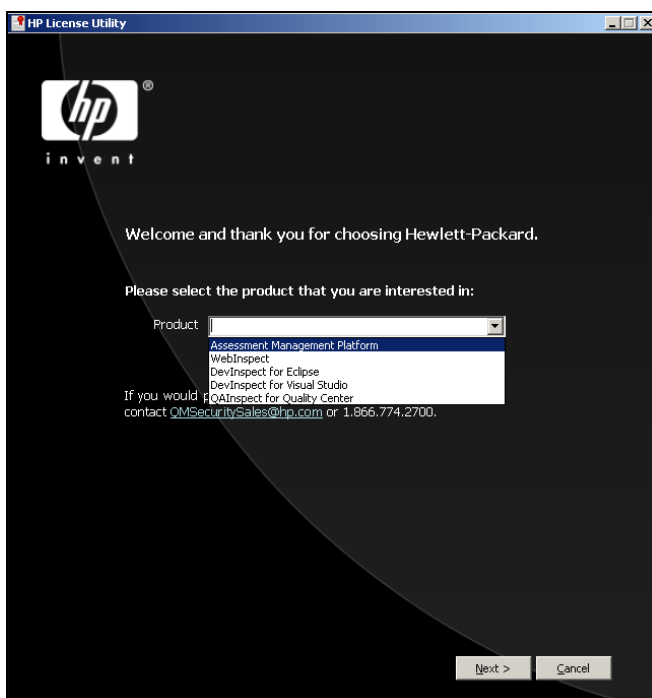
Use the following procedure to install the AMP Console.

- 1 Start the installation program.
- 2 On the Welcome page, click **Next**.
- 3 Review the license agreement. If you accept, select **I accept the terms in the License Agreement** and click **Next**; otherwise click **Cancel**.
- 4 Select the folder into which you want to install the software and click **Next**.
- 5 Click **Install**.
- 6 When the process is complete, click **Finish**.

If You Are Not Connected to the Internet

HP provides an offline licensing tool for use when installing software on a machine that does not have an Internet connection. You will create a file containing information about the computer and transfer the file to a portable device (diskette or flash drive). You will then go to an Internet-connected computer and run a program that will transmit the file to an HP server, which will download a license file that you can copy and install on the computer that is not connected to the Internet.

- 1 Collect the machine-specific information from the isolated machine.
 - a Close all HP applications. Also close Visual Studio, if present.
 - b Run C:\Program Files\HP\HP AMP 9.0 Server\AmpInitialize\LicenseUtilitySetup.exe. This installs the License Utility.
 - c Run the License Utility: Click **Start** → **All Programs** → **HP** → **HP License Utility** → **HP License Utility**.



- d For the **Product** field, select **Assessment Management Platform** and click **Next**.
 - e Select **I am not connected to the Internet** and click **Next**.
 - f Select **Generate License Request** and click **Next**.
 - g In the **Activation Token** field, enter the 32-digit license token sent to you by e-mail from HP. Omit any hyphens that may appear in the string (or simply copy the token, position your cursor in the first block of the **Activation Token** field, and press Ctrl + V).
 - h Select a location where the file will be saved. The name of the request file is formatted as **Assessment Management Platform_LicenseReq.xml**.

Be sure to save this file on a portable media or at a location that is accessible by a machine that has access to the Internet.
 - i (Optional) Enter the information requested in the **Registered User Information** group.

The information you provide is kept in strict confidence and is not shared with anyone outside the Hewlett-Packard Application Security Center. It allows you to participate in surveys designed to elicit ideas for improving HP products.
 - j Click **Next**.
 - k The License Utility displays a message that the license file was generated. For ease of use, do not close the program.
- 2 Transfer the file "Assessment Management Platform_LicenseReq.xml" (created in Step 1) to another machine that has Internet access. This process may involve a USB drive, floppy diskette, CD-RW, intranet access, etc.
 - 3 At the Internet-connected computer, open a browser and navigate to <HTTPS://LicenseService.HPSmartUpdate.com/OfflineLicensing.aspx>.
 - 4 On the Welcome page, select **Generated by another ASC product** and click **Next**.
 - 5 Browse to the generated request file (Assessment Management Platform_LicenseReq.xml) and click **Process Request File**.
 - 6 When notified that the license has been retrieved, click **Retrieve Response File**.
 - 7 Transport the response file (LicenseResp.xml) back to the isolated machine via USB Drive or other device and continue the License Utility by clicking **Next**.

Note: If you closed the License Utility, restart it and advance to this step.
 - 8 Select **Place License** and click **Next**.
 - 9 When prompted to select a license file, browse to the response file and click **Next**.
 - 10 Click **Finish**.



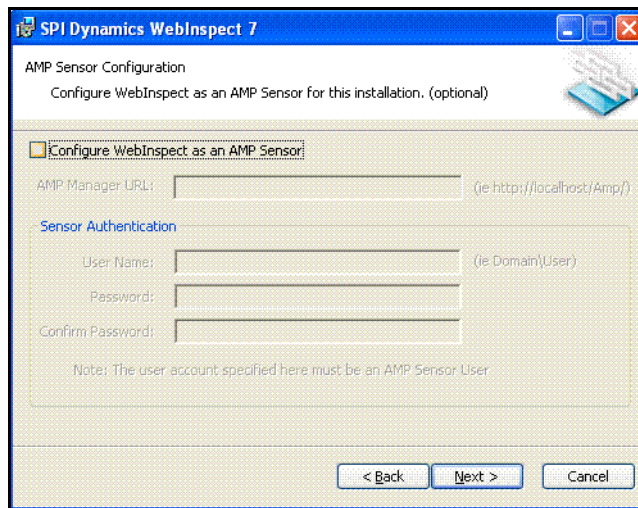
Note: Searching your hard drive for the pre-existing Assessment Management Platform_LicenseReq.xml file may be complicated by Microsoft's default omission of hidden directories. Be sure to enable hidden files and directories.

Sensor Installation

Use the following procedure to install WebInspect as a sensor. For client installation, refer to the WebInspect, DevInspect, or QAInspect User Manuals.

- 1 Start the installation program.
- 2 On the Welcome page, click **Next**.
- 3 Review the license agreement. If you accept, select **I accept the terms in the License Agreement** and click **Next**; otherwise click **Cancel**.
- 4 Select the folder into which you want to install the software and click **Next**.

The *AMP Sensor Configuration* window appears.



- 5 Select **Configure WebInspect as an AMP Sensor**.
- 6 Enter the URL of the AMP manager.
- 7 In the **Sensor Authentication** group, enter the Windows account credentials for this sensor. Be sure to add this account to the list of sensor users using the AMP Administration module.
- 8 Click **Next**.
- 9 When ready to install, click **Install**.
- 10 When the process is complete, click **Finish**.

Time Stamping and Scheduling

There may be installations where the manager and the console reside in different time zones. To accommodate this, the AMP manager uses Coordinated Universal Time (also known as Greenwich Mean Time or Zulu time) for all time storage and manipulation. When a time is to be displayed on the console, the manager converts the time to conform to the time zone in which the console resides. Alert e-mails and reports, however, are time-stamped according to the zone in which the manager resides.

Universal Time does not honor daylight saving time. Therefore, scheduled scan times will change by one hour after the transition between daylight saving time and standard time. To illustrate, suppose you schedule a scan to occur daily at 4 P.M. and you are in the Eastern time zone of the United States during the daylight saving time period. The AMP manager records the settings and will begin the scan each day at 8 P.M. Universal Time (which is the equivalent of 4 P.M. Eastern daylight time). However, when the transition to standard time occurs, your scheduled scan will begin at 3 P.M. local time instead of 4 P.M. Even though you set your clocks back one hour, the Universal Time continued unchanged.

Installations Lacking Internet Connection

All HP security products contain digital certificates of authority. When a product starts, the operating system attempts to connect to the Internet and download a certificate revocation list from the certificate's issuing authority (VeriSign) to determine if the product's certificate has been revoked. If the product cannot establish an Internet connection, it waits until the request times out, which substantially lengthens the product's start-up time. This inability to verify the certificate also causes other problems, including:

- Services fail to start.
- Multiple instances of scriptserver.exe are spawned.
- Scans fail to complete.

To avoid the complications caused by a lack of Internet access, consider the following solutions:

- Use Microsoft Windows Server Active Directory to store and publish a certificate revocation lists (CRL).
- Manually download the required CRL and install it.
- Disable CRL checking for the server.
- Change the default CRL timeout period for the Microsoft Cryptography API (CAPI).
- Disable the "Check for publisher's certificate revocation" option in Internet Explorer settings. To do so, click the Internet Explorer **Tools** menu and select **Internet Options**, click the **Advanced** tab, scroll to the Security section, clear the check box next to "Check for publisher's certificate revocation," then close and restart Internet Explorer.

The recommended solution is to manually download the CRL, and then install it to the local computer certificate store.

To download the CRL:

- 1 Open a browser.
- 2 Go to <http://crl.verisign.com/pca3.crl>.

- 3 When prompted, “Do you want to open or save this file,” click **Save**.
- 4 On the *Save As* dialog box, select a location and click **Save**.
- 5 Go to <http://csc3-2004-crl.verisign.com/CSC3-2004.crl>.
- 6 Repeat steps 3-4.

Note: Because the CRL is valid only for a limited time, you must retrieve a new CRL periodically.

To install a CRL to the local computer certificate store, follow these steps:

- 1 Log on to the computer as a member of the local administrators group.
- 2 Open the Certificates snap-in for the Computer account. To do this, follow these steps:
 - a Click **Start**, click **Run**, type `mmc`, and then click **OK**.
 - b On **File** menu, click **Add/Remove Snap-in**.
The *Add/Remove Snap-in* dialog box appears.
 - c On the **Standalone** tab, click **Add**.
The *Add Standalone Snap-in* dialog box appears.
 - d In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**.
 - e Select **Computer account**, and then click **Next**.
 - f Click **Local computer**, and then click **Finish**.
 - g Click **Close**, and then click **OK**.
- 3 Under the Console root, expand **Certificates**.
- 4 Right-click **Intermediate Certification Authorities**, click **All Tasks**, and then click **Import**.
The Certificate Import Wizard opens.
- 5 Click **Next**.
- 6 Click **Browse**.
- 7 On the *Open* dialog box, select **Certificate revocation list (*.crl)** from the **Files of type** list.
- 8 Locate and select `pca3.crl` and click **Open**.
- 9 Click **Next** and follow instructions in the wizard to complete the installation.
- 10 Go to Step 4 and repeat the process to import `CSC3-2004.crl`.

3 Preparing Your System for Audit

Introduction

HP scanners are aggressive Web application analyzers that rigorously inspect your entire Web site for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which scanning policy you apply and the options you select, it can affect server and application throughput and efficiency. When using the most aggressive policies, you should perform this analysis in a controlled environment while monitoring your servers.

Helpful Hints

If your system generates e-mail messages in response to user-submitted forms, you might want to consider disabling your mail server. Alternatively, you could redirect all e-mail messages to a queue and then, following the audit, manually review and delete those messages that were generated in response to forms submitted by HP scanners.

If for any reason you do not want to audit certain directories, you must specify those directories using the Excluded URLs settings of HP scanners.

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

Finally, HP scanners test for certain vulnerabilities by attempting to upload files to your server. If your server allows this, HP scanners will record this susceptibility in a scan report and will attempt to delete the file. Sometimes, however, the server will not allow a file to be deleted. For this reason, part of your post-scan maintenance should include searching for and deleting files whose name begins with “CreatedByHP”

Using Web Forms

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

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

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

- If, when a user normally submits a form, the application creates and sends e-mail messages or bulletin board postings (to a product support or sales group, for example), HP scanners will also generate these messages as part of their probe.
- If your system writes records to a back-end server (database, LDAP, etc.) based on forms submitted by clients, then forms submitted by HP scanners will create spurious records. Some users, before auditing their production system, create a copy of their database and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit, searching for and deleting records that contain one or more of the form values used by HP scanners. You can determine these values by opening the Web Form Editor.

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

4 Getting Started

Introduction

After installing the AMP software, allow the AMP server to initialize its database, and then perform the following tasks to configure your system and prepare for scanning.

Log On to AMP Console

The windows account of the person who installs the AMP Console software is assigned, by default, to the role of system administrator. This role is granted all permissions with no IP restrictions. No one else can log on until the system administrator assigns other users to roles.

- 1 Start the AMP Console.

The *Log On to AMP* dialog appears.

Note: This window does not appear if you previously selected the option **Automatically log on when this application starts** and if AMP uses the option **Log on as the current Windows user**.

- 2 Using the **Log on to** list, enter or select the URL of the AMP manager.
- 3 Select one of the following logon options:
 - a To log on using your Windows user account, select **Log on as the current Windows user**.
 - b To use a different account, select **Log on as**, then enter the user name and password for an account that has permission to access the console. For new installations, use the account name and password of the user who installed the AMP server software. This user is permitted to perform all restricted functions.
- 4 If you select **Automatically log on when this application starts**, users are logged on with their Windows account, bypassing the logon dialog.
- 5 To go through a proxy server to reach the AMP manager:
 - a Click the **Proxy** tab.
 - b Select one of the following:
 - **Use the Internet Explorer proxy.**
 - **Use the proxy below**, and then provide the proxy server's IP address and port number.
 - c Provide a valid user name and password.
- 6 Click **OK**.

Note: If you see the message "The AMP Server refused the request," you may have entered your user name and password incorrectly, or your account has not been assigned to a role.

Configure the Console

After installing a license, you can specify settings for the console.

To specify console settings:

- 1 From the **Tools** menu, select **Options**.
The *Options* window opens.
- 2 To refresh the display of AMP information periodically, select **Automatically refresh display** and specify how often (in seconds) the display should be updated.
- 3 Click **OK**.

Assign Administrators and Create Roles

Administrative authority within the Assessment Management Platform is distributed across three levels: system, organization, and project. Each level has at least one administrator.

System Level

The user account of the person who installed the AMP software is, by default, the system administrator. This user may add other accounts as system administrators and may also create, rename, and delete organizations. System administrators may also create roles that allow access to certain AMP Console features and assign users to those roles (thereby limiting the functions a specific user may perform).

Organization Level

The system administrator who creates an organization automatically becomes an administrator for that organization. An organization administrator may perform the following functions:

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

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

Project Level

The organization administrator who creates a project automatically becomes an administrator for that project. A project administrator may perform the following functions:

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

You first priority should be to create the organization and project hierarchy, define hierarchical roles, assign users to those roles, and perform the other functions available from the Administration - Roles and Permissions module.

For detailed instructions, see [Roles and Permissions](#) on page 55.

5 AMP Console

The Assessment Management Platform presents two separate user interfaces:

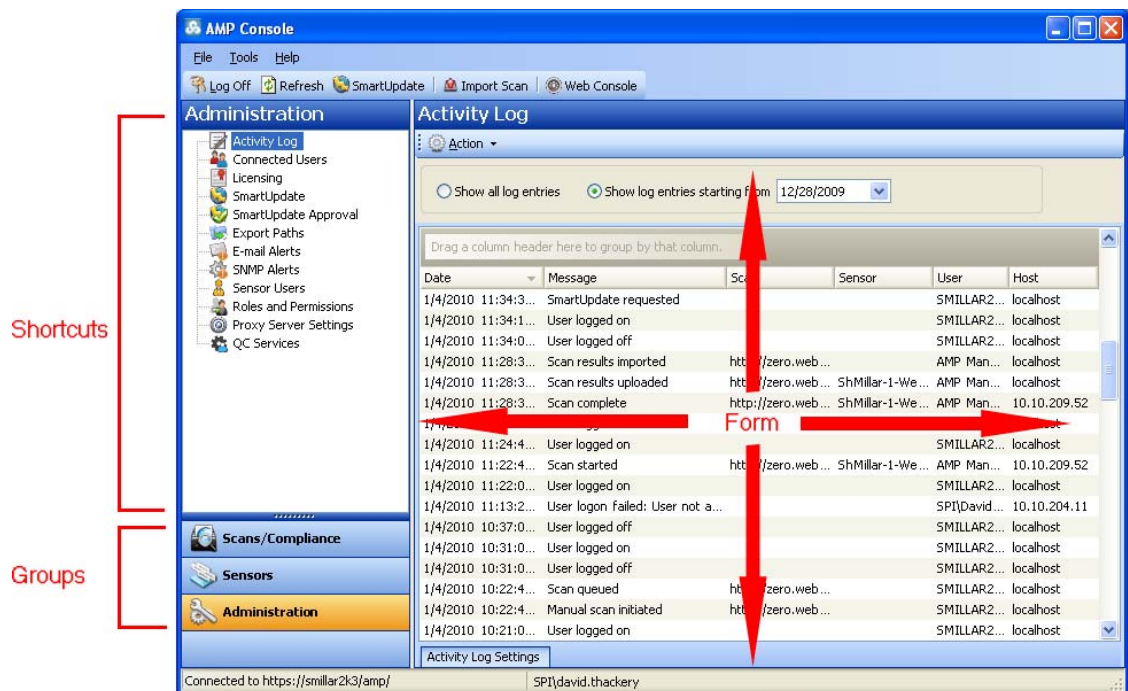
- The AMP Console, used for administrative and security functions.
- The AMP Web Console, a browser-based application used for running and managing scans.

This chapter describes the AMP Console.

User Interface

The AMP Console user interface comprises five main areas:

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



The buttons in the Groups pane represent groups of AMP functions.

Click a group button to expose associated shortcuts.

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

In the preceding illustration, the user selected the **Administration** group and then clicked the **Activity Log** shortcut to display a form containing a time-stamped history of AMP Manager activities.

The Group pane contains the following buttons:

Button	Associated Shortcuts
Scans/Compliance	Scan Queue Scan Policies Compliance Templates
Sensors	Sensors
Administration	Activity Log Connected Users Licensing Smart Update Smart Update Approval Export Paths E-Mail Alerts SNMP Alerts Sensor Users Roles and Permissions Proxy Server Settings QC Services

For forms containing lists (grids), you can initiate commands related to a list or to the individual objects on a list. Simply select an object and then choose a command from the **Action** menu (or from the shortcut menu that appears when you right-click an object). The availability of commands depends on the status of the selected object and the permissions granted to you by your assigned role (although system administrators have no restrictions on the functions they can perform).

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

Menu / Button	Description
File	Allows you to: <ul style="list-style-type: none">• Log off the application.• Refresh the display.• Exit the application.
Tools	Allows you to: <ul style="list-style-type: none">• Manually initiate a Smart Update.• Configure options for the console.• Launch a tool included in the HP toolkit.• Launch the Report Designer.
Help	Allows you to: <ul style="list-style-type: none">• Open this Help file.• Open your e-mail application to send an e-mail to HP Support.• Open the About Web Console dialog.
Log On/Off	Log on to or log off from the console application.
Refresh	Refresh the display.
Smart Update	Manually initiate a Smart Update call to the HP server.
Web Console	Log on to the AMP Web Console.

Scans/Compliance Group

The **Scans/Compliance** group contains three shortcuts:

- Scan Queue
- Scan Policies
- Compliance Templates

Scan Queue

For each scan that is running or waiting to run, this form displays (by default) the name assigned to the scan, the scan's priority, the date and time the scan request was created, the sensor that will conduct the scan, the scan's status, and the organization and project.

Select a scan request and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a request. The availability of commands depends on the status of the selected scan and on the permissions granted to you by your assigned role. To learn more about roles and permissions, see [Roles and Permissions](#) on page 55.

The commands are:

Command	Definition
Stop	Abort the scan. The results, although incomplete, are available for inspection.
Suspend	Halt the scanning process. You can resume the scan at the point at which it was interrupted.
Resume	Continue the scanning process following a suspension.
Delete	Remove the scan from the AMP database.
Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns should appear in the list.

Scan Policies

This form lists all policies configured in your environment. See [Appendix B, Policies and Components](#), for a description of each policy and its components.

Select a policy and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a policy. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
View	View the selected policy. You must install Microsoft SQL Server Express Edition SP1 before you can view or edit policies. Double-clicking the policy name also loads the policy into the Policy Manager.
Copy	Create a copy of the selected policy. After you rename the policy, the Policy Manager opens and loads the selected policy, allowing you to edit it. Once edited and saved, the policy is added to the list of scan policies.
Delete	Delete the selected policy from the repository. Prepackaged policies cannot be deleted.
Rename	Change the name of a custom policy, Prepackaged policies cannot be renamed (except when copied).
*Import	Import a policy from a standalone HP scanner.
*Export	Export a policy to a standalone HP scanner. Prepackaged policies cannot be exported.

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

Compliance Templates

This form lists all compliance templates configured in your environment. For each template, the list specifies the name, product, system, organization, and the date it was last updated. A check mark in the **System** column indicates that the template is one of the prepackaged templates distributed with AMP (as opposed to a template customized by the user).

Select a template and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a template. The availability of commands depends on the permissions granted to you by your assigned role.



Note: You must install Microsoft SQL Server Express Edition SP1 before you can edit or view compliance templates.

The commands are:

Command	Definition
View	View a template.
Copy	Copy the selected template.
Delete	Remove the selected template from the repository, unless the policy has “read only” status.

Command	Definition
Rename	Change the template name; used for creating a custom template.
*Import	Import a template from a standalone HP scanner.
*Export	Export a template to a standalone HP scanner.

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

The available templates are described below:

21CFR11

Part 11 of Title 21 of the United States Code of Federal Regulation (commonly abbreviated as “21 CFR 11”) includes requirements for electronic records and electronic signatures. To assist medical companies in compliance, the US Food and Drug Administration (FDA) has published guidance for the proper use of electronic records and electronic signatures for records that are required to be kept and maintained by FDA regulations. The guidance outlines “criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.”

Due to the law and FDA guidance, medical companies and organizations dealing with highly sensitive medical information are being required to ensure that electronic records and electronic signatures are trustworthy, reliable, and generally an equivalent substitute for paper records and handwritten signatures. As interaction between equipment, operators, and computers becomes commonplace, it is important to establish a secure means to communicate and store information.

Basel II

Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The BCBS is the international rule-making body for banking compliance. In 2004, central bank governors and the heads of bank supervisory authorities in the Group of Ten (G10) countries endorsed the publication of “International Convergence of Capital Measurement and Capital Standards: a Revised Framework,” the new capital adequacy framework commonly known as Basel II.

Basel II essentially requires banks to increase their capital reserves or demonstrate that they can systematically and effectively control their credit and operational risk. The framework defines operational risk as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events,” and highlights hacking and information theft through inadequate systems security as loss events. While banks around the world are experts at managing risk by virtue of operating in global financial markets, they are relatively new at understanding and controlling the risks inherent with operating online banking systems and keeping customer data secure.

Banks that practice effective information and systems security are able to demonstrate to regulators that they should qualify for lower capital reserves through reduced operational risk. The Basel II framework insists that banks demonstrate that an effective system of policies and processes are in place to protect information and that compliance to these policies and processes is ensured, but is not prescriptive in how banks should implement security

policies and processes. The international standard ISO/IEC 17799 Code of Practice for Information Security Management provides guidelines for implementing and maintaining information security and is commonly used as a model for managing and reporting operational risk related to information security in the context of Basel II.

CA OPPA

The California Online Privacy Protection Act (OPPA) was established in 2003 to require all businesses and owners of commercial web sites in the state of California to conspicuously post and comply with a privacy policy that clearly states the policies on the collection, use, and sharing of personal information. The policy identifies the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.

Any business, organization, or individual that operates a Web site that collects private personal information for a person residing in the state of California is bound by the provisions of the law, so the California OPPA has a much greater impact nationally than is typical for state legislation.

CASB 1386

California Senate Bill 1386 has established the most specific and restrictive privacy breach reporting requirements of any state in the United States. The law was enacted to force businesses, organizations, and individuals holding private personal information for legitimate business purposes to inform consumers immediately when their personal information has been compromised. The law also gives consumers the right to sue businesses in civil court for damages incurred through the compromise of information. Any business, organization, or individual that holds private personal information for a person residing in the state of California is bound by the provisions of the law.

COPPA

The Children's Online Privacy Protection Act (COPPA) was enacted in 2000 to protect the online collection of personal information about children under the age of 13. COPPA's goal was to protect children's privacy and safety online in recognition of the easy access that children often have to the Web. The law requires that Web site operators post a privacy policy on the site and outlines requirements for Web site operators to seek parental consent to collect children's personal information in certain circumstances.

The law applies not only to Web sites that are clearly directed toward children but to any Web site that contains general audience content where the Web site operators have actual knowledge that they are collecting personal information from children. An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area.

DCID

This directive establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems. For purposes of this directive, intelligence information refers to sensitive compartmented information and special access programs for intelligence under the purview of the Director of Central Intelligence.

DoD Application Security Checklist Version 2

DISA Field Security Operations (FSO) conducts Application SRRs to provide a minimum level of assurance to DISA, Joint Commands, and other Department of Defense (DoD) organizations that their applications are reasonably secure against attacks that would threaten their mission. The complexity of most mission critical applications precludes a comprehensive security review of all possible security functions and vulnerabilities in the time frame allotted for an Application SRR. Nonetheless, the SRR helps organizations address the most common application vulnerabilities and identify information assurance (IA) issues that pose an unacceptable risk to operations.

Ideally, IA controls are integrated throughout all phases of the development life cycle. Integrating the Application Review process into the development lifecycle will help to ensure the security, quality, and resilience of an application. Since the Application SRR is usually performed close to or after the applications release, many of the Application SRR findings must be fixed through patches or modifications to the application infrastructure. Some vulnerabilities may require significant application changes to correct. The earlier the Application Review process is integrated into the development life cycle, the less disruptive the remediation process will be.

EU Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. Like all other European Union privacy legislation, this directive also requires that personal data be collected, stored, changed or disseminated only with a citizen's express consent and with full disclosure as to the use of the data. The directive also prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. The United States has developed a Safe Harbor framework for U.S. organizations that are required to comply with this directive.

EU Directive on Privacy and Electronic Communications

European Union Directive on Privacy and Electronic Communications is part of a broader "telecoms package" of legislation that governs the electronic communications sector in the European Union. The directive reinforces a basic European Union principle that all member states must ensure the confidentiality of communications made over public communications networks and the personal and private data inherent in those communications. The directive governs the physical communication networks as well as the personal data that is carried on it.

FISMA

The United States Congress passed the E-Government Act of 2002 in recognition of the importance of information security to the economic and national security interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity and availability. FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

GLBA

The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions must protect consumers' personal financial information. The main provision affecting Web application security in the financial industry is the GLBA Safeguards Rule.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) mandates the privacy and security of personal health information from the various threats and vulnerabilities associated with information management. For more information on using HP scanners to achieve HIPAA compliance, read the HIPAA white paper.

ISO 17799

This is the most commonly accepted international standard for information security management. Use this policy as a baseline in crafting a compliance policy to meet the needs of your organization and its security policy.

ISO 27001

ISO/IEC 27001 is an information security management system standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. The basic objective is to help establish and maintain an effective information management system using a continual improvement approach. ISO 27001 specifies the requirements for the security management system itself. It is the standard, as opposed to ISO 17799, against which certification is offered. Additionally, ISO 27001 is "harmonized" with other management standards, such as ISO 9001 and ISO 14001.

JPIPA

Japan enacted the Personal Information Protection Act (JPIPA) in 2003 to protect individuals' rights and personal information while preserving the usefulness of information technology and personal information for legitimate purposes. The law establishes responsibilities for businesses that handle personal information for citizens of Japan and outlines potential fines and punishments for organizations that do not comply. The act requires businesses to communicate their purpose in collecting and using personal information. They must also take reasonable steps to protect personal information from disclosure, unauthorized use or destruction.

NERC

The North American Electric Reliability Council (NERC) was established in 1968 with the mission of ensuring that the electric system of the United States is reliable, adequate and secure. After President Bill Clinton issued Presidential Decision Directive 63 in 1998 to define infrastructure industries critical to the United States' national economy and public well-being, the U.S. Department of Energy designated the NERC to act as the coordinating agency for the electricity industry, which was named one of the eight critical infrastructure industries.

NIST 800-53

The United States Congress passed the E-Government Act of 2002 in recognition of the importance of information security to the economic and national interests of the United States. Title III of the act, entitled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology with developing

standards and guidelines to be used by all U.S. federal government agencies in implementing adequate information security as part of their information systems, underpinned by three security objectives for information systems: confidentiality, integrity, and availability.

OMB

This policy addresses major application security sections that were defined in December 2004 by the Office of Management and Budget for federal agency public Web sites. These are information resources funded in whole or in part by the federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-federal user group and support the proper performance of an agency function. Drop down section OWASP Top Ten

Many government agencies suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application.

OWASP Top 10 2004, 2007,2010

Many government agencies suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application. For more information on OWASP and its top 10 Web application vulnerabilities, visit <http://www.owasp.org/documentation/topten>.

PCI Data Security 1.2 and 2.0

The Payment Card Industry (PCI) Data Security Policy requires that all PCI Data Security members, merchants, and service providers that store, process or transmit cardholder data verify all purchased and custom Web applications, including internal and external applications.

PIPEDA

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is a new law that protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity. The Act, based on ten privacy principles developed by the Canadian Standards Association, is overseen by the Privacy Commissioner of Canada and the Federal Court. As of January 1, 2004, all Canadian businesses are required to comply with the privacy principles set out by PIPEDA. The Act covers both traditional, paper-based and on-line business.

Safe Harbor

The European Commission's Directive on Data Protection prohibits the transfer of personal data from European organizations to non-European Union nations and organizations that do not adequately protect the safety and privacy of personal data. Upon passage of this comprehensive European legislation, all businesses and organizations in the United States that share data with European Union organizations were obligated to comply with the regulations, which could have disrupted many types of trans-Atlantic business transactions. Due to the differences in approaches taken by the United States and European Union nations in protecting personal data privacy, the U.S. Department of Commerce, in consultation with the European Commission, developed a streamlined "Safe Harbor" framework through which U.S. organizations could comply with the Directive on Data Protection.

Organizations participating in the Safe Harbor are committed to complying with these seven principles designed to ensure that personal data is properly used, controlled and protected: Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement. Of particular significance to information technology:

The Notice principle requires organizations to inform individuals about the purposes for which it collects information, such as through a privacy policy.

The Security principle states that organizations will take reasonable precautions to protect personal data.

The Enforcement principle mandates that organizations have procedures in place for verifying that security commitments are satisfied, such as through comprehensive security testing.

Sarbanes-Oxley

The Sarbanes-Oxley Act, which falls under the umbrella of the U.S. Securities and Exchange Commission (SEC), was enacted on July 30, 2002. It focuses on regulating corporate behavior for the protection of financial records, rather than enhancing the privacy and security of confidential customer information. For more information on using HP scanners to achieve Sarbanes-Oxley compliance for your Web applications, read the Sarbanes-Oxley white paper.

UK Data Protection

The European Commission's Directive on Data Protection protects the fundamental rights of European Union citizens to privacy with respect to the processing of personal data. The primary focus of the directive is on the acceptable use and protection of personal data. The United Kingdom implemented the protections mandated by the directive through its Data Protection Act of 1998, summarized as follows:

- Personal data should be processed fairly and lawfully and only with consent.
- Personal data should be obtained only for specified and lawful purposes, and should not be further processed in any manner incompatible with those purposes.
- Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data should be accurate and kept up to date.
- Personal data processed for any purpose should not be kept for longer than is necessary for that purpose.
- Personal data should be processed in accordance with the rights of data subjects.
- Appropriate technical and organizational measures should be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data should not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Sensors

The Sensors group has one shortcut: Sensors.

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

This form displays the name, host name, status, and version of each sensor in the system. It also displays a status message for each sensor, indicating the result of the most recent action attempted.



Note: If you do not see a list of installed sensors, you must install the Microsoft .NET Framework version 3.5 Service Pack 1.

Select a sensor and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click a sensor. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Edit Sensor Details	Modify the name, location, and description.
Stop Scan	Abort the scan. The job cannot be resumed.
Suspend Scan	Interrupt the scan. The scan can then be manually resumed later.
Stop Discovery Scan	Abort the Discovery scan.
Pause Sensor	Temporarily halt the sensor. Note: This feature is a transient state held in memory on the sensor; it will not be remembered if the sensor service is ever restarted. For a long-term status, disable the sensor.
Continue Sensor	Enable the sensor after pausing. If the sensor was running a scan when paused, it will resume the scan automatically.
Enable/Disable	Turn the server on or off. You must be a member of the security administrator's group to enable a new sensor.
Rename Sensor	Change the sensor name.
Migrate Sensor	Reassign all schedules, pending scans, etc., from one sensor to another. Used primarily when installing a replacement sensor.
Delete Sensor	Disassociate the sensor from the AMP system. Note: To enable this command, you must stop the "AMP Sensor for WebInspect" service (Start/Control Panel/Administrative Tools/Services), taking the sensor offline.

Administration

The Administration group has 13 shortcuts:

- Activity Log
- Connected Users
- Licensing
- Smart Update

- Smart Update Approval
- Export Paths
- E-Mail Alerts
- SNMP Alerts
- Sensor Users
- Roles and Permissions
- Proxy Server Settings
- QC Services

Activity Log

The Activity Log lists each Assessment Management Platform activity. Each item includes (by default):

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

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

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

Select a command from the **Action** menu or from the shortcut menu that appears when you right-click an item in the list. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

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

Connected Users

This form lists each user who is currently logged in to the AMP system. Each item includes:

- Application Type

- Application Subtype
- Application Version
- The user's name
- IP Address
- The time and date when the user connected to the system
- Status

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

Select a command from the **Action** menu. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Release user license	Intended for use with licenses that permit multiple users. Disassociate the selected user from the license, allowing another user to occupy that position.
Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns should appear in the list.

Licensing

This form lists the license information and activation ID issued by HP for the operation of the Assessment Management Platform.

- Activation ID: The unique identifier for the license issued by HP.
- User Information: Information about the person to whom the license is granted.
- License Information
 - Licenses IP or Host Ranges: The IP addresses or hosts to which scans are restricted.
 - Bypass DNS: Indicates if the application is allowed to bypass a domain name server.
 - Valid To: The ending date of the period for which the license is valid.
 - Total Available Sensor Licenses: The maximum number of sensors that may be connected to AMP.
 - Total Available Client Licenses: The maximum number of clients that may be connected to AMP.
 - Total Scan Count: The maximum number of scans that may be conducted.
 - Maintenance End Date.
- License Usage Information

Important: If the AMP Console is installed on a machine that does not have Internet access, see [If You Are Not Connected to the Internet](#) on page 26 for instructions on activating the application.

Smart Update

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

Use Smart Update to obtain HP's latest adaptive agents, as well as vulnerability and policy information. Each time you log in to the AMP Console, it contacts the AMP server and downloads any available console binary updates.



If your AMP server cannot connect to the Internet, contact HP Support to obtain an offline SmartUpdate utility.

The Smart Update form contains a procedure log and a list of scheduled updates. You can obtain updates to the SecureBase, as well as binary updates for AMP-connected products such as WebInspect, through either a manual or scheduled process.

Select a command from the **Action** menu. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Clear Completed Updates	Delete the list of Smart Updates that have been completed.
Add Schedule	Open the <i>Smart Update Settings</i> window, allowing you to schedule a Smart Update.
Edit Schedule	Open the <i>Smart Update Settings</i> window, allowing you to modify the settings for the scheduled Smart Update selected in the Smart Update Schedules list.
Delete Schedule	Delete the Smart Updates selected in the Smart Update Schedules list.
History Column Setting	Open the <i>Column Setting</i> window, allowing you to specify which columns should appear in the Smart Update History list.

If you need to use a proxy server to communicate with the HP Smart Update database, select the **Proxy Server Settings** shortcut in the **Administration** group.

Smart Update Approval

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

The possible approval statuses are:

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

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

Typically, administrators prefer to update a single application instance and test it before performing a system-wide installation. This can be done by manually installing the updates on a test system. Sensor scans can be tested on a non-approved version of WebInspect by selecting the specific sensor when configuring the scan in AMP. Sensors that are running a non-approved version of WebInspect will not be used for AMP scans that are configured to run on “Any Sensor.”

Select a command from the **Action** menu or from the shortcut menu that appears when you right-click an item in the list. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

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

Export Paths

This form displays a list of destinations (paths) that may be used for saving scan results or exporting a report. AMP uses these paths to populate the drop-down list from which AMP Web Console users select a location for storing the data.

Select a path and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an export path. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Add	Open the <i>Export Path Settings</i> window, allowing you to specify export paths.
Edit	Open the <i>Export Path Settings</i> window, allowing you to modify export paths.
Delete	Remove the path from the form.

E-Mail Alerts

You can force AMP to send an e-mail message whenever certain events occur. Such a message is called an e-mail alert.

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

- The name of the alert
- The address of the e-mail recipient

- The IP addresses of scanned sites that may elicit an alert
- The events or actions about which the recipient is to be notified
- The organization
- The project

SMTP Settings

If necessary, click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings if you plan to send e-mail notifications for specific AMP events.

SMTP Server—The name of the server used for outgoing e-mail.

SMTP Port—The numbered port used for outgoing e-mail.

Sender—The text that will appear in the “From” field of the e-mail. It need not be a valid e-mail account, but it must be in the format `text@text.text`, where text is any text you care to enter.

Use SSL—Select this check box to use Secure Sockets Layer (SSL) protocol.

Authentication—If your server requires authentication, select **Basic** or **NTLM**, and then provide a user name and password.

Commands

Select an alert and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an alert. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Add	Specify settings for an alert.
Edit	Modify settings for an alert.
Delete	Remove the alert from the form.

SNMP Alerts

You can force AMP to send a Simple Network Management Protocol (SNMP) message whenever certain events occur. Such a message is called an SNMP alert.

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

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

SNMP Settings

If necessary, click **SNMP Settings** (at the bottom of the form) to configure SNMP settings if you plan to send SNMP notifications for specific AMP events.

SNMP Host—The IP address of the server that will receive the alert and forward it to the intended recipient.

SNMP Port—The port number for SNMP alerts on the SNMP host.

Community—An SNMP community is a text string that acts as a password for authenticating messages sent between the management station (the SNMP manager) and the device (the SNMP agent). There are typically two types of community names:

- A read-only community name that allows queries of the agent.
- A read-write community name that allows an NMS to perform set operations.

Commands

Select an alert and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an alert. The availability of commands depends on the permissions granted to you by your assigned role.

The commands are:

Command	Definition
Add	Specify settings for an alert.
Edit	Modify settings for an alert.
Delete	Remove the alert from the form.

Sensor Users

This form lists all WebInspect sensor accounts, which exist to run scans on behalf of AMP users.

You must create at least one Windows user account and assign it to the sensor service.

To add an account:

- 1 Click **Add**.
- 2 Enter the account assigned to the sensor.
- 3 Click **OK**.

To remove an account:

- 1 Select an account from the list.
- 2 Click **Remove**.

Roles and Permissions

This form allows you to assign administrators for three security levels (system, organization, and project). Administrators can then define roles, assign users to roles, and configure other security-related parameters. For an overview of the AMP hierarchical structure, see [Assign Administrators and Create Roles](#) on page 34.

Roles

A role is simply a named collection of permissions. You can allow other users to access the AMP system and limit the functions they are allowed to perform by assigning them to a role. Also, a single user may be a member of more than one role.

The roles for each security level (system, organization, and project) contain a different set of permission categories. Each category contains multiple permissions, such as Can Create, Can View, Can Update, Can Delete, etc.

System Roles

System roles contain the activity categories listed below.

- Activity Log
- Licensing
- SmartUpdate
- E-mail Alerts
- SNMP Alerts
- Export Paths
- Sensors
- QC (Quality Center) Service

Organization Roles

Organization roles contain the activity and object categories listed below.

- Blackouts
- Policies
- Compliance Templates
- Report Definitions
- Report Resources
- Scan Templates
- Discovery Scan Templates
- Report Templates
- E-mail Alerts
- SNMP Alerts
- Reports

Project Roles

Project roles contain the activity and object categories listed below. Note that project permissions apply to all sites within the project.

- Sites
- Assessments
- Scans
- Scan Templates
- Discovery Scans
- Discovery Scan Templates
- Scheduled Scans
- Scheduled Discoveries
- Reports
- Report Templates
- E-mail Alerts
- SNMP Alerts
- Blackouts
- HP Toolkit

Select an entry in the Project Hierarchy tree (AMP System, an organization, or a project) and then provide the information requested on each of the related tabs that appear in the Permissions section on the right-hand pane.

You can also choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an object in the Project Hierarchy tree. The commands are:

Command	Definition
Add Organization	Create an organization.
Rename Organization	Change the name of an organization.
Remove Organization	Delete an organization.
Add Project	Create a project.
Rename Project	Change the name of a project.
Remove Project	Delete a project
Role Membership	<p>Display roles assigned to a selected user or group.</p> <ol style="list-style-type: none">1 Enter an NT user or group name, or click Browse to select a user or group.2 Click Search. <p>If you enter your own user name or the name of a group of which you are a member, the program displays all the roles to which you are assigned.</p>

System Roles and Permissions

Creating an Organization

Use the following procedure to create an organization.

- 1 Select **AMP System** in the Hierarchy pane.
- 2 Click **Action** and select **Add Organization**.
Every system must have at least one organization.
- 3 On the *Create Organization* dialog, type a name for the organization and click **OK**.

Administrators Tab

To add or remove a system administrator:

- 1 Select **AMP System** in the Hierarchy pane.
- 2 Click the **Administrators** tab.
- 3 To add a system administrator:
 - a Click **Add**.
 - b Select a domain or work group in the **From this location** list.
 - c In the text box below, type a Windows account name.
 - d To verify the name, click **Check Names**.
 - e Click **OK**.
- 4 To delete a system administrator:
 - a Select a group or user name.
 - b Click **Remove**.

Roles Tab

To create a system role:

- 1 Select AMP System in the Hierarchy pane.
- 2 Click the **Roles** tab.
- 3 Click **Add**.

- 4 On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.



Having separate options for “Allowed,” “Unassigned,” and “Denied” may seem redundant in a binary world. However, it permits AMP to resolve conflicting permissions when a user is a member of more than one role. These are the controlling guidelines:

- “Allowed” outranks “Unassigned”—If the permission for a certain activity in Role A is “Allowed” and the permission for the same activity in Role B is “Unassigned,” then a user who is a member of both Role A and Role B may perform the activity.
 - “Denied” outranks “Allowed”—If the permission for a certain activity in Role A is “Allowed,” and the permission for the same activity in Role B is “Denied,” then a user who is a member of both Role A and Role B may not perform the activity.
 - “Unassigned” (only) equals “Denied”—If a user’s permission for a certain activity is “Unassigned” and no other permissions are assigned to that user in another role for the same activity, then the user may not perform the activity.
- 5 In the Permissions list, expand the nodes to view the activities associated with each category.
 - 6 To assign the same permission to all activities within a single category:
 - a Click the category name (such as “Activity Log”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.
 - 7 To change permission for a single activity:
 - a Click the activity name (such as “Can view log”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.

To assign groups or users to a role:

- 1 Select a name from the **Role name** list.
- 2 Click **Add** (on the far right of the Group or user names section).
- 3 On the *Select Users or Groups* dialog, select a domain or work group in the **From this location** list.
- 4 In the text box below, type a Windows account name.
- 5 To verify the name, click **Check Names**.
- 6 Click **OK**.

You can copy a role and keep it at the system level or assign it to an organization or project.

To copy a role:

- 1 Click the **Roles** tab.
- 2 Select a role from the **Role name** list.
- 3 Click **Copy**.

- 4 On the *Copy Role* dialog, select the organization or project to which the role will be assigned.

The same role can be assigned to multiple organizations and projects.

- 5 To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when placed in the location you specify.
- 6 To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying or moving a system role to an organization or a project.
- 7 Select the location where this copy of the role should be placed.

You cannot copy a role to an organization or project unless you are an administrator of that organization or project.

- 8 Click **OK**.

Organization Roles and Permissions

Administrators Tab

To add or remove an organization administrator:

- 1 Select an organization in the Hierarchy pane.
- 2 Click the **Administrators** tab.
- 3 To add an organization administrator:
 - a Click **Add**.

The *Select Users or Groups* window opens.
 - b Select a domain or work group in the **From this location** list.
 - c In the **Enter the object names to select** text box, type a Windows account name.
 - d To verify the name, click **Check Names**.
 - e Click **OK**.
- 4 To delete an organization administrator:
 - a Select a group or user name.
 - b Click **Remove**.

Configuration Tab

Maximum Scan Priority

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

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

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

Risk Levels

Each vulnerability in the HP SecureBase has an associated severity level ranging from critical to informational. SQL Injection, for example, is rated as critical, while Server Statistics Information Disclosure is considered a medium risk.

The AMP manager can calculate a “risk level” for each scan, based on the number of vulnerabilities detected, the severity of those vulnerabilities, and a value that you assign to each severity category.

In the text box next to each severity level, enter a numeric value.

The following example illustrates how AMP uses these values to calculate a risk level.:

Vulnerability Category	Assigned Risk (Weight)	Number of Vulnerabilities	Weighted Value
Critical	8	4	32
High	6	7	42
Medium	3	9	27
Low	1	7	7
Best Practices	1	7	7
Informational	0	12	0
Scan Risk Level Total = 115			

Roles Tab

To create an organization role:

- 1 Click **Add** (to the right of the **Role name** list).
- 2 On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.
- 3 In the **Permissions** list, expand the nodes to view the activities associated with each category.
- 4 To assign the same permission to all activities within a single category:
 - a Click the category name (such as “Blackouts” or “Policies”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.
- 5 To change permission for a single activity:
 - a Click the activity name (such as “Can create” or “Can view”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.

To assign users to a role:

- 1 Select a name from the **Role name** list.
- 2 Click **Add** (on the far right of the **Group or user names** section).
- 3 On the *Select Users or Groups* dialog, select a domain or work group in the **From this location** list.
- 4 In the text box below, type a Windows account name.
- 5 To verify the name, click **Check Names**.
- 6 Click **OK**.

You can create a copy of a role and place it at any level (system, organization, or project). You can also move a role from one organization to another (which will remove it from the original organization).



You cannot copy or move a role to an organization or project unless you are an administrator of that organization or project.

To copy or move a role:

- 1 Select a role from the **Role name** list.
- 2 Click **Copy**.
- 3 On the *Copy Role* dialog, select the organization or project to which the role will be assigned.

The same role can be assigned to multiple organizations and projects.

- 4 To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when copied to the location you specify.
- 5 To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying an organization role and assigning it to a project or the system.
- 6 Select the location where this copy of the role should be placed.
- 7 To place a copy of the role in the selected location, click **OK**.
- 8 To move the role from its original location to the selected location, click **Move**.

Resources Tab




You can specify which resources are available to an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them.

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

- 1 Select an item in the **Object Type** list.

If objects of the selected type have never been assigned, all instances of those object types are displayed in the **Available** column.

If object types have previously been assigned, then object types may be distributed between the **Available** and **Allowed** columns.
- 2 To move object types from the **Available** column to the **Allowed** column, select one or more object types and click .

- 3 To move all object types to the **Allowed** column, click .
- 4 To move selected object types from the **Allowed** column and return them to the **Available** column, select one or more object types and click .
- 5 To move all objects from the **Allowed** column and return them to the **Available** column, click .

Move/Copy Objects Tab

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

- 1 Select an organization from the Hierarchy tree.
- 2 Select an item from the **Object Type** list.
- 3 Click **Retrieve**.

All user-created objects of the selected type appear in the **Object Results** list.

- 4 Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.
- 5 Click **Move** or **Copy**.
- 6 On the *Move Objects* or *Copy Objects* window, select an organization from the **Target Organization** list.
- 7 (Optional) Select a project from the **Target Project** list.
- 8 Click **Move** or **Copy**.
- 9 If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list.

For example, if you are moving a user-created scan template from one organization to another, and that template uses a scan policy that is not in the target organization, then you must also move (or copy) the scan policy.

Similarly, when you move a site, all scans associated with that site must also be moved and therefore the scans constitute dependencies of the site. If one of those scans used a scan template, then the template is a dependency of the scan.

- 10 If objects appear in the **Object Dependencies** list, then for each dependent object, click the drop-down arrow in the **Action** column under Object Dependencies and select the appropriate action (such as **Move to**, **Copy to**, or **Allow**).
- 11 After you dispose of one dependency, AMP checks for additional dependencies. If any are discovered, you must also handle them, repeating this process until no additional dependencies are discovered.
- 12 If necessary, you can backtrack through the process and cancel individual steps by clicking **Back**. To discard all dependency activities and start again, click **Reset**.
- 13 When there are no dependencies or when all dependencies have been resolved, a dialog appears stating, "All dependencies have been satisfied. Would you like to commit?"
 - To complete the operation, click **Yes**.
 - To cancel the operation, click **No**.

Project Roles and Permissions

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

Creating a Project

Each organization can have one or more projects. Use the following procedure to create a project.

- 1 In the Hierarchy pane, select an organization.
- 2 Click **Action** and select **Add Project**.
The *Create Project* dialog appears.
- 3 Type a name for the project in the **Name** box.
- 4 If you want the project to have unrestricted access to all resources that are available to the organization, select **Allow access to all of the organization's current resources**.
- 5 Select the highest priority level that a user in this project may assign to a scan. Choices range from 1 (highest priority) to 5 (lowest priority).
If two or more scans are scheduled to occur during the same time period, the scan with the highest priority will take precedence. Your choices may be restricted by your organization.
- 6 In the **Scan Permissions** group, click **Add**.
- 7 In the **Host** box, type a host name (wild cards allowed), IP address, or IP address range, and click **OK**.
- 8 In the **Properties** group, you may:
 - a Change the IP address or host name.
 - b Change permissions for running a Web Site Assessment scan and Web Service Assessment scan.
 - c Change permissions for running a Discovery scan.
- 9 Click **OK** to close the *Create Project* dialog.

Notice that users who create an organization or project are automatically assigned as administrators of that organization or project.

Administrators Tab

To add or remove a project administrator:

- 1 Select a project in the Hierarchy pane.
- 2 Click the **Administrators** tab.
- 3 To add a project administrator:
 - a Click **Add**.
The *Select Users or Groups* window opens.
 - b Select a domain or work group in the **From this location** list.
 - c In the **Enter the object names to select** text box, type a Windows account name.

- d To verify the name, click **Check Names**.
 - e Click **OK**.
- 4 To delete a project administrator:
 - a Select a group or user name.
 - b Click **Remove**.

Configuration Tab

Maximum Scan Priority

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

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

IP and Host Permissions

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

- 1 Click **Add**.
A default IP address (192.168.1.1) appears in the **IP and Host Permissions** list and in the **Properties** pane.
- 2 In the **Properties** pane, replace the default IP address with the actual IP address, address range, or host name of a site that may be scanned by this project.
To specify a range of addresses, enter the lowest numerical address, followed by a dash (-), and then followed by the highest numerical address, such as 134.55.33.4-134.55.33.244.
You can also use wild cards, such as 134.55.33.* and www.mysite.*.
- 3 Select **Can Run Scan**, click the drop-down arrow that appears, and select either **True** (allowing scans to be run on the specified target) or **False** (prohibiting scans from being run).
- 4 Select **Can Run Discovery Scan**, click the drop-down arrow that appears, and select either **True** (allowing discovery scans to be run on the specified target) or **False** (prohibiting discovery scans from being run).
- 5 Repeat steps 1-5 to specify additional targets.

Roles Tab

- 1 Select a project in the Role Hierarchy pane.
- 2 Click the **Roles** tab.

To create a project role:

- 1 Click **Add** (to the right of the **Role name** list).
- 2 On the *New Role* dialog, enter a name for the role, select the default permission that will be assigned to each activity, and click **OK**.

- 3 In the **Permissions** list, expand the nodes to view the activities associated with each category.
- 4 To assign the same permission to all activities within a single category:
 - a Click the category name (such as “Blackouts” or “Policies”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.
- 5 To change permission for a single activity:
 - a Click the activity name (such as “Can create” or “Can view”).
 - b Click the drop-down arrow that appears on the far right end of the row.
 - c Select a permission.

To assign users to a role:

- 1 Select a name from the **Role name** list.
- 2 Click the **Role Users** tab.
- 3 Click **Add** (on the far right of the **Role Users** tab).
- 4 On the *Select Users or Groups* dialog, select a domain or work group in the **From this location** list.
- 5 In the text box below, type a Windows account name.
- 6 To verify the name, click **Check Names**.
- 7 Click **OK**.

You can create a copy of a role and place it at any level (system, organization, or project). You can also move a role from one project to another (which will remove it from the original project).

You cannot copy or move a role to an organization or project unless you are an administrator of that organization or project.

To copy or move a role:

- 1 Select a role from the **Role name** list.
- 2 Click **Copy**.
- 3 On the *Copy Role* dialog, select the organization or project to which the role will be assigned.

The same role can be assigned to multiple organizations and projects.

- 4 To retain the list of users assigned to this role, select **Copy Users**. Otherwise, the role will be copied, but no users will be associated with this role when copied to the location you specify.
- 5 To retain the permissions assigned to this role, select **Copy Permissions**. This option is not available when copying an organization role and assigning it to a project or the system.
- 6 Select the location where this copy of the role should be placed.
- 7 To place a copy of the role in the selected location, click **OK**.
- 8 To move the role from its original location to the selected location, click **Move**.





Resources Tab

You can specify which resources are available to projects within an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them. Of those 10 available, you might choose to allow only 5 to be used in your project.

- 1 Select an item in the **Object Type** list.

If objects of the selected type have never been assigned, all instances of those object types are displayed in the **Available** column.

If object types have previously been assigned, then object types may be distributed between the **Available** and **Allowed** columns.

- 2 To move object types from the **Available** column to the **Allowed** column, select one or more object types and click .
- 3 To move all object types to the **Allowed** column, click .
- 4 To move selected object types from the **Allowed** column and return them to the **Available** column, select one or more object types and click .
- 5 To move all objects from the **Allowed** column and return them to the **Available** column, click .

Move/Copy Objects Tab

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

- 1 Select a project from the Hierarchy tree.
- 2 Select an item from the **Object Type** list.
- 3 Click **Retrieve**.

All user-created objects of the selected type appear in the **Object Results** list.

- 4 Select one or more of the listed objects. If you select multiple objects, they cannot be moved or copied to different locations.
- 5 Click **Move** or **Copy**.
- 6 On the *Move Objects* or *Copy Objects* window, select an organization from the **Target Organization** list.
- 7 Select a project from the **Target Project** list.
- 8 Click **Move** or **Copy**.
- 9 If the object being moved or copied has dependent relationships with other objects, the related objects appear in the **Object Dependencies** list.

For example, if you are moving a user-created scan template from one organization to another, and that template uses a scan policy that is not in the target organization, then you must also move (or copy) the scan policy.

Similarly, when you move a site, all scans associated with that site must also be moved and therefore the scans constitute dependencies of the site. If one of those scans used a scan template, then the template is a dependency of the scan.

- 10 If objects appear in the **Object Dependencies** list, then for each dependent object, click the drop-down arrow in the **Action** column under Object Dependencies and select the appropriate action (such as **Move to**, **Copy to**, or **Allow**).

- 11 After you dispose of one dependency, AMP checks for additional dependencies. If any are discovered, you must also handle them, repeating this process until no additional dependencies are discovered.
- 12 If necessary, you can backtrack through the process and cancel individual steps by clicking **Back**. To discard all dependency activities and start again, click **Reset**.
- 13 When there are no dependencies or when all dependencies have been resolved, a dialog appears stating, “All dependencies have been satisfied. Would you like to commit?”
 - To complete the operation, click **Yes**.
 - To cancel the operation, click **No**.
- 14 When a dialog appears informing you that all dependencies have been satisfied and prompting you to confirm that transfer, click **Yes**.

Proxy Server Settings

If you use a proxy server to communicate with HP for Smart Updates and licensing issues, select **Use Proxy Server** and then provide the requested information.

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

QC Services

This form lists all hosts on which a Quality Center service is installed (for the purpose of communicating with an HP Quality Center application).

To integrate with HP Quality Center, you must identify the location of the AMP Quality Center service (installed as part of the AMP installation procedure) that allows AMP to communicate with Quality Center, as well as the URL of the Quality Center application.

AMP’s “Send to Quality Center” feature supports only Quality Center versions 9.2, 10, and 11 (which has been renamed “Application Lifecycle Management”) with all applicable service packs installed. Also, Quality Center supports only the following operating systems: Windows XP SP2 and SP3, and Vista (32-bit). If using Application Lifecycle Management, you must also install the HP Application Lifecycle Management Connectivity Add-in.



Note that QC URLs are treated as organization and project resources. To allow users to create a QC profile in the Web console, you must make QC URLs available to the project through Roles and Permissions - Resources.

Select a QC service and then choose a command from the **Action** menu or from the shortcut menu that appears when you right-click an alert. The availability of commands depends on the permissions granted to you by your assigned role. Only system administrators (and those users assigned to a system administrator role that grants appropriate permissions) may create, view, update, or delete QC services.

The commands are:

Command	Definition
Add	Specify a Quality Center URL and version.
Edit	Modify a Quality Center URL and version.
Delete	<p>Remove the Quality Center URL and version from the form.</p> <p>Note: To delete a service, you must first disassociate the service from the URL. To do so:</p> <ol style="list-style-type: none">1 Select the service.2 Click the Action menu and select Edit.3 On the <i>QC Service</i> dialog, click QC URLs.4 Clear the check box of the URL associated with the service.

When a QC service is installed, the installation program creates the file `QualityCenterService.conf`, which identifies the port number used by the service, specifies whether or not the service uses Secure Sockets Layer (SSL) protocol, and contains the certificate's serial number.

To specify the service used for communicating with HP Quality Control:

- 1 Click the **Action** menu and select **Add**.

There are two groups of QC Service settings:

- General
- QC URLs

- 2 Using the General settings, enter a host name (or IP address) of the resource on which the Quality Center service is installed.

Note: If you intend to use SSL, you must enter the machine name of the computer on which the service is installed. See [Certificates](#) on page 69 .

- 3 Enter the port number used by the service. The default port number is 8001. If you changed the port number after installing the service (by editing the `QualityCenterService.conf` file), enter the port number you specified.
- 4 If communication uses Secure Sockets Layer protocol, select **Use SSL**.

If you select this option, two additional settings appear.

- a **Allow Non-trusted Server Certificate**—The HP certificate created during QC service installation will be regarded by your server as non-trusted. Select this check box to allow use of this certificate or a non-trusted certificate that you alternatively specify in the `QualityCenterService.conf`.
- b **Use a client certificate**—If you authenticate the AMP server to the QC service, select this option and enter the serial number of the client certificate. The certificate must reside on the AMP server and must be listed in the server's client store.

- 5 Click **Test**.

If you entered the correct information, the program returns the Quality Center version number, the assembly name, and the AMP version number.

- 6 Click **QC URLs**.

This panel displays a list of all Quality Center URLs previously defined for the system.

- 7 Select the check box next to the URL that you want to associate with the QC service you defined under the General settings (steps 2-4).

To add a URL:

- a Click **Add**.
 - b In the **URL** box, enter the complete URL for the application, such as:
`http://qc.mysite.com/qcbin/`
 - c Click **OK**.
- 8 Click **OK**.

Certificates

When installing a QC service, the installation program creates a certificate and sets the Common Name to be the machine name of the computer on which the service is installed. If you are using SSL, you must specify this machine name in the **Host** text box. If you try to use a DNS name or IP address, then when you click **Test**, the program will display an error message indicating that the identity check failed.

Similarly, if you create your own certificate to use in place of the one created by the installation program, the machine name, DNS name, or IP address you enter in the **Host** text box must match the Common Name specified in your certificate.

For information on modifying the Quality Center service attributes, see [Quality Center Service Installation](#) on page 18.

Common AMP Console Tasks

Configure the Console

Use the following procedure to specify settings for the AMP Console.

- 1 From the **Tools** menu, select **Options**.
- 2 To refresh the display of AMP information periodically, select the **Automatically refresh display** check box and specify how often (in seconds) the display should be updated.
- 3 Click **OK**.

Suspend a Scan

After a scan has started, you can suspend it and then later restart it at the point at which it was suspended.

To suspend a scan:

- 1 Click the **Scans/Compliance** group.
- 2 Click the **Scan Queue** shortcut.
- 3 Select the scan you want to suspend.
- 4 From the **Action** menu, select **Suspend**.

-or-

Right-click a scan request and select **Suspend** from the shortcut menu.

The scan request displays a status message of “Suspended (Manual).”

Resume a Suspended Scan

To resume a suspended scan:

- 1 Click the **Scans/Compliance** group.
- 2 Click the **Scan Queue** shortcut.
- 3 Select the scan you want to resume.
- 4 From the **Action** menu, select **Resume**

-or-

Right-click a scan request and select **Resume** from the shortcut menu.

If the sensor that started the scan is available, then that sensor will reload the scan data and resume scanning.

If the sensor that started the scan is now running a different scan, then that sensor will compare the priority of both scans. If the first (suspended) scan has a lower priority, the sensor will place it back in the queue and continue running the current scan. If the first scan has a higher priority, the sensor will suspend the second scan (placing it in the queue), reload the data from the first scan, and resume scanning.

Resumed scans are always assigned to the same sensor on which the scan was initiated.

Stop a Scan

To stop a scan:

- 1 Click the **Scans/Compliance** group.
- 2 Click the **Scan Queue** shortcut.
- 3 Select the scan you want to stop.
- 4 From the **Action** menu, select **Stop**.

-or-

Right-click a scan request and select **Stop** from the shortcut menu.

The scan request is removed from the list.

Pause a Sensor

Use this function to pause a sensor. If a scan is running on that sensor, the job will be suspended.

This feature is used when conducting maintenance on the machine that contains the sensor, or when you simply want to prevent the sensor from accepting any scans.

- 1 Click the **Sensors** group.
- 2 Select the sensor you want to pause.

- 3 Select **Pause Sensor** from the **Action** menu (or from the shortcut menu that appears when you right-click a sensor).

Continue a Sensor

Use this function to enable a sensor that you previously disabled by using the Pause command. If a scan was running on that sensor when the sensor was paused, the scan will resume.

- 1 Click the **Sensors** group.
- 2 Select the sensor you want to continue. “Paused” must appear in the Status column.
- 3 Select **Continue Sensor** from the **Action** menu (or from the shortcut menu that appears when you right-click a sensor).

Perform a Smart Update

Use Smart Update to download HP’s latest adaptive agents and programs, as well as vulnerability and policy information.

To conduct a Smart Update, click the **Smart Update** icon on the toolbar

- or -

click the **Tools** menu and select **Smart Update**.

Schedule a Smart Update

To schedule a Smart Update:

- 1 Click the **Administration** group.
- 2 Click the **Smart Update** shortcut.
- 3 Click the **Action** menu and select **Add Schedule**.
- 4 In the General category:
 - a Type a name for the event in the **Scheduled Smart Update Name** box.
 - b In the **Start Time** box, specify the date and time when Smart Update should run.
 - c To change the date, click the drop-down arrow and select a date from the calendar.
 - d To define an iterative process, click the Recurrence category (in the left column).
- 5 In the Recurrence category:
 - a Select the **Recurring** check box.
Note: Do NOT select this option if you want to schedule a one-time-only event.
 - b Use the **Pattern** group to select the frequency of the event (daily, weekly, monthly, or yearly) and then provide the appropriate information.
 - c Using the **Range** group, specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the Smart Update should occur.
- 6 Click **OK** to schedule the update.

View Activity Log

You can view information about significant events that occur and are logged by the AMP manager. Each event is sorted according to the time and date at which the event occurred.

To view the activity log:

- 1 Click the **Administration** group.
- 2 Click the **Activity Log** shortcut.

Create E-Mail Alerts

You can instruct the AMP manager to send an e-mail message to someone whenever certain events occur.

- 1 Click the **Administration** group.
- 2 Select the **E-mail Alerts** shortcut.

The E-mail Alerts form lists all alerts configured for the system.

- 3 Select **Add** from the **Action** menu, or right-click in the **E-mail Alerts** list and select **Add** from the shortcut menu.
- 4 On the *E-Mail Alert Settings* dialog, enter the name and e-mail address of the person who should receive the alert.
- 5 If the alert should be sent only when selected actions occur related to a specific IP address or range of IP addresses, enter the address or range. For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254). Separate multiple addresses or ranges with a semicolon. Enter an asterisk (*) to allow alerts for all IP addresses.
- 6 Select one or more actions that will trigger the alert.
- 7 Click **OK**.
- 8 If necessary, click **SMTP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol (SMTP) settings, as follows:
 - **SMTP Server**—The name of the server used for outgoing e-mail.
 - **SMTP Port**—The numbered port used for outgoing e-mail.
 - **Sender**—The text that will be appear in the “From” field of the e-mail. It need not be a valid e-mail account, but it must be in the format text@text.text , where text is any text you care to enter.
 - **Use SSL**—Select this check box to use Secure Sockets Layer (SSL) protocol.
 - **Authentication**—If your server requires authentication, select Basic or NTLM, and then provide a user name and password.

Create SNMP Alerts

You can force the AMP manager to send a Simple Network Management Protocol (SNMP) message whenever certain events occur.

- 1 Click the **Administration** group.
- 2 Select **SNMP Alerts**.

- 3 Click the **Action** menu and select **Add**.
- 4 Enter a name for this alert in the **Name** box.
- 5 If the alert should be sent only when selected actions occur related to a specific IP address or range of IP addresses, enter the address or range. For a range, use a hyphen to separate the lower address from the higher (example: 111.222.254.254-125.254.254.254). Separate multiple addresses or ranges with a semicolon.

Enter an asterisk (*) to send e-mail alerts regardless of the IP address associated with the action.
- 6 Select one or more actions that will trigger the alert.
- 7 Click **OK**.
- 8 If necessary, click **SNMP Settings** (at the bottom of the form) to configure Simple Mail Transfer Protocol settings, as follows:
 - **SNMP Host**—The IP address of the server that will receive the alert and forward it to the intended recipient.
 - **SNMP Port**—The port number for SNMP alerts on the SNMP host.
 - **Community**—An SNMP community is a text string that acts as a password for authenticating messages sent between the management station (the SNMP manager) and the device (the SNMP agent). There are typically two types of community names:
 - A read-only community name that allows queries of the agent.
 - A read-write community name that allows a network management system to perform set operations.

Create Export Paths

To add or edit a path:

- 1 Click the **Administration** group.
- 2 Select the **Export Paths** shortcut.
- 3 In the **Path** box, enter path using the Universal Naming Convention
-or-

click the browse button to select a path from a tree diagram of the network.

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

- 4 Click **OK**.

6 AMP Web Console

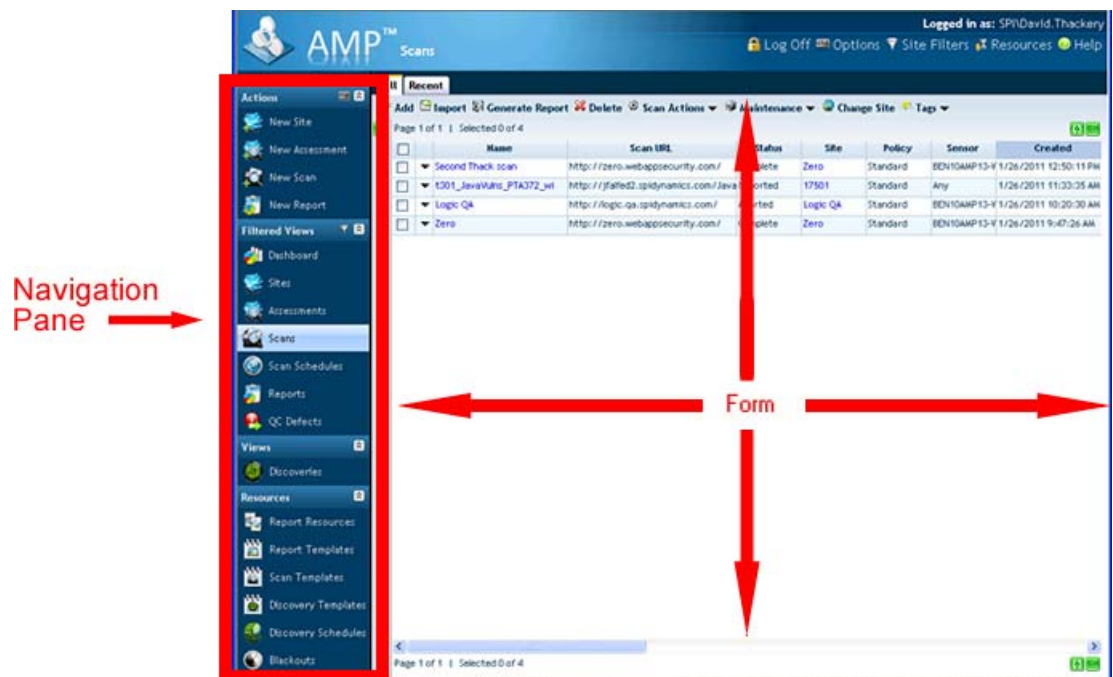
The Assessment Management Platform presents two separate user interfaces:

- The AMP Console, used for administrative and security functions.
- The AMP Web Console, a browser-based application used for conducting and managing scans.

This chapter describes the AMP Web Console.

The AMP Web Console user interface comprises three main areas:

- Toolbar
- Navigation pane
- Views and Forms




Click a button in the Navigation pane to display a form containing related information or controls associated with the selected function. In this illustration, the user selected the **Scans** button to display a form containing a .

Toolbar



The AMP Web Console toolbar contains the following icons:

Log Off	Logs you off the AMP Web Console application.
Options	Opens the <i>Configure Options</i> window, allowing you to set AMP Web Console options and select a default project.
Site Filters	Opens the <i>Configure Site Filters</i> window, allowing you to specify the type of data displayed in filtered views.
Resources	Opens the HP Assessment Management Platform home page.
Help	Opens the Help file.

In addition, you can click the AMP logo and name icon  to return to the home page of the AMP application.

Options

Click  on the toolbar to configure Web Console options. There are two categories:

- General
- Quality Center

General

Default Project

Select a default project that will be used by client applications that cannot specify a project.

A client application is WebInspect, QAIInspect, DevInspect, or any HP Application Security Center application that uses the AMP application programming interface. Client applications developed prior to AMP 8.10 will not be aware of AMP's new "project" object, so if AMP receives a call to create an object and the project is missing, the default project is used.

Each user account is associated with a default project.

Web Console Time Zone

Select the time zone in which you work. This setting is significant when you work in a time zone other than the one in which the AMP server resides.

Include Information Counts in Dashboard Charts

Informational items are not considered vulnerabilities. They simply identify interesting points in the site, or certain applications or Web servers discovered during an assessment or crawl. They normally are not represented in the dashboard charts.

Default to Advanced scan settings

When you initiate a scan, AMP displays one of the following option sets:

- **Advanced**—The full set of scanning options are presented.
- **Simple**—Only the scan template, site, and scan URL options are presented; for all other parameters, the scanner uses those settings specified in the Advanced option set.

If you select **Default to Advanced**, AMP displays the Advanced option set. If you do not select this option, AMP displays the Simple option set. In either case, however, you can switch from one to the other when you begin the scan.

Enable New Site Action

This option allows you to create a site from the AMP Web Console, using the New Site function in the Actions group.

Enable New Assessment Action

This option allows you to create an assessment from the AMP Web Console, using the New Assessment function in the Actions group.

Enable New Scan Action

This option allows you to initiate a scan from the AMP Web Console, using the New Scan function in the Actions group.

Enable New Scan Schedule Action

This option allows you to schedule a scan from the AMP Web Console.

Enable New Blackout Action

This option allows you to create and modify blackout periods from the AMP Web Console.

Enable New Report Action

This option allows you to generate a report, using the New Report function in the Actions group.

Quality Center

To integrate with HP Quality Center, you must specify a profile that describes the Quality Center server, project, defect priority, and other attributes.

Use the following procedure to create or edit a profile.

- 1 Select a profile from the **Profile Name** list, or click **Add** to create a profile name.
The remaining settings will be associated with this profile.
- 2 Select a server from the **Server URL** list.
- 3 Enter a user name and password that will allow you to access the Quality Center server.
This account must have permission (in the Quality Center application) to create defects. Also, this user name and password are not saved in the profile.
- 4 Click **Authenticate**.
If the authentication credentials are accepted, the server populates the **Domain** and **Project** lists.
- 5 Click **Connect**.
- 6 Click the **Defects** tab.

- a From the **State** list, select a state that will be assigned to all vulnerabilities reported to Quality Center using this profile.
 - b From the **Priority** list, select a priority that will be assigned to all vulnerabilities reported to Quality Center using this profile.
 - c Use the **Assign to** list to select the person to whom the defect will be assigned.
 - d Select an entry from the **Project found in** list.
 - e HP scanners (WebInspect, QAIInspect, and DevInspect) rate vulnerabilities as either informational, low, medium, high, or critical. You must specify how these vulnerability ratings should be mapped to Quality Center defect ratings when AMP publishes defects to the Quality Center system. If you select **Do Not Publish**, the vulnerability will not be exported. You must select at least one of the file mappings.
- 7 Click the **Subjects** tab and select a default subject.
 - 8 Click the **Fields** tab to display a list of optional/required fields defined for the Quality Center project.
 - a Click a field and enter or select the requested information.
 - b Click **OK**.
 - c Repeat until data for all desired and required fields has been entered. If you try to save your work without supplying a required field, AMP prompts you to enter it.
 - 9 Click **Save**.

Site Filters

AMP provides two default filters that determine which data will be displayed when using filtered views (which are Dashboard, Sites, Assessments, Scans, Scan Schedules, Reports, and QC Defects). These default filters are:

- **All**—Actually filters no data, allowing you to see all results.
- **Recent**—Limits the display of scan-related data to files created within the last three months.

Filters are represented by tabs that appear on each filtered view. You can create additional filters that allow you to view only those data that conform to a particular area of interest.

For more information and instructions on creating filters, see [Filtered Views](#) on page 79.

Navigation Pane

The Navigation pane is divided into four sections:

- Actions
- Filtered Views
- Views
- Resources

Selecting an option in the Navigation pane displays a corresponding form in the Form area.

Actions

New Site

The New Site action displays the Configure Site window, allowing you to specify the general characteristics of a site.

New Assessment

The New Assessment action displays the Configure Assessment window, allowing you to specify the general characteristics of an assessment.

New Scan

The New Scan action initiates a vulnerability scan by displaying windows that allow you to specify settings (options) for the scan. Either of two option sets are displayed:

- **Advanced**—The full set of scanning options are available. See [Advanced Scan Settings](#) on page 107 for details.
- **Simple**—Only the scan template, site, and scan URL options are available. See [Simple Scan Settings](#) on page 106 for details. For all other parameters, the scanner uses those settings specified in the Advanced option set.

You can switch from one option set to the other by selecting **Switch to Advanced** or **Switch to Simple** at the top of the dialog.

To specify which option set is displayed by default, click  **Options**.

New Report

The New Report action displays windows that allow you to specify settings for predefined enterprise reports. See [Enterprise Report Settings](#) on page 130 for details.



- To generate a scan report, select the Scans view, choose one or more scans, and then click the Generate Report icon.
- To generate an assessment report, select the Assessments view, choose one or more assessments, and then click the Generate Report icon

Filtered Views

Dashboard, Sites, Assessments, Scans, Scan Schedules, Reports, and QC Defects are termed “filtered views” because you can create filters that limit the display of data to a subset that you specify.

For very large installations, displaying details about all sites may consume considerable CPU, database, and intranet resources, even to the point where refreshing the display may interfere with or degrade system usability. To avoid this, or to simply focus on a specific subset of sites, you can use filters to prevent the display of information that is not in your area of interest.


The results will appear under a tab labeled with the filter name, and that tab will appear on all filtered views. The data displayed on each of those views, under the tab you create, is extracted exclusively from the sites that meet the criteria you specify when creating the filter.

Follow the steps below to create a filter:

- 1 Click the Site Filters icon on the toolbar.
- 2 On the *Configure Site Filters* page, click **New**.
- 3 Replace the default “New Filter” name with a name of your choice.
- 4 To force this filter to appear automatically (as a tab) whenever you log on, select **Default Filter**.
- 5 The following filter settings apply only to scans:
 - a If you do not want a filter based on the date, select **No Date Filter** and go to step 6.
 - b From the **Date Selector** list, choose either **Created**, **Started**, **Completed**, or **Latest**.

“Latest” is a relative reference to the other three times. Note that the “created” date for an imported scan is the date on which it was imported.
 - c Select either **Use Date Range** and specify a starting and ending date or **Use Relative Date** and specify the number of months.

Note: for a date range, If you omit a “From” date, all scans prior to the “To” date are listed. If you omit a “To” date, all scans occurring since the “From” date are listed.
- 6 The following filter settings apply only to sites:
 - a To view scans within a specific risk score range, select the **From** and **To** boxes and define the range by entering scores.
 - b To view data from sites associated with specific groups, clear the **Include All** check box and then move the group name from the **Available** column to the **Selected** column.
 - c To view data from sites associated with specific phases, clear the **Include All** check box and then move the phase name from the **Available** column to the **Selected** column.
 - d To view data from sites associated with specific tags, clear the **Include All** check box and then move the tag name from the **Available** column to the **Selected** column.

 If you select a combination of groups, phases, or tags, then only those sites that are members of all selected qualifiers will be displayed. For more information concerning phases and groups, see [About Phases and Groups](#) on page 137.
- 7 Click **Save**.

When you select a filtered view, a tab labeled with the filter name appears in the client area.

Dashboard

The Dashboard displays charts and graphs compiled from the AMP database. They are:

- **Top 10 Least Secure Sites**—A list of the sites having the highest risk scores. Click a risk score to view scan details. Click a site name to view site details.
- **Active Assessments**—A list of sites and the assessments to which they are assigned. Click an assessment name to view assessment details.
- **Last Completed Assessments**—A list of assessments whose status is “Complete.” Click the assessment name to view assessment details.
- **Worst Sites Trend (3 months)**—A graph showing the risk score of sites as calculated from scans that occurred during the past three months. Click the graph to view the data it represents.

- **Top 5 Vulnerabilities**—A bar chart showing the five vulnerabilities most often reported. Click the chart to view the data it represents.
- **Weighted Application Risk**—A bar chart showing, for each site, the weighted values for each vulnerability category (critical, high, medium, low, and informational). Click the chart to view the data it represents.
- **Severity Breakout**—A pie chart that illustrates the relative number of vulnerabilities by category. Click the chart to view the data it represents.
- **Weighted Risk Trend Analysis**—A graph that indicates, by month, the total number of vulnerabilities discovered in the last scan conducted for the month for each site in the defined groups. Click the graph to view the data it represents.
- **Vulnerabilities by Phase**—A bar chart that illustrates, for all sites assigned to each specific phase, the total number of vulnerabilities, delineated by severity. Click the chart to view the data it represents.
- **Lifecycle Vulnerability Trend (Weighted Score)**—A graph showing the total number of vulnerabilities detected, by phase, over a period of time. Click the graph to view the data it represents.

To rearrange the graphs and charts, click Dashboard Layout.

Dashboard Layout

Follow the steps below to rearrange the charts and graphs on the Dashboard.



Note: You cannot rearrange the dashboard if you are using Firefox.

- 1 Click the **Dashboard Layout** hyperlink (below the toolbar).
- 2 Click the **Close** button on each image to remove it from the display and add the image name to the Page Catalog.
- 3 To recreate the page:
 - a Select a zone from the **Add to** list.
 - b Select one or more images that you want to place in the selected zone.
 - c Click **Add**.
 - d Repeat until all images have been placed.
- 4 Click **Close**.

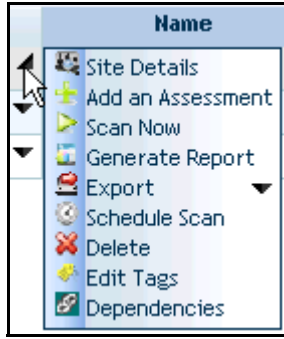
Sites

This form lists all sites that you have permission to view. If a scan request has been completed successfully, the list also contains starting and completion time stamps as well as the total number of vulnerabilities found, sorted by severity (if you have not modified the column settings).

This information is identical to the listings on the Scans form, except the information here is grouped by site.

To view or modify details about the site, click the site name.

You can perform additional functions by clicking the drop-down arrow next to a site name.



The functions unique to this menu are:

Add an Assessment—Displays the Configure Assessment form, where you can assign a name and description to a new assessment.

Scan Now—Allows you to configure settings for a scan of the selected site and initiate the scan.



Schedule Scan—Allows you to configure settings for the selected site, including the date and time when the scan should be conducted. When configuration is complete, the pending scan request is added to the Scan Schedules form.

Dependencies—Displays a list of reports and scans that are linked to this site. You cannot delete this site until you delete the associated scans (or move them to a different site) or delete the associated report. See [Dependencies](#) on page 101 for more information.

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

Icon	Function
Add	Create a site. See Site Settings on page 137 for a description of site settings.
Generate Report	Select options and create a report for the selected site.
Delete	Remove the selected site from the list.
Import	Load a comma-separated file containing site catalog details.
Export	Save a file containing site catalog details in either comma-separated value (csv) or Extensible Markup Language file (.xml) format.
Tags	Add, edit, or remove tags for the selected site. See Tags on page 110 for more information.

You can also use the icons illustrated below.

Icon	Function
	Repopulate the form.
	Change the number of rows on the page, modify column widths, specify which columns are displayed, and sort data by columns. For more information, see Editing the Layout on page 103.

Site Details

This form provides complete details about the selected site, categorized on the following tabs:

- **Assessments**—Lists all assessments associated with this site. Click an assessment name to view details for that assessment.
- **Scans**—Lists all scans conducted for the site. Archived scans appear in light gray italic font with the word “Archived” in the Status column. Icons allow you to add scans, generate reports, display vulnerabilities, delete scans, repeat scans, archive and restore scans, change sites for selected scans, create or modify tags. Click a scan name to view details for that scan.
- **Schedules**—Lists all scans scheduled for the site. Icons allow you to add or delete scheduled scans and create or modify tags. Click the schedule name to open the settings for the scan.
- **Reports**—Lists all reports generated for the site. Icons allow you to view or delete reports, cancel pending reports, and create or modify tags. Click a report name to view the report.
- **Properties**—Lists information about the site, including the site name and URL, the phase and/or group to which it is assigned, the scan template used, weight, auto-archive threshold, platform information, and the contact’s name and e-mail address.



For more information concerning phases and groups, see Site Settings on [page 137](#).

The auto-archive feature allows you to specify the number of days that scan data for this site will remain in the AMP database. When the threshold is reached, AMP compresses and exports the scan data to a reserved area, which noticeably improves performance. If the auto-archive value is set to zero, scans for this site are never automatically archived. Note that archiving does not occur immediately; it requires 30 minutes for scans to queue up for archiving when the archive threshold is reached.

- **Notes**—Allows you to create or view notations associated with the site.
- **Tags**—Lists all tags associated with the site. You can create tags and tag values, and assign or remove a tag name/value pair. If you edit the Sites layout to include a column for the tag, you can then group sites according to the values in the tag.
- **QC Defects**—Lists all vulnerabilities that were sent (or which a user attempted to send) to Quality Center. An icon allows you to resend defects to Quality Center.
- **Aliases**—Displays the primary URL for this site. To view, add, or change aliases associated with the primary URL, click the drop-down arrow next to the primary URL name and select **Edit**. For more information about aliases, see [Aliasing](#) on page 4.

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

Icon	Function
Scan Now	Display scan settings, as entered for the previous scan. You can modify the settings, if desired, before initiating the scan.
Schedule Scan	Open the Configure Scheduled Scan window, allowing you to enter settings for a scan and to schedule date and time on which the scan should occur.
Delete	Remove the selected site from the list.

Assessments

This form lists all assessments that you have permission to view.

An assessment is basically a collection of scans conducted against the same AMP-defined site. In addition, AMP correlates the results, identifying which vulnerabilities detected by one scan are identical to those detected by another, and combining them into a single reported vulnerability.

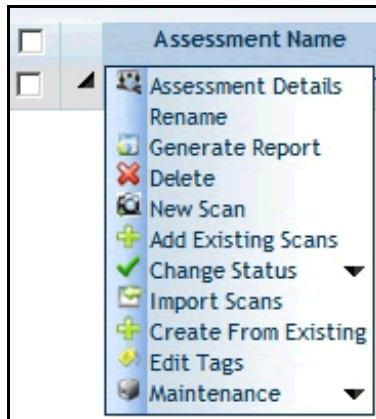
For each assessment defined in the system, the Assessments form displays (by default) the following information:

- Name assigned to the assessment
- Description
- Status
- System status
- Number of vulnerabilities detected (in columns sorted by severity)
- Risk score
- Number of scans
- Project name
- Organization name
- Site name

To view assessment details, click an assessment name.

To view site details, click a site name.

You can perform additional functions by clicking the drop-down arrow next to an assessment name.



The functions unique to this menu are:

Assessment Details—Display the Assessment Details form, which provides complete details about the selected assessment. You can also display this form by clicking the Assessment Name.

Rename—Modify the assessment name.

New Scan—Configure settings and run a scan to be included in this assessment.

Add Existing Scans—Select unassigned scans from the site with which this assessment is associated.

Change Status—Change status to In Progress, Completed, or Abandoned.

Create From Existing—Create a copy of the selected assessment.

Note: When scans are added to an assessment (through the **Add Existing Scans** command) or when a scan is initiated (through the **New Scan** command), AMP compares the results with existing scans in the assessment and determine which vulnerabilities are actually multiple occurrences of the same issue. It performs this correlation by comparing the location of the vulnerability (URL, parameters, etc.), the nature of the vulnerability (cross-site scripting, SQL injection, etc.) and other attributes. Matched vulnerabilities are grouped into a “finding.”

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

Icon	Function
Add	Create an assessment.
Generate Report	Select options and create a report for the selected assessment.
Delete	Remove the selected assessment from the list.
Tags	Add, edit, or remove tags for the selected assessment. See Tags on page 110 for more information.
Maintenance	Archive or restore (from archive) the selected assessment.

Assessment Details

This form provides complete details about the selected assessment, categorized on the following tabs:

- **Summary**—Provides summarized information about the findings associated with this assessment.
 - Findings: A bar graph showing correlated vulnerabilities by severity.
 - Findings to Vulnerabilities Comparison: A bar chart comparing uncorrelated and correlated vulnerabilities.
 - Findings by Type: A bar chart showing the number of vulnerabilities (by severity) for each analysis type (dynamic, static, runtime, hybrid, and manual)
 - Findings by Threat Classification: Displays the number of instances of the top three threats.
 - Most Vulnerable Scans: Displays vulnerability totals for the three scans having the most vulnerabilities.
- **Findings**—Lists the correlated vulnerabilities that were detected for this assessment. Icons allow you to export vulnerabilities; display “finding properties” (notes, false positive indicator, and ignore vulnerability indicator); send a vulnerability to Quality Center; add, edit, or remove tags; show or hide ignored vulnerabilities; merge findings.

Merging combines two or more findings into a single finding. For example, if “Finding 1” has 10 vulnerabilities and “Finding 2” has two vulnerabilities, merging them will create one finding with 12 vulnerabilities. To remove a vulnerability from a merged finding, click the drop-down next to the merged finding and select **Finding Details** (or simply click the Check Name of the merged finding). Then select the vulnerabilities you want to unmerge and click **Split Vulnerabilities**.

The drop-down menu next to each finding also allows you to edit or export findings, delete a finding, edit tags, and view finding details.

Clicking an entry in the Check Name column opens the Finding Details pane, which displays the following tabs containing information related to the selected finding:

- **Contributing Vulnerabilities:** A list of the vulnerabilities that were correlated into this finding.
 - **Request:** The HTTP request message that was used in the attack that discovered this finding.
 - **Response:** The HTTP response message.
 - **Runtime:** Source and sink information for findings detected by and imported from HP Fortify Security Scope.
 - **Source Code:** Stack trace and associated source code for findings detected by and imported from HP Fortify Source Code Analysis.
 - **Screenshots:** Screen capture images attached to the finding.
 - **Tags:** User-configurable tags designed to help group or sort various lists, such as scans, sites, blackout periods, and vulnerabilities.
 - **Properties:** A yes/no summary of manual findings, false positives, manual merges, and Quality Center IDs; also allows you to create a finding note, declare finding as a false positive, or ignore the finding.
- **Scans**—Lists all scans conducted for the assessment. Icons allow you to create a scan, add a scan to the assessment, remove a scan, mark a scan as contributing or non-contributing, generate a report, add/edit/remove tags, or start/stop/resume/suspend/repeat the selected scan. When scans are added to an assessment (or when a scan is initiated from the Assessment Details form), AMP compares the results with existing scans in the assessment and determine which vulnerabilities are actually multiple occurrences of the same issue. It performs this correlation by comparing the location of the vulnerability (URL, parameters, etc.), the nature of the vulnerability (cross-site scripting, SQL injection, etc.) and other attributes. Matched vulnerabilities are grouped into a “finding.”

Note: All findings from a non-contributing scan will be removed from the findings view.

The drop-down menu next to each scan allows you to view scan details or configuration, rename, copy, copy to schedule, copy to template, generate a report, access vulnerabilities, remove the scan from the assessment, mark as contributing or non-contributing, export the scan or scan settings, edit the tags, and start/stop/resume/suspend/repeat the scan.
 - **Reports**—Lists all reports generated for the assessment. Icons allow you to view or delete reports, cancel pending reports, and create or modify tags.

The drop-down menu next to each report allows you to view the report or report configuration, copy, rename, delete, cancel, send the report, or edit tags.
 - **Tags**—Displays tags used for the assessment. You can create tags and tag values, and assign or remove a tag name/value pair.
 - **Properties**—Displays the description, summary statement, and notes associated with this assessment.
 - **QC Defects**—Lists all vulnerabilities that have been sent to Quality Center as defects. Each defect includes (by default) the Change Request (CR) ID, status, vulnerable URL, status date, user name and created date.

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

Icon	Function
Delete	Delete the selected assessment.
Create from Existing	Copy the selected assessment and assign a different name and description.
Rename	Rename the assessment.
Report	Generate a report.
Change Status	Assign a status of In Progress, Complete, or Abandoned.
Archive	Archive the scan (which extracts the data, compresses it, and stores it in a separate database). This feature is available only if the status is Complete or Abandoned. Archived assessments can be deleted or restored.

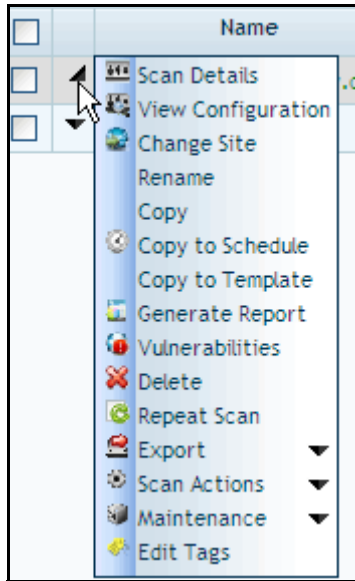
Scans

For each scan that has been uploaded to AMP, this form displays (by default) the following information:

- Name assigned to the request
- Target Web site URL or IP address
- Scan status
- Site to which this scan is assigned
- Policy used for the scan
- Sensor conducting the scan
- Date and time the scan request was created
- Date and time the scan started and completed
- Application type and version
- Results - If a check mark appears in the **Results** column, the number of vulnerabilities detected appears in columns sorted by severity
- Priority (used to determine precedence if a sensor scheduling conflict occurs)
- Risk
- Project name
- Organization name

Click a scan name to view scan details or (if the scan is part of an assessment) assessment details.

You can perform additional functions by clicking the drop-down arrow next to a scan name.



The functions unique to this menu are:

View Configuration—Allows you to view (but not edit) the settings used for the selected scan.

Rename—Allows you to assign a different name to the scan.

Copy—Copies all settings that were used for this scan and pastes them into the Configure Scan windows, allowing you to edit the settings before initiating the scan.

Copy to Schedule—Copies all settings that were used for this scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings before placing the scan request into the Scheduled Scans form.

Copy to Template—Copies all settings that were used for this scan and pastes them into the Configure Scan Template windows, allowing you to edit the settings before creating the template. You cannot copy an imported scan to a template.

Export—Exports the selected scan or the settings for the selected scan.

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

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

Icon	Function
Add	Start a new scan. See Advanced Scan Settings on page 107 for a description of scan settings.
Import	<p>Import a scan (WebInspect, QAIInspect, or Fortify scans). This feature invokes the AMP Scan Uploader, which allows you to assemble scans from AMP servers and upload them to a site (and optionally an assessment associated with the selected site).</p> <p>Note that scans can also be uploaded through the Scan Uploader service provided by the AMP Services Manager. If you scan a Web site with WebInspect, QAIInspect, or Fortify, you can copy the results to a location called a “dropbox.” The AMP Scan Uploader service (which is separate from the Scan Uploader utility) can access each dropbox periodically and, if files exist, upload those files to the AMP Manager. You can configure this feature through the AMP Services Configuration utility.</p>
Generate Report	Specify report settings for the selected scan.
Delete	Delete the selected scan.
Scan Actions	Stop, resume, or suspend a selected scan.
Maintenance	<p>Allows you to:</p> <ul style="list-style-type: none">• Archive all selected scans.• Restore selected archived scans .• Exclude selected scans from being archived automatically.• Include selected scans in the auto-archive function. <p>See Site Properties on page 83 for additional information on archiving scan data.</p>
Change Site	Reassign one or more scans to a different site.
Tags	Add, edit, or remove tags for the selected scan. See Tags on page 110 for more information.

Scan Details

This page provides complete details about the selected scan, categorized on the following tabs:

- **Scan Status**—Lists crawl and audit details, as well as information about the audit engines invoked during the scan. Also presents a detailed list sessions that occurred during the crawl, allowing you view the individual HTTP requests and responses.
- **Vulnerabilities**—Lists all vulnerabilities detected in the scan. Icons allow you to export vulnerabilities, view vulnerability properties, send vulnerabilities to Quality Center, create or modify tags, or show ignored vulnerabilities. Note that when viewing vulnerabilities for a scan that is running, a check mark appears in the Results column even though the scan is not complete. You cannot select items from the grid until the scan completes and results are uploaded successfully.

The drop-down menu next to each check ID allows you to view vulnerability details, export the vulnerability, and edit tags.

- **Scan Log**—Lists major events that occurred during the scan.

- **Reports**—Lists all reports generated for the site. Icons allow you to view or delete reports, cancel pending reports, and create or modify tags.

The drop-down menu next to each report allows you to view the report or report configuration, copy, rename, delete, cancel, send report, and edit tags.

- **Scan Activity Log**—Lists scan milestones, such as scan initiated, scan started, scan complete, etc.
- **Tags**—Displays tags used for the scan. You can create tags and tag values, and assign or remove a tag name/value pair.
- **QC Defects**—Lists all vulnerabilities that were sent (or which a user attempted to send) to Quality Center. An icon allows you to resend defects to Quality Center.

To obtain a graphical representation of the scan and easily investigate detected vulnerabilities, select **Scan Linkage** from the **Launch Analyzer** list.

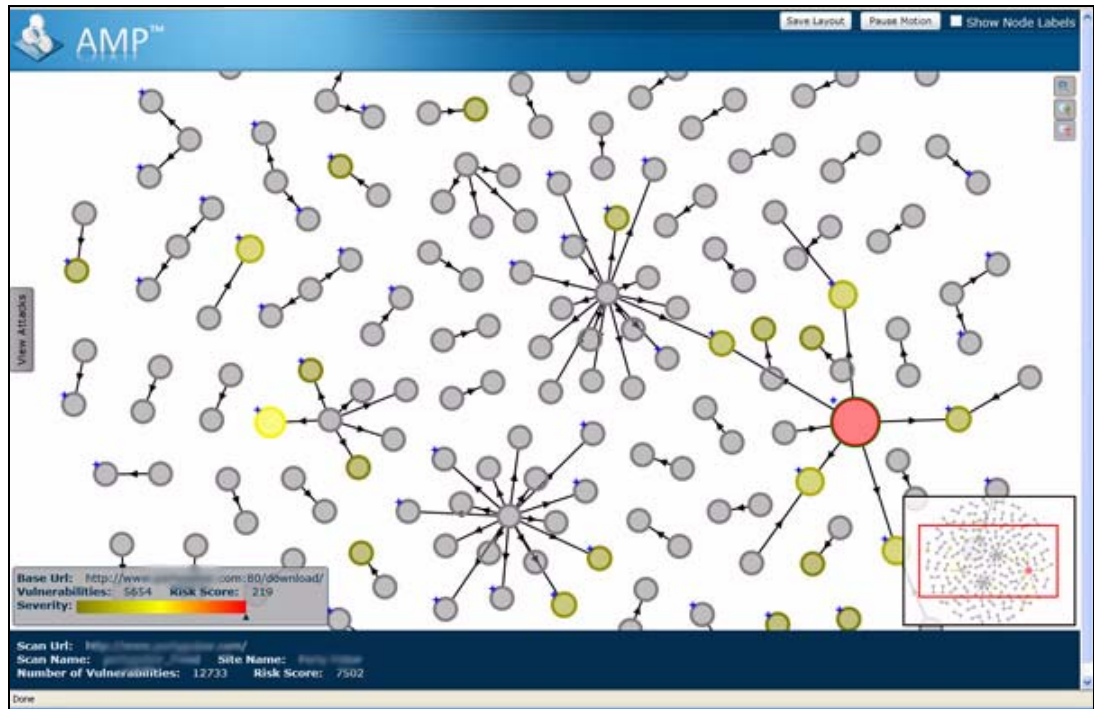
You can also perform additional functions using the icons at the top of the form.

Icon	Function
Configuration	View configuration settings for the scan.
Repeat scan	Repeat the scan.
Copy	Open the scan configuration forms using the settings from the selected scan, allowing you to modify some options and initiate a scan.
Copy to Schedule	Open the scan configuration forms using the settings from the selected scan, allowing you to modify some options and schedule a scan.
Delete	Delete the selected scan.
Change Site	Remove the scan from the current site and assign it to another site.
Rename Scan	Rename the scan.
Report	Generate a report.
Export	Export the scan to a file.
Scan Actions	Choose one of the following: <ul style="list-style-type: none"> • Stop the scan (if running) • Resume the scan (if paused) • Pause the scan (if running)
Maintenance	Choose one of the following: <ul style="list-style-type: none"> • Archive: Archive this scan • Include: Include this scan in the auto-archive function. • Exclude: Exclude this scan from being archived automatically. See Site Details on page 83 for additional information on auto-archiving.

Scan Linkage Analyzer

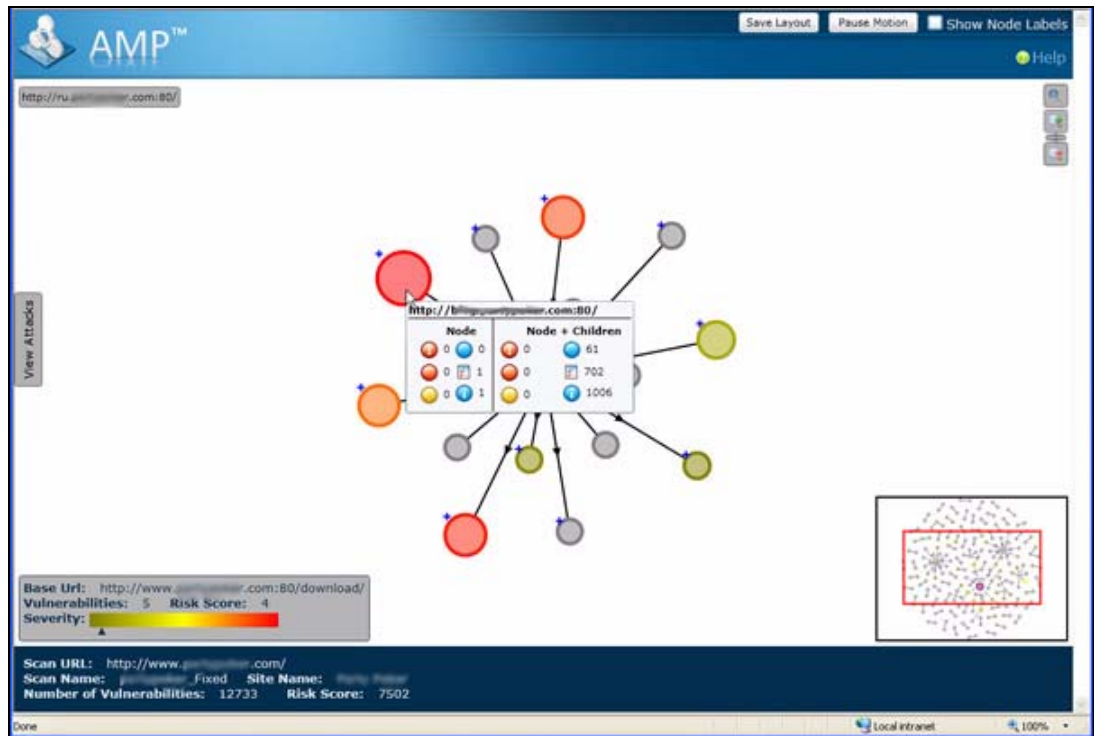
The Scan Linkage Analyzer presents a graphic visualization of the relationships between nodes in the hierarchical structure of the target site. Each node represents a page or folder. A plus sign (+) on the periphery of a node indicates the existence of at least one child node. The arrow on the line connecting two nodes points away from the calling node and toward the node referenced by a hyperlink.

To use this feature, you must install Microsoft Silverlight.

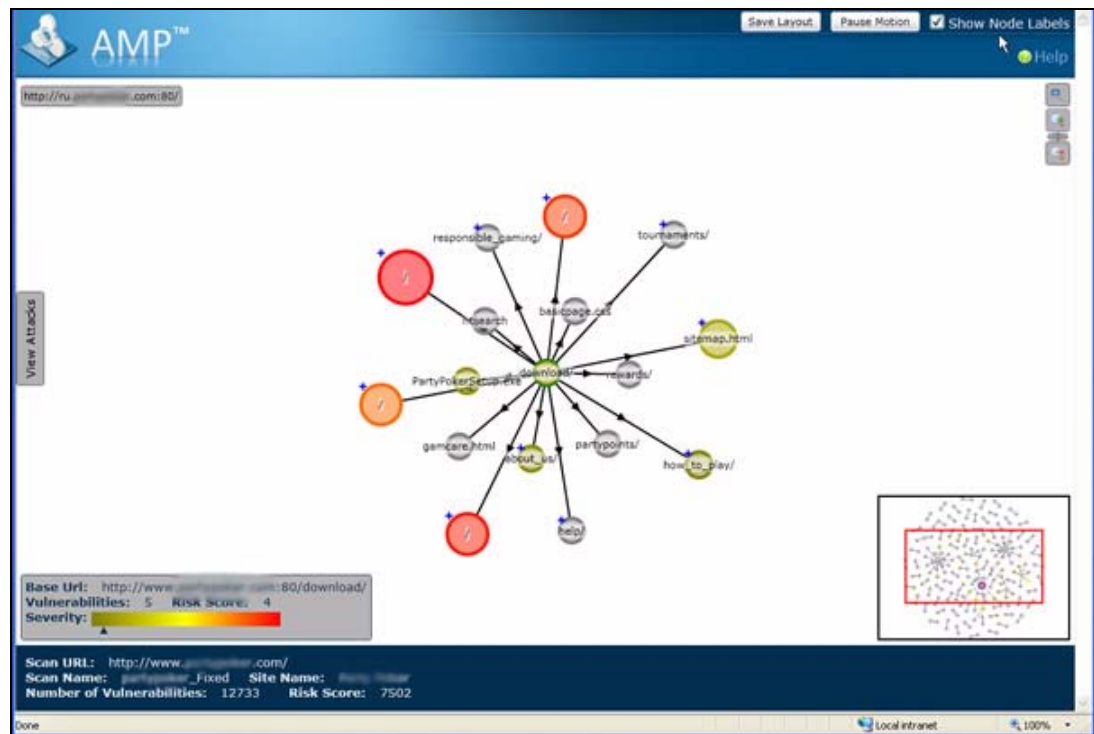


The size and color of each node (with the color ranging from grey to red), indicates the relative severity of the combined vulnerabilities discovered in that node and in its child nodes.

To begin investigating vulnerabilities, double-click (or Ctrl-click) a node. In the following illustration, the large red node above was selected. Hover the mouse pointer over a node to display statistics about vulnerabilities detected in that node and its children (if any).



Click **Show Node Labels** (in the upper right) to display file names (or folder indicators) for the nodes. You can also display labels temporarily by holding down the Shift key. Click **View Attacks** (on the middle left margin of the window) to display a list of vulnerabilities found in the selected node.



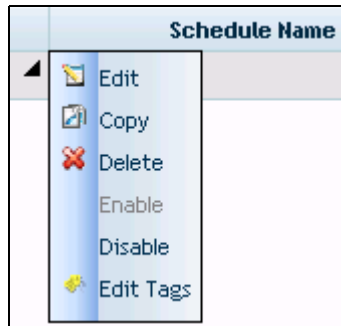
Buttons at the top of the window provide the following functions:

- **Save Layout**—Preserves the current view. When the current user accesses this feature again, the program presents the saved view.
- **Pause/Resume Motion**—This button enables or disables the property that programmatically separates nodes spatially.

Scan Schedules

This view displays information about each scheduled scan request.

You can perform additional functions by clicking the drop-down arrow next to a schedule name.



The functions unique to this menu are:

Edit—Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings for this scheduled scan request.

Copy—Copies all settings that were used for the selected scheduled scan and pastes them into the Configure Scheduled Scan windows, allowing you to edit the settings and create an additional scheduled scan request.

Enable—Activates a disabled scheduled scan request. Requests are enabled, by default, when created.

Disable—Deactivates a scheduled scan request. The request remains in the grid, but the scan will not be executed unless the request is enabled prior to the scheduled time and date.

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

Icon	Function
Add	Schedule a scan. See Scheduled Scan Settings on page 138 for a description of settings.
Delete	Remove the scheduled event.
Tags	Add, edit, or remove tags for the selected scheduled scan. See Tags on page 110 for more information.

Reports

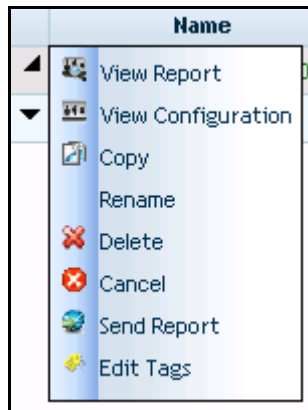
This form lists all reports that you have permission to view.

Each entry, by default, contains the following:

- Report name
- URL of the scanned site
- Status
- Description
- Name of the user who created the report
- Format
- Type
- Scan Count
- Template name
- Date and time the report was created
- Date and time the report was completed

To view a report, click the report name, or click the drop-down arrow next to a report name and select **View Report**.

You can perform additional functions by clicking the drop-down arrow next to a check ID.



The functions unique to this menu are:

- **View Configuration**—Allows you to view (but not edit) the settings used for the selected report.
- **Copy**—Copies all settings that were used for the selected report and pastes them into the Configure Report window, allowing you to edit the settings before generating the report.
- **Rename**—Allows you to assign a different name to the report.
- **Send Report**—Creates an e-mail containing a hyperlink to the report.

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

Icon	Function
View	View the selected report.
Delete	Remove the selected report.
Cancel	Halt a report that is being generated.
Tags	Add, edit, or remove tags for the selected report. See Tags on page 110 for more information.

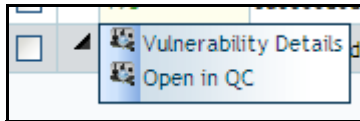
QC Defects

This form lists all vulnerabilities that have been sent to Quality Center as defects. For each item, the following information is displayed (by default).

- The identification number of the change request (CR)
- Status
- The URL containing the vulnerability
- Status date
- Created date
- User
- Profile used for submitting defect to Quality Center
- Project name
- Organization name
- Scan name
- Scan status

Click an entry in the CR ID column to launch HP Quality Center and open the selected defect.

You can perform additional functions by clicking the drop-down arrow next to a CR ID.



The function unique to this menu is:

- **Vulnerability Details**—Opens the Vulnerability Viewer, which presents detailed information about the vulnerability.

You can also perform one additional function using an icon at the top of the form

Icon	Function
Resend to QC	Resubmit the vulnerability to Quality Center. A dialog prompts you to enter a profile name, your user name, and your password. You can also click Manage to create a profile.

Views

Discoveries

This view displays information about each Discovery scan request.

A Discovery scan is an attempt to discover and identify Web servers within a range of IP addresses and ports that you specify. To do so, the scanner sends packets to the IP addresses and searches the HTTP response messages for specific information. For example, one of the predefined packets sent by the scanner contains the following HTTP request:

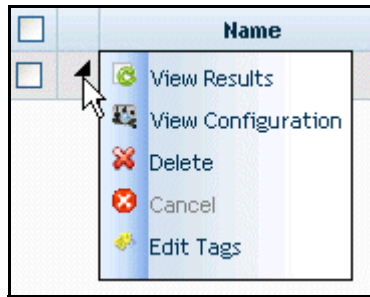
GET / HTTP/1.0

The scanner searches the HTTP response for the string “HTTP”; if it finds the string, it records 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.

For each Discovery scan request, the form displays the IP address and port ranges, the date and time the scan request was created, the time and date the scan started and completed, and the scan’s status.

To view the results for a listed Discovery scan, click an entry in the Name column.

You can perform additional functions by clicking the drop-down arrow next to a discovery name.



The functions unique to this menu are:

- **View Results**—Displays the Discovery Result Details form, which lists information about sites that were revealed as a result of a Discovery scan.
- **View Configuration**—Copies all settings that were used for this Discovery scan and pastes them into the Configure Discovery Scan windows. The settings cannot be edited.

You can perform additional functions by clicking the drop-down arrow next to a discovery name.

Icon	Function
Add	Create a Discovery scan request. See Discovery Scan Settings on page 139.
Delete	Remove the selected Discovery scan request
Cancel	Halt a Discovery scan that is being generated
Tags	Add, edit, or remove tags for the selected Discovery scan. See Tags on page 110 for more information.

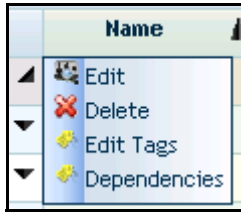
Resources

Report Resources

This view lists resources (such as graphics and style sheets) that are available for inclusion in a report.

To edit a resource, click an entry in the **Name** column.

You can perform additional functions by clicking the drop-down arrow next to a resource name.



The function unique to this menu is:

Edit—Displays the Configure Report Resource form, which allows you to edit the selected resource.

Dependencies—Displays a list of objects that are linked to this report resource. You cannot delete this resource until you remove it from the associated object (template or scan) or delete the associated object. See [Dependencies](#) on page 101 for more information.

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

Icon	Function
Add	Add a resource.
Delete	Delete the selected resource.
Tags	Add, edit, or remove tags. See Tags on page 110 for more information.

To associate a different file with the current resource name:

- 1 Click an image name in the Name column.
- 2 Click **Browse**.
- 3 Using the *Choose File* dialog, select an image.
- 4 Click **Open**.

The selected file is uploaded to the AMP server.

To add an image:

- 1 Click **Add**.
- 2 Enter a name for the image in the **Name** box.
- 3 Click **Browse**.
- 4 Using the *Choose File* dialog, select an image.
- 5 Click **Open**.

The selected file is uploaded to the AMP server.

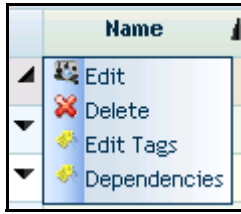
Note: You cannot add or edit stylesheets.

Report Templates

This view lists all report templates for which you have permission to view.

To view or modify template settings, click the template name.

You can perform additional functions by clicking the drop-down arrow next to a template name.



The function unique to this menu is:

Edit—Displays the Configure Report Template form, allowing you to modify the template. This function is available only for user-defined templates.

Dependencies—Displays a list of objects that are linked to this report template. You cannot delete this template until you either remove it from the associated object, delete the associated object, or cancel the incomplete report or scan. See [Dependencies](#) on page 101 for more information.

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

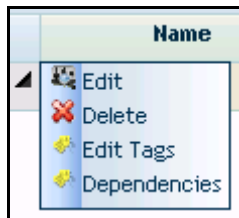
Icon	Function
Add	Create a report template. See
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template. See Tags on page 110 for more information.

Scan Templates

This view lists all scan templates that you have permission to view.

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

You can perform additional functions by clicking the drop-down arrow next to a template name.



The function unique to this menu is:

Edit—Displays the Configure Scan Template form, allowing you to modify the settings defined for the selected template.

Dependencies—Displays a list of scans, scheduled scans, and sites that are linked to this template. You cannot delete this template until you either delete the scheduled scan, assign a different template to the scheduled scan, delete the site, or cancel the scan (if it is currently running). See [Dependencies](#) on page 101 for more information.

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

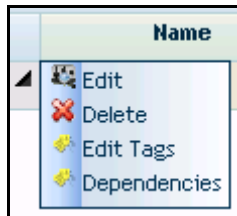
Icon	Function
Add	Create a template. See Scan Template Settings on page 133.
Add From	Select Oracle Settings to create a template that contains settings that are optimized for these sites.
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template. See Tags on page 110 for more information.

Discovery Templates

This form lists all discovery templates that you have permission to view.

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

You can perform additional functions by clicking the drop-down arrow next to a template name.



The functions unique to this menu are:

Edit—Allows you to configure settings for the selected discovery template.

Dependencies—Displays a list of discovery scans and scheduled discovery scans that use this template. You cannot delete this template until you either delete the scheduled discovery scan or assign a different template to it (or cancel the scan, if it is currently running). See [Dependencies](#) on page 101 for more information.

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

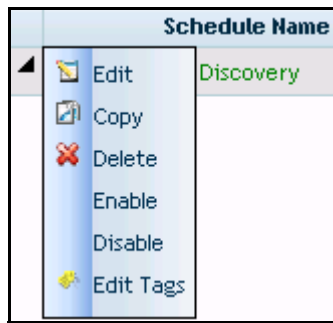
Icon	Function
Add	Create a template. See Discovery Template Settings on page 142.
Delete	Delete the selected template.
Tags	Add, edit, or remove tags for the selected template. See Tags on page 110 for more information.

Discovery Schedules

This form displays information about each Discovery scan that has been scheduled.

To view settings for a scheduled Discovery scan, click an entry in the Schedule Name column.

You can perform additional functions by clicking the drop-down arrow next to a schedule name.



The functions unique to this menu are:

Copy—Copies all settings that were used for the selected scheduled discovery scan and pastes them into the Configure Scheduled Discovery form, allowing you to edit the settings and create an additional scheduled discovery scan request.

Enable—Activates a disabled scheduled discovery scan request. Requests are enabled, by default, when created.

Disable—Deactivates a scheduled discovery scan request. The request remains in the grid, but the scan will not be executed unless the request is enabled prior to the scheduled time and date.

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

Icon	Function
Add	Schedule a Discovery scan. See Discovery Schedule Settings on page 145.
Delete	Delete the selected Discovery scan request.
Tags	Add, edit, or remove tags for the selected Discovery scan. See Tags on page 110 for more information.

Blackouts

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.



Note: Discovery scans are neither subject to nor controlled by blackout periods.

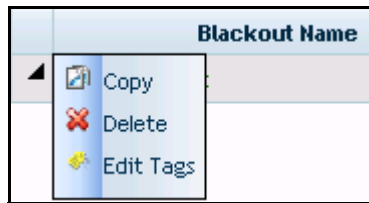
For each blackout defined in the system, the Blackouts form displays (by default) the following information:

- Blackout Name
- Type - Allow or deny scans during this period
- IP Range
- Status - Future, or Scans Disallowed, or Scans Allowed

- Recurrence - One time only, or the defined recurrence pattern
- Next Occurrence
- Next Occurrence (Target)
- Project Name
- Organization Name

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

You can perform additional functions by clicking the drop-down arrow next to a blackout name.



The function unique to this menu is:

Copy—Copies all settings that were used for the selected blackout and pastes them into the Configure Blackout form, allowing you to edit the settings and create an additional blackout object.

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

Icon	Function
Add	Schedule a blackout period. See Blackout Settings on page 148.
Delete	Delete the selected blackout period.
Tags	Add, edit, or remove tags for the selected blackout period. See Tags on page 110 for more information.

Dependencies

Certain objects in AMP are linked together, meaning that the existence of one object is dependent on another. You must dissolve this relationship before you are allowed to delete the parent object. For example, if you have a site that contains scans, you cannot delete that site unless you first delete the scans or assign them to a different site.

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


Parent Object	Dependent Objects
Discovery Template	<ul style="list-style-type: none"> • Scheduled discovery scan • Discovery scan (only if scan has not completed)
Scan Template	<ul style="list-style-type: none"> • Scheduled scan • Scan (only if scan has not completed) • Site

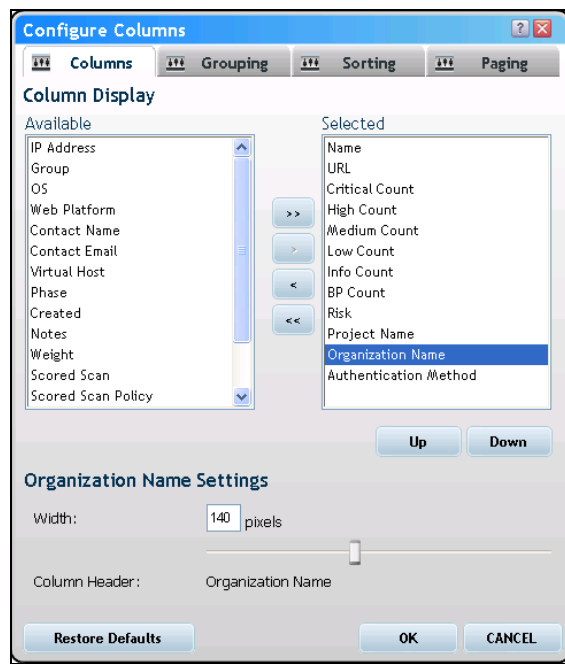
Parent Object	Dependent Objects
Site	<ul style="list-style-type: none"> • Scan • Report
Report Resources	<ul style="list-style-type: none"> • Discovery template • Report template • Scan template • Scan • Discovery scan • Scheduled scan • Scheduled discovery scan
Report Template	<ul style="list-style-type: none"> • Discovery template • Report (only if report has not completed) • Scan template • Scheduled discovery scan • Scheduled scan • Scan (only if scan has not completed) • Discovery scan (only if scan has not completed)

If you click a dependent object, AMP closes the *Dependencies* window and navigates to the appropriate form that allows you to dissolve the dependency. For example, if you click a scan name while viewing the list of site dependencies, AMP opens the *Scan Details* form, which allows you to delete the scan or assign it to a different site.

A limited number of dependencies can be listed. If you click **Export**, AMP displays all dependencies in a comma-separated values (CSV) file. You can then navigate to the appropriate form that allows you to dissolve the dependency by copying the dependent object's URL and pasting it into the Address bar of your Web browser.

Editing the Layout

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



This dialog has four tabs:

- Columns
- Grouping
- Sorting
- Paging

Columns

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



To change the column width:

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

To modify the name of a column header derived from a tag:

- 1 Select a column header.
- 2 Change the name in the **Column Header** box.
- 3 Click **Update**.

Five column names require further explanation. They are:


- Scored Scan Policy
- Scored Scan Created
- Scored Scan Started
- Scored Scan Ended

The vulnerability counts and risk scores displayed for a site are obtained from the last scan that was run in that site and for which results are available (or obtained from an imported scan, if that was the most recent activity). The “scored scan” attributes identify and are associated with that scan.

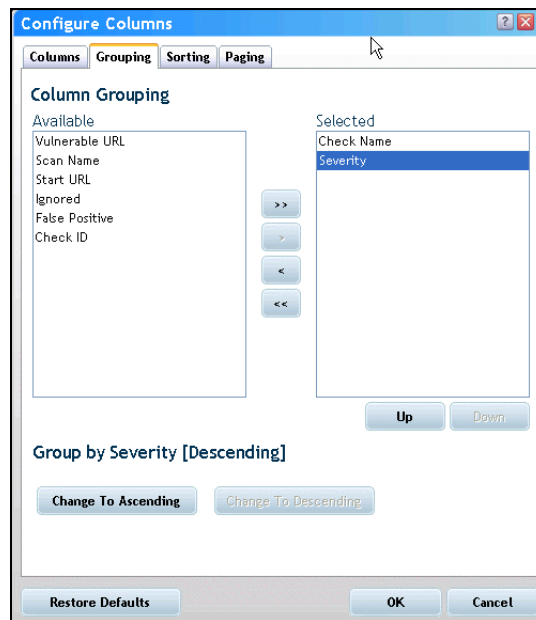
Grouping

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

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

- 1 In the Navigation pane under **Filtered Views**, click **Sites**.
- 2 Click a Site name (or click the drop-down arrow next to a site name and select **Site Details**).
- 3 On the Site Details form, click the **Scans** tab.
- 4 Click the name of a scan (or click the drop-down arrow next to a scan name and select **Scan Details**).
- 5 Click the Edit Layout icon .
- 6 On the *Configure Columns* dialog, click the **Grouping** tab.
- 7 In the **Available** list, select **Check Name** and click >.
- 8 Select **Severity** and click >.

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



Note: In addition to column headers, you can also use tags to group results.

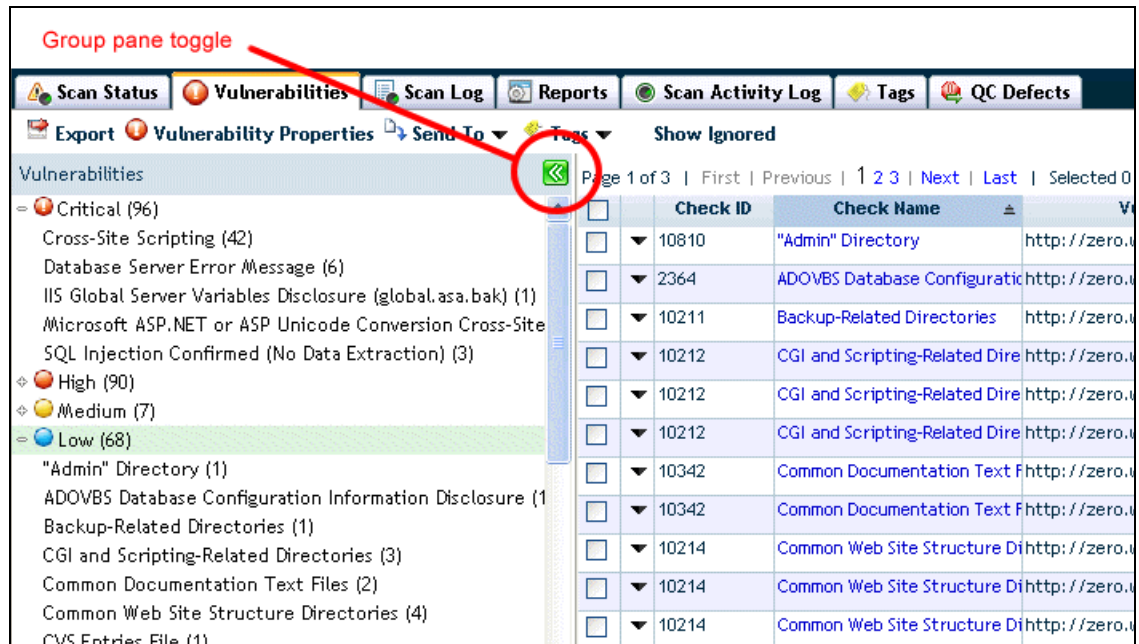
- 9 Select **Severity** and click **Up**.

The order determines how the data is sorted. In this example, vulnerabilities will be listed by severity and then by check name within each severity category.

- 10 Click **OK**.

When you return to the **Vulnerabilities** tab, the Group pane displays the grouped results. When you select a parent group name (such as Low), AMP displays those vulnerabilities having a severity level in the selected category. Redundant items (check names, in this example) are combined and the number of instances is reported in parentheses following the check name.

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



Sorting

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

Paging

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

Simple Scan Settings

Scan Template

Instead of specifying each individual setting that an HP scanner requires every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list.

Some templates allow you to change the settings. To do so, select the **Create custom scan from template** check box.

You are not required to use a template.

Scan

Enter a name for the scan.

Site

Click in the **Site Name** box and select a site from the list.

To create a site, enter a name, click **New Site**, and then provide the requested information.

Assessment

(Optional) Select an assessment from the **Name** list, or click **New Assessment** to create an assessment with which this scan will be associated.

Scan URL

In the **URL** box, type the complete URL or IP address of the site you want to examine.

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

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

Authentication

- **Use Network Authentication**—Select this option if server authentication is required. Then choose an authentication method and enter a user name and password.
- **Use Login Macro**—Select this option to use a macro for Web form authentication. When recording this type of macro, be sure to select **Enable Check For Logout** and then specify the application's log-out signature. Select a macro from the list or click **Browse** to locate a macro.

If, when recording the macro, you selected the Smart Credentials option, then you can enter a **Smart Credentials User Name** and **Smart Credentials Password**. When scanning the page containing the input control associated with this entry, the scanner will substitute these credentials for those used in the macro.

Reporting

Select this option to create a report of your scan findings. Then select either **Report Template** or **Report Definition**, and select a template or definition from the list.

Advanced Scan Settings

Categories of settings appear as groups in the left column. They are:

- Scan
- Scan Settings
- Crawl Settings
- Audit Settings
- Scan Behavior
- Reports
- Export

Each group has one or more subcategories.

Scan

General

Project

Select a project from the list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Scan Template** list. You are not required to use a template, but if you do, you may also select the following options:

- **Create custom scan from template**—When you select this option, all settings for this scan (including any deviations from the template) will be saved and permanently associated with the scan request. A rescan (or a scheduled scan) will use the saved settings and not the template. This is useful when you intend to conduct a series of identical scans and do not want to introduce any subsequent modifications that someone may make to the template. Your assigned role may not allow you to select this option.
- **Customize Scan Settings**—Select this option if you want to modify any of the scan settings prescribed by the template. If the selected template does not allow modifications, this option is not enabled.

Scan

Enter a name for the scan.

Site

Click inside the **Site Name** box to display a list of sites associated with the selected project. Only the first 20 sites are displayed. Choose a site name, or begin typing the site name. To create a site, enter a name and click **New Site**.

Assessment

(Optional) Select an assessment from the **Name** list, or click **New Assessment** to create an assessment with which this scan will be associated.

Scan URL

Select one of the following scan types.

- **Standard Scan**

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

- 1 In the **Start URL** box, type or select the complete URL or IP address of the site you want to examine. If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, you will not scan WWW.MYCOMPANY.COM or any other variation (unless you specify alternatives in the Allowed Hosts setting).

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

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

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

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

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

The scanner audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application.

Click **Browse** and select a macro.
- **Web Service Scan**

When performing a Web Service scan, the scanner crawls the WSDL site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. It then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

Click **Browse** to open a standard file-selection dialog and choose a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Priority

Select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority will take precedence.

Sensor

Select which sensor should conduct the scan. You can choose a specific sensor or select the **Any Available** option.

A sensor can perform only one scan at a time. If it is conducting a scan when another scan is scheduled to occur, then:

- If the currently running scan has a higher priority, the AMP Manager will place the second scan request in a queue until the first scan finishes or until another sensor becomes available.

- If the currently running scan has a lower priority, the AMP Manager will suspend that scan, assign the second scan request to that sensor, and then reassign the suspended request to the sensor when the higher priority scan is complete.

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

Tags

Tags are user-configurable fields designed to help you group or sort various lists, such as scans, sites, blackout periods, and vulnerabilities.

For example, you might want to categorize your sites geographically into four regions. To do so, you could create a tag named “Region” and assign four possible values to it: North, East, West, and South. You could then assign one of these tags to every site.

Similarly, you could create a tag named “Tester” and then assign as possible values the name of each Quality Assurance engineer who is responsible for conducting scans. You could then assign one of these tags to each scan, allowing you to group together all scans conducted by the same person.


To create tags:

- 1 Enter a name in the **Tag Name** box.
- 2 In the **Tag Value** box, enter one of the values to be associated with the tag name.
- 3 Click **Add**.
- 4 Repeat steps 2-3 to create additional values for the tag name.



Note: In some cases, if you create a tag using the same name as an existing tag, AMP will not accept the value you attempt to assign to that tag unless you select the option **Override existing tag values** (where available). This is the equivalent of editing the value assigned to a tag.

To select a tag for the function you are performing:

- 1 If necessary, click  to expand the list of values associated with a tag name.
- 2 Select a value.
- 3 Click **Add**.

To remove a tag:

- 1 Select a tag value in the **Selected** list.
- 2 Click **Remove**.

Scan Settings

The project and scan template settings are reproduced on each settings dialog, allowing you to change the project and scan template selection at any point. The description of these settings is not repeated in the following topics.

Method

Scan Mode

Select one of the following modes:

- **Crawl Only**—This option completely maps a site’s hierarchical data structure, but does not audit the site. The scan is saved to the database, allowing you to open the scan at a later date and conduct an audit.
- **Crawl and Audit**—In this mode, the scanner crawls the entire site, mapping the site’s hierarchical data structure, and conducting an audit.
- **Audit Only**—The scanner applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the Web site. No links on the site are followed or assessed.

Crawl and Audit Mode

Select one of the following:

- **Simultaneously**—As a scanner maps the site’s hierarchical data structure, it audits each resource (page) as it is discovered (rather than crawling the entire site and then conducting an audit). This option is most useful for extremely large sites where the content may possibly change before the crawl can be completed.
- **Sequentially**—In this mode, the scanner crawls the entire site, mapping the site’s hierarchical data structure, and then conducts a sequential audit, beginning at the site’s root. If you select this option, you can specify the order in which the crawl and audit should be conducted.
 - Test each engine type per session: The scanner audits all sessions using the first audit engine, then audits all sessions using the second audit engine, continuing in sequence until all engine types have been deployed.
 - Test each session per engine type: The scanner runs all audit engines against the first session, then runs all audit engines against the second session, continuing in sequence until all sessions are audited.

Scan Behavior

You can select any of the following optional behaviors:

- **Use a login macro for forms authentication**—This type of macro is used primarily for Web form authentication. It incorporates logic that will prevent the HP scanner from terminating prematurely if it inadvertently logs out of your application. When recording this type of macro, be sure to select **Enable Check For Logout** and then specify the application’s log-out signature. The drop-down list contains the names of all macros that have been uploaded to AMP. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.

If, when recording the macro, you selected the Smart Credentials option, then you can enter a **Smart Credentials User Name** and **Smart Credentials Password**. When scanning the page containing the input control associated with this entry, the scanner will substitute these credentials for those used in the macro.

- **Use a startup macro**—This type of macro is used most often to focus on a particular subsection of the application. It specifies URLs that the scanner will use to navigate to that area. It may also include login information, but does not contain logic that will prevent the scanner from logging out of your application. The scanner visits all URLs in the macro, collecting hyperlinks and mapping the data hierarchy. It then calls the Start URL and begins a normal crawl (and, optionally, audit). The drop-down list contains the names of all macros that have been uploaded to AMP. You can select one of these, or you can click **Browse** to locate a macro on your PC and upload it.

- **Auto-fill Web forms during crawl**—If you select this option, the scanner submits values for input controls found on all HTML forms. The values are extracted from a file you create using the Web form editor. Use the browse button to specify the file containing the values you want to use. Alternatively, you can select **Edit** (to modify the currently selected file) or **Create** (to record new Web form values).

General

Scan Details

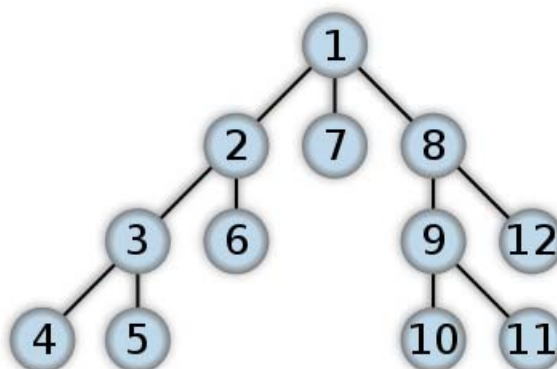
You may choose the following options:

- **Enable Path Truncation**—Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. The scanner truncates paths, looking for directory listings or unusual errors within each truncation. Example: If a link consists of `http://www.site.com/folder1/folder2/file.asp`, then truncating the path to look for `http://www.site.com/folder1/folder2/` and `http://www.site.com/folder1/` will cause the server to reveal directory contents or will cause unhandled exceptions.
- **Attach debug information in request header**—If you select this option, the scanner includes a “Memo:” header in the request containing information that can be used by support personnel to diagnose problems.
- **Case-sensitive request and response handling**—Select this option if the server at the target site is case-sensitive to URLs.
- **Compress response data**—If you select this option, the scanner saves disk space by storing each HTTP response in a compressed format in the database.
- **Maximum crawl-audit recursion depth**—When an attack reveals a vulnerability, the scanner crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions.

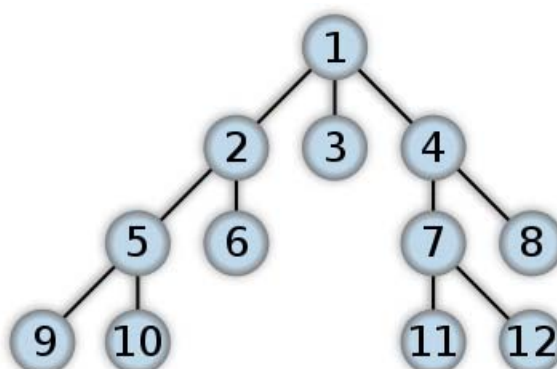
Crawl Details

You may choose the following options:

- **Crawler**—Select either **Depth First** or **Breadth First**.
Depth-first crawling accommodates sites that enforce order-dependent navigation (where the browser must visit page A before it can visit page B). This type of search progresses by expanding the first child node (link) and crawling deeper and deeper until it reaches a node that has no children. The search then backtracks, returning to the most recent node it hasn’t finished exploring and drilling down from there. The following illustration depicts the order in which linked pages are accessed using a depth-first crawl. Node 1 has links to nodes 2, 7, and 8. Node 2 has links to nodes 3 and 6



By contrast, breadth-first crawling begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



When performing a depth-first crawl, the scanner pursues links in a fashion that more closely represents human interaction. While slower than breadth-first crawling, the depth-first method accommodates applications that enforce ordering of requests (such as requiring the user to visit a “shopping cart” page before accessing the “check-out” page).

- **Enable keyword search audit**—A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
- **Perform redundant page detection**—Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, scanners would never be able to finish the scan. This option, however, allows scanners to identify and exclude processing of redundant resources.
- **Limit maximum single URL hits to**—Use this field to limit the number of times a single link will be followed during a crawl. Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL.
- **Limit maximum link traversal sequence to**—This option restricts the number of hyperlinks that can be sequentially accessed as the scanner crawls the site. For example, if five resources are linked as follows

Page A contains a hyperlink to Page B
Page B contains a hyperlink to Page C
Page C contains a hyperlink to Page D
Page D contains a hyperlink to Page E

and if this option is set to “3,” then Page E will not be crawled. The default value is 15.

- **Limit maximum crawl folder depth to**—The Crawl Depth value determines how deeply the scanner traverses the hierarchical levels of your Web site. If set to 1, the scanner drills down one level; if set to 2, the scanner drills down two levels; and so on. The maximum value is 1000.
- **Limit maximum crawl count to**—This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.
- **Limit maximum Web form submissions to**—Normally, when the scanner encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed.

There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named “State” contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form.

Use this setting to limit the total number of submissions that the scanner will perform.

Audit Details

If you select a depth-first crawl, you can also elect to retrace the crawl path for each parameter attack, as opposed to applying all attacks as the crawl progresses. This considerably increases the time required to conduct a scan.

Content Analyzers

Flash—If you enable the Flash analyzer, the scanner analyzes Flash files, Adobe’s vector graphics-based resizeable animation format.

JavaScript/VBScript—The JavaScript/VBScript analyzer is always enabled. It allows the scanner to crawl links defined by JavaScript or VisualBasic script, and to create and audit any documents rendered by JavaScript.

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

There are settings associated with the JavaScript/VBScript content analyzer. Click the analyzer name (JavaScript/VBScript) and configure the settings described below.

Parser Settings

- **Crawl links found from script execution**—If you select this option, the crawler will follow dynamic links (i.e., links generated during execution of JavaScript or Visual Basic script).
- **Reject script include file requests to offsite hosts**—Pages downloaded from a server may contain scripts that retrieve files and dynamically render their content. An example JavaScript “include file” request is:


```
<script type="text/javascript" src="www.badsite.com/yourfile.htm"></script>
```

The scanner will download and parse such files, regardless of their origin or file type, unless you select the Reject Script option. It will then download the files only if permitted by the parameters normally governing file handling (such as session and attack exclusions, allowed hosts, etc.).

- **Isolate script analysis (out-of-process execution)**—The scanner analyzes and executes JavaScript and VBScript to discover links to other resources. Applications or Web sites containing an inordinate number of links can sometimes exhaust the amount of memory allocated to this process. If this occurs, you can assign this function to a separate (remote) process, which will accommodate an infinite number of links. You may, however, notice a slight increase in the amount of time required to scan the site.
- **Create DOM sessions**—The scanner creates and saves a session for each change to the Document Object Model (DOM).
- **Verbose script parser debug logging**—If you select this setting AND if the Application setting for logging level is set to Debug, the scanner logs every method called on the DOM object. This can easily create several gigabytes of data for medium and large sites.
- **Log JavaScript errors**—The scanner logs JavaScript parsing errors from the script parsing engine.
- **Maximum script events per page**—Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999.

Requestor

Requestor Performance

Select one of the following:

- **Use a shared requestor**—The crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This replicates the technique used by previous versions of HP scanners and is suitable for use when maintaining state is not a significant consideration. You also specify the maximum number of threads (up to 75).
- **Use separate requestors**—The crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans. You also specify the maximum number of threads that can be created for each requestor. The crawl requestor can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the maximum for the audit requestor is 50. Increasing the thread count will increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.



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

Requestor Settings

You may select the following options:

- **Limit maximum response size to**—Select this option to limit the size of accepted server responses and then specify the maximum size (in kilobytes). The default is 1000 kilobytes. Note that Flash files (.swf) and JavaScript “include” files are not subject to this limitation.
- **Request retry count**—Specify how many times the scanner will resubmit an HTTP request after receiving a “failed” response (which is defined as any socket error or request timeout).
- **Request timeout**—Specify how long the scanner will wait for an HTTP response from the server. If this threshold is exceeded, the scanner resubmits the request until reaching the retry count. If it then receives no response, the scanner logs the timeout and issues the first HTTP request in the next attack series.

Stop Scan if Loss of Connectivity Detected

There may be occasions during a scan when a Web server fails or becomes too busy to respond in a timely manner. You can instruct the scanner to terminate a scan by specifying a threshold for the number of timeouts.

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

Session Storage

Log Rejected Session to Database

You can specify which rejected sessions should be saved to the database. This saved information can be used for two purposes.

- If you pause a scan, change any of the settings associated with the Reject Reasons in this panel, and then resume the scan, the scanner retrieves the saved data and sends HTTP requests that previously were suppressed.
- Hewlett-Packard support personnel can extract the generated (but not sent) HTTP requests for analysis. Sessions may be rejected for the reasons cited in the following table:

Reject Reason	Explanation
Invalid Host	Any host that is not specified in Default (or Current) Scan Settings/Scan Settings/Allowed Hosts.
Excluded File Extension	Files having an extension that is excluded by scan settings.
Excluded URL	URLs or hosts that are excluded by scan settings.

Reject Reason	Explanation
Outside Root URL	If the Restrict to Folder option is selected when starting an advanced assessment, any resource not qualified by the available options (Directory Only, Directory and Subdirectories, or Directory and Parent Directories).
Maximum Folder Depth Exceeded	HTTP requests were not sent because the value specified by the “Limit maximum crawl folder depth to” option has been exceeded.
Maximum URL Hits	HTTP requests were not sent because the value specified by the “Limit Maximum Single URL hits to” option has been exceeded.
404 Response Code	The option “Determine File Not Found (FNF) using HTTP response codes” is selected and the response contains a code that matches the requirements.
Solicited File Not Found	The option “Auto detect FNF page” is selected and the scanner determined that the response constituted a “file not found” condition.

Session Storage

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

Session Exclusions

The following settings apply to both the crawl and audit phases of a vulnerability assessment. To specify exclusions for only the crawl or only the audit, use the Crawl Settings - Session Exclusions or the Audit Settings - Sessions Exclusions.

Excluded or Rejected File Extensions

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

- **Reject**—The scanner will not request files of the type you specify.
- **Exclude**—The scanner will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.

Excluded MIME Types

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

Excluded or Rejected URLs and Hosts

You can identify a URL or host (using a regular expression) and then specify whether you want to exclude or reject it.

- **Reject**—The scanner will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed.

- **Exclude**—During a crawl, the scanner will not examine the specified URL or host for links to other resources. During the audit portion of the assessment, the scanner will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, select the **Exclude** option, but do not select **Reject**. For example, to check for broken links on URLs that you don't want to process, select only the **Exclude** option.

You must use a regular expression to designate a host or URL.

Example 1

To ensure that you ignore and never send requests to any resource at Microsoft.com, enter the following regular expression and select **Reject**.

Microsoft\.com

Note that the period (or dot) is preceded by a backslash, indicating that the next character is special (i.e., it is not the character used in regular expressions to match any single character except a newline character).

Example 2

Enter a string such as logout. If that string is found in any portion of the URL, the URL will be excluded or rejected (depending on which option you select). Using the logout example, the scanner will exclude or reject URLs such as logout.asp or applogout.jsp.

Example 3

If you enter /myApp / then the scanner will exclude or reject all resources in the myApp directory, such as: http://www.test.me /myApp /filename.htm.

If you enter /W3SVC[0-9]*/ then the scanner will exclude or reject the following directories:

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

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

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

Follow the steps below to add a URL or host:

- 1 Click **Add**.
- 2 From the **Type** list, select either **Host** or **URL**.
- 3 In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
- 4 Select one of the following:
 - **Reject**—Do not send request to targeted URL or host.
 - **Exclude**—Send request, but do not process response.
- 5 Click **Update**.

Allowed Hosts

Use the Allowed Host settings to add domains that may be crawled and audited. If your Web presence uses multiple domains, add those domains here. For example, if you were scanning “Wlexample.com,” you would need to add “Wlexample2.com” and “Wlexample3.com” here if those domains were part of your Web presence and you wanted to include them in the crawl or audit.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify `www.myco.com` as the scan target and you enter “myco” as an allowed host. As the scanner scans the target site, if it encounters a link to any URL containing “myco,” it will pursue that link and scan that site’s server, repeating the process until all linked sites are scanned. For this hypothetical example, the scanner would scan the following domains:

- `www.myco.com:80`
- `contact.myco.com:80`
- `www1.myco.com`
- `ethics.myco.com:80`
- `contact.myco.com:443`
- `wow.myco.com:80`
- `mycocorp.com:80`
- `www.interconnection.myco.com:80`

Note that if you specify a port number, then the allowed host must be an exact match.

If you use a regular expression to specify a host, select **Regex**.

HTTP Parsing

HTTP Parameters Used for State

If your application uses URL rewriting or post data techniques to maintain state within a Web site, you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named `SID`, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

```
.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01
```

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (`PHPSESSID` in this example), then the scanner will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include `userid=slbhkelvbk173dhj`. In this case, “userid” is the parameter you would identify.



Note: You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

The scanner can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, “1234567” is the session information:

```
http://www.onlinestore.com/bikes/(1234567)/index.html
```

The regular expression for identifying the parameter would be: `/\([\w\d]+\)/`

Determine State from URL Path

If your application determines state from certain components in the URL path, select this check box and add one or more regular expressions that identify those components. The defaults identify ASP.NET cookieless session IDs.

HTTP Parameters Used for Page (Resource) Identification

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

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

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

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

Ordinarily, the scanner would assume that these three requests refer to identical resources and would conduct a vulnerability assessment on only one of them. Therefore, if your target Web site employs this type of architecture, you must identify the specific resource parameters that are used.

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

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

To identify resource parameters:

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

The string you entered appears in the Parameter list. Repeat this procedure for additional parameters.

Advanced HTTP Parsing

Most Web pages contain information that tells the browser what character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) the scanner should use.

Filters

Use the Filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use the scanner or those who have access to the raw data or generated reports. If the text you specify is found, the scanner reports it on the **Information** tab as a “Hidden Reference Found” vulnerability.

Filter HTTP Request Content

Use this area to specify search-and-replace rules for HTTP requests.

Filter HTTP Response Content

Use this area to specify search-and-replace rules for HTTP responses.

Follow the steps below to add a regular expression rule for finding or replacing keywords in requests or responses:

- 1 In either the **Request Content** or the **Response Content** group, click **Add**.
- 2 From the **Section** list, select an area to search.
- 3 In the **Find Condition** box, type (or paste) the string you want to locate (or enter a regular expression that describes the string). You can also click the list button to insert regular expression elements.
- 4 Type (or paste) the replacement string in the **Replace** box.
- 5 For case-sensitive searches, select the **Case-Sensitive** check box.
- 6 Click **Update**.

Cookies/Headers

Standard Header Parameters

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

- **Include 'referer' in HTTP request headers**—Select this check box to include referer headers in HTTP requests. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
- **Include 'host' in HTTP request headers**—Select this check box to include host headers with HTTP requests. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Append Custom Headers

Use this section to add, edit, or delete headers that will be included with each audit the scanner performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when the scanner is auditing that site. You can add multiple custom headers. Follow the steps below to add a custom header:

- 1 In the top box, enter the header using the format <name>: <value>.
- 2 Click **Add**.

The new header appears in the list of custom headers.

Append Custom Cookies

Use this section to specify data that will be sent with the Cookie header in HTTP requests sent by the scanner to the server when conducting a vulnerability assessment. Follow the steps below to add a custom cookie:

- 1 In the top box, enter the header using the format <name>=<value>.

For example, if you enter

CustomCookie=ScanEngine

then each HTTP-Request will contain the following header:

Cookie:CustomCookie=ScanEngine

- 2 Click **Add**.

The new cookie appears in the list of custom cookies.

Proxy

Proxy Settings

Select one of the following options:

- **Direct Connection (proxy disabled)**—Select this option if you are not using a proxy server.
- **Auto detect proxy settings**—If you select this option, the scanner will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's web proxy settings.
- **Use Internet Explorer proxy settings**—Select this option to use the proxy server settings configured for the Internet Explorer browser on the machine that will conduct the scan.
- **Use Firefox proxy settings**—Select this option to use the proxy server settings configured for the Firefox browser on the machine that will conduct the scan.



Selecting to use browser proxy settings does not guarantee that you will access the Internet through a proxy server. If the Firefox browser connection settings are configured for “No proxy,” or if the Internet Explorer setting “Use a proxy server for your LAN” is not selected, then a proxy server will not be used

- **Configure a proxy using a PAC file**—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. For proxy servers accepting https connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information.
- 1 In the **Server** box, type the URL or IP address of your proxy server.
 - 2 In the **Port** box, enter the port number (for example, 8080).
 - 3 Select a protocol for handling TCP traffic through a proxy server: SOCKS4, SOCKS5, or standard.
 - 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.

Authentication

Scan Requires Network Authentication

Select this option if users must log on to your Web site or application. Then select an authentication method and specify a user name and password.



Warning: The scanner will crawl all servers granted access by this password (if the sites/servers are included in the “allowed hosts” setting). To avoid potential damage to your administrative systems, do not use a user name and password that has administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional, or contact HP technical support .

The authentication methods are:

- **Basic**—A widely used, industry-standard method for collecting user name and password information. The Web browser displays a dialog box for a user to enter a previously assigned user name and password and then attempts to establish a connection to a server using the user's credentials. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established. Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.
- **NTLM**—An authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network. Use NTLM authentication for servers running IIS. If NTLM authentication is enabled, and the scanner has to pass through a proxy server to submit its requests to the Web server, the scanner may not be able to crawl or audit that Web site. Use caution when configuring a scanner for scans of sites protected by NTLM. After scanning, you may want to disable the NTLM authentication settings to prevent any potential problem.
- **Kerberos**—Kerberos uses the Needham-Schroeder protocol as its basis. It uses a trusted third party, termed a Key Distribution Center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). The client authenticates itself to AS, then demonstrates to the TGS that it is authorized to receive a ticket for a service (and receives it). The client then demonstrates to a Service Server that it has been approved to receive the service.

This authentication method will be successful only if the Web server has been configured to return a response header of "WWW-Authenticate: Kerberos" instead of "WWW-Authenticate: Negotiate."

To use Kerberos, the preferred choice is Negotiate (see below).

- **Digest**—The Windows Server 2003 operating system implements the Digest Authentication protocol as a security support provider (SSP), a dynamic-link library (DLL) that is supplied with the operating system. Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.
- **Automatic**—Allow the scanner to determine the correct authentication type. Automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
- **Negotiate**—This authentication method attempts to use Kerberos. If unsuccessful, the scanner uses NTLM.

Use Client Certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. Follow the steps below to use client certificates.

- 1 Select **Use Client Certificate**.
- 2 Click **Browse** to choose a certificate.

File Not Found

Determine File Not Found" Using HTTP Response Codes

Select this option to rely on HTTP response codes to detect a file-not-found response from the server. You can then identify the codes that fit the following two categories.

- **Forced Valid Response Codes (Never an FNF)**—You can specify HTTP response codes that should never be treated as a file-not-found response.
- **Forced FNF Response Codes (Always an FNF)**—Specify those HTTP response codes that will always be treated as a file-not-found response. The scanner will not process the response contents.

Enter a single response code or a range of response codes. For ranges, use a dash or hyphen to separate the first and last code in the list (for example, 400-404). You can specify multiple codes or ranges by separating each entry with a semicolon.

Determine File Not Found from Custom Supplied Signature

Use this area to add information about any custom 404 page notifications that your company uses. If your company has configured a different page to display when a 404 error occurs, add the information here. False positives can result from 404 pages that are unique to your site.

You can specify a signature using either plain text, a regular expression, or SPI Regex (see [Regular Expression Extensions](#) on page 202 for information on SPI Regex).

Auto-Detect File Not Found Page

Some Web sites do not return a status “404 Not Found” when a client requests a resource that does not exist. Instead, they may return a status “200 OK” but the response contains a message that the file cannot be found. Select this check box if you want the scanner to detect these “custom” file-not-found pages.

The HP scanner attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as “Sorry, the page you requested was not found”), with the possible exception being the name of the requested resource. If you select this option, you can specify what percentage of the response content must be the same. The default is 90 percent.

Policy

Scan Policy

A policy is a collection of audit engines and attack agents that a scanner uses when auditing or crawling your Web application. Each component has a specific task, such as testing for cross-site scripting susceptibility, building the site tree, probing for known server vulnerabilities, etc. See [Appendix B, Policies and Components](#), for policy descriptions.

For a Web Service assessment, you can select only the SOAP policy.

Crawl Settings

Link Parsing

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

Follow the steps below to add a specialized link identifier:

- 1 Click **Add**.
- 2 In the **Custom Links** box, enter a regular expression designed to identify the link.
- 3 (Optional) Enter a description of the link in the **Comments** box.
- 4 Click **Update**.

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the crawl, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Crawl Settings - Session Exclusions) allows you to specify additional objects to be excluded from the crawl.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited. Follow the steps below to add a file extension:

- 1 Click **Add**.
- 2 In the **File Extension** box, enter a file extension.
- 3 Select either **Reject**, **Exclude**, or both.
- 4 Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. Follow the steps below to add a MIME Type:

- 1 Click **Add**.
- 2 In the **Exclude Mime-type** box, enter a MIME type.
- 3 Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option. Follow the steps below to add a URL or host:

- 1 Click **Add**.
- 2 From the **Type** list, select either **Host** or **URL**.
- 3 In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
- 4 Select one or both of the following:
 - **Reject**—Do not send request to targeted URL or host
 - **Exclude**—Send request, but do not process response

- 5 Click **Update**.

Audit Settings

Session Exclusions

All items specified in the Scan Settings - Session Exclusions are automatically replicated in the Session Exclusions for both the Crawl Settings and the Audit Settings. These items are listed in gray (not black) text. If you do not want these objects to be excluded from the audit, you must remove them from the Scan Settings - Session Exclusions panel. This panel (Audit Settings - Session Exclusions) allows you to specify additional objects to be excluded from the audit.

Excluded or Rejected File Extensions

If you select **Reject**, files having the specified extension will not be requested. If you select **Exclude**, files having the specified extension will be requested, but will not be audited. Follow the steps below to add a file extension:

- 1 Click **Add**.
- 2 In the **File Extension** box, enter a file extension.
- 3 Select either **Reject**, **Exclude**, or both.
- 4 Click **Update**.

Excluded MIME Types

Files associated with the MIME types you specify will not be audited. Follow the steps below to add a MIME Type:

- 1 Click **Add**.
- 2 In the **Exclude Mime-type** box, enter a MIME type.
- 3 Click **Update**.

Excluded or Rejected URLs and Hosts

The URLs or hosts you specify will not be accessed if you select the **Reject** option. However, you may want to access the URL or host (do not select **Reject**), but not process the HTTP response (select **Exclude**). For example, you should usually reject any URL that deals with logging off the site, since you don't want to log out of the application before the scan is completed. To check for broken links to URLs that you don't want to process, select only the **Exclude** option. Follow the steps below to add a URL or host:

- 1 Click **Add**.
- 2 From the **Type** list, select either **Host** or **URL**.
- 3 In the **URLs and Hosts** box, enter a URL or fully qualified host name, or a regular expression designed to match the targeted URL or host.
- 4 Select one or both of the following:
 - **Reject**—Do not send request to targeted URL or host.
 - **Exclude**—Send request, but do not process response.
- 5 Click **Update**.

Attack Exclusions

Excluded Parameters

Use this feature to prevent the scanner from using certain parameters in the HTTP request to attack the Web site. This feature is used most often to avoid corrupting query and POSTDATA parameters.

To prevent certain parameters from being modified:

- 1 In the **Excluded Parameters** group, click **Add**.
- 2 In the **Parameter** box, enter the name of the parameter you want to exclude.
- 3 Choose the area in which the parameter may be found: HTTP query data or HTTP POST data. You can select both areas, if necessary.
- 4 Click **Update**.

Excluded Cookies

Use this feature to prevent the scanner from using certain cookies in the HTTP request to attack the Web site. This feature is used to avoid corrupting cookie values. This setting requires you to enter the name of a cookie. In the following example HTTP response ...

Set-Cookie: FirstCookie=Chocolate+Chip; path=/

... the name of the cookie is "FirstCookie."

Follow the steps below to exclude certain cookies.

- 1 In the **Excluded Cookies** group, click **Add**.
- 2 In the **Parameter** box, type a cookie name or enter a regular expression that you believe will match the cookies you want to exclude.
- 3 Click **Update**.

Excluded Headers

Use this feature to prevent the scanner from using certain headers in the HTTP request to attack the Web site. This feature is used to avoid corrupting header values.

To prevent certain headers from being modified, create a regular expression using the procedure described below.

- 1 In the **Excluded Headers** group, click **Add**.
- 2 In the **Parameter** box, type a header name or enter a regular expression that you believe will match the headers you want to exclude.
- 3 Click **Update**.

Audit Inputs Editor

Using the Audit Inputs Editor, you can create additional parameters for audit engines and checks that require inputs.

To load inputs that you previously created using the editor, click the **Browse** button next to the **Import Audit Inputs** button.

Attack Expressions

Additional Regular Expression Languages

You may select one of the following language code-country code combinations (as used by the `CultureInfo` class in the .NET Framework Class Library):

ja-jp: Japanese and Japan

ko-Kr: Korean and Korea

zh-cn: Chinese and China (PRC)

The `CultureInfo` class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of `DateTimeFormatInfo`, `NumberFormatInfo`, `CompareInfo`, and `TextInfo`. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Vulnerability Filters

Select Vulnerability Filters to Enable

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

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

To add a filter to your default settings, select a filter in the *Available* area and click >. The filter is removed from the **Available** list and added to the **Selected** list.

To disable a filter, select a filter in the **Selected** list and click <. The filter is removed from the **Selected** list and added to the **Available** list.

To add all available filters, click >>.

To remove all selected filters, click <<.

Smart Scan

Enable Smart Scan

Smart Scan is an “intelligent” feature that discovers the type of server that is hosting the Web site and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, the scanner will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

If you select this option, you can choose one or both of the identification methods described below.

- **Use regular expressions on HTTP responses**—This method searches the server response for strings that match predefined regular expressions designed to identify specific servers.
- **Use server analyzer fingerprinting and request sampling**—This advanced method sends a series of HTTP requests and then analyzes the responses to determine the server type.

Custom Server/Application Type Definitions

If you know the server type for a target domain, you can select it using the Custom server/application type definitions section. This identification method overrides any other selected method for the server you specify.

If you know the server type for a target domain, you can select it using the Custom server/application type definitions section. This identification method overrides any other selected method for the server you specify.

- 1 Click **Add**.
- 2 In the **Server** box, enter the domain name or host, or the server's IP address.
- 3 In the **Identification** box, enter a Server/Application type (such as Abyss, Apache, ASP, aspnet, etc.).
- 4 Click **Update**.

Scan Behavior

Blackout Action

A blackout period is a block of time during which scans are not permitted.

If a blackout period begins while a scan is running, you may either stop the scan or suspend it. The scanner will resume a suspended scan when the blackout period ends.

Reports

General

Generate Report—Select this option to create a report.

Report

- **Automatically generate report name**—Select this option if you want AMP to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
- **Report Name**—If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **Report Name** box.
- **Description**—Enter a brief description of the report.

Export Report

Select this option to export a report, and then provide the following information.

- **Output Type**—Choose a format for the exported report.
- **Export Path**—Select a destination for the exported report. Export paths are specified by the AMP administrator.
- **Automatically generate file name**—Select this option if you want the AMP manager to assign a name to the exported report based on the time and date. Otherwise, clear this option and enter a name in the **File name** box.

Options

Report Type

Select one of the following options and then select the template or definition from the appropriate list;

- Use Report Template
- Use Report Definition

Report Definitions

The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.

E-mail

To send an e-mail containing the URL of the report:

- 1 Type an e-mail address in the **New E-mail Recipient** box.
- 2 Click **Add**.
- 3 Repeat as necessary.

The e-mail recipient must have a valid AMP account to view the report.

Export

General

Export Scan Results

Select this option to export the scan results. Then provide the requested information.

- **Export Path**—Select a destination for the exported scan. Export paths are specified by the AMP administrator.
- **Export Format**—Select how you want the exported file to be formatted. Your choices are WebInspect Scan File or XML.
- **Automatically generate file name**—If you select this option, the name of the file will be formatted as <scan name> <date/time>.[xml or scan]. For example, if the scan name is “mysite” and the scan is generated at 6:30 on April 5, the file name would be “mysite 04_05_2007 06_30.scan [or .xml].” This is useful for recurring scans.

If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **File Name** box.

Enterprise Report Settings

When you click **New Report** in the Actions group, three categories of settings appear in the left column. They are:

- General

- Options
- Tags

General

Project

Select a project or organization from the list. If **Use Organization** is not selected, the list contains all projects. If **Use Organization** is selected, the list contains all organizations.

Report Location

If **Use Organization** is not selected, you can choose to locate the report with the project or with the organization of the selected project. If **Use Organization** is selected, the report will be located with the organization of the selected project.

Report

- **Automatically generate report name**—Select this option if you want the AMP manager to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
- **Report Name**—If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the Report Name box.
- **Description**—Enter a brief description of the report.

Options

Report Type

Select one of the following options and then select the template or definition from the appropriate list:

- Use Report Template
- Use Report Definition

Report Definitions

The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as reports. See [Tags](#) on page 110 for instructions on creating tags.

Report Template Settings

Template

Project

Select a project or organization from the list. If **Use Organization** is selected, the list contains all organizations. If **Use Organization** is not selected, the list contains all projects. This option is repeated on every settings form (except Tags).

Report Template

Enter a name for the report template.

Description

Enter a brief description of the report.

Report Style Sheet

Select a style sheet from the Report Style Sheet list.

Master Report

Master Report

A Master Report is the “container” for a report. It includes a cover page, logo, header/footer, and graphics. Use the Report Designer tool to create a Master Report.

Select a master report from the list.

Report Parameters

Enter report parameters for the selected master report.

If you select **Changeable**, then the person who uses this template to generate a report may modify the parameters.

Report Definitions

Report Type

Select a report type from the list. The options are:

- **General**—An enterprise-wide report that is not related to a specific scan or site.
- **Scan**—A report using queries filtered by scan data.
- **Site**—A report using queries filtered by site data.
- **Session**—A report pertaining to a specific session in a scan.
- **Assessment**—A report optionally showing findings that fail a selected compliance policy, assessment findings, and an assessment summary.

Report Definitions

Select one or more of the listed report definitions and enter the requested information. Not all definitions require you to specify options. Definitions are created using the Report Designer tool.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled report templates. See [Tags](#) on page 110 for instructions on creating tags.

Scan Template Settings

Settings for a scan template are the same as those described for a scan (see [Advanced Scan Settings](#) on page 107), except for the following:

Scan

General

Project

Select a project or organization from the list. If **Use Organization** is selected, the list contains all organizations. If **Use Organization** is not selected, the list contains all projects.

Scan Template Created From

This is a read-only field indicating the source of the settings. If you started to create the template by clicking **Add**, you are using default settings; if you started to create the template by clicking **Add From**, you are using settings optimized for an Oracle site. Note that additional options for **Add From** will be available in future releases.

Scan Template Name

Enter a name for this template.

Custom Scan Settings

If you select **Can customize scan settings** when applying this template, users may modify the settings prescribed by this template.

Maximum Priority

Specify the maximum priority that can be assigned to a scan that uses this template.

Restrict To Folder Mode

If you select this option, you can limit the scope of the assessment to the area you choose from the drop-down list. They are:

- **Directory Only**—The HP scanner will crawl and/or audit only the URL you specify. For example, if you select this option and specify a URL of `www.mycompany/one/two/`, The HP scanner will assess only the “two” directory.

- **Directory and subdirectories**—The HP scanner will begin crawling and/or auditing at the URL you specify, but will not access any directory that is higher in the directory tree.
- **Directory and parent directories**—The HP scanner will begin crawling and/or auditing at the URL you specify

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scan templates. See [Tags](#) on page 110 for instructions on creating tags.

Sensors

Select one or more sensors from the **Available** list. The selected sensors will be available for creating a scan when this scan template is used.

To allow unrestricted access to sensors, select the **Use Any Available** check box.

To restrict access to specific sensors:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add a sensor, select a sensor in the **Available** area and click >. The sensor is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a sensor, select a sensor in the **Selected** list and click <. The sensor is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available sensors, click >>.
- 5 To remove all selected sensors, click <<.

Scan URLs

If you select **Allow user to specify any URL**, the template will not restrict scans based on URL. Alternatively, you can clear this option and then create a list of URLs from which a user must select.

To create a list of allowed URLs:

- 1 Clear the **Allow user to specify any URL** check box.
- 2 In the text box, enter the complete URL or IP address of a site you want to allow users to scan. An improperly formatted URL or IP address will result in an error. If you want to scan from a certain point in a hierarchical tree, append a starting point for the scan, such as `http://www.myserver.com/myapplication/`.
- 3 Click **Add**.

List-Driven Scan

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

- 1 Select the **Allow user to specify any URL** check box.
- 2 Click **Browse** and select a text file or XML file containing the list of URLs you want to scan.
- 3 Click **View** to view the contents of the selected file.

Workflow-Driven Scan

The scanner audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application.

- 1 Select the **Allow user to specify any URL** check box.
- 2 Click **Browse** and select a macro.

You may select more than one macro.

Web Service Scan

When performing a Web Service scan, the scanner crawls the Web Service Definition Language (WSDL) site and submits a value for each parameter in each operation it discovers. These values are extracted from a file that you must create using the Web Service Test Designer. The scanner then audits the site by attacking each parameter in an attempt to detect vulnerabilities such as SQL injection.

- 1 Select the **Allow user to specify any URL** check box.
- 2 Click **Browse** and choose a Web Service Test Design (WSD) file that was previously created using the Web Service Test Designer.

Reports

Templates

Select one or more report templates from the **Available** list. The selected templates will be available for configuring a report when this template is used.

To allow unrestricted access to report templates, select the **Use Any Available** check box.

To restrict access to specific templates:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add a template, select a template in the **Available** area and click >. The template is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a template, select a template in the **Selected** list and click <. The template is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available templates, click >>.
- 5 To remove all selected templates, click <<.

Compliance Templates

Select one or more compliance templates from the **Available** list. The selected templates will be available for configuring a compliance report when this template is used.

To allow unrestricted access to templates, select the **Use Any Available** check box.

To restrict access to specific templates:

- 1 If necessary, clear the **Use Any Available** check box.

- 2 To add a template, select a template in the **Available** area and click >. The template is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a template, select a template in the **Selected** list and click <. The template is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available templates, click >>.
- 5 To remove all selected templates, click <<.

Resources

Select one or more report resources from the **Available** list. The selected resources will be available for configuring a report when this template is used.

To allow unrestricted access to resources, select the **Use Any Available** check box.

To restrict access to specific resources:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add a resource, select a resource in the **Available** area and click >. The resource is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a resource, select a resource in the **Selected** list and click <. The resource is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available resources, click >>.
- 5 To remove all selected resources, click <<.

Export Paths

Select one or more paths from the **Available** list. The selected paths will be available for saving a report when this template is used.

To allow unrestricted access to export paths, select the **Use Any Available** check box.

To restrict access to specific paths:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add an export path, select an export path in the **Available** area and click >. The export path is removed from the **Available** list and added to the **Selected** list.
- 3 To remove an export path, select an export path in the **Selected** list and click <. The export path is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available export paths, click >>.
- 5 To remove all selected export paths, click <<.

Export

Export Paths

Select one or more paths from the **Available** list. The selected paths will be available for exporting a scan when this template is used.

To allow unrestricted access to export paths, select the **Use Any Available** check box.

To restrict access to specific paths:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add an export path, select an export path in the **Available** area and click >. The export path is removed from the **Available** list and added to the **Selected** list.
- 3 To remove an export path, select an export path in the **Selected** list and click <. The export path is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available export paths, click >>.
- 5 To remove all selected export paths, click <<.

Site Settings

General

Project

Select a project from the list.

Site

- **Site Name**—Enter a name that identifies this site.
- **Scan Template**—Select a template.
- **URL**—Enter a fully qualified domain name or an IP address.
- **Phase**—(Optional) Enter the name of a phase or select an existing name from the **Phase** list. If you assign phases to sites, you can optionally display only those sites that are members of a specific phase. See [About Phases and Groups](#) below.
- **Group**—(Optional) Enter the name of a group or select an existing name from the **Group** list. If you create groups of sites, you can optionally display only those sites that are members of a specific group. See [About Phases and Groups](#) below.
- **Authentication**—If authentication is required, select a type from the list.
- **Weight**—Weight is used to calculate the risk score that appears on the Sites form. The risk score for a site is equal to the risk score of the most recent completed scan of that site multiplied by the value you enter here. It allows the user to indicate that some sites are more important or have a higher risk than others. For example, the risk associated with vulnerabilities in an external-facing site could be weighted higher than vulnerabilities in an internal-only site because of the level of exposure. The weight can be any value between zero and 10.



About Phases and Groups

“Phase” and “Group” are simply generic terms that allow you to categorize sites. For example, you could create groups based on business function (such as Accounting, Manufacturing, HR, and Marketing) or geographic area (such as North America, South America, Europe, and Asia). Similarly, you could create phases that reflect certain stages of product development (such as Prototype, QA, and Production). The definition and use of phases and groups is completely flexible as well as optional.

Host

Add or select an IP address for each server that hosts a portion of the Web site.

If the Web site is configured on a server that hosts more than one domain name, select **Virtual Host**.

Information

Project

Select a project from the list.

Platform

- **Operating System**—Enter the name of the operating system used by servers at this site.
- **Web Platform**—Specify the Web platform.

Contact

Enter the name and e-mail address of the contact person.

Notes

Enter any notes about this site that may be helpful.

Tags

Tags are user-configurable fields designed to help you group or sort sites and other objects. See [Tags](#) on page 110 for instructions on creating tags.

Scheduled Scan Settings

To schedule a scan, click the Add icon and then specify the scan settings. These settings are the same as described in [Advanced Scan Settings](#) on page 107, with the following additions:

Schedule

General

Schedule

- **Schedule Name**—Enter a name that identifies this scheduled scan request.
- **Start Time**—Enter the date and time you want the scan to begin. If you click the drop-down arrow, you can select the date from a calendar.
- **Time Zone**—The time zone specific to the start time specified for the scheduled scan. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the AMP server is in a different time zone, you should usually select the server's time zone and specify the Start time using local time. For example, if you are

in New York City, USA (UTC-05) and the AMP server is in Rome, Italy (UTC+01), and you want to schedule a scan to begin at 8 a.m. Rome time, you could do either of the following:

- Select the UTC+01 time zone (Rome) and specify a Start time of 8 a.m.
- Select the UTC-05 time zone (New York City) and specify a Start time of 2 a.m.
- **Next Scheduled Time**—For a scan that is scheduled to recur, this read-only field displays the time and date of the next scheduled scan.
- **Last Occurred On**—For a scan that is scheduled to recur, this read-only field displays the time and date when the scan last occurred.

Recurrence

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

Pattern

Use the **Pattern** group to select the frequency of the event (daily, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled scan requests. See [Tags](#) on page 110 for instructions on creating tags.

Discovery Scan Settings

Schedule

General

Project

Select a project from the list.

Discovery Template

Instead of specifying each individual setting every time you conduct a Discovery scan, you can create templates that contain different settings and then simply select a template from the **Use Discovery Template** list.

You are not required to use a template, but if you do, you may also select the following options:

- **Create custom Discovery from template**—When you select this option, all settings for this scan (including any deviations from the template) will be saved and permanently associated with the scan request. A rescan (or a scheduled scan) will use the saved settings and not the template. This is useful when you intend to conduct a series of identical scans and do not want to introduce any subsequent modifications that someone may make to the template. Your assigned role may not allow you to select this option.
- **Customize Template's Scan Settings**—Select this option if you want to modify any of the scan settings prescribed by the template. If the selected template does not allow modifications, this option is not enabled.

Schedule Name

Enter a name that identifies this scheduled scan request.

Start Time

Enter the date and time you want the scan to begin. If you click the drop-down arrow, you can select the date from a calendar.

Time Zone

Select the time zone specific to the start time specified for the discovery scan. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the AMP server is in a different time zone, you should usually select the server's time zone and specify the discovery scan's start time using local time.

For example, if you are in New York City, USA (UTC-05) and the AMP server is in Rome, Italy (UTC+01), and you want to schedule a discovery scan to begin at 8 a.m. Rome time, you could do either of the following:

- Select the UTC+01 time zone (Rome) and specify a Start time of 8 a.m.
- Select the UTC-05 time zone (New York City) and specify a Start time of 2 a.m.

Next Scheduled Time

For a scan that is scheduled to recur, this read-only field displays the time and date of the next scheduled scan.

Last Occurred On

For a scan that is scheduled to recur, this read-only field displays the time and date when the scan last occurred.

Recurrence

Recurring

To schedule a Discovery on a recurring basis, select the **Recurring** check box. Do NOT select this option if you want to schedule a one-time-only event.

Pattern

Use the Pattern group to select the frequency of the event (daily, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the Range group to specify the starting date and the ending date (or select **Never** if the event is to recur indefinitely). You can also limit the number of times the event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled scan requests. See [Tags](#) on page 110 for instructions on creating tags.

Discovery

General

Discovery Sensor

Choose a sensor to conduct the scan. You can choose a specific sensor or select the **Any Available** option.

Scan Discovered Sites

If you do not, under any conditions, want to scan a discovered site, select **Never scan**.

If you want to assess the vulnerabilities of a discovered site that is not already in the site catalog, select **Scan new sites only**. To scan all discovered sites, regardless of whether they have been scanned previously, select **Always scan**. If you choose either of the two scanning options, then:

- The Discovered Site Scan Settings group appears. Use the Selected Sensor list to choose the sensor that will scan the discovered site, then select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority takes precedence.
- Several settings panels appear in the left navigation pane. Use these to configure settings for scanning the discovered site. These settings are the same as described in [Advanced Scan Settings](#) on page 107.

Settings

IP Range

Select an entry from the list, or type a range of addresses using the following guidelines:

To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.

Example: 172.16.10.2-172.16.10.99

You can specify multiple individual addresses or ranges by separating each entry with a semicolon or comma.

Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254

Port Range

Select an entry from the list or type a range of port numbers, using a hyphen to separate the lowest port number from the highest. Separate multiple entries with a semicolon.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, AMP will close the socket and terminate the scan.

Sockets

Specify the number of open sockets. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be set to 10. If you increase this setting, you will increase the likelihood that the scanner will fail to detect servers. This occurs because Microsoft has limited the number of open sockets to 10.

Run Script

If you select **Run script when a new site is discovered**, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- **SPIIPAddress**—The IP address of the site
- **SPIPort**—The port number
- **SPIProtocol**—The protocol (HTTP or HTTPS)

Use the **Command** text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).



Caution: Scripts are executed under the network service account, which has elevated privileges and may therefore present significant security risk.

Discovered Site Tags

Add or select the tags to be used when scanning a site that is revealed by this Discovery scan.

Discovery Template Settings

To create a scan Discovery template, click **Add** and then specify the template settings, which are described below:

Discovery

General

Discovery Template Name

Enter a unique identifier for this template.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, the scanner will close the socket and terminate the scan.

Sockets

Specify the number of open sockets. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be set to 10. If you increase this setting, you will increase the likelihood that the scanner will fail to detect servers. This occurs because Microsoft has limited the number of open sockets to 10.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as Discovery scan templates. See [Tags](#) on page 110 for instructions on creating tags.

Sensors

Select one or more sensors from the **Available** list. The selected sensors will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to sensors, select the **Use Any Available** check box.

To restrict access to specific sensors:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add a sensor, select a sensor in the **Available** area and click >. The sensor name is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a sensor, select a sensor in the **Selected** list and click <. The sensor name is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available sensors, click >>.
- 5 To remove all selected sensors, click <<.

IP Ranges

Specify the IP addresses that will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to IP addresses, select **Allow user to specify any IP Ranges**.

To restrict access to specific IP addresses:

- 1 If necessary, clear the **Allow user to specify any IP Ranges** check box.
- 2 In the **IP Range** box, type a range of addresses or multiple individual addresses using the following format:
 - To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.
Example: 172.16.10.2-172.16.10.99
 - You can specify multiple individual addresses or ranges by separating each entry with a semicolon.
Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254
- 3 Click **Add**.
- 4 Repeat for additional entries.

Port Ranges

Specify the ports that will be available for conducting a discovery scan when this template is used.

To allow unrestricted access to port numbers, select the **Allow user to specify any Port Ranges** check box.

To restrict access to specific ports:

- 1 If necessary, clear the **Allow user to specify any Port Ranges** check box.
- 2 In the **Port Ranges** box, type a range of port numbers or multiple individual port numbers using the following format:
 - To specify a range, type the lowest port number in the range followed by a hyphen and then the highest port number in the range.
Example: 1-8080
 - You can specify multiple individual ports or ranges by separating each entry with a semicolon.
Example: 1-55;80;443;8080
- 3 Click **Add**.
- 4 Repeat for additional entries.

Scan Discovered

General

Scan Discovered Sites

Specify if and how you want discovered sites to be scanned.

- **Never Scan**—Discovered sites will be reported, but not scanned.
- **Scan new sites only**—Sites that have not been scanned previously will be scanned.
- **Always scan**—All discovered sites will be scanned, even if that site already exists in the scan database.

If you choose to scan a discovered site, settings options appear in the left column. These settings are the same as those described for a scan (see [Advanced Scan Settings](#) on page 107). In addition, there is a **Sensors** option (in the Scan Discovered group) that allows you to select the sensor that should be used for conducting the scan of a discovered site.

Run Script

If you select this check box, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- **SPIIPAddress**—The IP address of the site
- **SPIPort**—The port number
- **SPIProtocol**—The protocol (HTTP or HTTPS)

Use the **Command** text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).

Custom Scan Settings

This option appears if you elect to scan a discovered site. Select this check box if you want to permit the user to change scan settings when applying this template.

Maximum Priority

This option appears if you elect to scan a discovered site. Assign a priority to scans conducted with this template. Priority ranges from 1 (the highest) to 5 (the lowest).

Sensors

This selection appears only if you elect to scan discovered sites.

Select one or more sensors from the **Available** list. The selected sensors will be available for scanning discovered sites when this template is used.

To allow unrestricted access to sensors, select the **Use Any Available** check box.

To restrict access to specific sensors:

- 1 If necessary, clear the **Use Any Available** check box.
- 2 To add a sensor, select a sensor in the **Available** list and click >. The sensor is removed from the **Available** list and added to the **Selected** list.
- 3 To remove a sensor, select a sensor in the **Selected** list and click <. The sensor is removed from the **Selected** list and added to the **Available** list.
- 4 To add all available sensors, click >>.
- 5 To remove all selected sensors, click <<.

Discovery Schedule Settings

To schedule a Discovery scan, select Discovery Schedules from the navigation pane, click **Add** and then specify the settings. These are the same settings used for scheduling a scan, which are described [Scan Schedules](#) on page 93.

Schedule

General

Project

Select a project from the list.

Scan Template

Instead of specifying each individual setting every time you conduct a scan, you can create templates that contain different settings and then simply select a template from the **Use Discovery Template** list.

You are not required to use a template, but if you do, you may also select the following options:

- **Create custom Discovery from Template**—When you select this option, all settings for this scan (including any deviations from the template) will be saved and permanently associated with the scan request. A rescan (or a scheduled scan) will use the saved settings and not the template. This is useful when you intend to conduct a series of identical scans and do not want to introduce any subsequent modifications that someone may make to the template. Your assigned role may not allow you to select this option.
- **Customize Template's Scan Settings**—Select this option if you want to modify any of the scan settings prescribed by the template. If the selected template does not allow modifications, this option is not enabled.

Schedule

- **Schedule Name**—Enter a name that identifies this scheduled scan request.
- **Start Time**—Enter the date and time you want the scan to begin. If you click the drop-down arrow, you can select the date from a calendar.
- **Time Zone**—The time zone specific to the start time specified for the discovery scan. The time zone defaults to the zone in which you are working (as selected using the Configure Options window). If the AMP server is in a different time zone, you should usually select the server's time zone and specify the discovery scan's start time using local time. For example, if you are in New York City, USA (UTC-05) and the AMP server is in Rome, Italy (UTC+01), and you want to schedule a discovery scan to begin at 8 a.m. Rome time, you could do either of the following:
 - Select the UTC+01 time zone (Rome) and specify a Start time of 8 a.m.
 - Select the UTC-05 time zone (New York City) and specify a Start time of 2 a.m.
- **Next Scheduled Time**—For a scan that is scheduled to recur, this read-only field displays the time and date of the next scheduled scan.
- **Last Occurred On**—For a scan that is scheduled to recur, this read-only field displays the time and date when the scan last occurred.

Recurrence

Recurring

Select this check box to conduct recurring scans. Do NOT select this option if you want to schedule a one-time-only event.

Pattern

Use the **Pattern** group to select the frequency of the event (daily, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as scheduled scan requests. See [Tags](#) on page 110 for instructions on creating tags.

Discovery

General

Discovery Sensor

Choose a sensor to conduct the scan. You can choose a specific sensor or select the **Any Available** option.

Scan Discovered Sites

If you do not, under any conditions, want to scan a discovered site, select **Never scan**.

If you want to assess the vulnerabilities of a discovered site that is not already in the site catalog, select **Scan new sites only**. To scan all discovered sites, regardless of whether they have been scanned previously, select **Always Scan**.

If you choose either of the two scanning options, then:

- The Discovered Site Scan Settings group appears. Use the **Selected Sensor** list to choose the sensor that will scan the discovered site, then select a priority from 1 (highest) to 5 (lowest). If a scheduling conflict occurs, the scan with the highest priority takes precedence.
- Several settings panels appear in the left navigation pane. Use these to configure settings for scanning the discovered site.

Settings

IP Range

Select an entry from the list, or type a range of addresses using the following guidelines:

- To specify a range, type the lowest IP address in the range followed by a hyphen and then the highest IP address in the range.

Example: 172.16.10.2-172.16.10.99

- You can specify multiple individual addresses or ranges by separating each entry with a semicolon or comma.

Example: 172.16.10.2;172.16.10.55;188.22.33.1-188.22.33.254

Port Range

Select an entry from the list or type a range of port numbers, using a hyphen to separate the lowest port number from the highest. Separate multiple entries with a semicolon.

Timeout

If there is no activity on an open socket for the number of consecutive seconds that you specify, AMP will close the socket and terminate the scan.

Sockets

Specify the number of open sockets. 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.

Note: If the scanner runs on Windows XP with Service Pack 2 (SP2), the number of Open Sockets should be set to 10. If you increase this setting, you will increase the likelihood that the scanner will fail to detect servers. This occurs because Microsoft has limited the number of open sockets to 10.

Run Script

If you select **Run script when a new site is discovered**, you can execute a program (a script or any executable) on the AMP server whenever the scanner discovers a new site. AMP sets the following environmental variables to pass information about the discovered site:

- **SPIIPAddress**—The IP address of the site
- **SPIPort**—The port number
- **SPIProtocol**—The protocol (HTTP or HTTPS)

Use the **Command** text box to specify an executable, such as C:\FolderA\filename.exe (where C refers to the AMP server's drive).

Discovered Site Tags

Add or select the tags to be used when scanning a site that is revealed by this Discovery scan.

Tags are user-configurable fields designed to help you group or sort various objects, such as Discovery scans. See [Tags](#) on page 110 for instructions on creating tags.

Blackout Settings

A blackout period is a block of time during which scans are not permitted. You can also create a partial ban by specifying that scans should not be conducted on specific hosts (identified by URL or IP address) during the time period you specify.

You may alternatively assign a contrary definition to the blackout, specifying that scans may occur only during this time period. In effect, this creates a blackout period covering all but the period of time you specify.

General

Project

Select a project or organization from the list. If **Use Organization** is selected, the list contains all organizations. If **Use Organization** is not selected, the list contains all projects.

Name

Enter a unique identifier for this blackout period.

Address

The URL or IP address (or range of IP addresses) that are affected by this blackout period. The value can be a single URL or IP address, or a range of IP addresses. If you need to exclude multiple ranges, you must create additional (overlapping) blackout periods. To specify a range, separate the beginning address and ending address with a hyphen. You can use the

asterisk (*) as a wild card. The default setting (an asterisk) means all addresses. Wildcards in IP addresses must be at the end of the address as shown, but wildcards for host names must be at the beginning.

Examples:

192.16.12.1-192.16.12.210

192.16.12.*

*.domain.com

Schedule

- **Start Time**—The date and time at which the blackout period begins.
- **End Time**—The date and time at which the blackout period expires.
- **Time Zone**—The time zone specific to the start and end times specified for the blackout. The time zone defaults to the zone in which you are working (as selected using the *Configure Options* window). If the AMP server is in a different time zone, you should usually select the server's time zone and specify the blackout period using local time. For example, if you are in New York City, USA (UTC-05) and the AMP server is in Rome, Italy (UTC+01), and you want to schedule a blackout to begin at 8 a.m. Rome time, you could do either of the following:
 - Select the UTC+01 time zone (Rome) and specify a Start time of 8 a.m.
 - Select the UTC-05 time zone (New York City) and specify a Start time of 2 a.m.
- **Duration**—The length of time during which the blackout is in effect. This value is calculated automatically after you specify the Start Time and End Time. Alternatively, if you specify the Start Time and the Duration, the End Time is calculated. If you edit the Duration, the End Time is recalculated. The format is:

d.hh.mm

where

d = the number of days

hh = the number of hours

mm = the number of minutes

Blackout Type

- **Allow**—Scans of the specified targets are allowed only during the specified time period.
- **Deny**—Scans of the specified targets are prohibited during the specified time period.

Allow and deny work very much like allow and deny for permissions. Deny always takes precedence over allow, so a scan can occur only at a particular time if there are no blackout periods that deny that time. An allow blackout period means deny scans UNLESS you are in the allowed range, as opposed to allow scans ONLY if you are in the allowed range. If you configure two separate “allow” blackout periods, a scan will be allowed only during the union of those periods. For example, if period A allows scans from 1 P.M. to 3 P.M. and period B allows scans from 2 P.M. to 6 P.M., then scans will be allowed only from 2 P.M. to 3 P.M.

Recurrence

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

Recurring

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

Pattern

Use the **Pattern** group to select the frequency of the blackout (daily, weekly, monthly, or yearly) and then provide the appropriate information.

Range

Use the **Range** group to specify the starting date and the ending date (or select **Never** if the event is to run indefinitely). You can also limit the number of times the event should occur.

Tags

Tags are user-configurable fields designed to help you group or sort various objects, such as blackout periods. See [Tags](#) on page 110 for instructions on creating tags.

7 Reporting

Introduction

The AMP Web Console allows you to generate a variety of reports.

You can create a scan report using one of the standard templates or you can create a unique report by selecting options from the list of available components.

You can also generate a compliance report for a scan or an assessment. This report provides a pass/fail score for each statement in the compliance portion of the policy used for auditing your site. The summary area reports, for each statement, the total number of checks, the number of checks that passed, and the percentage that passed. The detail area provides a description of each vulnerability.

If you are using AMP's assessment feature, you can also generate an assessment report that shows findings, summary, and compliance information, depending on the options you select.

Finally, you can generate an enterprise report for your organization or for individual projects within your organization.

Generating a Scan Report

There are two ways to create a scan report. You can schedule a report to be generated as part of a scheduled scan, or you can manually initiate a report after any scan (including a scheduled one) is complete.

Manual Report

To initiate a report manually from the AMP Web Console:

- 1 Click either the **Scans** or **Sites** button in the Navigation pane.
- 2 Do one of the following:
 - Select the check box of a scan that has a check mark in the **Results** column and click the **Generate Report** icon. You can select multiple scans.
 - Click the drop-down arrow next to a scan name and select **Generate Report** from the context menu.

There are three categories of settings: General, Options, and Tags.

- 3 On the General settings window, select a naming convention:
 - If you want the AMP manager to assign a name to the file based on the time and date, select **Automatically generate report name**. Use this option if you are generating reports for recurring scans and you want to preserve each report.

- If you want to specify a file name, clear the **Automatically generate report name** check box and then type a name in the **Name** box. Do not use this option for recurring scans unless you want to overwrite the old report each time the scan is conducted.
- 4 Enter a brief description of the report.
 - 5 Click the **Options** category and select one of the following from the Report Type group:
 - **Use Report Template**
 - **Use Report Definition**
 - 6 If you select **Report Template**, choose an entry from the **Report Template** list.
 - 7 If you select **Use Report Definition**, choose an entry from the **Report Definition** list.
 - 8 The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.
 - 9 Click the **Tags** category to assign tags to the report. See [Tags](#) on page 110 for specific information.
 - 10 Click **Finish** to generate the report.

The AMP manager will create an entry on the Reports form, where you can view the report.

Scheduled Report

Follow the steps below to create a report with a scheduled scan, using the AMP Web Console:

- 1 Click the **Scan Schedules** button in the Navigation pane.
- 2 Click the **Add** icon to create a scheduled scan.
 After providing all the requested information pertaining to the scan, select the choices in the **Reports** category of settings. The choices are: General, Options, and E-Mail.
- 3 Click **General**.
 - a Select **Generate Report**.
 - b Enter a report name and description.
 - c Select **Automatically generate report name** if you want the AMP manager to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
 - d If you want to specify a name, clear the **Automatically generate report name** check box and then type the name in the **Report Name** box.
 - e Enter a brief description of the report.
 - f Select **Export Report** to export a report, and then provide the following information.
 - **Output Type**—Choose a format for the exported report.
 - **Export Path**—Enter or select a destination for the exported report. Because the AMP Manager service writes the output, the specified path must be writable by the Manager service user. You should use a UNC pathname (e.g., \\AmpServer\Amp\Output\) so that it will be accessible to both the AMP Manager and end users. You may alternatively specify a drive letter and path (e.g., C:\Amp\Output\), but the path will apply to the AMP Manager server and may not be accessible to end users.

- **Automatically generate file name**—Select this option if you want the AMP manager to assign a name to the exported report based on the time and date. Otherwise, clear this option and enter a name in the **File name** box.
- 4 Click **Options**.
 - a Select one of the following options and then select the template or definition from the appropriate list.
 - **Use Report Template**
 - **Use Report Definition**
 - b The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these settings and select the options you want to use for your report.
- 5 Click **E-Mail**. To send a copy of a report by e-mail:
 - a Type an e-mail address in the New E-mail Recipient box.
 - b Click **Add**.
 - c Repeat as necessary.
- 6 Click **Finish** to generate the report.

Generating an Assessment Report

- 1 In the Navigation pane under Filtered Views, click **Assessments**.
- 2 Select the check box next to an assessment name and click the **Generate Report** icon. Alternatively, you can click the drop-down arrow next to an assessment name and select **Generate Report**.
Categories of settings are displayed in the left column. They are:
 - General
 - Options
 - Tags
- 3 Using the General settings, select a project or organization from the **Report On** list. If **Use Organization** is not selected, the list contains all projects. If **Use Organization** is selected, the list contains all organizations.
Note: This field is repeated for each category of settings.
- 4 If **Use Organization** is not selected, you can choose to store the report with the project or with the organization of the selected project. If **Use Organization** is selected, the report will be located with the organization of the selected project.
Note: You will not be able to store a report with an organization unless you are assigned to a role in that organization.
- 5 Select **Automatically generate report name** if you want the AMP manager to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
- 6 If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **Report Name** box.

- 7 Enter a brief description of the report.
- 8 Click the **Options** category.
- 9 Select one of the following options and then select the template or definition from the appropriate list:
 - **Use Report Template** - The only available template is Assessment.
 - **Use Report Definition** - Select either **Assessment Compliance**, **Assessment Findings**, or **Assessment Summary**.
- 10 The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.
- 11 Click the **Tags** category to assign tags to the report. See [Tags](#) on page 110 for specific information.
- 12 Click **Finish** to generate the report.

Generating an Enterprise Report

You can generate enterprise reports for an organization or for a single project within an organization, using the AMP Web Console.

- 1 Click **New Report** in the Actions group on the Navigation pane.

Categories of settings are displayed in the left column. They are:

 - General
 - Options
 - Tags
- 2 Using the General settings, select a project or organization from the **Report On** list. If **Use Organization** is not selected, the list contains all projects. If **Use Organization** is selected, the list contains all organizations.

Note: This field is repeated for each category of settings.
- 3 If **Use Organization** is not selected, you can choose to store the report with the project or with the organization of the selected project. If **Use Organization** is selected, the report will be located with the organization of the selected project.

Note: You will not be able to store a report with an organization unless you are assigned to a role in that organization.
- 4 Select **Automatically generate report name** if you want the AMP manager to assign a name to the report based on the time and date. This is helpful when you are exporting results for recurring scans and you want to preserve each results file.
- 5 If you want to specify a name, clear the **Automatically generate file name** check box and then type the name in the **Report Name** box.
- 6 Enter a brief description of the report.
- 7 Click the **Options** category.
- 8 Select one of the following options and then select the template or definition from the appropriate list:

- **Use Report Template**
 - **Use Report Definition**
- 9 The list of parameters appearing in the Report Definitions section is determined by your Report Type selection. Expand each of these and select the options you want to use for your report.
 - 10 Click the **Tags** category to assign tags to the report. See [Tags](#) on page 110 for specific information.
 - 11 Click **Finish** to generate the report.

Creating a Report Template

You can specify a report template when configuring settings for a scan or when generating a scan report.

AMP provides 11 predefined report templates:

- Basic
- Compliance
- Comprehensive
- Developer
- Executive
- False Positive
- General
- QA
- Session
- Site
- Standard

Each template has a different selection of report components.

You cannot delete or change a predefined template. However, you can create a template that contains any combination of report options. Unlike the predefined (locked) templates, you can modify or delete the templates that you create.

Follow the steps below to create a report template using the AMP Web Console:

- 1 Click the **Report Templates** button on the Navigation pane.
- 2 Click the **Add** icon at the top of the form.

Categories of settings are displayed in the left column. They are:

- Template
- Master Report
- Report Definitions
- Tags

- 3 Using the Template settings, select a project or organization from the list. If **Use Organization** is selected, the list contains all organizations. If **Use Organization** is not selected, the list contains all projects.
- 4 Enter a name for the report template.
- 5 Enter a brief description of the report.
- 6 Select a style sheet from the **Report Style Sheet** list.
- 7 Click the **Master Report** category.

A Master Report is the “container” for a report. It includes a cover page, logo, header/footer, and graphics. Use the Report Designer tool to create a Master Report.
- 8 Select a master report from the list.
- 9 Enter report parameters for the selected master report.
- 10 If you select **Changeable**, then the person who uses this template to generate a report may modify the parameters.
- 11 Click the **Report Definitions** category.
- 12 Select a report type from the list. The options are:
 - **General**—An enterprise-wide report that is not related to a specific scan or site.
 - **Scan**—A report using queries filtered by scan data.
 - **Site**—A report using queries filtered by site data.
 - **Session**—A report pertaining to a specific session in a scan.
- 13 Select one or more of the listed report definitions and enter the requested information. Not all definitions require you to specify options. Definitions are created using the Report Designer tool.

Note: A report template may contain multiple report definitions. However, if you generate a report without using a template, you may specify only one report definition.
- 14 Click the **Tags** category to assign tags to the report. See [Tags](#) on page 110 for specific information.
- 15 Click **Finish** to create the template.

Viewing a Report

You must first generate a report. You can do this either manually or as part of a scheduled scan.

Follow the steps below to view a report using the AMP Web Console:

- 1 Click the **Reports** button on the Navigation pane.
- 2 Do one of the following for a report whose status is complete:
 - Click the report name.
 - Select the check box next to a report name and click the View icon at the top of the form.
 - Click the drop-down arrow next to a report name and select **View Report** from the context menu.

Alternatively, you can view reports from the Scan Details form.

- 1 Click the **Scans** button on the Navigation pane.
- 2 Click the name of the scan for which a report has been generated (or click the drop-down arrow next to the scan name and select **Scan Details**).
- 3 On the Scan Details form, click the **Reports** tab.
- 4 Click the report name, or select the check box next to the name and click View icon at the top of the form.

You can also view reports from the Site Details form.

- 1 Click the **Sites** button on the Navigation pane.
- 2 Click the name of the site for which a report has been generated (or click the drop-down arrow next to the site name and select **Site Details**).
- 3 On the Site Details form, click the **Reports** tab.
- 4 Click the report name, or select the check box next to the name and click View icon at the top of the form.

A AMP Tools

Introduction

The AMP Console includes a robust set of tools and configuration options. The following tools are available from the AMP Console Tools menu:

- Smart Update
- Options
- Encoders/Decoders
- HTTP Editor
- Regex Editor
- Web Proxy
- Web Form Editor
- Web Macro Recorder (Session-Based)
- Web Macro Recorder (Event-Based)
- Web Service Test Designer
- SQL Injector
- Web Brute
- Web Discovery
- Cookie Cruncher
- Web Fuzzer
- Server Analyzer
- Report Designer

In addition, the following tools are also available:

- Policy Manager (accessible from the AMP Console using the Scan Policies form in the Scans/Compliance group)
- Audit Inputs Editor (accessible from the Policy Manager's **Tools** menu)
- Compliance Manager (accessible from the AMP Console using the Compliance Templates form in the Scans/Compliance group)

Certain tools are not enabled unless HP WebInspect and the AMP Console are installed on the same machine.

Options

Use the following procedure to specify settings for the AMP Console.

- 1 From the **Tools** menu, select **Options**.
- 2 To refresh the display of AMP information periodically, select the **Automatically refresh display** check box and specify how often (in seconds) the display should be updated.
- 3 Click **OK**.

Policy Manager

A policy is a collection of audit engines and attack agents that HP scanners use when auditing or crawling your Web application. Each component has a specific task, such as testing for susceptibility to cross-site scripting, building the site tree, probing for known server vulnerabilities, etc. These components are organized into the following groups

- Audit Engines
- Audit Options
- Directory Enumeration
- Unknown Application Testing
- Web Application Servers
- Web Applications
- Web Servers
- 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 Web site for vulnerabilities.

AMP contains several prepackaged policies designed to accommodate the majority of 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

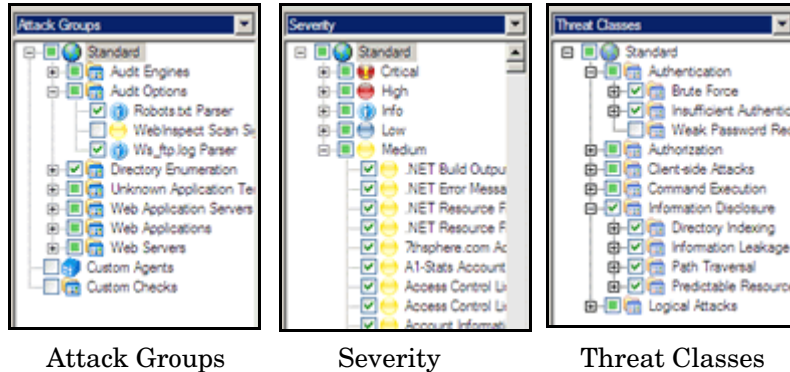
The Policy Manager has two different views, selectable from the **View** menu or by clicking icons on the toolbar. They are:

- Standard
- Search

Standard View

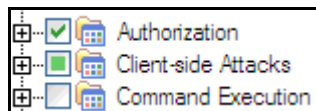
This view displays, by default, a list of checks categorized by threat class (according to classifications established by the Web Application Security Consortium). Alternatively, a drop-down list allows you to display all attack agents by severity, or a list of audit engines and attack groups.

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.

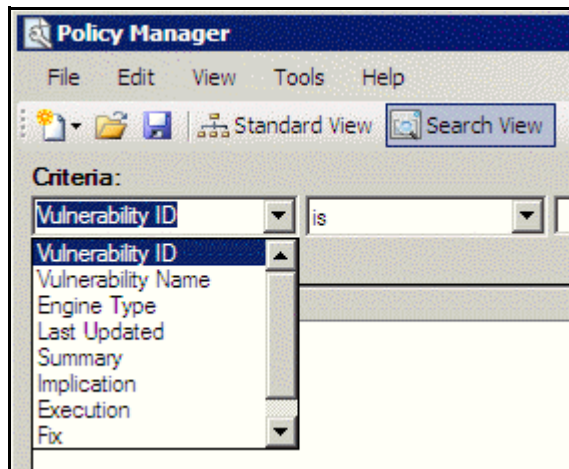
- A check means all objects are selected.
- A green square means some objects are selected.
- An empty box means no objects are selected.



Click the plus sign to expand a node.

Search View

The Search view allows you to locate attack agents containing the text you specify in a selected report field (i.e., summary, implication, execution, recommendation, and fix). 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.



Creating or Editing a Policy

You cannot permanently change the policies that are packaged with AMP. However, you may open any of them as a template, modify their contents to create a custom policy, and save the customized policy under a new name. A custom policy may be edited and saved without changing its name.

Follow the steps below to edit a policy:

- 1 On the AMP Console, click the **Scans/Compliance** group.
- 2 Click the **Scan Policies** shortcut.
- 3 Select a policy.
- 4 Click the **Action** menu and select **Copy**.

The AMP Console downloads the policy from the AMP server and loads it into the Policy Manager.

- 5 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.
- 6 To rename an attack group:
 - a Right-click the attack group.
 - b Choose **Rename** from the shortcut menu.
- 7 To add an attack group:
 - a Right-click any existing attack group and choose **New Attack Group** from the shortcut menu. A highlighted entry named New Attack Group appears.
 - b Right-click the new group and choose **Rename**.
 - c Populate the group by dragging and dropping attack agents onto it.
- 8 You may also create a custom check. See [Creating a Custom Check](#) on page 162 for more information.
- 9 If you select the **Auto Update** check box, HP scanners determine if any updated or new attack agents downloaded from the HP 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 the scanner 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.

New vulnerability checks downloaded via Smart Update are not added automatically to any custom policies you may have created.
- 10 Select **File** → **Save As**. Type a name for your custom policy in the **File name** box and then click **Save**. You cannot save a policy using the name of a prepackaged policy (Assault, Blank, Standard, etc.).

Creating a Custom Check

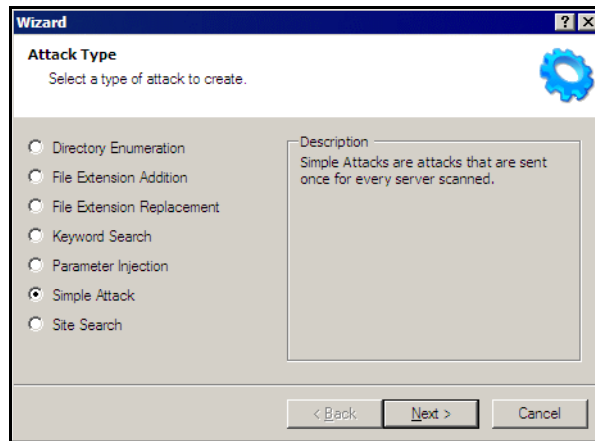
Although HP scanners rigorously inspect your entire Web site for real and potential security vulnerabilities, you may require a custom check to detect vulnerabilities that are unique to your application.

Follow the steps below to create a custom check:

- 1 On the AMP Console, click the **Scans/Compliance** group.
- 2 Click the **Scan Policies** shortcut.
- 3 Select a policy.
- 4 Click the **Action** menu and select **Copy**.

The AMP Console downloads the policy from the AMP server and loads it into the Policy Manager.

- 5 Make sure the Standard view is selected, with attack groups listed in the left pane.
- 6 Right-click on **Custom Checks** and select **New Custom Check** from the shortcut menu.
- 7 When the Custom Check Wizard appears, select an attack type.



The attack types are listed below. See Steps 9-10 for entering attack and signature information.

- **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 the scanner 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 the scanner 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, one standard check searches for files having an extension of “old.” During the crawl, whenever the scanner 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 body of 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

- **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 variations.

- 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]\[boot\sloder\]

– 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: AAAAA...AAAAA [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:

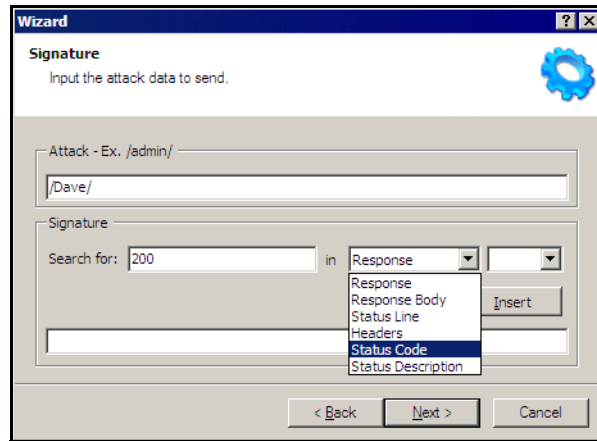
Attack Type: Site Search
Attack: xanadu.html
Signature: [STATUSCODE]2\d\d OR [STATUSCODE]40[1]

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)

8 Click **Next**.

- 9 In the **Attack** box, enter the data you want to use for the attack. In the following example of directory enumeration, the check will search for a directory named “Dave” by appending the attack string (/Dave/) to the target URL or IP address.



- 10 You must specify a signature, which is simply a regular expression (i.e., a special text string for describing a search pattern). When the scanner 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** box 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.

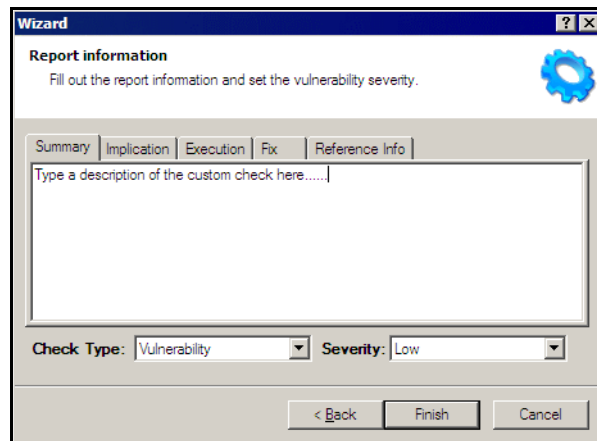
To use the **Search for** box:


- a Enter the text you want to locate.

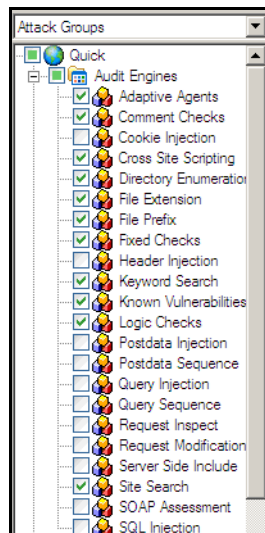
Enter only text; do not enter a regular expression.

- b In this example (searching for a directory named “Dave”), the server would return a status code of 200 if the directory exists, so enter “200” in the **Search for** box. Realistically, however, you might also accept any status code in the 200 or 300 series, or a status code of 401 or 403.
- c Click the drop-down arrow to specify the section of the HTTP response that should be searched.
- d (optional) To create a complex search, click the second drop-down and select a Boolean operator (AND, OR, or NOT).
- e Click **Insert**.
- f (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.

- 11 Click **Next**.



- 12 On the Report Information panel, click each tab and enter the text that will appear in the vulnerability description.
- 13 Select an entry from the **Check Type** list.
- 14 Select a severity level from the **Severity** list.
- 15 Click **Finish**.
- 16 Change the default name “New Custom Check” to reflect the purpose of the check.
- 17 Click  to expand the Audit Engines folder.



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

Table 1 Correlation of Attack Type to Audit Engine

This Attack Type...	Uses this Audit Engine...
Simple Attack	Fixed Checks
Parameter Injection	Post Data Injection
Site Search	Site Search

Table 1 Correlation of Attack Type to Audit Engine (cont'd)

This Attack Type...	Uses this Audit Engine...
File Extension Replacement	File Extension
File Extension Addition	File Extension
Directory Enumeration	Directory Enumeration
Keyword Search	Keyword Search

19 Click **File** → **Save**.

20 Enter a name for the new policy and click **Save**.

All custom checks are added to every policy, but they are not enabled. To enable the custom check in other policies, see [Creating or Editing a Policy](#) on page 162.

Disabling a Custom Check

Follow the steps below to disable a custom check:

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

Deleting a Custom Check

Follow the steps below to delete a custom check:

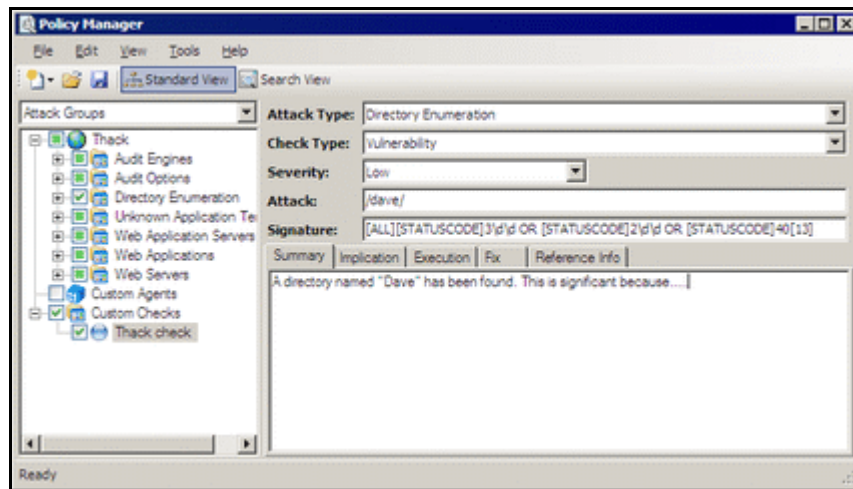
- 1 Right-click a custom check.
- 2 Select **Delete** from the short-cut menu.

Editing a Custom Check

Follow the steps below to edit a custom check:

- 1 Open a policy.
- 2 Select a custom check.

- 3 Using the right pane of the Policy Editor, modify the custom check properties.



- 4 Click the Save icon.

Searching for Attack 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.

Follow the steps below to search for attack agents:

- 1 Open a policy in the Policy Manager.
- 2 Click **View** → **Search**.
- 3 From the **Criteria** list, select the property that you want to search.

The description of every attack agent contains “report fields” such as summary, implication, execution, fix, and reference information. The Search feature allows you to locate attack agents that contain the text you specify in a selected report field. In addition, you can search for a vulnerability ID, vulnerability name, engine type, or the date when last updated.

- 4 Choose an operator from the drop-down list (is, is greater than, is less than, contains).
- 5 In the text box, type the text or number you want to find.
- 6 Click **Search**.








The Policy Manager lists in the **Checks** area all attack agents that match your search criteria. An active agent will have a check mark next to its name. Select (or clear) a check box to activate (or deactivate) an agent.

- 7 Click **Save** to save the revised policy.

Policy Manager Icons

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

Table 2 Policy Manager Icons

Icon	Definition
	The policy.
	Attack Group Folder: Contains vulnerability assessments.
	Audit Methodology: A set of checks that compose an audit methodology. For example, Site Search is part of the Audit methodology.
	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 Inputs Editor

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

Access the Audit Inputs Editor from the Policy Manager (using the Policy Manager's **Tools** menu) 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 Inputs Editor's toolbar or select **File** → **Open**.

You must import into the AMP scan configuration the saved file containing your check input modifications. To do so:

- 1 Create a new scan in the AMP Web Console.
- 2 Under Audit Settings, select **Attack Exclusions**.
- 3 Next to **Import Audit Inputs** (at the bottom of the page), click **Browse**.
- 4 Select the file you created and click **Open**.

Engine Inputs

Follow the steps below 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 scanner's default 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
 - a To add an item to the list, click **Add**.
 - b To edit an item, select an item and click **Edit**.
 - c To delete an item, select the item and click **Remove**.
 - d 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
 - a Unselect the **Use value from defaults** check box.
 - b Select an option from the drop-down list.
- 6 Click the **File** menu and select **Save** or **Save As**.

Check Inputs

Certain checks require inputs that accommodate the specific design of the target Web site. The scanner conducts these checks using default values, which you may need to change.

Follow the steps below to create or modify inputs for specific checks.

- 1 Click the **Check Inputs** tab.
- 2 Select a check (see list below).
- 3 Enter the requested input values.
- 4 Click **File** → **Save** (or **Save As**).

4719: IIS Mapping

Microsoft IIS extension handlers historically have been the source of many vulnerabilities. This check probes for each known IIS extension, and flags a vulnerability for each extension/handler that is found to be enabled. However, in certain cases, an extension handler may be legitimately enabled and used by the target Web site.

Required Input: One or more extensions that identify the handlers that are legitimately enabled and which should be excluded. Valid input is printer, idc, idq, ida, htr, htw, stm, shtm, and shtml.

4721: Admin Section Must Require Authentication

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires authentication before allowing access. This check attempts to access a sensitive directory that should require authentication. The default check input is /admin.

Required Input: The directory (relative to the root) containing administrative or sensitive data.

4722: Logins Sent Over Unencrypted Connection

Any area of a Web application that possibly contains sensitive information or access to privileged functionality (such as remote site administration functionality) should utilize SSL or another form of encryption to prevent login information from being sniffed or otherwise intercepted or stolen.

Required Input: Login forms. The name of file containing login form.

4723: Logins Sent Over Query

Information in query strings is directly visible to the end user via the browser interface, which can cause security issues. Recommendations include performing server-side input validation to ensure data received from the client matches expectations.

Required Input: Login forms. The name of file containing login form.

4724: Password Field Masked

Basic Web application security measures include “masking” all passwords entered by a user when logging on to a Web application. Normally, each character in a password entered by a user is instead represented with an asterisk. Recommendations include requiring all password fields in your Web application be masked to prevent other users from seeing this information.

Required Input: The name attribute of input controls containing a password.

4726: Secure Section Only Accessible Via SSL

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires that the pages under the secure section of the site are only accessible via SSL.

Required Input: The name of the secure directory, relative to the root. The default is /secure.

4728: Persistent Cookies

Persistent cookies are stored on the browser’s hard drive. This can cause security and privacy issues depending on the information stored in the cookie and how it is accessed. This check calculates how many seconds until a received cookie is set to expire. If the expiration date/time is less than the specified number of seconds (default: 600), the check considers the cookie’s life span to be excessive, increasing the chances of session ID recovery and session hijacking.

Required Input: The lifetime allowed for cookies (in seconds).

4729: User supplied data without POST

An area of the Web application that possibly contains sensitive information or access to privileged functionality (such as remote site administration functionality) uses query strings to pass information between pages. Information in query strings is directly visible to the end user via the browser interface, which can cause security issues. The input value for this check is a space-separated list of regular expressions that are used to identify sensitive URL parameter names when used in GET queries. Generally, information such as passwords, social security numbers, etc., should not be sent as parameters to GET queries, since the GET

query (and thus the sensitive information) can persist in Web server and proxy logs and the Web browser's history. You will need to adjust the regular expressions accordingly to specify the parameter names your application typically uses to denote sensitive information.

Required Input: Sensitive parameter (a regular expression). An example is:

`p|P]ass(word)? [u|U]ser_?([N|n]ame)? [s|S][s|S][n|N]`

4731: Script Directory Check

A directory containing an object referenced in a post request or query string should not have a name that could easily be guessed by an attacker. The primary danger from an attacker discovering this directory would arise from the information he could gather from its contents, such as what language was used to code the Web application. This check is used to determine if a dynamic form action points to a file/URL that is in a directory whose name is included in the list.

Required Input: Names of directories containing scripts.

4732: Script File Extension Disclosure

Any area of the Web site or Web application that contains sensitive information or access to privileged functionality (such as remote site administration) requires the file extension of all scripts to be checked as it may lead to information disclosure related to the technology used by the application. The use of certain CGI-related file extensions can indicate certain types of technology in use, which results in a mild information disclosure. The default list of check input values is generally applicable, but some sites may legitimately use a certain technology (such as Perl) and this check may incorrectly elicit false-positive issues in flagging all Perl extensions (.pl). In such cases, you should remove the legitimate extensions from the list.

Required Input: File extensions of scripts used in the Web application (such as cgi, pl, and py).

5151: Arbitrary Remote File Include

This check attempts to discover if the Web application can fetch and incorporate data from arbitrary URLs supplied by an attacker.

This is the most complex check to configure, because its extreme flexibility enables it to work in many environments and topologies. Basically, the check injects URL values into application parameters, attempting to force the application to make an HTTP request to the supplied URL. This activity looks for "remote file inclusion" vulnerabilities caused by the application attempting to remotely retrieve the specified file/URL and include the response into the application's processing. In certain extreme circumstances found in PHP environments, the application will remotely retrieve the file and execute any PHP script contained therein, making the activity capable of arbitrary code/script execution.

Check 5151 can operate in two modes: static and server (controlled by the "Audit Mode" parameter).

Static Mode

You specify the target external URL as the **Static Mode Target URL**, and a corresponding regular expression signature as the **Static Mode Signature**. If you want to use external targets, then you should use static mode. By default, the check uses static mode and the test URL of "http://216.183.127.201/serverinclude.html?" which is a special page hosted on an HP Web server located on the public Internet at IP address 216.183.127.201. The signature contains a specific value that is returned by the indicated test URL. If you do not want to use the HP

Web server (particularly if the target server cannot access the Internet), then you should adjust the test URL (and corresponding signature) to a URL hosted by a server. When configuring static mode:

- Specify a full, absolute URL (i.e., it should begin with “http://”).
- For best results, use non-SSL URLs (although SSL URLs are allowed).
- Include a question mark (?) at the end of your URL to ensure the URL is not affected if the application appends additional data to the end of the URL.

Server Mode

In this mode, the scanner runs its own Web server and attempts to get the target/scanned server to connect to the scanning system. The added benefit of Server mode is that it can detect “blind” remote file inclusion vulnerabilities, resulting in potentially fewer false negatives. To use Server mode, the check conceptually needs three pieces of information:

- **Server Mode Target IP**—The IP address the server/target should use to access the host (particularly if the scanning system’s network IP is different than what the server would need to access, due to a firewall or a multi-homed scanning system). The default value is empty/blank, meaning that it uses the same IP address ultimately used or determined by the Server Mode Server IP.
- **Server Mode Server Port**—The port number to run the listening Web server on. Using a specific port may be necessary due to network/access restrictions. The default value is 8181. If you leave this value blank, then the Remote File Include engine will dynamically choose a port between 25000 and 25100.
- **Server Mode Server IP**—The local IP address of the scanning system to bind the Web server on, if the system is multi-homed and/or you do not want to bind the Web server listening on the first local IP address. The default value is “0.0.0.0”, which instructs the scanner to use the first available IP address on the system.

Although the default values fit most configurations, certain circumstances require specific modification.

- If your system has multiple IP addresses (due to multiple network adapters), then you may need to specify the explicit IP address to bind to (i.e., the one that is most appropriate for receiving requests from the system you are scanning). You can determine the list of your system’s IP addresses by running “biconvex” from a Windows command prompt.
- If you are running multiple scans from the same scanning system using server mode, then you should leave the **Server Mode Server Port** value blank, causing the scanner to dynamically pick the port. This is because two scans cannot run two separate Web servers listening on the same port. One specific port can only be used by one scan at a time.
- If your system is behind a firewall and you are using port-forwarding to receive the incoming HTTP requests, or you are on a network that uses NAT, then the IP address used by the server to access your system will be different from the IP address actually assigned to your system. In this case, you will need to specify the IP address the target server should use for the **Server Mode Target IP**.

Required Inputs: Static mode target URL, Audit mode (static or server), Server mode server IP, Server mode Server port, Server mode target IP, static mode signature (a regular expression)

5546: Privacy Policy Not Present

This check is associated with the scanner's compliance policies. Many legislative initiatives require organizations to place a publicly accessible document within their Web application that defines their information privacy policy. If the scanner does not find the specified file, it creates a vulnerability in the Best Practices category.

Required Inputs: The relative directory and file name of the privacy policy.

10183: Allowed Top-Level Domain

Certain organizations (especially branches of the U.S. federal government) must use a restricted set of DNS top-level domain names (TLDs), such as .gov, .mil, or .fed. This check ensures that all allowed hosts encountered during the scan use one of the specified TLDs. Most public corporations arbitrarily use any TLD they desire (.com, .net, .org, etc.); those corporations should either disable this check (preferable) or change the default values to include .com, .net, and .org (and/or any other appropriate TLDs).

Required Inputs: All allowed top-level domains.

10274: Proxy CONNECT Access

Some proxy servers accept the CONNECT method to make an HTTP connection to another server. Usually, this method should be restricted to internal use only. If it is not restricted, your server can be used by an attacker on the Internet to disguise himself as your own server. Thus, any attack will appear to come from your server. This type of vulnerability is usually caused by not properly configuring the proxy server. Attackers can masquerade as your proxy server when conducting other attacks. Attackers may be able to access internal machines through the CONNECT proxy. This attack can also be used to enumerate your local network.

This check attempts to treat the target server as a proxy server for SSL requests. The check issues a CONNECT request to the target server, which essentially asks the server to make a connection to another external site. You can control which external site is used via the input values for this check. By default, the value "https://www.google.com/" is used, causing the server to make an external request to the host www.google.com on port 443. You may wish to modify this value to point to a more appropriate internal host. If so:

Use a server that has SSL enabled on the standard SSL port 443, if possible. Some proxies refuse connections to ports other than 443 due to explicit configuration.

Use the https:// URL format.

If you need to specify a port other than 443, use the normal URL format to specify a port after the host name (e.g., https://example.com:8443/).

Only the host name and port number are used; the remainder of the URL is ignored.

10275: Proxy GET Access

This check is virtually identical to check 10274, except it issues a proxy-qualified GET request to the target server instead of a CONNECT request. There are many servers that are willing to take a proxy-qualified GET request and treat it as a normal GET request (ignoring the proxy-specific aspects of the request), so it is necessary for the check to evaluate the response content to ensure the response is truly from the external server and not a normal response from the target. That is why check 10275 has two check inputs: one for specifying the external target host, and one for specifying a regular expression to match against the response content. By default the check attempts to access "http://www.google.com/" and looks for the phrase "Google Search" in the response. You will need to adjust the check input values if you need to

use a different external host or an internal host. You can change the external target simply by adjusting the target check input value, and then specifying a unique value from the target page as the check input regex value.

- The URL target must begin with `http://` or `https://`. For best results, use `http://`.
- If you need to specify a specific port other than 80/443, use the normal URL format to specify a port after the host name (such as `http://example.com:8080`).
- Unlike check 10274, the target URL you specify for 10275 is used in its entirety; if you specify a specific page/URL, then that specific page/URL will be requested.
- Try to select a unique value/phrase from the target URL to use as the response regex value, one that is not likely to appear elsewhere on the target scanned site; using the value in the `<title>` tags usually is sufficient (you can also include the “`<title>`” tags in the regex value itself).
- Remember to properly escape any regex-specific metacharacters (periods, parentheses, etc.).
- The check does not follow redirects (HTTP 302 responses), so you will need to specify an explicit final URL destination.

Required Inputs: Proxy GET target and Proxy GET target response (regular expression).

10280: Price-Related Form Fields

Forms containing price-related field names could harbor price manipulation vulnerabilities that would allow the attacker to change the price of the product.

Required Inputs: Names of price-related fields.

10287: Local File Include

Several types of attacks involve malformed filename requests that result in reading local files from the Web server. The Local File Include engine generates requests that contain variously encoded file names, and then evaluates the responses to determine if the contents of those files were recovered.

Mode

The Mode parameter relates to the platform assumptions made by the engine. The default mode value, **Auto**, causes the engine to look for both “`c:\windows\win.ini`” (Windows) and “`/etc/passwd`” (Unix) files and to use both Windows and Unix parent directory references accordingly. If the engine gets a visual response that explicitly indicates the underlying platform (Windows vs. Unix), it will automatically switch to using only the values for appropriate target platform for the remainder of the auditing for that application parameter value. If you already know what the underlying platform is before you scan (i.e., Windows vs. Unix), you can change the mode to **Windows** or **Unix**, which can save scan time since it reduces the number of values that need to be sent. At this time the engine does not support platforms that do not use a Windows (“\”) or Unix (“/”) path separator.

User-Specified File

If you want to use a specific target file, specify it here. There are occasions when the default file name values (“`c:\windows\win.ini`” and “`/etc/passwd`”) may not work in your environment. For example, your Web application can be hosted on a Windows drive other than ‘C:’, or your Web application could be operating out of a Unix chroot environment. In both cases, parent directory references will not be able to locate the specified target files even if a vulnerability

does exist. For this situation you should either use an existing file that is in the root directory of the same drive/chroot of the Web application, or explicitly create a text file in the root directory of the drive/chroot used by your Web application and place a unique value inside the text file. Then you inform the LFI engine to look for your specific file by setting the **UserOnly** mode option, and specifying the absolute path to your target file in the **User Specified File** check input. You will also need to specify a corresponding **User Specified File Regex** check input value; the regex value should uniquely identify/match the contents of your specified file while not matching any content typically found on the scanned Web site. You can also select the **UserAndAuto** mode, which would let you specify a file and still use the default “c:\windows\win.ini” and “etc/passwd” values.

User-Specified File Regex

If you use a specific target file, then you need to specify a regular expression that matches the contents of the target file.

Audit Disposition

The Audit Disposition parameter default value **Adaptive** treats Web application parameters in one of two ways: parameters with existing values that resemble file names receive significant (aggressive) scrutiny, while all other parameters receive basic scrutiny. The premise is that if the parameter has a value that resembles a filename, then there is a higher likelihood that the value is used in a file system operation; because of that higher likelihood, it makes sense for the engine to try more variations (particularly minor variations) to ensure that is not the case. However, trying additional minor variations can extend scan time, because it results in more attacks to be sent. That is why the **Adaptive** disposition tries to determine when it seems appropriate to spend the extra effort in auditing a particular parameter. However, if you desire the utmost level of scrutiny for all parameters, change the Audit Disposition value to **Aggressive**.

Required Inputs: Mode and Audit disposition.

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 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 login form, the user will proceed to the application’s beginning page.

Some sites (such as HP’s example banking application zero.webappsecurity.com) contain many different forms for completing a variety of transactions. If the scanner is 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 DevInspect encounters an input control whose name attribute is not matched in the file you create, it will submit a default value (12345).

For server authentication (logging in to a server with a user name and password), you can enter values here or on the **Authentication** tab of the *Settings* window.



If you are using a proxy server, the WebForm Editor will not use the default settings from WebInspect. You must first configure Internet Explorer to use the desired proxy.

There are two ways to create a list of form values:

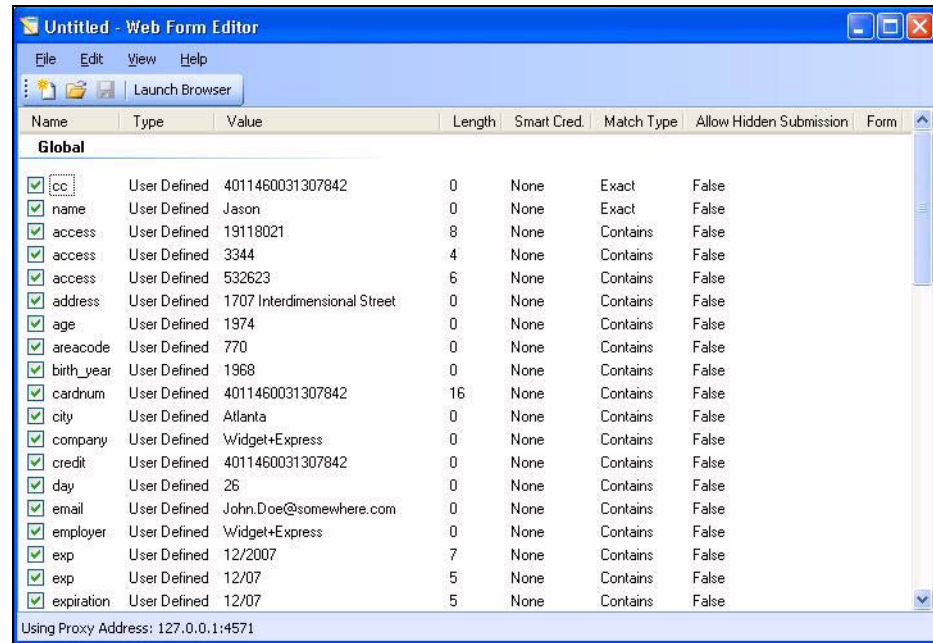
- Create the list manually.
- Record the values as you navigate through the application.

Manually Creating a Web Form List

Use the following procedure to create a Web Form list manually.

- 1 Click **Tools** → **WebForm Editor**.

The *WebForm Editor* window appears.



The WebForm Editor loads a prepackaged default file.

- a To load a different file, select **File** → **Open**.
 - b To create a new file, select **File** → **New**.
- 2 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.

- 3 In the **Name** box, type (or modify) the name attribute of the input element.
- 4 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).

- 5 In the **Value** box, type the data that should be associated with the input element (for example, a password).
- 6 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.
- 7 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**.
 - 8 Click **Add** (or **Modify**).
 - 9 If necessary, you can assign additional attributes by right-clicking an entry and using the shortcut menu.
 - To submit the form value for any input control having the same name attribute, regardless of the URL at which it occurs, choose **Make Global**.
 - 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**.

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.”

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 clicking **Edit** → **Settings**.

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 **File** → **New** (or click the New icon on the toolbar).
- 2 To add form values to an existing list, select **File** → **Open** (or click the Open icon on the toolbar) and choose a file using the standard file-selection dialog.
- 3 Click **Launch Browser**.
- 4 Using the browser’s **Address** bar, enter or select a URL and navigate to a page containing a form.

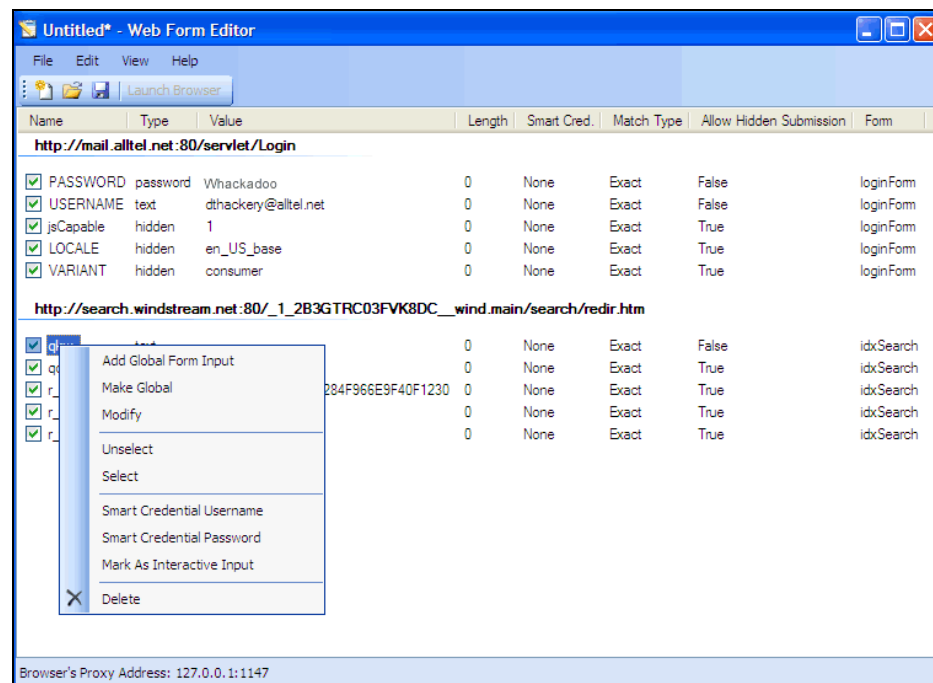
Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, the Web Form Editor will not receive such traffic. This is a documented Microsoft defect. To access a site on “localhost” when using IE7, place a period or dot after “localhost” (for example, <http://localhost.:8080/test.html>).

- 5 Complete the form and submit it (usually by clicking a button such as **Log In**, **Submit**, **Go**, etc.).
- 6 Navigate to additional pages and submit forms until you have traversed all the links you wish to follow.
- 7 The Web Form Editor displays a list of name and value attributes for all input controls found in all forms on the pages you visited.

For example, the first two entries in the following illustration 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.



- 8 If necessary, you can modify items by right-clicking an entry and using the shortcut (pop-up) menu.
 - To submit the form value for any input control having the same name attribute, regardless of the URL at which it occurs, choose **Make Global**.
 - 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**.
- To force the scanner to pause 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 will pause the scan and display a window that allows 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 will 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).

- 9 Click **File** → **Save** (or **Save As**).

Importing a Web Form File

You can import a file that was designed and created for earlier versions of the scanner and convert it to a file that can be used by the current Web Form Editor.

- 1 Click **File** → **Import**.
The *Convert Web Form Values* window appears.
- 2 Click the ellipses 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 ellipses 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**.

Scanning with a Web Form File

When scanning a site, you specify which Web Form file you want to use by selecting **Auto-fill web forms during crawl** and then selecting a file.

- 1 Click the **New Scan** action.
- 2 On the *Configure Scan* window, click **Switch to Advanced**.
- 3 In the **Scan Settings** group, select **Method**.
- 4 Select **Auto-fill Web Forms During Crawl**.
- 5 Click **Browse**.
- 6 Using the standard file-selection window, select a file containing the Web form values you want to use and click **Open**.

Web Form Editor Settings

Follow the steps below to modify the Web Form Editor settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **General** or **Proxy** category and enter the settings described in the following sections.
- 3 Click **OK**.

General

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 IP address and port by selecting **Edit** → **Settings**.

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 by selecting an entry from the **Assumed 'charset' Encoding** list.

Proxy

Use these settings to access the Web Form Editor 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, the Web Form Editor will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

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

Web Form Logic

When crawling a Web application and submitting Web form values, the 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.”

Table 3 Rules for Matching Web Form Values

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).

Table 3 Rules for Matching Web Form Values (cont'd)

	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 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 for the record allows for submission to any field length (wildcard field length match).
	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."

Web Brute

This tool will determine if your users are employing user names and passwords that an unauthorized intruder might be able to guess easily. For example, if one of your customers is accessing your Web site by using a username of "customer" and a password of "password," you might want to warn that user about his susceptibility and suggest that he change his password and/or username.

Web Brute will attempt a "brute force" attack of a login form or authentication page, using two prepared lists of user names and passwords.



This is an intrusive attack and can break into a secure area. Brute force attacks are intended for testing purposes only, and should not be used against unsuspecting Web sites.

Mounting a Brute Force Attack

Follow the steps below to use a brute force authentication attack:

- 1 On the AMP Console menu bar, click **Tools** → **Web Brute**.
- 2 In the **Enter URL** box, type the URL of the site you want attack and click **Next**.
- 3 Select the authentication type used by the target site. See [Authentication](#) on page 122 for a description of the available authentication types.
- 4 If necessary, use the **Domain** box to specify the domain that should be used for authentication. Web Brute will prefix this string to each user name that it submits. Do not include a backslash.
- 5 Click **Next**.
- 6 If you selected **Web Form** in Step 3, a Web browser opens. If necessary, navigate to the login page.
- 7 On Web Brute's **Form Field Setup** panel, select (check) the fields you want to brute force. If you already know the value that should be entered for a field, remove the check mark, double-click the cell in the **Value** column for that field, and enter the value.

Web Brute

File Edit View AMP Help


Launch Browser Brute Stop Clear

Form field setup.
Check the fields you wish to brute and select a dictionary.

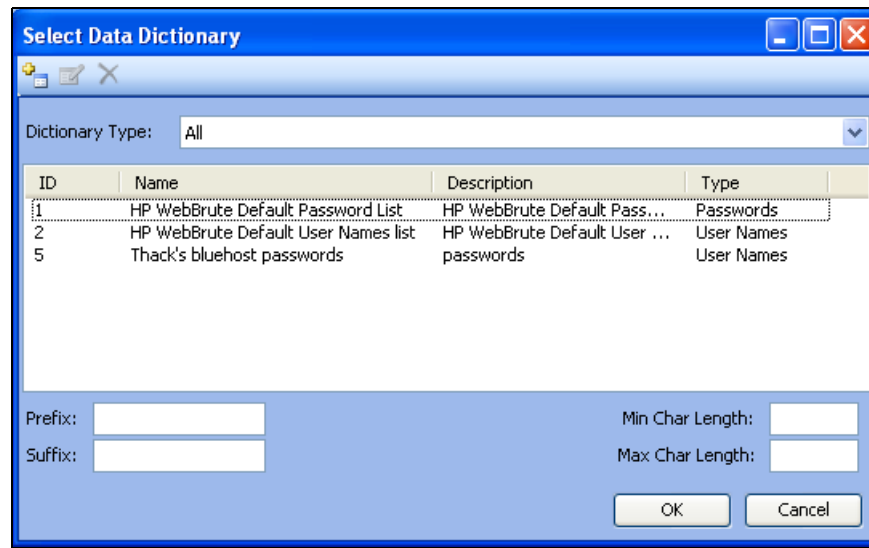
	Name	Type	Value	Length	Smart Cred.	Form	Dictionary	Join
	http://mysql-win2k3:80/Pugnose/login.asp							
<input checked="" type="checkbox"/>	password	password		0	None	fromLogin	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	uid	text		0	None	fromLogin	<input type="checkbox"/>	

Cancel < Back Next > Brute

Browser's Proxy Address: 127.0.0.1:2937

- 8 For fields you have selected (checked), click  in the **Dictionary** column to select a list of names or passwords to be submitted.

The *Select Data Dictionary* window appears, listing all currently defined dictionaries. You can limit the display of dictionary names by selecting an entry in the **Dictionary Type** list.



These dictionaries are in a database that is not directly accessible. To create your own dictionary or merge a list into an existing dictionary, see [Creating and Importing Lists](#) on page 190.

9 Select a list.

10 (Optional) Enter the following:

- **Prefix:** A string that will be added to the beginning of each entry in the list.
- **Suffix:** A string that will be added to the end of each entry in the list.
- **Min Char Length:** The minimum number of characters allowed for each entry; entries that are shorter will not be submitted.
- **Max Char Length:** The maximum number of characters allowed for each entry; entries that are longer will not be submitted.

11 Click **OK**.

12 Repeat steps 7-11 for each authentication field to be submitted.

13 If you want to “join” two or more lists, click the **Join** column associated with each list.

If a list of user names is joined with a list of passwords, then Web Brute will submit user names with passwords in the order in which they appear in the lists. That is, the first name in the user name list will be submitted with the first password in the password list, the second name will be submitted with the second password, etc.

If the two lists are not joined, then Web Brute submits each user name with all passwords. This feature is used most often for Web form authentication where the user must re-enter the password. In this case, Web Brute would use two lists, but the password list would be specified for both the “password” and “confirm password” fields. You would then join these fields, forcing the same password to be submitted for each field.

14 To modify the parameters that Web Brute uses during an authentication attack, select **Edit** → **Settings**. See [Web Brute Settings](#) on page 191 for more information.

15 Click **Next**.

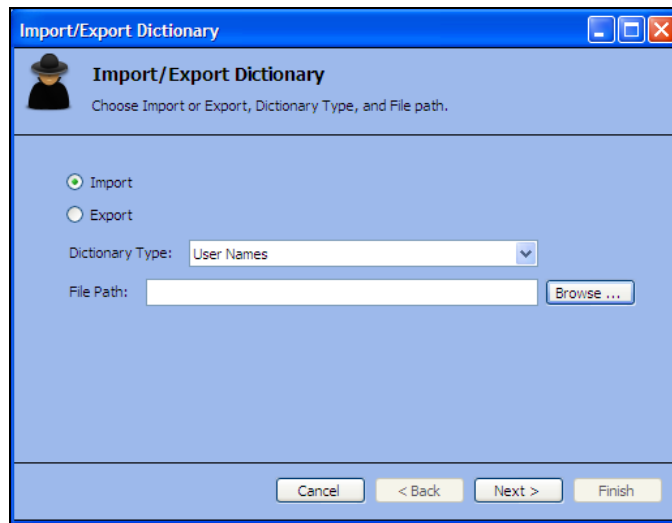
- 16 To see a list of failed name/password attempts (in addition to successful attempts), select **Show Failed**.
- 17 Click **Brute**.

Web Brute attacks the site and displays the results. If you double-click a result (either successful or failed), Web Brute opens the HTTP Editor, allowing you to inspect both the HTTP request and response.

Creating and Importing Lists

To use your own list of passwords or user names, you must first create a list and then import it into Web Brute as a “dictionary,” using the following procedure:

- 1 Create a text file where each entry is delimited by a carriage return and line feed.
- 2 Click **File** → **Import/Export Dictionary**.
- 3 On the *Import/Export Dictionary* window, select **Import**.



- 4 From the **Dictionary Type** list, select either **User Names**, **Passwords**, or **E-mails**.
- 5 Click **Browse** and select the file containing the list you want to import.
- 6 Click **Next**.
- 7 On the *Import Dictionary* window, specify a name for the dictionary and enter a description.
- 8 Click **Next**.
- 9 Click **Finish**.

Exporting Dictionaries

Use the following procedure to create a text file from a Web Brute dictionary:

- 1 Click **File** → **Import/Export Dictionary**.
- 2 On the *Import/Export Dictionary* window, select **Export**.

- 3 In the **File Path** box, enter the path and name of the text file in which the dictionary contents will be saved, or click **Browse** and use the *Save As* window to specify the name and path.
- 4 Click **Next**.
- 5 On the *Export Dictionary* window, select a dictionary type from the list.
- 6 Select a dictionary.
- 7 Click **Next**.
- 8 Click **Finish**.
- 9 Click **Done**.

Web Brute Settings

Follow the steps below to modify the Web Brute settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **Options**, **Authentication**, or **Proxy** tab and enter the settings described in the following sections.
- 3 Click **OK**.

Options

Timeout in seconds

Enter the number of seconds that Web Brute will wait for a response. If a response is not received during this period, Web Brute will resend the request, up to the number of times specified in the Retry Count setting.

Retry Count

Enter the number of times that Web Brute will resend a request that has not been acknowledged.

Apply State

If you select this option, Web Brute will attempt to maintain state during the procedure.

Apply Proxy

If you select this option, Web Brute will use the settings on the Proxy tab to connect to the target site (if the Direct Connection option is not selected).

Logging

Select the types of messages that should be logged.

Max Concurrent Threads

Enter or select the number of requests that Web Brute may send before requiring a response to the first request.

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 Brute should use.

Authentication

- 4 If required, select an authentication method and provide credentials. The methods are:
 - **None**—Select this option if the site does not require authentication.
 - **Automatic Authentication**—This allows Web Brute to determine the correct authentication type.
 - **HTTP Basic Authentication**—This is a widely used, industry-standard method for collecting user name and password information. Normally, a Web browser displays a window for a user to enter a previously assigned user name and password, also known as credentials. The Web browser then attempts to establish a connection to a server using the user's credentials.
 - **NTLM Authentication**—NTLM (NT LanMan) is an authentication process that is used by all members of the Windows NT family of products. Like its predecessor LanMan, NTLM uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.

After selecting an authentication method, enter a user name and password. To avoid typographic errors, re-enter the password in the **Confirm Password** box.

Proxy

Use these settings to access the Web Brute 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, Web Brute will use the Web Proxy Autodiscovery Protocol (WPAD) to automatically locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

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.

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

Web Discovery

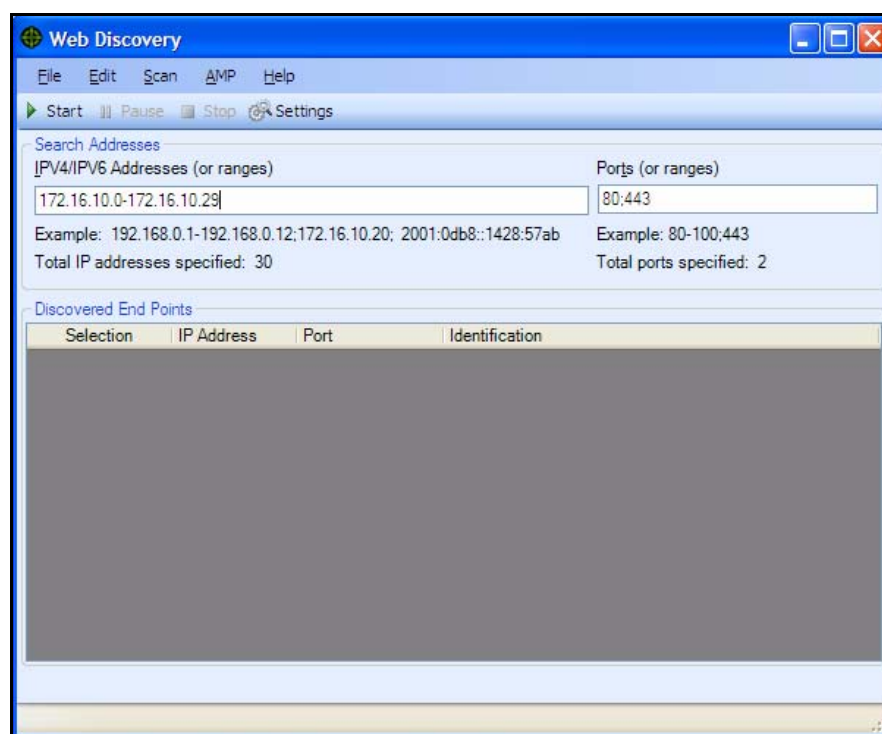
Use Web Discovery to find all open hosts in your enterprise environment.

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.



Discovering Sites

To discover sites using Web Discovery:

- 1 In the **IP 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.
- 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](#) on page 195 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 *Settings Properties* window and view the raw request and response.

To save the list of discovered servers:

- 1 Click **File** → **Export**.
- 2 Use the standard file-selection window to name and save the file.

Web Discovery Settings

Follow the steps below to modify the Web Discovery settings:

- 1 Click **Edit** → **Settings**.
- 2 Enter the settings described in the following sections.
- 3 Click **OK**.

Select Protocols

Choose the packet type you want to send by selecting or clearing the check box next to the protocol name.

Logging

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.

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.

Connectivity

Set the following timeouts (in milliseconds):

- **Connection:** 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:** When sending a message to the remote IP endpoint, 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:** 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.

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



If you are using Windows XP with Service Pack 2 (SP2), your **Open Sockets** setting is set to 10. If you increase this setting, you will increase the likelihood that the scanner will fail to detect servers. This occurs because Microsoft has limited the number of open sockets to 10.

Encoders/Decoders

This tool allows you to encode and decode values using Base64, 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

Follow the steps below to encode a string:

- 1 Type (or paste) a string into the **Text** area, or load the contents of a file by selecting **File** → **Open**.
- 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 198.
- 4 If necessary, type a key in the **Key** box. 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).

Decoding a String

Follow the steps below 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**.
- 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.

- 4 If necessary, type a key in the **Key** box.
- 5 Click **Decode**.

You can also use the 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 three 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** 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 allows you to select the encoding types described below.

- 3DES is 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 is an encryption algorithm that can be used as a replacement for the DES algorithm.
- DES (Data Encryption Standard) is 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 is hexadecimal.
- MD5 produces a 128-bit “fingerprint” or “message digest” of whatever data you enter.
- RC2 is 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 is 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 is a simple Caesar cipher used for obscuring text by replacing each letter with the letter thirteen places down the alphabet.

- SHA1 is 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 uses 256-bit encryption.
- SHA384 uses 384-bit encryption.
- SHA512 uses 512-bit encryption.
- ToLower changes upper-case letters to lower-case.
- ToUpper changes lower-case letters to upper-case.
- TwoFish is 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 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.

Prefixed

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.

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 verify regular expressions.


Follow the steps below to use the Regular Expression Editor:

- 1 Click **Tools** → **Regex Editor**.


The *Regular Expression Editor* window opens.





- 2 In the **Expression** box, type or paste a regular expression that you believe 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 special Regular Expression Extensions to restrict your search to certain areas of an HTTP message.

	Any single character	.
	Zero or more	*
	One or more	+
	Or	
	Word boundary	\b
<hr/>		
	IPv4 address	{...}
	URL	{...}

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

- 3 In the **Search Text** box, 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. To do so:

- 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 the 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 If you want 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 will be highlighted in red.

- 7 If you selected the **Replace** option, click **Replace** to substitute all found strings with the replacement string.

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.

Table 4 Characters Used in Regular Expressions

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/([^ec].* e[^n].* c[^a].* .{3,})[/][./*] 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.”

Table 4 Characters Used in Regular Expressions (cont'd)

Character	Description
?	Matches the preceding character zero or one time. <code>/a?ve?/</code> matches the “ve” in “never.”
.	Matches any single character except a newline character.
[xyz]	A character set. Matches any one of the enclosed characters. <code>/[abc]/</code> matches the “a” in “plain.”
\b	Matches a word boundary, such as a space. <code>/ea*r\b/</code> matches the “er” in “never early.”
\B	Matches a nonword boundary. <code>/ea*r\B/</code> matches the “ear” in “never early.”
\d	Matches a digit character. Equivalent to <code>[0-9]</code> .
\D	Matches a nondigit character. Equivalent to <code>[^0-9]</code> .
\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 <code>[\f\n\r\t\v]</code>
\S	Matches any nonwhite space character. Equivalent to <code>[^ \f\n\r\t\v]</code>
\w	Matches any word character including underscore. Equivalent to <code>[A-Za-z0-9_]</code> .
\W	Matches any nonword character. Equivalent to <code>[^A-Za-z0-9_]</code> .

Regular Expression Extensions

Hewlett-Packard 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

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

- [METHOD]
- [REQUESTLINE]
- [VERSION]
- [POSTDATA]
- [URI]

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 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 that 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
```

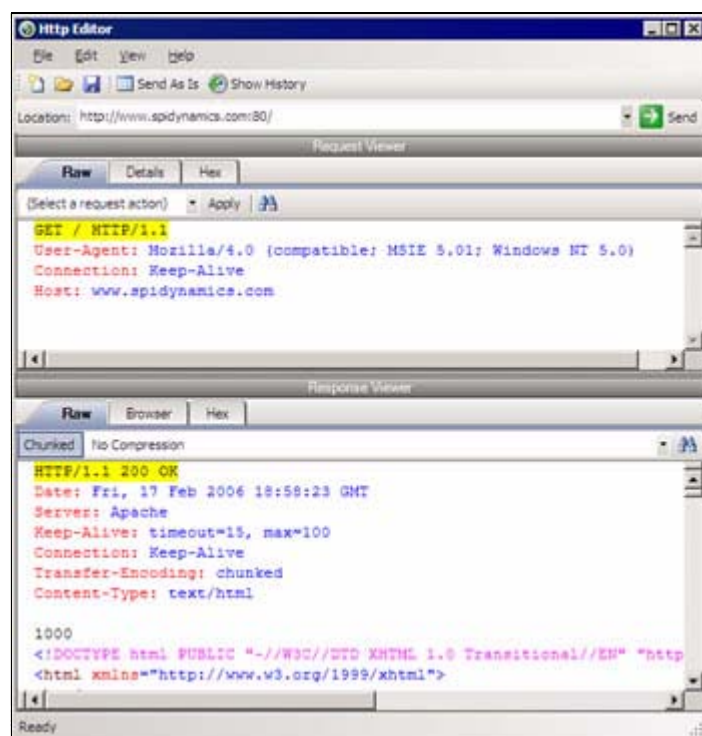
To detect a response containing a specific string (such as “Please Authenticate”) in the Reason-Phrase portion of the status line, use the following regular expression:

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

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 that 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 pane contains the HTTP request message, which you can view in three 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 (Note: This tab appears only if the request contains XML-formatted data).

Response Viewer

The Response Viewer pane contains the HTTP response message, which you can also view in three 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 (Note: This tab appears only if the response contains XML-formatted data).

HTTP Editor Menus

File Menu

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

- **New Request**—Deletes all information from previous sessions and resets the Location URL.
- **Open Request**—Allows you to load a file containing an HTTP request saved during a previous session.
- **Save Request**—Allows you to save an HTTP request.
- **Save Request As**—Allows 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 allows 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 most standard HTTP proxy servers cannot process non-compliant HTTP requests.

- **Exit**—Closes the HTTP Editor.

Edit Menu

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

- **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 window that allows you to search for text that you specify.
- **Settings**—Allows you to configure request, authentication, and proxy parameters for the HTTP Editor.

View Menu

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

- **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 Web sites offers significant cost savings over the use of legacy character sets. Unicode enables a single software product or a single Web site 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** list on the Request 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 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, 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].


Editing and Sending Requests

Follow the steps below to edit and send a request.

- 1 Modify the request message in the Request Viewer pane.
To change certain features of the request, select an item from the **Action** list and click **Apply**.
- 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**).
- 5 To save a request, select **File** → **Save Requests**.

Searching for Text

Follow the steps below 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**.

HTTP Editor Settings

Follow the steps below to modify the HTTP Editor settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **Options**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.
- 3 Click **OK**.

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 allows 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 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 WebInspect and a scan tab has focus (that is, after opening or while conducting a scan). If you select this option, the HTTP Editor applies the Filters settings from WebInspect's Default Scan Settings to add search-and-replace rules for HTTP requests and responses. Note that if you change WebInspect's Current or Default Scan Settings, the changes will not be applied.
- **Apply Header** — This option appears only when you invoke the HTTP Editor while using WebInspect and a scan tab has focus (that is, after opening or while conducting a scan). If you select this option, the HTTP Editor applies the Cookies/Headers settings from WebInspect's Default Scan Settings for HTTP requests. Note that if you change WebInspect's Current or Default Scan Settings, the changes will not be applied.

Enable Active Content

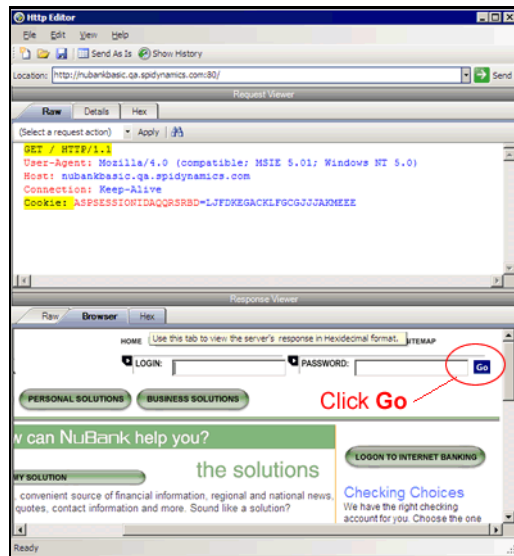
Select this option to allow execution of JavaScript and other dynamic content in all browser windows.

Navigation

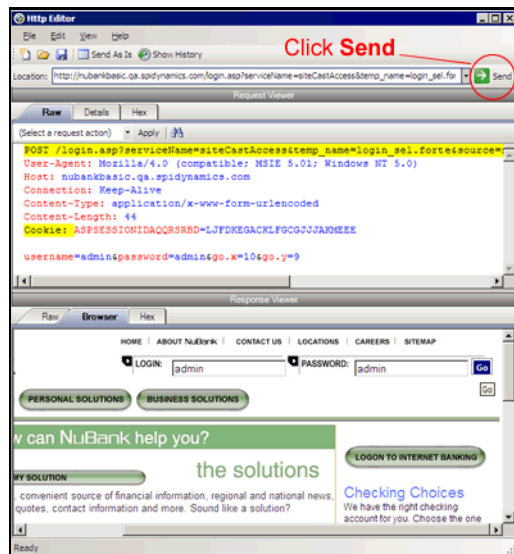
In the **Navigation** group, select either **None**, **Interactive**, or **Browser Mode**.

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 nubankbasic.qa.spidynamics.com (shown below), you could enter a user name (“admin”) and password (“admin”), and then click **Go**.



The HTTP Editor formats the request (which uses the POST method to the login1.asp 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.

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 HTTP Editor should use.

Authentication

If authentication is required, select a type from the **Authentication** list. See [Authentication](#) on page 122 for a description of the available authentication types.

After selecting an authentication method, enter a user name and password. To avoid typographic errors, re-enter the password in the **Confirm Password** box.

Proxy

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

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

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information (as described in the preceding table).

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 the 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 Startup macro or a Login macro that you can use with WebInspect or the Access Management Platform (AMP).

Before using Web Proxy with your browser, you must configure your browser's proxy settings. If using Internet Explorer:

- 1 Click **Tools** → **Internet Options**.
- 2 Click the **Connections** tab.
- 3 Click **LAN Settings**.
- 4 On the *LAN Settings* window, select **Use a Proxy Server for your LAN** and enter the address and port of the proxy server you want to use. By default, Web Proxy uses your local host settings (127.0.0.1:8080).




Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, Web Proxy will not receive such traffic. This is a documented Microsoft defect. To access a site on “localhost” when using IE7, place a period or dot after “localhost” (for example, <http://localhost.:8080/test.html>).


You should also configure Microsoft Internet Explorer to use HTTP 1.1 through proxy connections. On Internet Explorer:

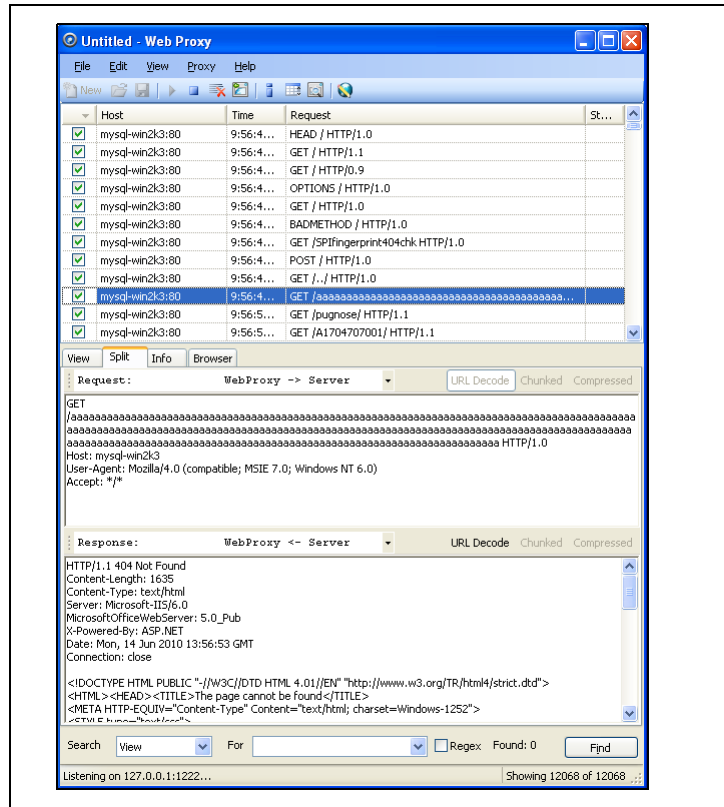
- 1 Click **Tools** → **Internet Options**.
- 2 Click the **Advanced** tab.
- 3 In the “HTTP1.1 settings” section, select **Use HTTP 1.1 through proxy connections**.

Using Web Proxy

Follow the steps below to use Web Proxy with a browser:

- 1 Click **Tools** → **Web Proxy**.
The *Web Proxy* window opens.
- 2 Click  or select **Proxy** → **Start**.
“Listening on <server:port number>” displays in the Web Proxy status bar.
- 3 Click Launch Browser .
- 4 Manually navigate the site for which you want to view requests/responses.
- 5 If Web Proxy receives a request for a certificate from a Web Server, it displays a dialog 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 click **Proxy → Stop**).
- 7 Each session (a request and matching response) you recorded is listed in the top pane. To view the actual HTTP message, select an entry. The message appears in the bottom frame. By default, the **View** tab is selected.




- 8 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 WebInspect 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%20information_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 allows you to view the original response received by Web Proxy as well as the de-chunked or decompressed response.

- 9 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).
- 10 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  (or 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 proxy session file (.psf) 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 a WebInspect scan. All **File** menu commands apply to “check-marked” requests.

Use the **File** menu to save selected requests to an xml file and later load them for analysis. You can also save a sequence of requests as a Web Macro that you can use when conducting a scan. All **File** menu commands apply to “check-marked” requests.

Click the top of any column to sort the requests by that selection. For example, to sort the requests by the time they were made, click the top border of the **Time** column.



You must stop Web Proxy when you want to change Web Proxy settings.

Creating a Web Macro

You can use either the Web Macro Recorder or Web Proxy to create a Start macro or a Login macro.

A Start macro is used most often to focus on a particular subsection of an application. It specifies URLs that an HP 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.

A Login macro is used for Web form authentication, allowing the scanner (or the AMP sensor) to log in to an application. You can also incorporate logic that will prevent the scanner from inadvertently logging out of your application.

Follow the steps below to create a macro using sessions 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 **File** → **Create Web Macro**.
- 3 (Optional) On the *Create Web Macro* dialog, 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.

Background: 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 condition, the scanner searches every response message for this phrase. Whenever it detects the phrase, the scanner attempts to log in again by sending an HTTP request containing the username 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 background 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\s\snice\sday" as the regular expression ("\" 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.

- 4 Enter a name in the **Save macro as** box.
- 5 Click **OK**.

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.

Table 5 Web Proxy Tabs

Tab	Description
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). You can cut, paste, and copy the raw request, and right-click to see a shortcut menu of encoding options. However, you cannot save an edited request from the Web Proxy tool. Use the HTTP Editor to save an edited request.
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 Settings

To access this feature, click **Edit** → **Settings**.



You cannot change settings while Web Proxy is running. Click **Proxy** → **Stop**, change settings, and then restart Web Proxy.

Task 1: Configure General Settings

- 1 Select the **General** tab.
- 2 In the **Proxy Listener Configuration** group, 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.

Both Web Proxy and your Web browser must use the same IP address and port. If using Internet Explorer, click **Tools** → **Internet Options**; click the **Connections** tab and click **LAN Settings**; on the *LAN Settings* window, select **Use a Proxy Server for your LAN** and enter the address and port of the proxy server you want to use.

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.

- 3 Use the **Do Not Record** option to create a regular expression filter that prevents 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.
- 4 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 when you click the **Allow** button.

- 5 In the **Logging** group, 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.
- 6 Most Web pages contain information that tells the browser what language encoding to use. This is accomplished by using a META tag with an HTTP-EQUIV attribute in the HEAD section of the HTML document, as in the following example:

```
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
```

For pages that do not announce their character set, choose an option from the **Assumed 'charset' Encoding** list to select the language (and implied character set) that Web Proxy should use.

Task 2: Configure Proxy Servers Settings

- 1 Click the **Proxy Servers** tab.

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).

- 2 In the **Proxy Address** box, type the IP address of the server through which you want to route Web Proxy requests.
- 3 Specify the port number in the **Proxy Port** box.
- 4 Select the type of proxy (standard, SOCKS4, or SOCKS5) from the **Proxy Type** list.
- 5 If this proxy server requires authentication, select an authentication type and enter your authentication credentials in the **Username** and **Password** boxes. See [Authentication](#) on page 122 for a description of the available authentication types.
- 6 Click **Add** to add the server and display its IP address in the **Available Proxy Servers** list.

You can also import a file containing a list of proxy servers by clicking **Import**. The file containing proxy information must be formatted as follows:

- Each line contains one record followed by a line feed and carriage return.
- Each field in the record is separated by a semicolon.
- The fields appear in the following order: address;port;proxytype;user name;password.
- The user name 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
```

```
127.153.0.3;80;socks4;;
```

```
128.121.6.9;443;socks5;myname;mypassword
```

- 7 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.

- a Click **Add** in the **Bypass Proxy List** group.

The *Bypass Proxy* window appears.

- b 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.*
```


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 resolves to the IP address that you specify, Web Proxy will still send the request to a proxy server.

- c Click **OK**.

Task 3: Configure Search-and-Replace Settings

- 1 Click the **Search and Replace** tab.

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

- 2 Click **Add** to create a default entry in the table.

- 3 Click the **Search Field** column of the entry.

- 4 Click the drop-down arrow and select the message area you want to search.

- 5 In the **Search For** column, type the data (or a regular expression representing the data) you want to find.

- 6 In the **Replace With** column, type the data you want to substitute for the found data.

- 7 Repeat this procedure 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.

Task 4: Configure Flag Settings

- 1 Click the **Flag** tab.

This feature allows you to find and highlight keywords in requests or responses.

- 2 Click **Add** to create a default entry in the table.

- 3 Click the **Search Field** column of the entry.

- 4 Click the drop-down arrow and select the message area you want to search.

- 5 In the **Search** column, type the data (or a regular expression representing the data) you want to find.

- 6 Click the **Flag** column of the entry.

- 7 Click the drop-down arrow and select a color with which to highlight the data, if found.

Task 5: Configure Evasion Settings

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.



This feature is intended for use as a penetration testing tool. Do not use it or enable it when conducting vulnerability assessment scans.

Use the following procedure to enable evasions:

- 1 Select the **Evasions** tab.
- 2 Select **Enable Evasions**.

Choose one or more evasion techniques, as described below.

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/ HTTP/1.1
```

Web Proxy sends the following message to the server:

```
HEAD http://www.microsoft.com/ 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<CRLF><CRLF>
```

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<CRLF><CRLF>
```

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 device 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
```

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 **Allow**. 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 **Proxy** tab on the *Web Proxy Settings* window, you can force Web Proxy to pause after each request, after each response, or after locating specific text in either the request or response.



Follow the steps below to turn on interactive mode:

- 1 Click **Proxy** → **Stop**.
- 2 Click **Proxy** → **Interactive**
-or-
click  on the toolbar.
- 3 Click **Proxy** → **Start**.

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.

Smart Update

Each time you log in to the AMP Console, it contacts the AMP server and downloads any available console binary updates.

You can obtain updates to the SecureBase, as well as binary updates for AMP-connected products such as WebInspect, through either a manual or scheduled process.

For details, see [Smart Update](#) on page 51 and [Smart Update Approval](#) on page 51.

Cookie Cruncher

The Cookie Cruncher analyzes cookies to determine the relative ease with which an attacker could predict or determine the value of a session ID generated by a server and delivered to a client via a cookie.

Background

The Web's Hypertext Transfer Protocol (HTTP) is stateless, meaning that each communication is discrete and unrelated to those that precede or follow. Because there is no continuity inherent in the protocol, application designers introduced the concept of "session." A session is defined as all activity by a user with a unique IP address on a Web site during a specified period of time. When a user logs into an application, a session is created on the server to maintain the state for other requests originating from the same user.


Each session has a unique identifier (session ID). This text string is transmitted between the client and the server, and may be stored in cookies, URLs, or hidden fields of Web pages. One problem with session IDs, however, is that many Web sites generate them using algorithms based on easily predictable variables, such as time or IP address. This predictability makes the Web sites vulnerable to session hijacking.


Session hijacking involves an attacker using session IDs to seize control of a legitimate user's session while that session is still in progress. The attacker can then gain complete access to the user's data, and can perform all operations that are normally available to the legitimate owner of the session.

Using the Cookie Cruncher

Follow the steps below to use the Cookie Cruncher:

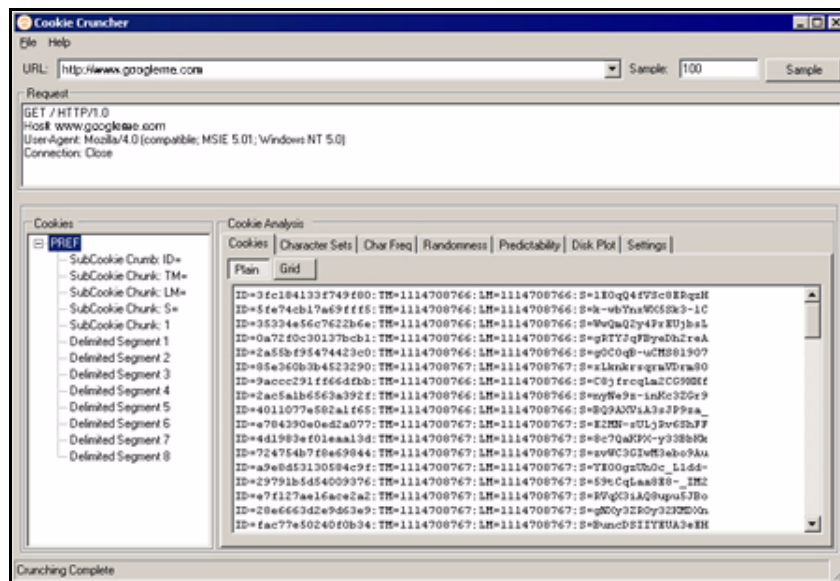
- 1 In the **URL** box, enter the URL of the site you want to test.

If you are using the Cookie Cruncher to examine a site you have scanned with WebInspect, follow these steps:
 - a In the WebInspect navigation pane, click the cookies icon  **Cookies**. All HTTP responses containing a "Set-Cookie:" header are listed in the information pane.
 - b Double-click one of the listed responses.
 - c Click **Request**.
 - d Copy the request and paste it into the Cookie Cruncher's **Request** area.
- 2 In the **Sample** box, enter the number of requests the Cookie Cruncher should send to the server (expecting a cookie to be returned). A higher number of samples increases processing time, but produces more reliable result; a minimum of 100 is suggested.
- 3 Click **Sample**.

As cookies are collected, the Cookie Cruncher organizes them into a tree hierarchy displayed in the vertical pane on the left side of the window.
- 4 Click a cookie in the tree hierarchy to analyze it. If subcookies are found, the Cookie Cruncher modifies the tree hierarchy; click the plus sign  to expand the level. Repeat as necessary.
- 5 To view the analysis, select a cookie or subcookie and click the various tabs.

- 6 To save the sampled cookies for future analysis, click **File** → **Save**.

▶ Cookie Cruncher cannot open and display a saved cookie file (.sck) if it contains fewer than four cookies.



Subcookies

Subcookies are either portions of cookie values that are common to many cookies, or interpreted values.

When the same string of characters appears in multiple cookies, you can choose that as a subcookie. The recurring expression will be eliminated from the cookies that contain it, and those cookies will be re-analyzed. The portion that is removed (the recurring expression) is called a “subcookie crumb.”

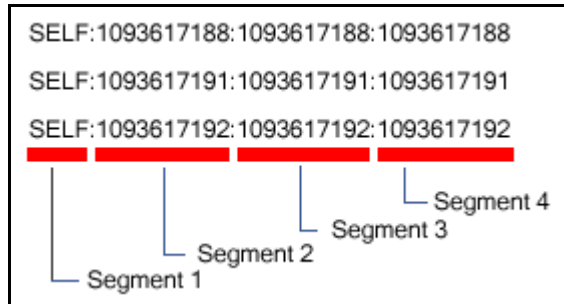
In the following sample, “086-” would be detected as a recurring expression:

086-1123
086-1127
087-6281
086-1132
088-0518
087-6282

Analysis of those cookies containing the recurring expression (1123, 1127, 1132) would reveal the (most likely) incrementing cookie values that were interleaved with values from some other source.

If the detected character set of a sample consists of just 10 characters (Q-Z), these characters could possibly represent the digits 0-9. Choosing the re-encode option would run the cookies through an appropriate decoder algorithm (base-10, base-16, base-64, etc.) and re-analyze the cookies.

The “Delimited Segment” option(s) allow you to select the delimited portions of cookies. For example, the following subcookies contain four delimited segments.



To analyze the second segment of all subcookies, you would click the **Select Subcookie** list and select **Delimited Segment 2**.

For more information, see the white paper [Automated Cookie Analysis](#).

Cookie Cruncher Tabs

Use the Cookie Cruncher tabs to analyze the sampled cookies. The tabs are:

- Cookies
- Character Sets
- Char Freq
- Randomness
- Predictability
- Disk Plot

Cookies Tab

This tab lists all cookies received from the server. You can view them either in plain or grid format by clicking the appropriate button.

Character Sets Tab

This tab displays the character set used to format the cookie:

A = alphabetic character (letters A-Z)

N = numeric character (numbers 0-9)

H = hexadecimal character (0-F)

T = Text A-Z, a-z

I = Illegal (anything else)

D = delimiter

Char Freq Tab

This tab displays a graph showing the number of times each ASCII character appeared in the total sample of cookies. A pale blue dot indicates an ASCII character whose number of appearances equals the number of cookies. A highlighted character indicates that it may be a delimiter (which is usually a character such as a comma, colon, or semicolon, but could also be something unusual such as “Z”).

Randomness Tab

This tab attempts to differentiate between random and non-random portions of cookies, based on the sample obtained.

Use the Grid view to illustrate the analysis of each column. The color key is:

- Red = No randomness (or very little)
- Orange = Somewhat random
- White = Random

The top row of the grid indicates the numeric position of each character.

The second row displays, for each character position, a number representing the relative randomness of the character. This is actually the average number of bits that change per column from one cookie to the next.

Use the Graph view to illustrate the randomness level in a graphic format. The dashed green line represents the optimum (best practice) level of randomness. The red line represents the randomness of the cookies in the sample. In a well designed cookie, the red line should follow the green line. When the graph view is selected, you can save the graph (in BMP, GIF, PNG, or JPG format) using the **Save Graph** command in the **File** menu.

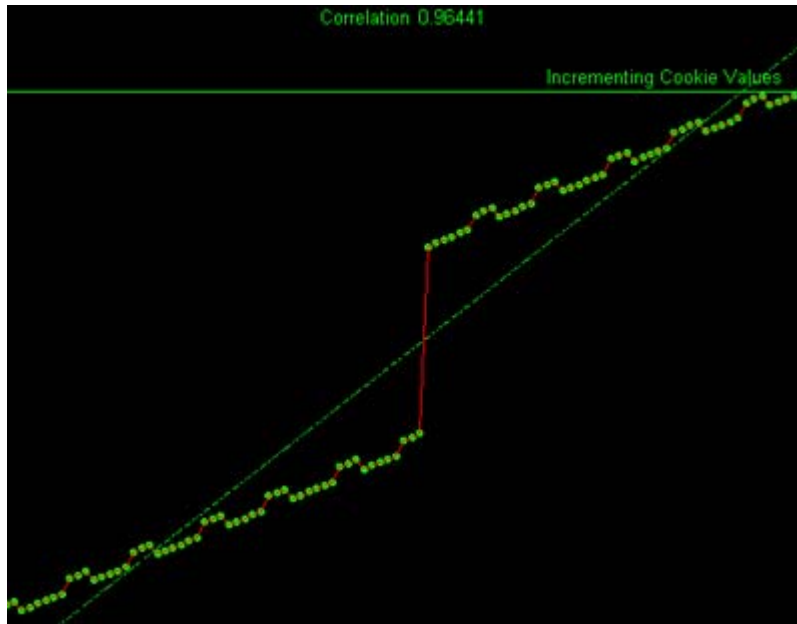
Predictability Tab

The Cookie Cruncher analysis produces a correlation value ranging from 0 to 1 and displays it at the top of the graph. A low value indicates that cookie generation is more random; a higher value indicates greater predictability.

The value of each cookie is plotted (on the Y axis) against the time the cookie was received (on the X axis). A scattered distribution indicates randomness, whereas a pattern approaching a line indicates predictability.

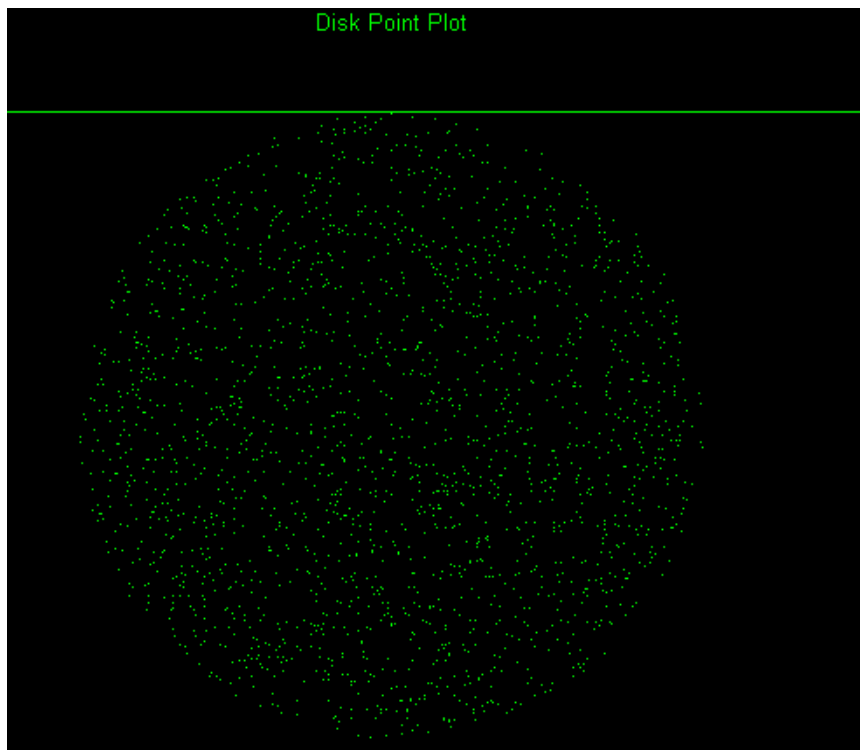
If the correlation is .9 or greater, the graph displays the header “Incrementing Cookie Values” or “Decrementing Cookie Values” and draws a “best fit” line.

Only decimal or hexadecimal values can be plotted.



Disk Plot Tab

This graph plots a cookie's value against the sine and cosine functions. When random data is plotted, the points are evenly distributed around the plotting area. Only decimal or hexadecimal values can be plotted.



Cookie Cruncher Settings

Follow the steps below to modify the Cookie Cruncher settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **General**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.
- 3 Click **OK**.

General

Thread Count

Specify the maximum number of threads that can be created. The Cookie Cruncher can be configured to send up to 75 concurrent HTTP requests before waiting for an HTTP response to the first request. The default setting is 10. Increasing the thread count will increase the speed of the process, but might also exhaust your system resources as well as those of the server you are scanning. While most servers can handle a large number of requests, servers in development environments sometimes have licensing limitations that allow only five or fewer users to be connected at a single time. In such cases, you should reduce the thread count to be less than 5.

Socket Timeout

Specify the maximum number of open sockets permitted. A higher number of open sockets results in a faster process. However, a setting that exceeds a server's threshold may result in false positives.

If the Cookie Cruncher runs on Windows XP with Service Pack 2 (SP2), the number of open sockets should be set to 10.

Custom Delimiters

The Cookie Cruncher interprets certain characters (such as /.-!,:;=) as delimiters. In some cases, you may want to substitute your own list. For example, a cookie having a value of "ABC123456-C:Program" contains two default delimiters — a dash (-) and a colon (:) — and would therefore be split into three parts. However, if you specify only the dash as a delimiter, the cookie would be split into just two parts.

The user-specified list, if present, will cause an extra subcookie type to appear in the tree, in addition to the regularly parsed subcookie types. The subcookie item may not appear when the number of cookies having the delimiter(s) is less than 10 percent of the total cookie sample.

To create a list of custom delimiters, select the **Parse with Custom Delimiters** check box and then enter one or more delimiters in the **Characters** box.

Authentication

Authentication Method

If authentication is required, select a type from the **Authentication** list:

Authentication	Description
Automatic	Allow the Cookie Cruncher to determine the correct authentication type. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
HTTP Basic	<p>A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.</p> <p>The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.</p>
NT LAN Manager (NTLM)	<p>NTLM is an authentication process used by all members of the Windows NT family of products. It uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.</p> <p>Use NTLM authentication for servers running IIS.</p>

Authentication Credentials

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

Proxy

Use these settings to access the Cookie Cruncher 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, the Cookie Cruncher will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information (as described in the preceding table).

Web Fuzzer

“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 simply generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

The Web Fuzzer 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, and buffer overflows, as well as protocol implementation problems.

Using the Web Fuzzer

Follow the steps below to use the Web Fuzzer:

- 1 Click **Edit** → **Server**.
- 2 Enter the fully qualified domain name or IP address of a Web site, along with other server configuration information, and click **OK**.
- 3 Click **Edit** → **Settings**.
- 4 Configure the settings and click **OK**. For more information, see [Web Fuzzer Settings](#) on page 239.
- 5 To create a session, click **Session** and select either **Create** or **Raw Create**.
 - a If you select **Create**, Web Fuzzer displays a tabbed property sheet that identifies each section of an HTTP request and allows you to replace an HTTP element with generated data or with text that you enter. This structured approach is recommended for novice users. For detailed information, see [Using the Session Editor](#) on page 236.
 - b If you select **Raw Create**, Web Fuzzer displays a standard GET request formatted as regular text. You can edit the request. You can also place the cursor anywhere in the request, right-click to invoke a shortcut menu, and then insert a generator that will fuzz the selected HTTP element. If you highlight any portion of the request, the highlighted portion will be replaced by the generator.

Table 6 Fuzzer Generators

Generator	Function
Number	Inserts a whole number, within the range you specify, in each request; you specify the starting and ending number, the increment, and the number of times to loop through the series.
ASCII	Inserts one ASCII character, within the range you specify, in each request; you 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; you specify the minimum and maximum number of characters, and an increment.

Table 6 Fuzzer Generators (**cont'd**)

Generator	Function
Decimal Number	Inserts a fractional number, within the range you specify, in each request; you specify the starting and ending 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; you specify the number of requests.
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.
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.
Cross-Site Scripting	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>
Method	Inserts a method (GET, POST, PUT, etc.); you specify the protocol version (0.9, 1.0, 1.1, or all).

- 6 After creating the request, click **OK**.
- 7 You can use filters so that only those server responses meeting criteria you specify will be displayed.
- 8 On the *Web Fuzzer Request* window, click **Start**.
The **Sessions** area lists each session (request and response) generated by the tool.
- 9 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.
- 10 To edit the request that you constructed, select a session in the **Sessions** group, then click the **Session** menu and choose either **Edit** or **Raw Edit**.

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]

You access the *Filters* dialog by selecting **Filters** → **Edit**.

In addition to enabling a specific rule, you must also enable the use of rules in general by selecting **Filters** → **Enable**.

Creating a Filter

Follow the steps below to create a filter:

- 1 Click **Add**.
The tool creates a rule named Default Rule.
- 2 Modify the Name, Description, and Rule.
- 3 Click **Apply** to save the definition.

Using a Filter

Follow the steps below to use a filter in a session:

- 1 Select a filter from the **Filters** list.
- 2 Select the **Enable** check box.

Deleting a Filter

Follow the steps below to delete a filter:

- 1 Select a filter from the **Filters** list.
- 2 Click **Delete**.

Editing a Filter

Follow the steps below to edit a filter:

- 1 Select a filter from the **Filters** list.
- 2 Modify the Name, Description, or Rule.
- 3 Click **Apply** to save the modifications.

Using the Session Editor

Use this tabbed property sheet 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.

Follow the steps below to use the Session Editor:

- 1 Click a tab.
- 2 You can either:
 - Edit the data appearing in text boxes, or
 - Select the **Use Generator** check box and click **Generator** to insert a generator.
- 3 To change other areas, click a different tab.
- 4 After configuring the areas you want to change, click **OK**.
- 5 When you return to the *Web Fuzzer* window, click **Start**.

Creating a Query String

Follow the steps below to create a query string:

- 1 Click **Add**.
The text “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 click **Generator**).
- 3 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 click **Generator**).
- 4 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 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** group, 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 click **Generator**).
- 7 To add another parameter, click **Add** and repeat Steps 2-6.

Session Editor Tabs

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, and 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.
```

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 also can be separated into four fuzzing opportunities.

Creating Headers

Follow the steps below to create headers:

- 1 Click **Add**.
The text “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 click **Generator**).
- 3 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.
- 4 Click the **Value** tab. You can edit the “value” text or you can substitute a generator for it.
- 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** group, you can edit the character that separates headers or you can substitute a generator for it.
- 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.

Creating Cookies

Follow the steps below to create cookies:

- 1 In the **Cookies** group, click **Add**.
“Cookie:” appears in the list, representing the cookie you are creating.
- 2 Click **Cookie:** (in the Cookies list) and then click **Add** (in the **Cookie** group).
The text “name=value” appears.
- 3 In the **Cookie** group, click the **Cookie Name** tab. You can edit the name or you can substitute a generator for it.
- 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.
- 5 Click the **Value** tab. You can edit the “value” text or you can substitute a generator for it.
- 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** group, you can edit the character that separates headers or you can substitute a generator for it.
- 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.

Creating POST Data

Follow the steps below to create post data:

- 1 Click **Add**.
The text “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.

- 3 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.
- 4 Click the **Value** tab. You can edit the “value” text or you can substitute a generator for it.
- 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** group, you can edit the character that separates headers or you can substitute a generator for it.
- 7 To add another post data element, click **Add** and repeat Steps 2-6.

Web Fuzzer Settings

Follow the steps below to modify the Web Fuzzer settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **General** or **Proxy** category and enter the settings described in the following sections.
- 3 Click **OK**.

General

Enable Filters

Select this option to enable filter support.

Auto scroll view

Select this option to enable automatic scrolling in the **Sessions List** view. This will force the view to scroll down to the latest session automatically.

Show ToolTips

Select this option to enable the display of tool tips when you hover your mouse pointer over certain controls.

Sockets

Enter the maximum number of sockets and the sockets send timeout (in seconds).

Protocol Compliance

Select **Enforce Content-Length** to automatically adjust the Content-Length value in the request when needed. If this feature is enabled, you cannot fuzz the content-length header.

Select **Enforce Host header** to include the Host header in all requests. If this feature is enabled, you cannot fuzz the host header.

Proxy

Use these settings to access the Web Fuzzer 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, the Web Fuzzer will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information (as described in the preceding table).

SQL Injector

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 as database types and also supports multiple language systems including Japanese.

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 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.

Using the SQL Injector

Follow the steps below 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. See [SQL Injector Settings](#) on page 243 for additional information.
- 2 Select **File** → **New**
- or -
click the New Request icon.
- 3 In the **Location** box, 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
```

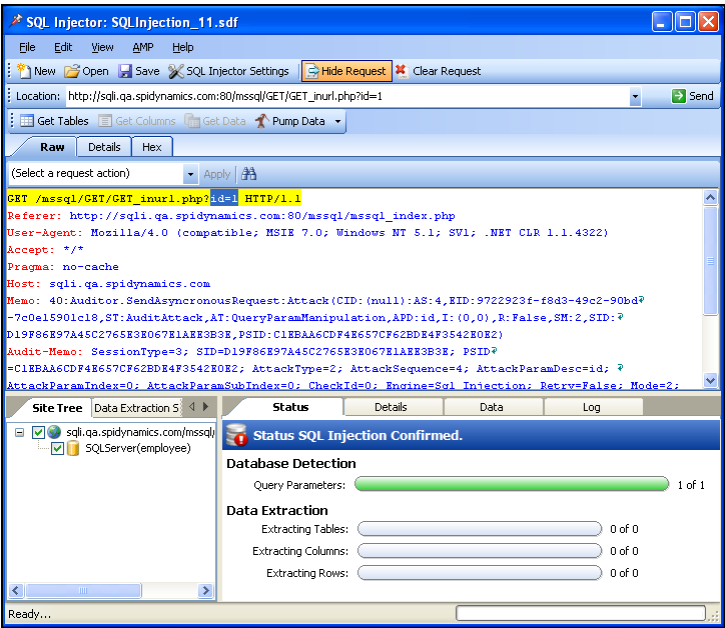
```
Content-Length: 22
```

```
Content-Type: application/x-www-form-urlencoded
```

```
login=qqq&password=aaa
```

- 4 Click **Send**.

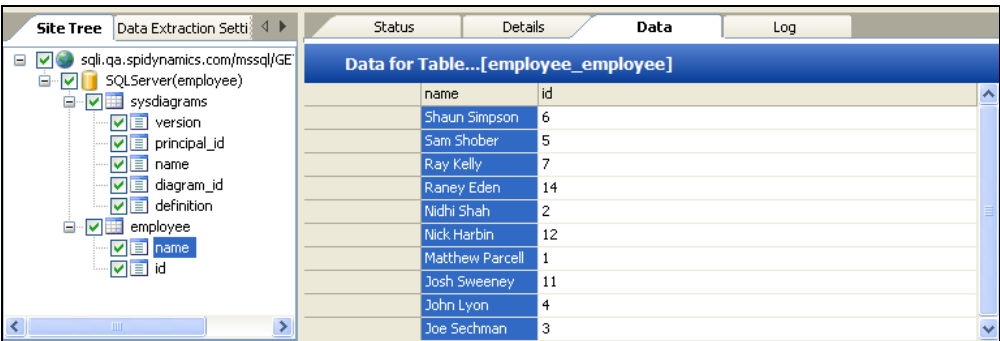
If SQL injection is successful, “SQL Injection Confirmed” appears on the **Status** tab and the beginnings of a data hierarchy tree appear on the **Site Tree** tab in the lower left pane.



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

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 box.
 - 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 column values.



SQL Injector Tabs

Request Pane

The Request pane contains three 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 two 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 four 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

Follow the steps below to modify the SQL Injector settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **Options**, **Authentication**, or **Proxy** category and enter the settings described in the following sections.
- 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 My Documents\SPI dynamics\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

Select this option to use a startup macro; then click  to select, edit, or create 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 a type from the **Authentication** list:

Authentication	Description
Automatic	Allow the SQL Injector to determine the correct authentication type. Note that automatic detection slows the scanning process. If you know and specify one of the other authentication methods, scanning performance is noticeably improved.
HTTP Basic	<p>A widely used, industry-standard method for collecting user name and password information. The Web browser displays a window for a user to enter a previously assigned user name and password. If the Web server verifies that the user name and password correspond to a valid user account, a connection is established.</p> <p>The advantage of Basic authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that Web browsers using Basic authentication transmit passwords in an unencrypted form. By monitoring communications on your network, an attacker can easily intercept and decode these passwords using publicly available tools. Therefore, Basic authentication is not recommended unless you are confident that the connection between the user and your Web server is secure.</p>
NT LAN Manager (NTLM)	<p>NTLM is an authentication process used by all members of the Windows NT family of products. It uses a challenge/response process to prove the client's identity without requiring that either a password or a hashed password be sent across the network.</p> <p>Use NTLM authentication for servers running IIS.</p>

Authentication Credentials

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

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

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

For proxy servers accepting HTTPS connections, select **Specify Alternative Proxy for HTTPS** and provide the requested information (as described in the preceding table).

Compliance Manager

HP scanners employ an extensive arsenal of attack agents designed to detect security flaws in Web-based applications. They probe 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.

You 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 HP scanners, you can assess your application and then generate a Compliance Report that measures how well your application satisfies this HIPPA 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).

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. For maximum flexibility, you can even create your own agents and associate them with a user-defined requirement.

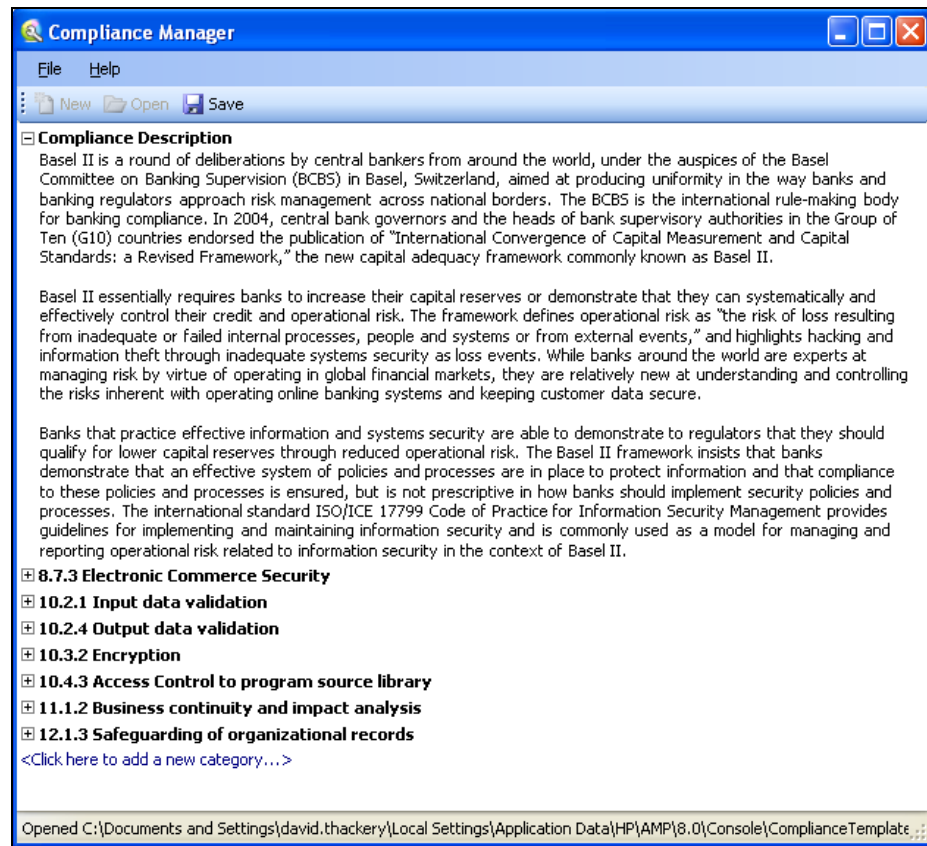
AMP includes sample compliance templates that you can edit to fit your company’s specific requirements.


Creating/Editing a Compliance Template

Follow the steps below to create (edit) a compliance template.

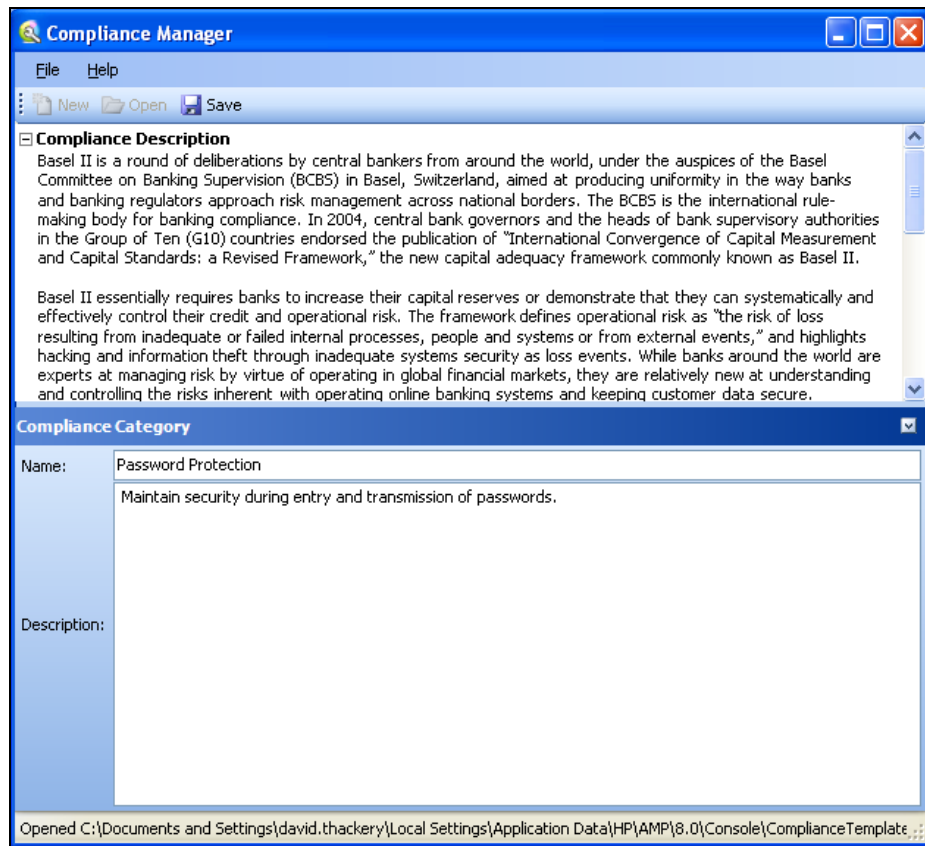
- 1 Click the **Scans/Compliance** group.
- 2 Click the **Compliance Templates** shortcut.
- 3 Select a template and then select **Copy** from the **Action** menu.
 **Note:** After creating a custom template, you can edit it by selecting **Edit** from the **Action** menu (or from the context menu).
- 4 If you have access to any custom policies, the *Select Custom Policy* dialog appears, prompting you to choose a custom policy. This occurs to accommodate any custom checks that you may have created in that policy. If there are no custom checks, or if you do not want to include custom checks, click **No**.
- 5 On the *Copy Compliance Template* dialog, rename the template and click **OK**.


The *Compliance Manager* window opens, displaying template contents. The following illustration depicts the Basil II template.



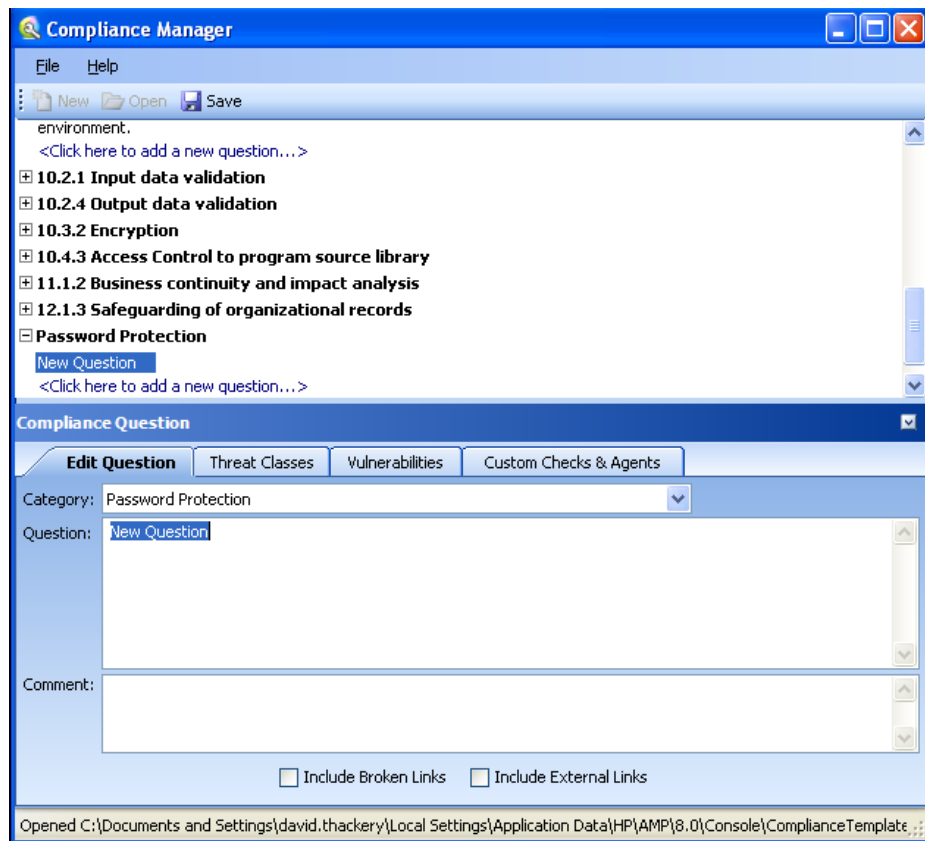
- 6 Click the plus sign  to expand a node.
- 7 To edit a section, right-click the section and select **Edit**.
- 8 To remove a section, right-click the section and select **Remove**.
- 9 To add a category, click the phrase "<Click here to add a new category...>." "New Category" appears.

- 10 Click the phrase “New Category” and, in the editing area, enter the name and description of the new category (“Password Protection” in this example).



- 11 Click the plus sign  to expand the node labeled Password Protection.
- 12 Click the phrase “<Click here to add a new question...>.”
- 13 Click the phrase “New Question.”

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

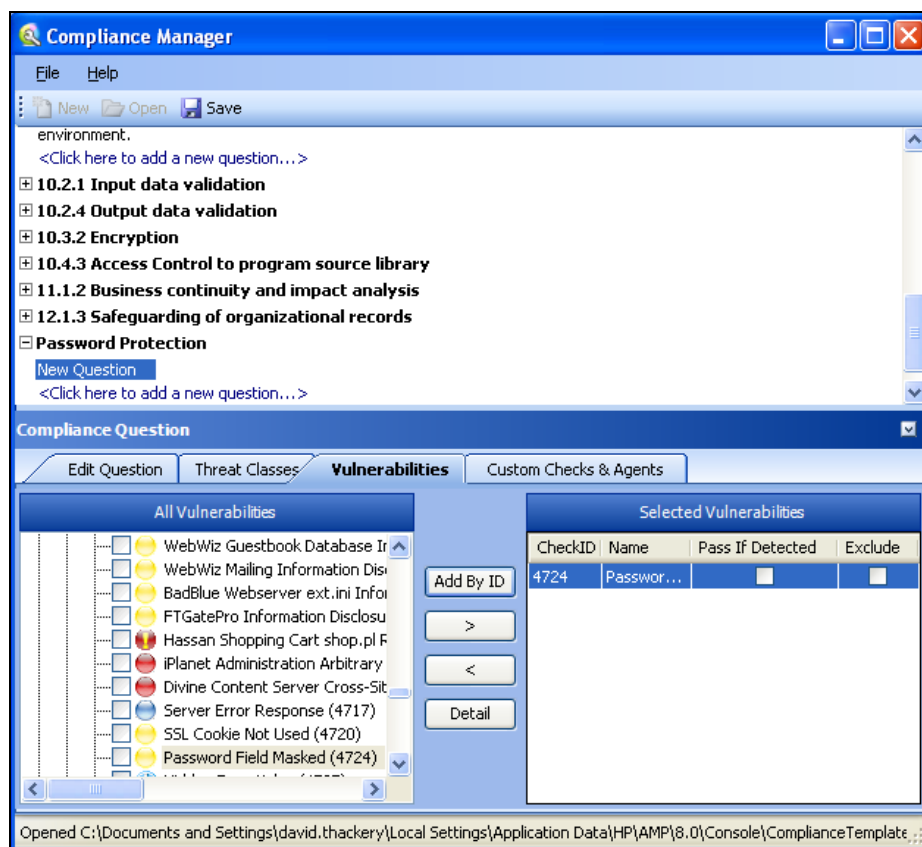


- 14 In the **Question** area, type a question related to the category (such as, “Is each character of entered password displayed as an asterisk?”)
- 15 You can associate this question with threat classes, vulnerabilities defined by HP, or a custom check or agent that you previously created. For this example, click the **Vulnerabilities** tab and then click **Add By ID**.

You can also select a vulnerability and click  to include it in the **Selected Vulnerabilities** section for this question.

- 16 On the *Add Check By ID* dialog, enter 4724 and click **OK**. [4724 is the ID number of the “Password Field Not Masked” check.]

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



17 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.

- 18 Continue adding threat classes, vulnerabilities, or custom checks until you have included all that sufficiently test your application for the compliance question.
- 19 Create additional questions and categories using the above procedures until the compliance template is complete.
- 20 Click **Save**.

Testing for Compliance

Follow the steps below to test your Web site for compliance:

- 1 Create a compliance template.
- 2 Scan your Web site.
- 3 In the AMP Web Console, select the **Scans** view.
- 4 Select a scan and click **Generate Report**.

- 5 Provide the requested information.
- 6 On the Options settings, do one of the following:
 - Select **Use Report Template** and then select **Compliance** from the **Report Template** list.
 - Select **Use Report Definition** and then select **Compliance** from the **Report Definition** list; provide the requested information for report definitions.
- 7 Click **Finish**.

Web Macro Recorder (Session-Based)

A macro is a recording of the HTTP requests that are generated when you navigate through a Web site or application using the Web Macro Recorder. You can instruct WebInspect to use this recording to enter your Web site and (optionally) navigate through your application.

Any activity you record in a macro will override the scanner settings. For example, if you specify a URL in the Excluded URL setting, and then you actually navigate to that URL when creating a macro, the scanner will ignore the exclusion when it replays the macro.

When starting a Web site assessment with the WebInspect Scan Wizard, you have two opportunities to specify a macro:

- **Workflow-Driven Assessment:** WebInspect audits only those URLs included in the macro that you previously recorded 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 the application. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application.
- **Site Authentication:** The macro specifies a log-in page and contains a user name and password that allows you to log on to the target site. The macro must also contain a “logout condition,” which indicates when an inadvertent logout has occurred so WebInspect can rerun this macro to log on again.

Note that when you play a macro, the HP scanner will not send any cookie headers that may have been incorporated in the recorded macro.

Creating a Macro

Follow the steps below to create a macro:

Task 1: Prepare the Web Macro Recorder

- 1 Close all browsers.
- 2 Start the Web Macro Recorder.
- 3 Click **Edit** → **Settings** to configure general settings and proxy settings.
- 4 You can exclude the recording of requests containing certain objects by selecting **Filter Rules** from the Macro Recorder’s **View** menu. See Filter Rules on [page 262](#) for more information.

Task 2: Browse the Web Site

- 1 Do one of the following:
 - Select **File** → **New**.
 - Click the New icon on the toolbar.
 - Click the Record icon.
- 2 Using the browser’s Address bar, enter or select a URL.



Note: Internet Explorer version 7 and the .NET Framework are hard-coded not to send requests for localhost through any proxies. Therefore, the Web Macro Recorder will not receive such traffic. This is a documented Microsoft defect. To access a site on “localhost” when using IE7, place a period or dot after “localhost” (for example, <http://localhost.:8080/test.html>).

- 3 Browse the pages that you want to include in your macro.
- 4 If you want to include a login, be sure to navigate to a page that requires Web form authentication. Then enter a valid user name and password, and submit the data (usually by clicking a button such as **Log On**, **Go**, **Submit**, etc.).
- 5 When finished, close the browser.




If recording a login macro, do not log out before closing.

Task 3: Finish the Macro

- 1 When you close the browser, a dialog box displays the message:
“Are you recording a login macro? (By clicking Yes, auto-detection of the logout condition will be performed.)”

Explanation: When a scanner encounters a hyperlink to another resource, it navigates to that URL and continues 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 logout occurs, the scanner can either run this macro to log in or request user intervention. In either case, the process hinges on the scanner’s ability to recognize when it is no longer logged in.
 - Click **Yes** if you want the Web Macro Recorder to analyze the recorded sessions and attempt to detect a “logout” condition.
 - If you do not require a “logout” condition, click **No** and go to Step 6.
 - If you want to specify a condition manually, click **No** and go to Step 3.
 - If your application uses URL rewriting or post data techniques to maintain state within a Web site, click **No**. See [URL Rewriting and Request Parameters](#) on page 257 for further instructions.
- 2 If the attempt to detect a logout condition is successful, a dialog box displays the following message:
“Would you like to test your login macro?”
 - a To bypass the test, click **No**. Go to Step 3.
 - b To test the macro, click **Yes**.
 - c On the *Test Login Macro* window, the **Address** box contains the URL of a page believed to be viewable only after logging in. If this is, indeed, a “protected” page, click **Go**. Otherwise, enter the URL of a protected page.
 - d Browse to various sections of the site to verify that you are logged in.
 - e Log out and verify that you are prompted to replay the macro.
 - f Click **Done**.
- 3 If the attempt to detect a logout condition is not successful, or if you elected to bypass the auto-detect feature:
 - a On the **Sessions** tab, select a session that you accessed after logging in and click **Detect Logout Condition** (on the toolbar). Do not select the session where you actually logged in.
 - b If the Macro Recorder is unable to determine the logout condition, try selecting other sessions.

- c If the Macro Recorder is still unable to determine a logout condition, you can manually enter one. Click **Edit Logout Condition** and, on the *Logout Condition Editor* window, select either **Use Regular Expression Extensions** or **Use Text Matching**.
 - 4 For a login macro, you may want to delete extraneous sessions (i.e., those not related to or required by the login procedure). To do so, remove the check mark from the unneeded sessions. You should then click **Test Login Macro** to ensure that you retained all necessary sessions.
 - 5 Specify which action the scanner should take if it detects that it has logged out of the application. Click either **Play Macro** or **Launch Interactive** (which will allow you to manually log back in).
- Note: If you select **Launch Interactive**, the scanner pauses the scan and presents a dialog allowing you to enter log-in information. This is useful when scanning a site that incorporates a CAPTCHA (i.e., a challenge-response test placed within Web forms to ensure that the response is not generated by a computer). This feature is also used when the Web Macro Recorder is not able to determine a logout condition and the user is not able to define the condition using regular expressions or text matching.
- 6 To save the macro, click **File** → **Save** (or **Save As**) or click .

Editing the Logout Condition

You can create or edit the criteria used by the Web Macro Recorder to detect a “logged out” condition.

To access the feature, click **Edit Logout Condition**.

If detection of a logout is not required, select **Do no use logout condition**. Otherwise, you can instruct the Web Macro Recorder to use either a regular expression or text matching.

Regular Expression Extensions

If you want the Web Macro Recorder to use a regular expression to detect a logged out condition:

- 1 Select **Use Regular Expression Extensions for a logout signature**.
- 2 Type (or edit) a regular expression that identifies a unique text or phrase that occurs in the server’s HTTP response when a user logs off or when a user who is not logged on requests access to a protected URL.

For example, if your server returns a message such as “Have a nice day” when a user logs off your application, then enter “Have\s\sa\s nice\sday” as the regular expression (“\s” is used in regular expressions to denote a space).

The scanner can also detect that it has logged off 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.” In this case, “[STATUSCODE]302 AND [ALL] http://login.myco.com/config/mail?” might be a typical regular expression.

- 3 Click **OK**.

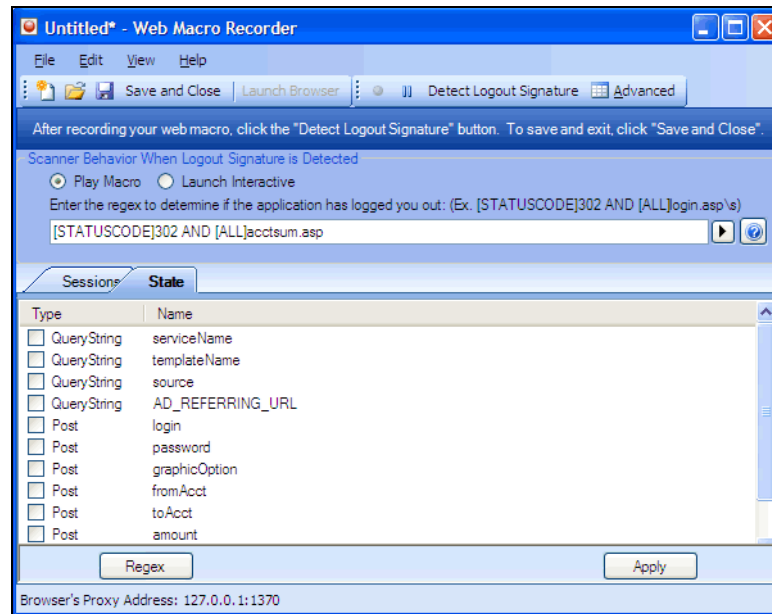
Text Matching

This technique for recognizing “logged out” or “logged in” state assumes that you know that certain text strings will be displayed when either condition occurs. For example, a site may display pages that contain the text “Log In” (usually a hyperlink) whenever a user is not logged in. Similarly, the site may display pages containing text such as “Sign Out,” “Log Out,” or “Log Off” when the user is logged in.

- 1 Select **Use text matching to determine logged-in state**.
- 2 Under the **Text fragments that indicate logged out state** column, click **Add**.
- 3 In the pop-up window that appears, enter a text string and click **OK**. For example, you might enter “Log In” or “sign in”; note that the search is not case-sensitive.
- 4 Repeat Step 2-3 if additional or alternative text fragments are also present during a “logged out” state.
- 5 In the **Number of text fragments to match** box, enter the number of specified strings that must exist on a page before the Web Macro Recorder considers that page to be in a “logged out” state.
- 6 Under the **Text fragments that indicate logged in state** column, click **Add**.
- 7 In the pop-up window that appears, enter a text string and click **OK**. For example, you might enter “Log Out” or “Sign out.”
- 8 Repeat Step 6-7 if additional or alternative text fragments are also present during a “logged in” state.
- 9 In the **Number of text fragments to match** box, enter the number of specified strings that must exist on a page before the Web Macro Recorder considers that page to be in a “logged in” state.
- 10 (Optional) Click **Advanced**.
 - a In the pop-up dialog, enter a URL that should be used to evaluate the state if a page does not contain enough text fragments.
 - b Click **OK**.
- 11 Click **OK**.

URL Rewriting and Request Parameters

If your application uses URL rewriting or request parameters to maintain state within a Web site, select the **State** tab.



You must identify which parameters are used for state management. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01

Because session IDs change with each connection, a recorded macro containing this URL would create an error when you tried to replay it. However, if you identify the parameter (PHPSESSID in this example), then the scanner will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include `userid=slbhkelvbk173dhj`. In this case, “userid” is the parameter you would identify to the Web Macro Recorder.

► **Note:** You need to identify parameters only when the application uses URL rewriting, posted data or query parameters to manage state. It is typically not necessary when using cookies to manage state. Exception: Delete (uncheck) any cookie that is required for normal operation.


The Web Macro Recorder can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, “1234567” is the session information:

`http://www.onlinestore.com/bikes/(1234567)/index.html`

The regular expression for identifying the parameter would be:

`/\([w\d]+\)/`

- 1 To enter a regular expression, click **Regex** and then use the Regular Expression Editor to create an expression. When you click OK (on the regular Expression Editor), the expression is added to the **Type/Name** list.

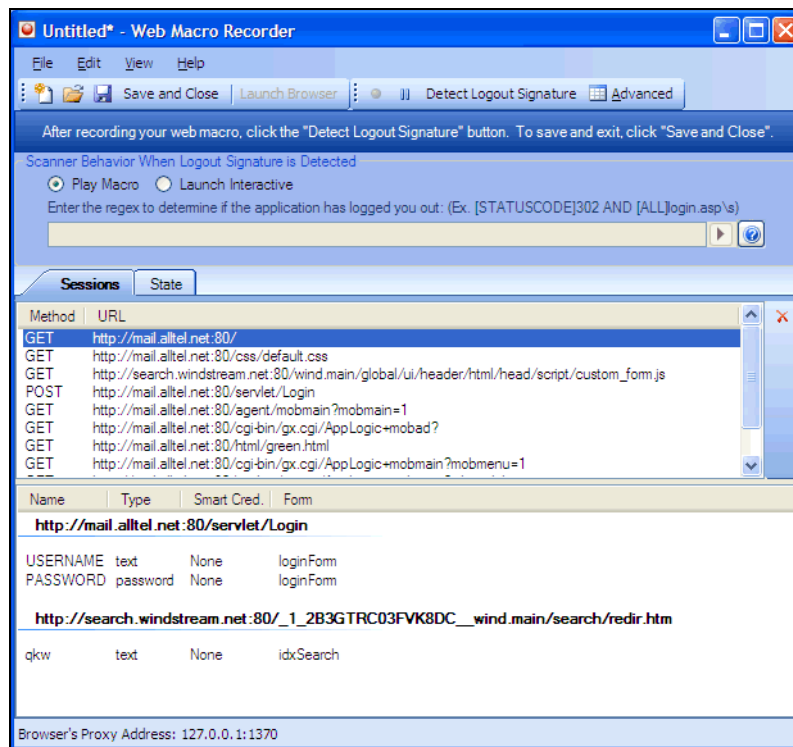
- 2 Select a parameter in the **Type/Name** list (such as “login” in the preceding illustration).
- 3 Click **Apply**.
- 4 To save the macro, select **File** → **Save** (or **Save As**)
-or-
click .

Inspecting and Editing a Macro

As you navigate through the target Web site, the Web Macro Recorder transcribes each session, displaying on the **Sessions** tab the method and URL associated with each HTTP request sent to the server.

- 1 Select a session on the **Sessions** tab.

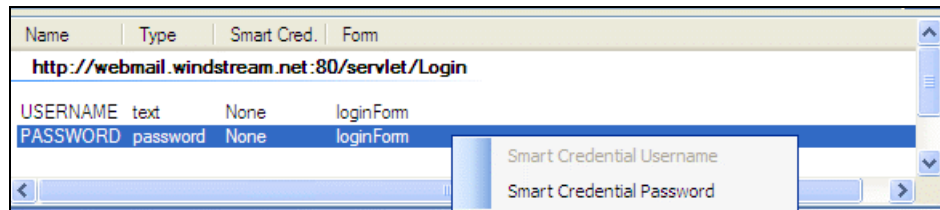
If the associated HTTP response includes “text” or “password” input controls, their name and type are displayed in the lower pane.



In this example, the form and the controls were rendered by the following HTML statements:

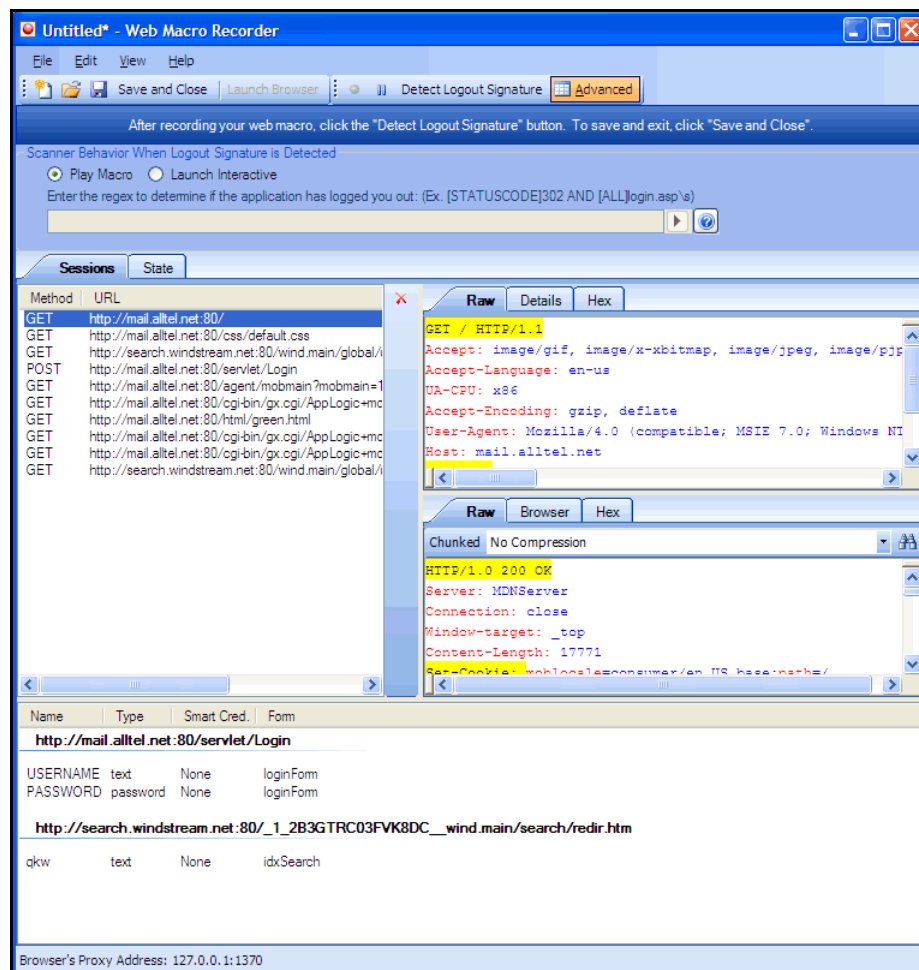
```
<form name="loginForm" action="/servlet/Login" method="POST">
<input type="text" size="16" name="USERNAME" value="">
<input type="password" size="16" name="PASSWORD">
```


-
- 2 You can designate a control as a “Smart Credential” user name or password. Right-click the control name and select an option from the shortcut menu, as shown below.



If you start an assessment using a macro that includes Smart Credentials, then when you scan the page containing the input elements associated with these entries, the scanner will substitute the password specified in the Authentication options (or, if no user name is specified, the name of the current Windows user). This allows you to create the macro using your own user name and password, yet when someone else runs the scan using this macro, the scanner will submit that user's name and password.

-
-
- 3 If you click the **Advanced** button, the Web Macro Recorder displays the contents of the HTTP request and response in separate panes.



-
-
-
- 4 You can also edit an HTTP request if, for example, you need to change or remove headers, or edit passwords or user names. Simply right-click a session and select **Edit with HTTP Editor** from the shortcut menu to launch the HTTP Editor.

- 5 You can exclude a specific session from the macro by clearing its associated check box, or you can delete a session by selecting the session and clicking the red **X** on the right side of the **Sessions** list (or by right-clicking a session and selecting **Delete Session** from the pop-up menu).

Session-Based Web Macro Recorder Settings

Follow the steps below to modify the Web Macro Recorder settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **General** or **Proxy** category (described below) and enter the settings.
- 3 Click **OK**.

General

Proxy Listener

The Web Macro Recorder 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.

To avoid the possibility of specifying a port that is already in use, select **Automatically Assign Port**.

Save Files in clear text

Select this option if you do not want to save macros in an XML format using Base 64 encoding (which is the default). Saving files in clear text allows you to read the XML tags. The actual data, however, is not rendered in ASCII format and is not human readable.

Keep window always on top

Select this option to keep the Web Macro Recorder displayed on your screen when you switch programs or windows.

Keep params as state only during macro playback

This option affects how the Post and Query parameters in the **State** tab are used. If this setting is off, then the Post and Query parameters that are checked are imported into the scan settings in the **HTTP Parameters Used For State** list. If this setting is on, then the Post and Query parameters that are checked are used as state only during the playback of the macro being recorded.

Automatically follow redirects during playback

If this option is selected, then for any sessions in the macro being recorded that result in a redirect (a 301 or 302 status code, for example), the new redirect will automatically be followed when the macro is played back. The session that is recorded (that is the result of the redirect) will not be played back.

Prompt for credentials when webserver requests authentication

If you select this option, the Web Macro Recorder displays a dialog allowing you to enter a user name and password whenever the server requires authentication to access a site (that is, whenever the server returns a “401 Unauthorized” status).

Note: Certain AJAX, Flash, and ActiveX controls may elicit a 401 status code when authentication, in fact, is not required. You can recognize this situation when the Web Macro Recorder prompts for credentials, but a browser accessing the site does not. For sites where this occurs, this option should not be selected.

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 Macro Recorder should use.

Proxy

Use these settings to access the Web Macro Recorder 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, the Web Macro Recorder will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

Configure proxy using a PAC File URL

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

Explicitly configure proxy

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

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

Web Macro Recorder Menus

The Web Macro Recorder contains the following menus:

File

- **New**—Launch Internet Explorer and begin recording.
- **Open**—Load a previously recorded macro for editing.
- **Save**—Save a macro.
- **Save As**—Save an edited macro under a different file name.
- **Exit**—Close Web Macro Recorder.

Edit

- **Cut**—Delete the selected string and save it to the clipboard.
- **Copy**—Copy the selected string to the clipboard.
- **Paste**—Insert contents of the clipboard.
- **Edit with HTTP Editor**—Open the HTTP Editor and load the selected session.
- **Delete Session**—Remove the selected session from the macro.
- **Start Capture**—Begin recording HTTP requests.
- **Stop Capture**—End recording to HTTP requests.
- **Find**—Specify a string and search for it when using the Advanced view.
- **Settings**—Modify Web Macro Recorder settings.

View

- **Launch Browser**—Open Internet Explorer to navigate through Web site.
- **Test Login Macro**—Open the *Test Login Macro* window to verify creating of a logout condition.
- **HTTP Editor**—Open the HTTP Editor.
- **Toolbars**—View or hide the Detect Logout Condition, Test Login Macro, and Advanced buttons.
- **Filter Rules**—Select a resource type or status code to exclude. For example, sessions where the server response contains an HTTP status code of “404 Object Not Found” are normally not useful. Similarly, sessions that request images are normally not necessary when

creating a macro, and simply add clutter to the session list. By selecting **Images** from the Filter Rules list, you avoid the needless recording of sessions such as GET http://www.mywebsite.com:80/services.gif.

- **Advanced**—View or hide panes that display the contents of HTTP requests and responses. Note that when editing a saved macro, pages will not be rendered in the **Browser** tab.

Help

- **Web Macro Recorder Help**—Open the Help file to the default topic.
- **Index**—Open the Help file, displaying the index pane.
- **Search**—Open the Help file, displaying the search pane.
- **About Web Macro Recorder**—Open a window that displays information about the Web Macro Recorder.

Web Macro Recorder (Event-Based)

A macro is a recording of the events that occur when you access and log in to a Web site using the Event-Based Web Macro Recorder. You can subsequently instruct the HP scanner (WebInspect or QAInspect) to begin a scan using this recording.


A login macro should contain events recorded during a login procedure and incorporates logic that will prevent WebInspect from terminating prematurely if it inadvertently logs out of your application. When scanning a site, WebInspect analyzes every server response to determine the state. If the scanner determines at any time that it is logged out, it runs this macro to log in, and then resumes crawling or auditing the site at the point where the logout occurred. When beginning a scan through the WebInspect scan wizard, you can specify a login macro at Step 2 under Site Authentication.

You can access the event-based Web Macro Recorder in several ways:

- When starting a site scan, select Site Authentication (on Step 2 of the WebInspect Scan Wizard) and click **Record**.
- On the WebInspect toolbar, click **Tools** → **Web Macro Recorder**.
- In default scan settings, click **Scan Settings** → **Authentication** → **Use a login macro**.
- From the Windows Start menu: Click **Start** → **HP** → **HP Security Toolkit** → **Web Macro Recorder**.

Recording a Log-In Macro

After opening the Web Macro Recorder, use the following procedure to record a log-in macro.

- 1 Select **File** → **New** → **Login Macro**.
- 2 Click **Record**.
- 3 In the **Address** box, enter the URL of the target Web site and click  (or press **Enter**).
The Web Macro Recorder renders the resource like a browser and records each event on the Events tab in the dockable pane positioned (by default) at the bottom of the window.
- 4 If necessary, navigate to the login screen.
- 5 Enter a valid user name and password, and submit the credentials (usually by clicking a button such as Log On, Go, Submit, etc.).
- 6 Click **Stop** (to the right of the Address bar) or **Stop Recording** (on the Status bar).
- 7 When prompted to play your macro, click **OK**.

The macro plays by sequentially executing each enabled event listed on the Events tab. A message prompts you to either confirm the success of the macro and specify a logout condition or (assuming that the macro was not successful) troubleshoot the macro.

- 8 Do one of the following:
 - To specify a logout condition, select **Yes** and click **Finished**. Go to Specifying a Logout Condition (below).
 - To troubleshoot, select **No** and click **Next**. Go to [Troubleshooting a Macro](#) on page 265.

Specifying a Logout Condition

- 1 Navigate to a page where you are logged out (usually by clicking a button such as **Log Out**, **Log Off**, or **Exit**).
- 2 Do one of the following:
 - If the browser always displays this page when you log out, click **This page displays when I have logged out** (on the Selection Mode bar that appears directly under the Web Macro Recorder toolbar).
 - If the browser displays a page that contains an element or control that appears only when you are logged out, click **Select Logout Indication** (on the Selection Mode bar) and then click the element or control. For example, if a Login button appears when you have logged out, click **Select Logout Indication** and then click the Login button. Your selection appears on the **Logout Elements** tab.
 - If you want the scanner to search each page for a condition that matches a regular expression that you create, click **Add logout regex**. See [Regular Expression Editor](#) on page 200 for details.
- 3 Select **File** → **Save** (or **Save As**).

Note: You can specify a logout condition at any time by clicking **Actions** → **Add Logout Condition**.

Specifying a Confirmation Element

After creating the macro, you may optionally identify a “confirmation element” that indicates that you have logged in successfully. This is particularly useful for those sites that, following a successful login, display a specific element or control on every page. Some sites, for example, always present a “Log Out” button after the user has logged in. Identifying this confirmation element increases the probability that WebInspect will be able to recognize the “logged in” condition.

Once you identify a confirmation element, if the scanner does not detect that element on the page, it assumes the macro has failed and will attempt to replay the macro up to three times. If the confirmation hint is not detected during one of these playbacks, the scanner produces an error and stops trying to use the macro.

- 1 Navigate to a page that appears after you log in.
- 2 Click **Actions** → **Add Confirmation Element**.
- 3 Do one of the following:
 - If this page always appears after you log in, select **This page displays when I have logged in**.
 - Click **Select Confirmation Element** and then click an element on the page that appears only when you are logged in.

Troubleshooting a Macro

When troubleshooting your recorded macro, you have the following choices:

- **Replay Macro** - Try this solution first. The Web Macro Recorder normally plays the macro at the fastest possible speed, which may compromise performance. Use the slider to select either **Fast** (which is half the speed at which the macro was recorded) or **Original** (which mimics the speed at which the macro was originally recorded).

- **Switch to Traffic Mode** - This closes the Event-Based Web Macro Recorder and opens an alternate web macro recorder that attempts to create macros by analyzing the http traffic. This tool was included with WebInspect version 8.1 and earlier.
- **Adjust macro hints** - Allows you to add or change confirmation elements and/or logout conditions.
- **Re-record Macro** - This choice deletes all data and returns you to the beginning point, where you can try again to create a successful macro.

Dynamic 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). The simplest example is where the challenge asks for a password and the valid response is the correct password.

Many Web sites now present multiple challenges to the user. Typically, when a user first registers with a Web site, 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 Web site presents two or more of these challenges. Some sites also create groups of challenges, and present questions from different groups on each subsequent log-in attempt,

For instructions on building a macro that can accommodate this technique, see the on-line Help.

Editing a macro

After recording a macro, you can modify its contents by excluding certain events.

For example, if you entered the wrong validation credentials while attempting to log in, and then entered the correct credentials, you can remove the erroneous log-in events simply by clearing the check box (in the Include column of the Events tab) next to the event you want to exclude.

Events Logout Elements Confirmation Elements		
Include	Type	Info
<input checked="" type="checkbox"/>	SetValue	Set the value of the [uid] element to [dthackery@windstream.net]
<input checked="" type="checkbox"/>	SelectElement	Select the [password] element
<input checked="" type="checkbox"/>	SetValue	Set the value of the [password] element to [*****]
<input checked="" type="checkbox"/>	SelectElement	Select the [Submit] element

Ordinarily, the best practice is to re-record the macro instead of editing it. However, for an extremely lengthy or complex macro, you can first attempt to modify it. Excluded events are not actually removed until you save the macro, so be sure to test the modified macro (by playing it) before you save it. The Web Macro Recorder events are defined in the following table.

Event	Definition
NavigateTo	Navigate to the specified URL.
Click	Occurs when an element is clicked.
FormSubmit	Occurs when a form has been submitted.
SetValue	Occurs when a value is changed.
SelectElement	Occurs when focus is set on an element.
WaitForPageLoad	Wait for the browser to complete the processing of pages.
Blur	Occurs when an element loses focus.
MouseUp	Occurs when any mouse button is released over an element.
MouseDown	Occurs when any mouse button is pressed while the pointer is over an element.
MouseOver	Occurs when the mouse pointer moves while over an element.
MouseMove	Occurs when the mouse pointer moves.
KeyDown	Occurs when a key is pressed.
KeyUp	Occurs when a key is released.
KeyPress	Occurs before KeyUp, but after button is released.
OnSubmit	Occurs when the submit button in a form is clicked.
NewWindow	Occurs before the new browser window is opened.
NewWindowClosing	Occurs before the new browser window is closed.
ReHookEvents	Not used.
DoubleClick	Occurs when the user double-clicks a control.
Back	Navigate back.
Forward	Navigate forward.
Refresh	Refresh page.
WaitOnUser	Pause until user creates event.
WaitNumberOfSeconds	Wait for timer to expire.
WaitForElement	Wait for element to be rendered on current page.
Unknown	Web Macro Recorder could not determine event.

Dynamic 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). The simplest example is where the challenge asks for a password and the valid response is the correct password.

Many Web sites now present multiple challenges to the user. Typically, when a user first registers with a Web site, the site presents a list of questions to which the user provides answers. For example:

- What is your favorite color?
- What was the name of your first pet?
- In what town or city were you born?
- What was the make of your first automobile?

When the user later attempts to log in, the Web site presents two or more of these challenges. Some sites also create groups of challenges, and dynamically present questions from different groups on each subsequent log-in attempt, as demonstrated in the following example.

When registering for the following example Web site, the user is asked to provide answers to nine questions, which are arranged into three groups of three questions each, as follows.

Group 1

- “What is your name?”, “Smith”
- “What is your favorite color?”, “blue”
- “What is the name of your first grade teacher?”, “Williams”

Group 2

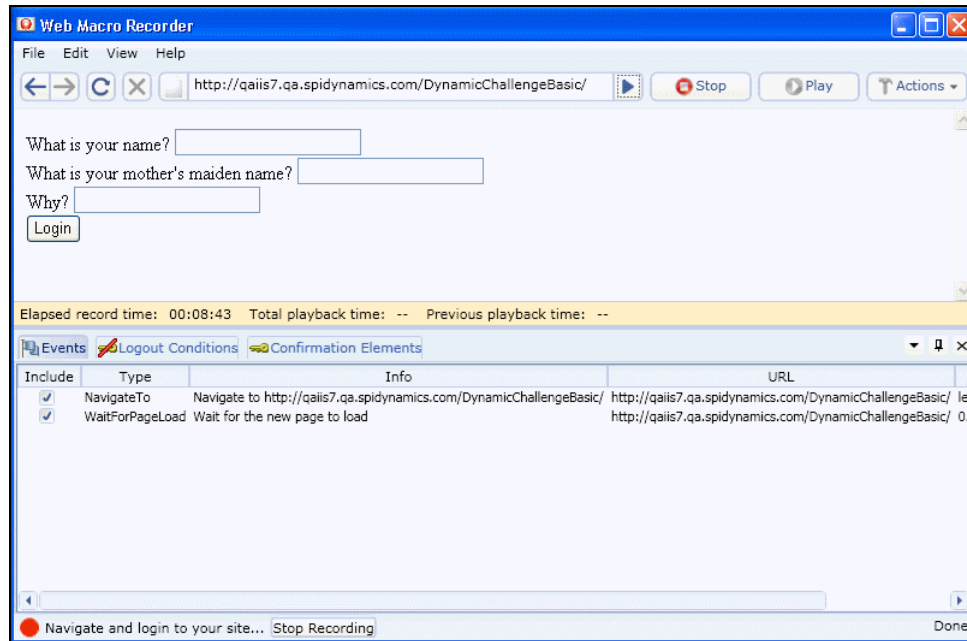
- “What is your mother's maiden name?”, “Larrimore”
- “In what state were you born?”, “Delaware”
- “What is the name of your favorite pet?”, “Rusty”

Group 3

- “Why?”, “Albatross”
- “What is your paternal grandmother's first name?”, “Esther”
- “What is the capital of the state you live in?”, “Atlanta”

In this example, the application randomly selects a number between 1 and 3 (inclusive) and then displays the corresponding ordinal question (first, second, or third) from each group.

- 1 Start the Web Macro Recorder, click Record, and enter the URL of the log-in page.



The source code for pertinent area of the form is:

```
<label for="Q1"> What is your name?</Label><input id="Q1" name="Q1" /> <br>
```

```
<label for="Q2"> What is your mother's maiden name?</Label><input id="Q2" name="Q2" /> <br>
```

```
label for="Q3"> Why?</Label><input id="Q3" name="Q3"/> <br><input type="submit" value="Login" />
```

This illustrates that the label for each question is Q1, Q2, and Q3; similarly, the ID and name for each text box into which the user enters the response is Q1, Q2, and Q3.

- 2 On the log-in page, enter a value for each input element and click **Login**.
- 3 Assuming that you logged in correctly, click **Stop**.
- 4 When prompted to play your macro, click **Cancel**.

To modify the macro so that it accommodates a random presentation of authentication questions:

- 1 Navigate to the log-in page.
- 2 Click the **Events** tab.
- 3 Right-click the first SetValue element and choose Select security question for this element.
 - a Click **Select Security Question** (just below the toolbar).
 - b Click on the label for the first security question (in this example, "What is your name?").

The *Question-Answer Groups* dialog appears.

- c In this example, we know that the first question is a member of the Q1 group. So click the **Add** button, enter "Q1" in the Group Name box, and click **OK**.

Note: If your program does not divide questions and answers into groups, but presents the same set of questions at each log-in attempt, ignore the Group Name controls.

- d Click **Click here to add new question/answer pair**.
 - e Enter the first question and answer pair. In this example:
Question: What is your name?
Answer: Snouck
 - f Repeat Steps 3d-3e, entering the second and third question/answer pair in Group 1.
 - g Click **OK**.
Note that a **Sec. Questions** column is added to the **Events** tab.
 - h Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select Q1.
- 4 Right-click the second SetValue element and choose **Select security question for this element**.
 - a Click **Select Security Question** (just below the toolbar).
 - b Click on the label for the second security question (in this example, "What is your mother's maiden name?").
 - c Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select Manage.
 - d On the *Question-Answer Groups* dialog, click **Add**, enter a group name of "Q2" and click **OK**.
 - e Add the three security question/answer pairs for the Q2 group, following the procedure outlined in Step 3.
 - 5 Right-click the third SetValue element and choose **Select security question for this element**.
 - a Click **Select Security Question** (just below the toolbar).
 - b Click on the label for the third security question (in this example, "Why?").
 - c Click the drop-down arrow for this element in the **Sec. Questions** column on the **Events** tab and select Manage.
 - d On the *Question-Answer Groups* dialog, click **Add**, enter a group name of "Q3" and click **OK**.
 - e Add the three security question/answer pairs for the Q3 group, following the procedure outlined in Step 3.
 - 6 Click **Play** to test the macro.

When troubleshooting the macro, it is usually helpful to right-click an entry on the **Events** tab and select **Playback macro to this event**.

Logout Elements




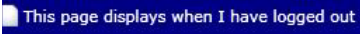

When the *Playback Successful?* dialog appears, the first of three messages at the bottom of the dialog pertains to logout conditions. These are elements, pages, or regular expressions that indicate to the Web Macro Recorder (and the scanner) that the user is no longer logged in to the site or application.

If the message is "Logout conditions have been specified for this macro," the Web Macro Recorder has recognized the logout condition you specified.

However, if the message is “Unable to auto-detect logout conditions,” then either:

- You did not instruct the Web Macro Recorder to automatically detect logout elements (see Settings).
- The Web Macro Recorder was unable to auto-detect elements.
- You did not manually specify a logout condition.

To correct this defect, click **Edit** → **Settings** → **Auto-Detection** and do one of the following:

- Select **Auto-detect logout conditions** and choose one or more of the standard logout elements (or create a custom logout element).
- Clear **Auto-detect logout conditions**, click **OK** to save the settings, and then:
 - a Click  and select **Add Logout Condition**.
 - b Use the Forward and Back buttons  to navigate to a page that contains a logout element.
 - c Do one of the following:
 - Click  and then click the page element that appears only when you are in a “logged out” condition.
 - If the entire page appears only after the user has logged out, click .
 - If you want the scanner to search each page for a logout condition that matches a regular expression that you create, click .

To delete a logout condition from the macro, click the **Logout Conditions** tab (in the Web Macro Recorder's lower pane), right-click a condition, and select **Delete**.

Using a Regular Expression for Logout Detection

If you want the scanner (and Web Macro Recorder) to use a regular expression to detect a logged out condition:

- 1 Select **Add Logout Regex**.

The Regular Expression Editor opens.

- 2 Enter a regular expression that identifies a unique text or phrase that occurs in the server's HTTP response when a user logs off or when a user who is not logged on requests access to a protected URL.

For example, if your server returns a message such as “Have a nice day” when a user logs off your application, then enter “Have\s\sa\s\nice\sday” as the regular expression (“\s” is used in regular expressions to denote a space).

The scanner can also detect that it has logged off 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.” In this case, “[STATUSCODE]302 AND [ALL] http://login.myco.com/config/mail?” might be a typical regular expression. See Regular Expression Extensions for more information.

- 3 Click **OK**.

Confirmation Elements (Hints)





When the *Playback Successful?* dialog appears, the second of three messages at the bottom of the dialog pertains to confirmation elements. These are elements or pages that indicate to the Web Macro Recorder (and the scanner) that the user is logged in to the site or application.

If the message is “Confirmation elements have been specified for this macro,” the Web Macro Recorder has recognized the element that you specified as indicating that the user is logged in.

However, if the message is “Unable to auto-detect confirmation conditions,” then either:

- You did not instruct the Web Macro Recorder to automatically detect confirmation elements (see Settings).
- You instructed the Web Macro Recorder to automatically detect confirmation elements, but the Web Macro Recorder could not recognize the element you specified (or you failed to specify an element).
- You did not manually specify a confirmation element.

To correct this defect, click **Edit** → **Settings** → **Auto-Detection** and do one of the following:

- Select **Auto-detect confirmation** conditions and choose one or more of the standard elements (or create a custom element).
- Clear **Auto-detect confirmation** conditions, click **OK** to save the settings, and then:
 - a Click  and select **Add Confirmation Element**.
 - b Use the Forward and Back buttons  to navigate to a page that contains a confirmation element.
 - c Do one of the following:
 - Click  and then click the page element that appears only when you are in a “logged in” condition.
 - If the entire page appears only after the user has logged in, click .

Unsupported Elements

While recording your macro, the Web Macro Recorder displays a warning if you click an unsupported element. These non-HTML elements include objects created using the following technologies:

- Applets
- ActiveX
- Silverlight
- Flash
- Cross-Domain Iframes

If these objects are not required components of your macro, there is no problem. The Web Macro Recorder simply ignores the object and continues to record events as you generate them by navigating through the site.

However, if an unsupported element contains an essential component (such as a login form), the macro will not succeed.

You might avoid this issue by switching to the session-based Web Macro Recorder.

Event-Based Web Macro Recorder Settings

Follow the steps below to modify the Web Macro Recorder settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **Application** or **Macro** category (described below) and enter the settings.
- 3 Click **OK**.

Application Settings

General

Show startup window

The startup window appears when the Web Macro Recorder is launched and displays a shortcut menu that allows you to begin creating or editing a login macro.



Compress macro files

Applies a compression algorithm to reduce the size of the saved macro.

Encrypt macro file

Applies an encryption algorithm to the saved macro to provide security.

Network Authentication Credentials

If network authentication is required, provide a user name and password that will allow access to the network.

Troubleshooting

Highlight failed events

If you select this option, the program displays failed events with a background color.

- Red highlight: The macro event caused the macro to fail.
- Orange highlight: The event failed, but playback continued.

Ignore events after final page load

In most cases, the events that occur after loading the final page in the macro are not significant and do not affect the playback of the macro.

Auto-Detection

During the recording process, you can manually specify a logout element (an object that appears on the page to indicate that you have logged in successfully) and a confirmation element. If auto-detection is enabled and the program automatically detects a logout element during the recording process, the wizard that appears once playback is complete will reflect this and you will not be prompted to select a logout element .

To instruct the Web Macro Recorder to automatically detect elements, select **Auto-detect logout elements** and/or **Autodetect confirmation hints**.

To identify which of the standard elements will trigger automatic detection, select or clear the associated check box next to the element in the Standard list.

To create a custom element:

- 1 Click **Add**.
- 2 In the **Value** box, enter a text string that appears somewhere within the page.
- 3 Click **OK**.

The element appears in the Custom list.

- 4 In the **Type** column, click the down arrow and select the element type: **Confirmation** or **Logout**.

Proxy

If you need to use a proxy server to access the target Web site:

- 1 Select **Use Proxy**.
- 2 Enter the IP address or host name of the server.
- 3 Enter the server's port number.

IE Dialogs

Microsoft's Internet Explorer may sometimes display dialogs that are not related to the actual content of the Web page. For example, the browser's security feature may present a modal dialog with the following message: "Do you want to view only the webpage content that was delivered securely?" If this occurs during playback of a macro, the scanner will halt until the user presses **Yes** or **No**. You can avoid this interruption by selecting **Use IE Dialog Suppression**.

Several conditions are defined by default. You may, however, define a condition that meets your specific requirements. To do so:

- 1 Click **Add**.
- 2 Enter the requested information.
 - Dialog Caption: Enter the text that appears on the title bar of the dialog box.
 - Dialog Text: Enter the text that appears as the message content.
 - Button: Enter the text that appears on the button that the macro should automatically "press."

The utility that performs this check is case-sensitive, so be sure to enter the text string exactly as it appears.

- 3 Click **OK**.

Macro Settings

General

Smart Credentials

If you start a scan using a macro that includes Smart Credentials, then when you scan the page containing the input elements associated with these entries, WebInspect will substitute the user name and password specified here. This allows you to create the macro using your own user name and password, yet when other persons run the scan using this macro, they can substitute their own user name and password.

To enable this feature, you must first record a macro and then associate one SetValue event in the Events grid as a user name and another SetValue event as a password.

Replacement URL

If you select **Enable URL Replacement**, the host name entered as the Start URL in the Scan Wizard will be dynamically inserted into each URL for this macro. For example, suppose you record a macro for `www.testsite.com`. At a later point in time, `www.testsite.com` is renamed to `www.testsite2.com`. Instead of recording an entirely new macro, you could reuse the original one and enable URL replacement.

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 the scanner should submit when conducting a Web service scan.

- 1 Select **Tools** → **Web Service Test Designer**.
- 2 On the startup dialog, 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.

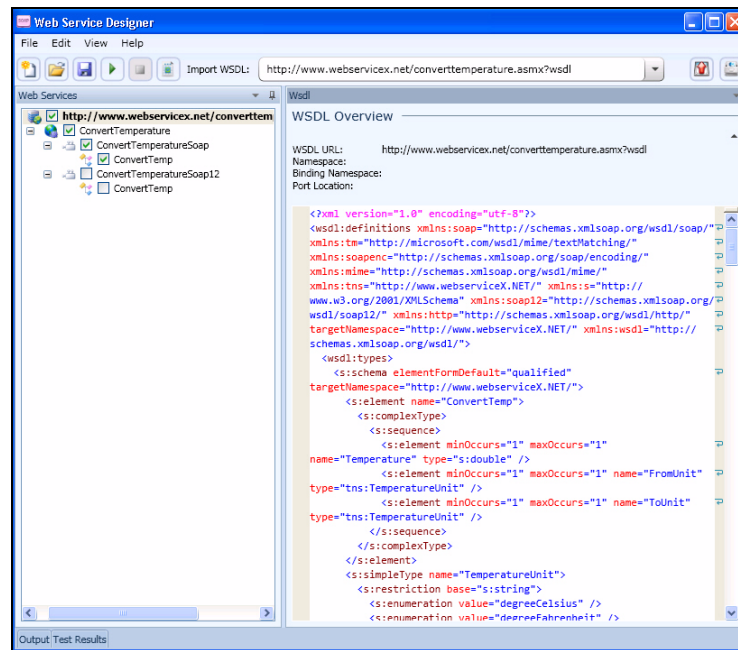
- 3 Do one of the following:
 - In the **Import WSDL** box, type or select the URL of the WSDL site and click **Import WSDL** .

Example: <http://www.webservicex.net/stockquote.asmx?WSDL>.

- Click **Browse for WSDL**  and select a WSDL file that you previously saved locally.

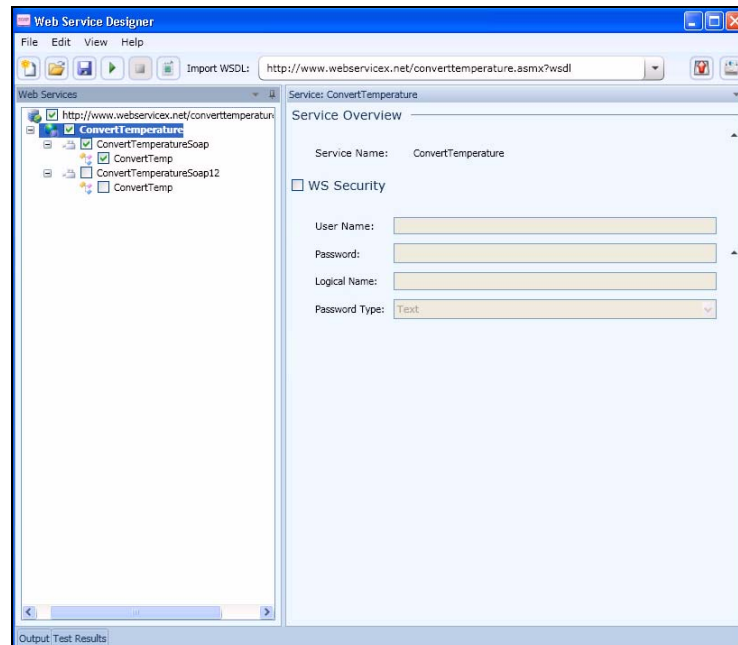
Note: If authentication is required, or if SOAP requests need to be made through a proxy server, see [Web Service Test Designer Settings](#) on page 281 for more information.

The WSDL endpoint (typically represented by a simple http URL string) appears in the left pane, followed by the service name and a hierarchical listing of the operations defined for that service. The right pane (by default) contains the WSDL URL and, when available, the namespace, binding namespace, and the port location.



The above illustration shows a simple WSDL that converts a temperature from one scale to another (for example, from Celsius to Fahrenheit).

- 4 Select the service in the left pane to display service overview information in the right pane.

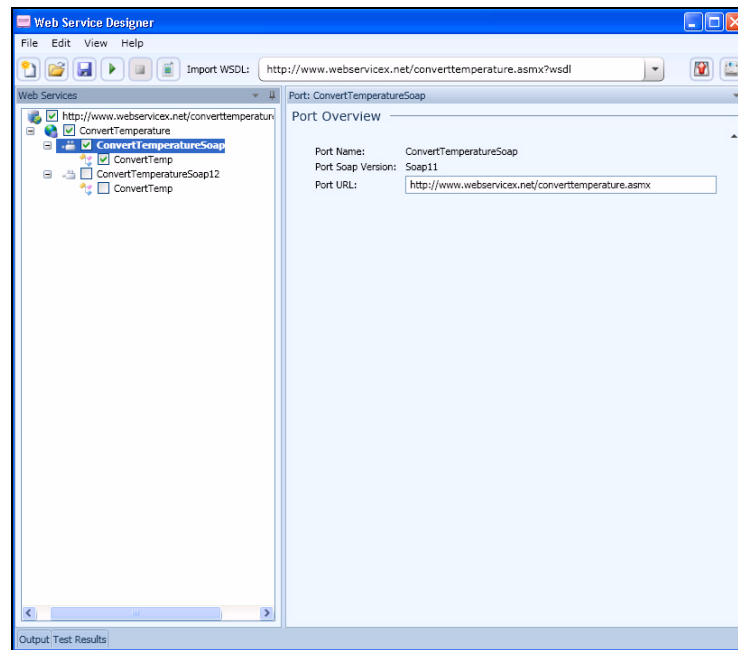


Note that if the description of the WSDL includes both SOAP version 1.1 and version 1.2, and if the operations in both descriptions are the same, the versions are assumed to be identical and the services in version 1.1 only are configured. If you wish to attack both versions, then you must select the check box for each version 1.2 operation.

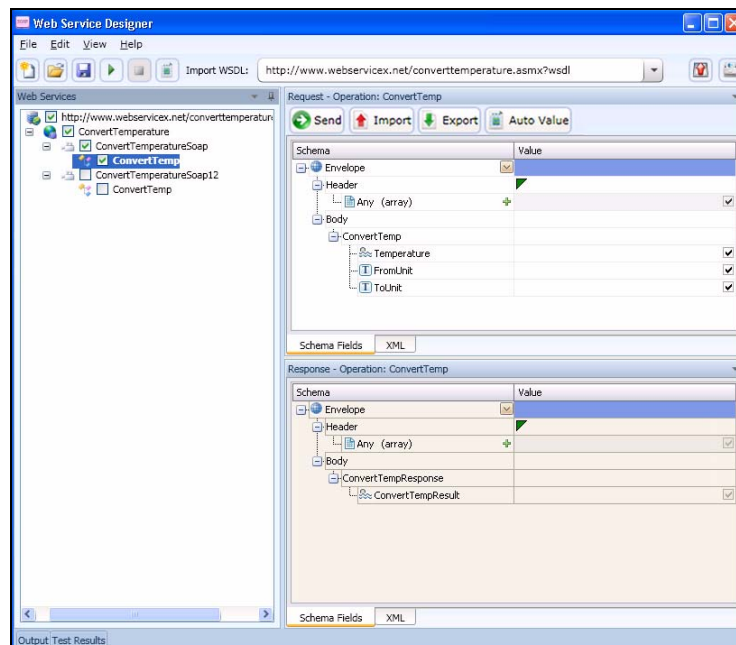
If authentication is required, select WS Security and provide the required credentials.

- 5 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.

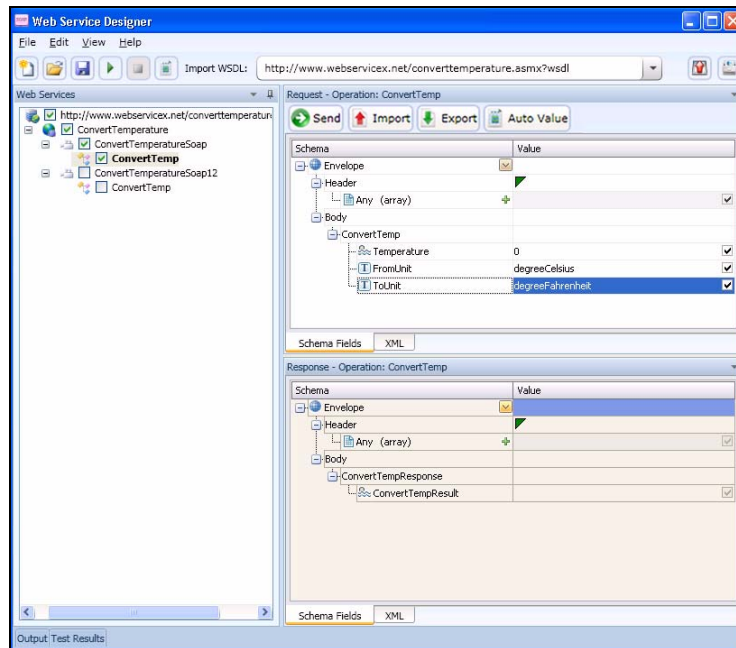
Note that RPC-encoded operations are not supported. These operations cannot be configured and will not be audited.



- 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).

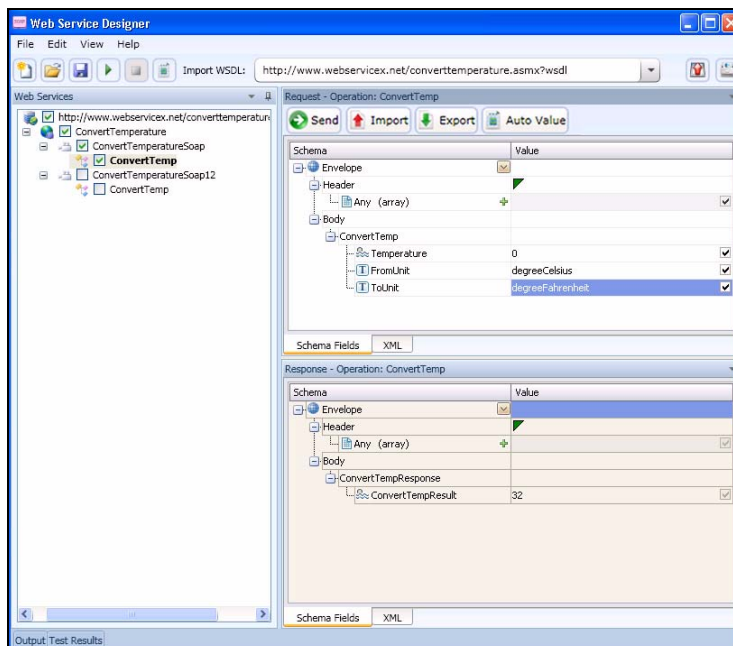


- 7 Enter a value for each parameter in the operation. In this example, there are three parameters: Temperature, FromUnit, and ToUnit. Acceptable values for those parameters are specified in the WSDL. As you type, the program attempts to auto-select a valid value. In this example, the parameters and values entered are Temperature: 0; FromUnit: degreeCelsius; ToUnit: degreeFahrenheit.



- 8 Click **Invoke** .

Results appear in the lower portion. You can alternate between the Schema and XML views by clicking the appropriate tabs.




- 9 When you have assigned and tested values for each operation:

- a Click **File** → **Save**.
- b Using the standard file-selection dialog, select a name and location for the Web Service Design file (.wsd).

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.

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>HPQ</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.

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.

Web Service Test Designer Settings

The Web Services Designer has two categories of settings:

- Network Proxy
- Network Authentication

To access settings, click **Edit** → **Settings**.

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 Internet Explorer**: Import your proxy server information from Internet Explorer.

- **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,” or if the Internet Explorer setting “Use a proxy server for your LAN” is not selected, 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:
 - 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** box. Use commas to separate entries.
- 4 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.

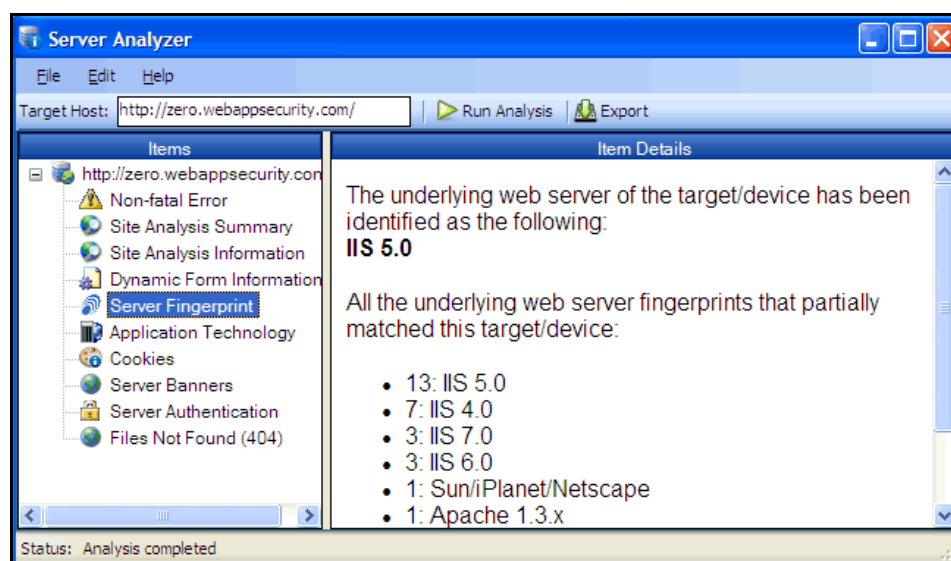
Server Analyzer

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

Analyzing a Server

Follow the steps below to analyze a server:

- 1 In the **Target Host** box, enter the URL or IP address of the target server.
- 2 If host authentication is required, or if you are accessing the host through a proxy server, select **Edit** → **Settings** and provide the requested information. See [Server Analyzer Settings](#) for detailed information.
- 3 Click the **Run Analysis** icon.



Server Analyzer Settings

Follow the steps below to modify the Server Analyzer settings:

- 1 Click **Edit** → **Settings**.
- 2 Select either the **Host Authentication** or **Proxy** category and enter the settings described in the following sections.
- 3 Click **OK**.

Authentication Method

If authentication is required, select a type from the **Authentication** list. See [Authentication](#) on page 122 for a description of the available authentication types.

Authentication Credentials

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

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

Proxy

Use these settings to access the Server Analyzer 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, the Server Analyzer will use the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings.

Use Internet Explorer proxy settings

Select this option to import your proxy server information from Internet Explorer.

Use Firefox proxy settings

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

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

- 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. See [Authentication](#) on page 122 for a description of the available authentication types.
- 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.

HTTPS Proxy Settings

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

Exporting Results

Follow the steps below 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**.

Report Designer

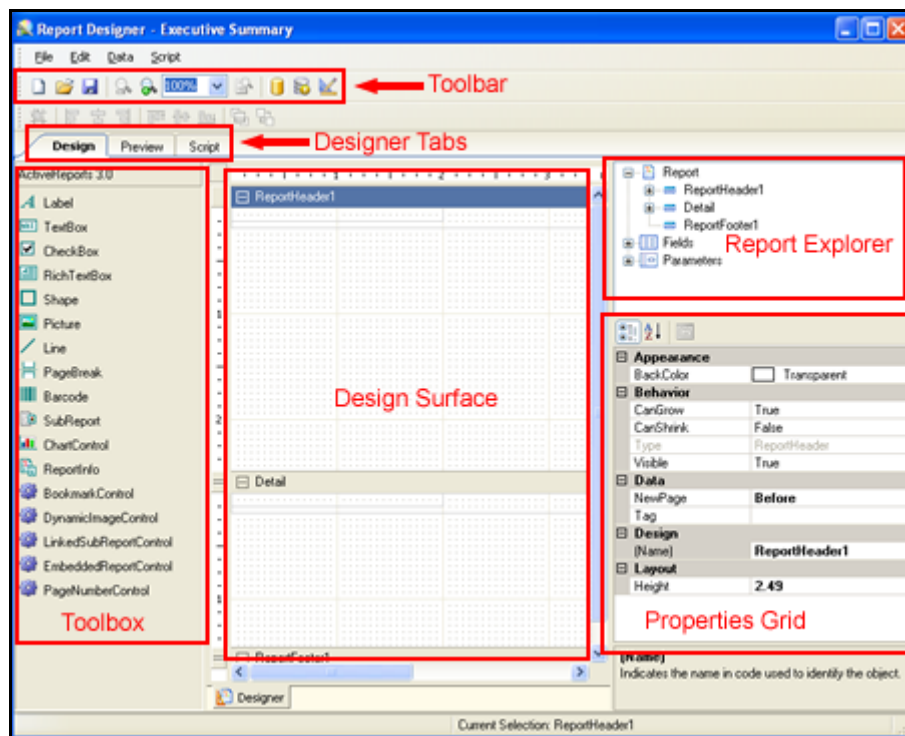
The Report Designer is an HP integration of the ActiveReports® 3.0 report designer developed by Grape City - Data Dynamics. It provides the ability to create and modify reports.

For complete information on using ActiveReports, refer to the ActiveReports User Guide and Class Library.

User Interface

The Report Designer contains six main components, as depicted in the following illustration:

- Toolbar
- Designer Tabs
- Toolbox
- Design Surface
- Report Explorer
- Properties Grid



Toolbar

The Report Designer toolbar is illustrated below.

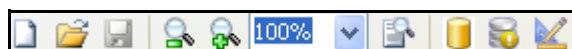












Table 7 Report DesignerToolbar

Icon	Function	Description
	New	Opens the <i>Create Report Definition</i> window, allowing you to select the queries to be included in the report.
	Open	Opens the <i>Open a Report</i> dialog, allowing you to select a report or subreport for editing.
	Save	Saves the open report.
	Zoom In	Increases the magnification of the design surface at 50 percent increments.
	Zoom Out	Decreases the magnification of the design surface at 50 percent increments.
	Magnification Percentage	Allows you to select a magnification setting for the design surface.
	Actual Size	Returns the magnification of the design surface to 100 percent.
	Set Data Source	Allows you to specify the scan that will provide the data.
	Set Custom Data Source	Allows you to specify a custom data source.
	Parameter Designer	Opens the Parameter Designer tool.

Menus

The Report Designer contains the following menus:

Table 8 Report Designer Menus

Menu	Command	Description
File	New	Opens the <i>Create Report Definition</i> dialog, allowing you to select a definition for a new report.
	Open	Opens the <i>Open a Report</i> dialog, allowing you to select a report for editing.
	Save	Saves the open report.
	Save As	Saves the open report to a file you specify.
	Export	Saves the report in a format you specify.
	Enable Console Output	If enabled, WebInspect presents a pane (at the bottom of the window) that displays the status of each report page being generated. If a problem is encountered, this pane displays an exception message and stack trace. This pane is also visible on the Preview tab of the Report Designer.
	Exit	Terminates the Report Designer.
Edit	Parameter Designer	Opens the Parameter Designer tool.
	Modify/Create Report	Opens the <i>Modify Report Definition</i> dialog, allowing you to change the report definition.
	Delete	Deletes the selected object.
	Cut	Deletes the selected object and saves it to the clipboard.
	Copy	Copies the selected object to the clipboard.
	Paste	Inserts the contents of the clipboard.
	Undo	Reverses the last operation performed.
Data	Redo	Reverses the last Undo operation.
	Set Scan and Report Inputs	Allows you to select a scan and specify report parameters.
	Set Custom Data Source	Opens the <i>Report Data Source</i> dialog, allowing you to connect to various sources.
	Edit Global Styles	Opens the Report Styles Editor. Use this to create or modify a style sheet.
	Edit Report Styles	Opens the Report Styles Editor. Use this to create or modify styles for the report on which you are currently working
Script	Edit Report Settings	Opens the <i>Report Settings</i> dialog, allowing you to modify many facets of your report.
	Import	Allows you to select a script from the script library to import into the designer.

Table 8 Report Designer Menus (cont'd)

Menu	Command	Description
	Compile	Compiles the script.
	Find	Opens the Script tab and presents the <i>Find/Replace</i> dialog, allowing you to search for the text you specify.
	Script Editor	Opens the Script Editor.

Designer Tabs

The Report Designer contains the following three tabs.

Design Tab

By default, when you create or open a report, the Design tab is selected. Use this area to perform all design-time and run-time functions associated with your report, such as creating a layout, binding to data sources, creating event-handling methods, and more.

Script Tab

Selecting the Script tab opens the script editor, which gives you the ability to add scripting to your report. The Script editor allows you to create event-handling methods. In the Report Events tab on the right, there is a combo box where you can select any report section to attach an event-handling method.

Preview Tab

The Preview tab allows you to view what your report looks like at run time with actual scan data. This makes it easy to quickly see the run-time impact of changes you make in the designer or the code-behind. Use the Preview toolbar to navigate the report and add annotations.

Toolbox

The toolbox displays a variety of controls. To add a control, drag it from the toolbox and drop it on the design surface (canvas), where you can modify its size, position, alignment, and properties.

- Barcode — Inserts an ActiveReports Barcode control; can be bound to a database field.
- ChartControl — Inserts a chart in any of a variety of styles.
- Checkbox — Inserts a check box; can be bound to a database field.
- Label — Inserts a new static label control; can be bound to a database field.
- Line — Inserts a line control.
- PageBreak — Inserts a page break within a selection.
- Picture — Inserts an image loaded from a file; can be bound to a database field.
- ReportInfo — Displays report information in a number of format strings such as {PageNumber} of {PageCount}; can be bound to a database field.
- Textbox — Inserts a textbox; can be bound to a database field
- Shape — Inserts a rectangle, circle or square shape.

- Subreport — Inserts a Subreport control to link to another report.
- RichTextBox — Inserts an ActiveReports RichTextBox control; can be bound to a database field.
- BookmarkControl — Inserts a hyperlink in the table of contents; clicking the hyperlink navigates to the bookmark.

Note: Bookmark text can be formatted as follows:

```
{=MainReportName}\<static-text>\{=<field-name>}
```

where

MainReportName is optional (and doesn't need to appear first)

\ indicates the beginning of a hierarchical level

<static-text> is any text you assign to the bookmark

<field-name> is the name of a bound or calculated field

- DynamicImageControl — Allows you to associate an image selector control with an image (using the Parameter Designer), so the user can select an image a run time. Can be bound to a database field.
- LinkedSubreportControl — Creates a link to the subreport you select. Use the AssociatedFields property to pass values to the subreport.
- EmbeddedReportControl — Allows you to design a subreport “on the fly” (rather than using a LinkedSubreportControl) using the DataTableField property.
- PageNumberControl — Allows you to place a page number in the report (usually in the page footer).

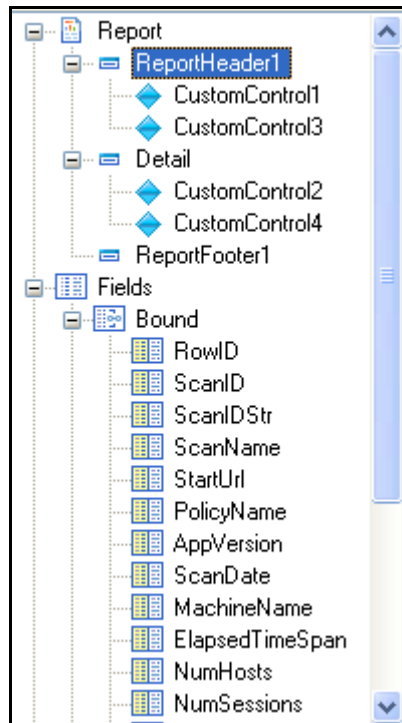
Design Surface

The default design surface contains the following base components:

- PageHeader section--This section can be used to print column headers, page numbers, page titles, or any information that needs to be printed once at the top of each page. Bound controls in the PageHeader or PageFooter are not supported. The data in such controls may not be synchronized with the data displayed in other sections on the page.
- Detail section--This section is the body of the report that prints once for each record in the data source. A report's layout may contain only one Detail section.
- PageFooter section--This section can be used to print page totals, page numbers or any other information that needs to be printed once at the bottom of each page.
- Designer/Script/Preview tabs--The Designer and Script tabs can be clicked to toggle between design and script views, while the Preview tab allows for a fully functional design-time preview of how a report will look and behave at run time.

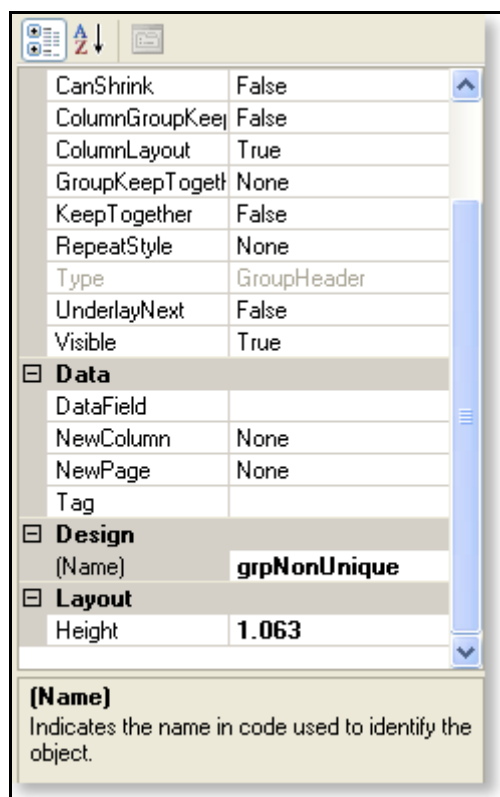
Report Explorer

The Report Explorer serves as the information focal point for your report. From it, you can gain a quick overview of the elements that compose the report, remove individual controls, add parameters and calculated fields, bind data fields to text box controls, and modify properties and report behavior via the Properties grid.



Properties Grid

The Properties Grid allows you to view or modify properties for an object selected on either the Design Surface or the Report Explorer.



Creating a Report

- 1 Open or create a report definition.

To create a report definition:

- a Click **File** → **New** (or click the New icon on the toolbar).
- b Create a report definition.
- c Enter a name and (optionally) a brief description for the report.
- d Select a report context: either **Scan** or **Session**.

When a scan is open, users can generate a session report by right-clicking a session and selecting **Generate Session Report** from the context menu.

- e If you want the report name to be included in the list of WebInspect reports, select **Exposed in Product**.

Typically, you do not select this option if you are creating a subreport.

- f If you are creating a header/footer template, select **Header/Footer Template**.
- g Select one or more views from the View Name list. To see the view parameters and fields, click the view name.
- h Click **OK**.

To open a report definition:

- a Click **File** → **Open** (or click the Open icon on the toolbar).
- b Select a report or subreport.
- c Click **OK**.

- 2 Design your report. For complete information on using ActiveReports, refer to the ActiveReports User Guide and Class Library.
- 3 To modify the script associated with this report, click the **Script** tab.
- 4 To modify or create parameters associated with this report, click **Edit** → **Parameter Designer**.
- 5 To modify the styles associated with this report, click **Data** → **Edit Report Styles**.
- 6 To preview your work:
 - a Click the **Preview** tab.
 - b On the *Generate a Report* dialog, select a scan and click **Next**.
 - c If the report includes parameters, select parameters.
 - d Click **Finish**.

Report Script Editor

Use the Report Script Editor to create or modify scripts maintained in a script library. You can then import these scripts into reports.

All scripts must be written using the C# language.

The Report Script Editor menu bar contains the following menus:

Table 9 Report Script Editor Menus


Menu	Command	Description
File	Save	Save the script to a library.
	Refresh	Redisplay the script.
	Exit	Terminate the Script Editor.
Edit	Find	Open a <i>Find / Replace</i> dialog, allowing you to search for and optionally replace text in the script.
Script	Import	Incorporate a script library into the script you are developing.
	Compile	Compile the script.
Help	Help	Open the Help file.

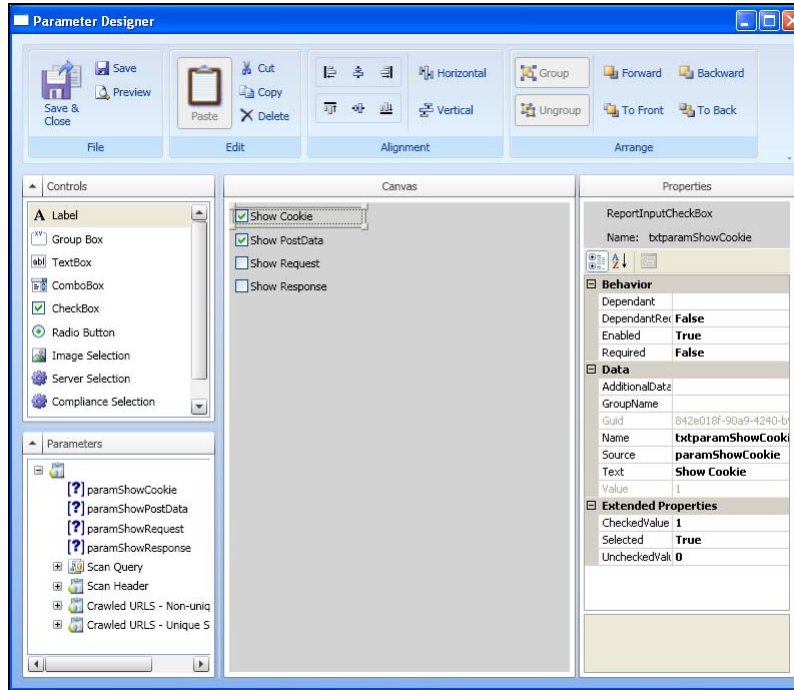
Parameter Designer

Reports have three types of inputs that can be used for filtering data or supplying custom content to reports. They are:

- **Data View parameters (query parameters)** – Data View parameters are used to pass values to the underlying Data View of the report for filtering data. Parameter names begin with @.
- **Report Parameters** – Report parameters are used to pass values entered by the user to the report. These values are then used by the report to alter report behavior or format.
- **Replacements** – Replacements are tokens that exist in the data view. Replacement inputs are used to pass values to these tokens. Replacements are used to change the sort order of a data view or to provide additional criteria to the data view.

Users have the opportunity to provide values for these inputs when generating a report. Before a user can be prompted to enter inputs, however, report designers must specify which inputs will be displayed to the user and how they will be presented. This is accomplished by using the Parameter Designer.

To open the Parameter Designer, from an open report in the Report Designer, click the Parameter Designer icon  on the toolbar or choose **Parameter Designer** from the **Edit** menu.



The Parameter Designer has five areas.

Toolbar

The toolbar provides easy access to all of the functions of the designer:

- **Save and Close** – Saves the current design to the report and closes the *Parameter Designer* window.
- **Save** – Saves the current design to the report.
- **Preview** – Opens a window showing what the designed inputs will look like at run time.
- **Cut, Copy, Paste, Delete** – Manipulate controls on the canvas.
- **Alignment** – Align one or more selected controls on the canvas.
- **Group/Ungroup** – A designer can group two or more selected controls on the canvas. When controls are grouped together, they can be moved together on the canvas.
- **Forward** – Bring the selected control forward one layer.
- **Backward** – Send the selected control backward one layer.
- **To Front** – Bring the selected control to the top most layer.
- **To Back** – Send the selected control to the bottom most layer.

Canvas

The canvas is the design area, which constitutes a visual representation of the parameters that are presented at run-time. Controls can be added, modified, and deleted from the canvas.

Properties Grid Pane

This area displays the properties of object(s) selected in the design canvas or the Parameters pane, whichever has the focus.

Controls Toolbox


The Controls toolbox lists the types of controls that may be added to the report. They include, in addition to the standard self-explanatory controls, the following special controls:

- **Server Selection**—A drop-down list of available servers in the selected scan.
- **Compliance Selection**—A list of compliance templates; suitable for compliance reports only.
- **Sort Control**—Allows you to select how you want the report data to be sorted.

To add a control, drag it from the toolbox and drop it on the canvas.

Report Parameters Pane

This pane displays a hierarchical representation of all parameters available to the current report and its subreports. Icons indicate the parameter type.

Query 

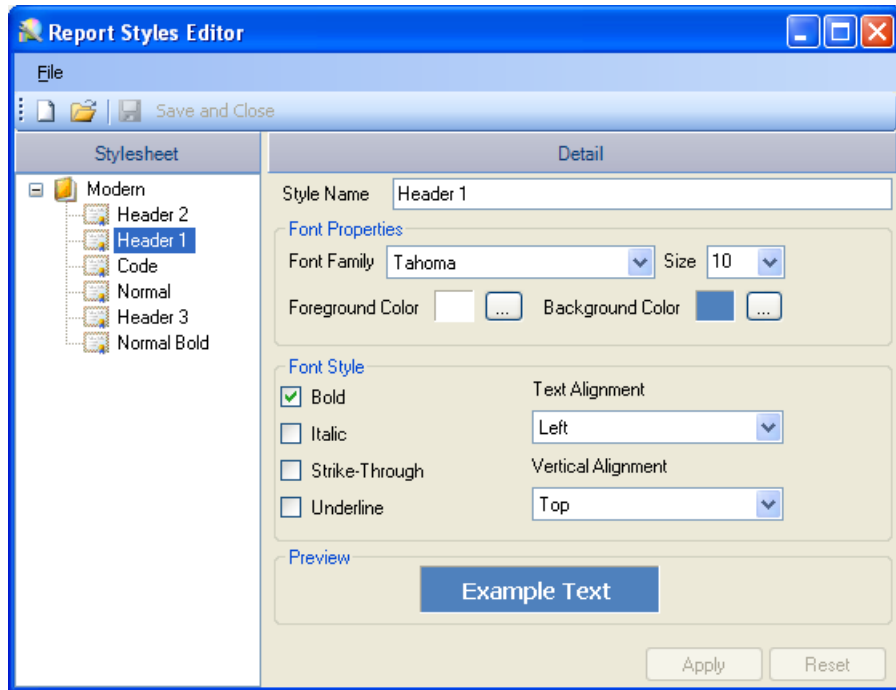
Report 

Replacement 

Report Styles Editor

When creating or modifying a report, the Report Designer uses the style sheet that is specified as the default. If you want to create or modify styles for the report on which you are currently working, select **Edit Report Styles** from the **Data** menu. New styles will be added to the report; modified styles will override the default definition for this report.

Conversely, if you want to create or modify a style sheet, select **Edit Global Styles** from the **Data** menu. You can then edit or create stylesheets, and specify the style sheet that will be initially assigned to all reports as the default.



Report Structure

Report Structure

A report section contains a group of controls that are processed and printed at the same time as a single unit. ActiveReports defines the following section types.

Report Header

A report can have one report header section that prints at the beginning of the report. This section generally is used to print a report title, a summary table, a chart or any information that needs only to appear once at the report's start.

Report Footer

A report can have one report footer section that prints at the end of the report. This section is used to print a summary of the report, grand totals, or any information that needs to print once at the report's end.

Page Header

A report can have one page header section that prints at the top of each page. Unless the page contains a report header section, the page header will be the first section that prints on the page. The page header section is used to print column headers, page numbers, a page title, or any information that needs to appear at the top of each page in the report.

Page Footer

A report can have one page footer section that prints at the bottom of each page. It is used to print page totals, page numbers, or any other information that needs to appear at the bottom of each page.

Group Header/Footer

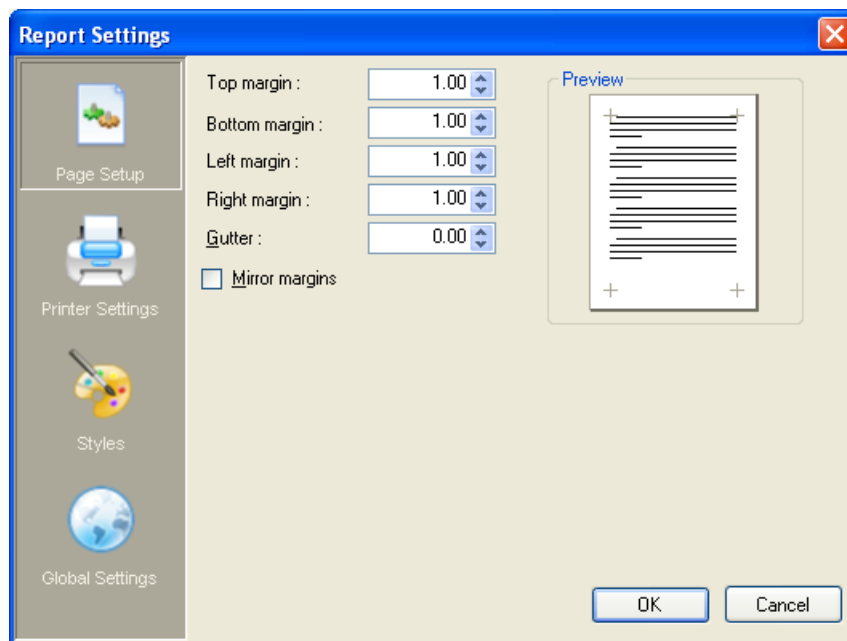
A report can consist of single or multiple nested groups, with each group having its own header and footer sections. The header section is inserted and printed immediately before the detail section. The footer section is inserted and printed immediately after the detail section.

Detail

A report has one detail section. The detail section is, in some cases, the body of the report and one instance of the section is created for each record in the report.

Report Settings

You can modify facets of your report, such as the page setup, printer settings, styles, and global settings of your report at design time. To make changes, access the *Report Settings* dialog by selecting Data > Edit Report Settings.



Charts

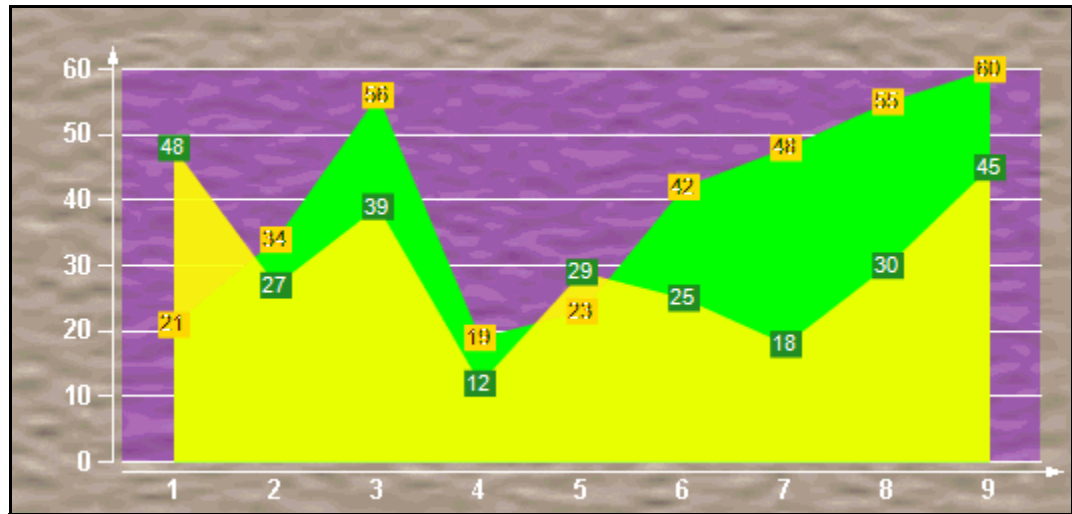
Chart Types

Chart types include Common Charts, 3D Charts, and XY Charts. See the on-line Help for more extensive illustrations of chart types.

Common Charts

- **Area Charts**

Use an area chart to compare trends over a period of time or in specific categories.



Number of Y values/data points: 1

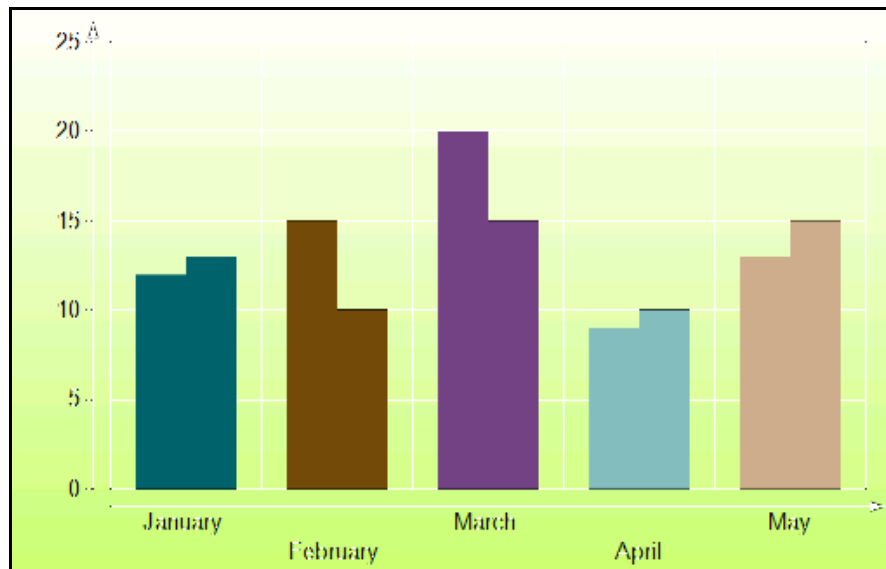
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **Bar2D Charts**

Use a bar chart to compare values of items across categories.



Number of Y values/data point: 1

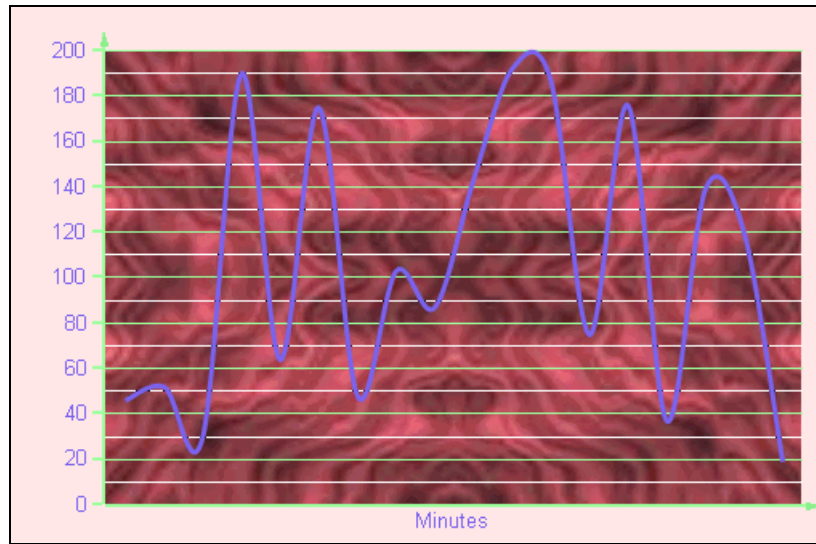
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value

- **Bezier Charts**

Use a Bezier or spline chart to compare trends over a period of time or in certain categories. It is a line chart that plots curves through the data points in a series.



Number of Y values/data point: 1

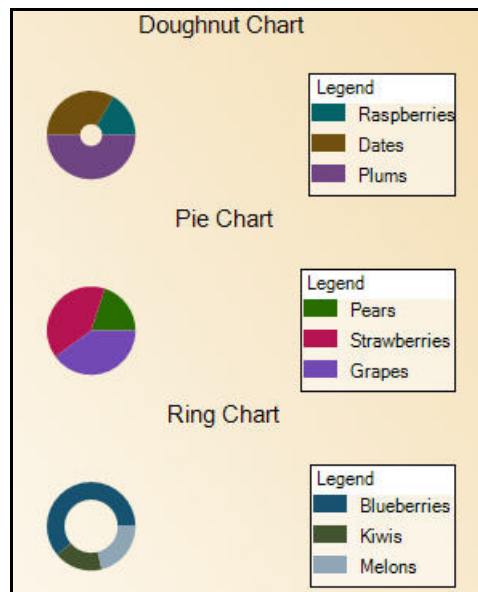
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **Doughnut/Pie Charts**

A doughnut chart shows how the percentage of each data item contributes to the total.



Number of Y values/data point: 1

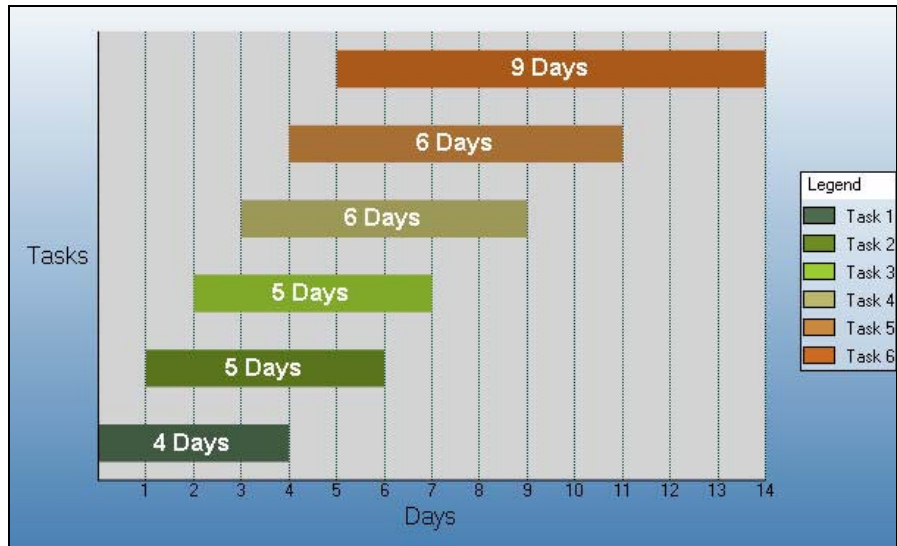
Number of Series: 1

Marker Support: Series or Data Point

Custom Properties: ExplodeFactor gets or sets the amount of separation between data point values. HoleSize gets or sets the inner radius of the chart. OutsideLabels gets or sets a value indicating whether the data point labels appear outside the chart. StartAngle gets or sets the horizontal start angle for the series.

- Gantt Charts**

The Gantt chart is a project management tool used to chart the progress of individual project tasks. The chart compares project task completion to the task schedule.



Number of Y values/data point: 2

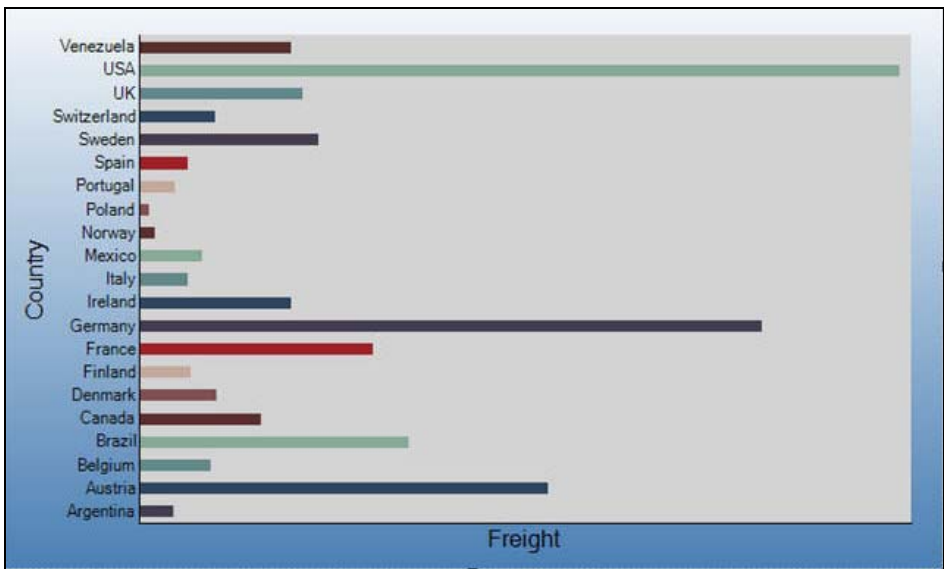
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value.

- HorizontalBar Charts**

Use a horizontal bar chart to compare values of items across categories with the axes reversed.



Number of Y values/data point: 1

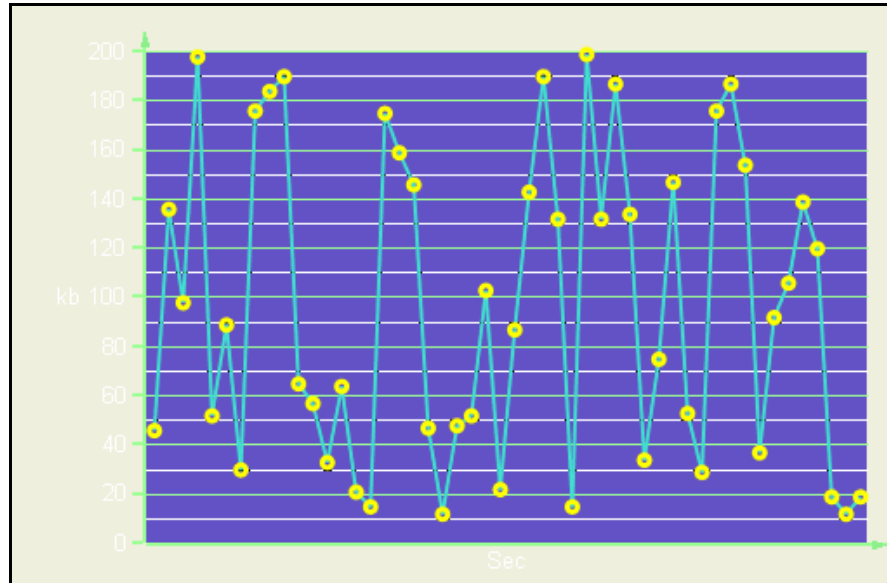
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value.

- **Line Charts**

Use a line chart to compare trends over a period of time or in certain categories.



Number of Y values/data point: 1

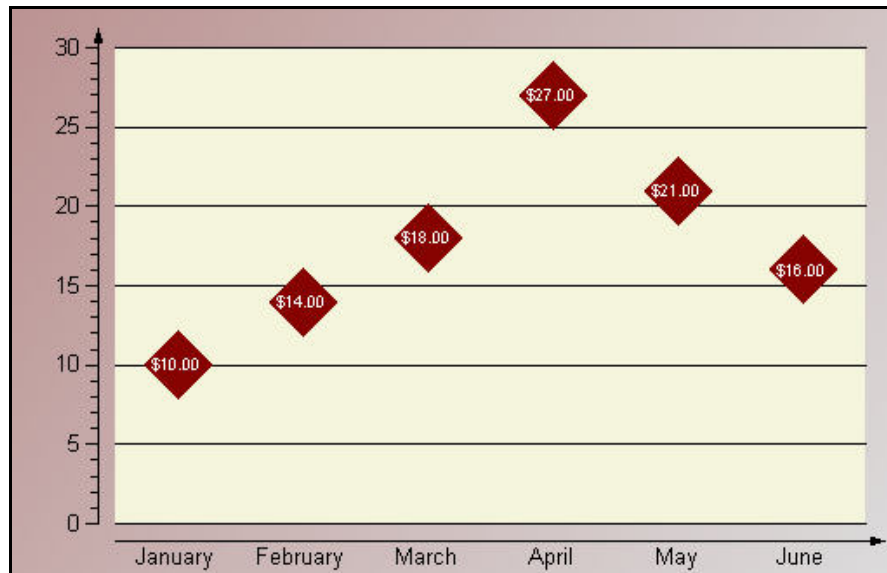
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **Scatter Charts**

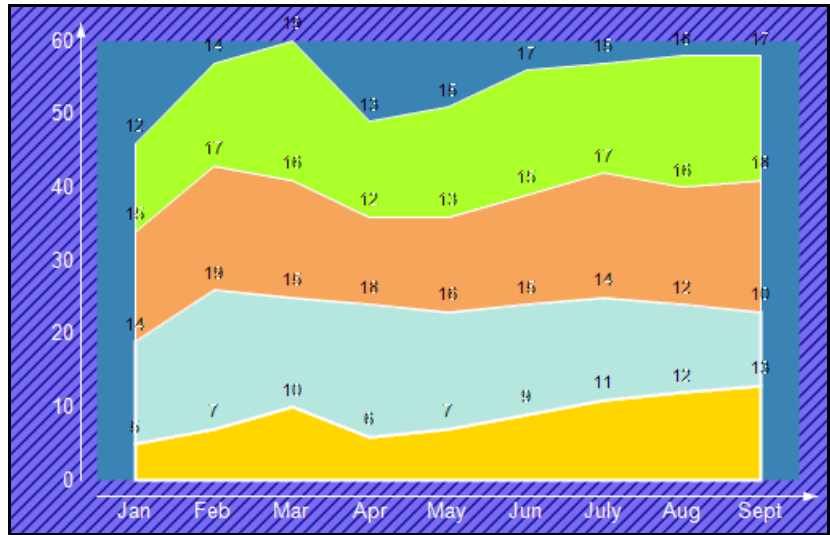
Use a scatter chart to compare values across certain categories.



Number of Y values/data point: 1
Number of Series: 1 or more
Marker Support: Series or Data Point
Custom Properties: None

• **StackedArea Charts**

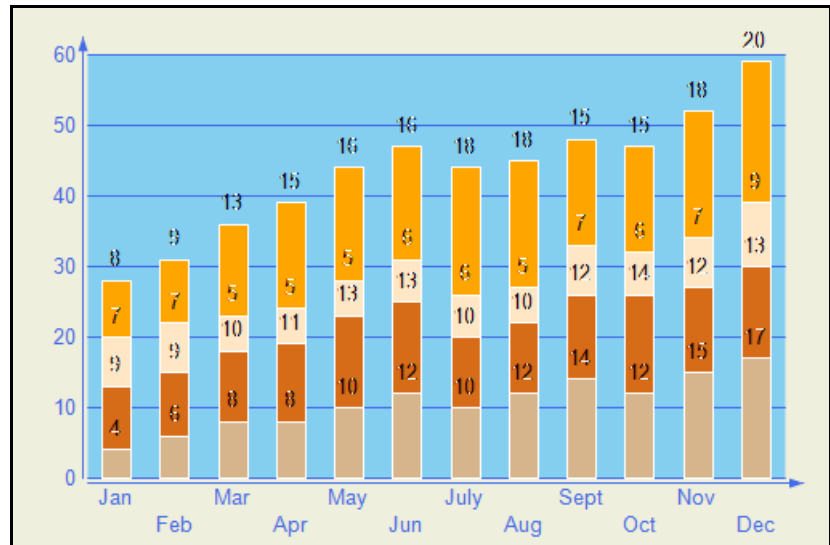
A stacked area chart is an area chart with two or more data series stacked one on top of the other. Use this chart to show how each value contributes to a total.



Number of Y values/data point: 1
Number of Series: 1 or more
Marker Support: Series or Data Point
Custom Properties: None

• **StackedBar Charts**

A stacked bar chart is a bar chart with two or more data series stacked one on top of the other. Use this chart to show how each value contributes to a total.



Number of Y values/data point: 1

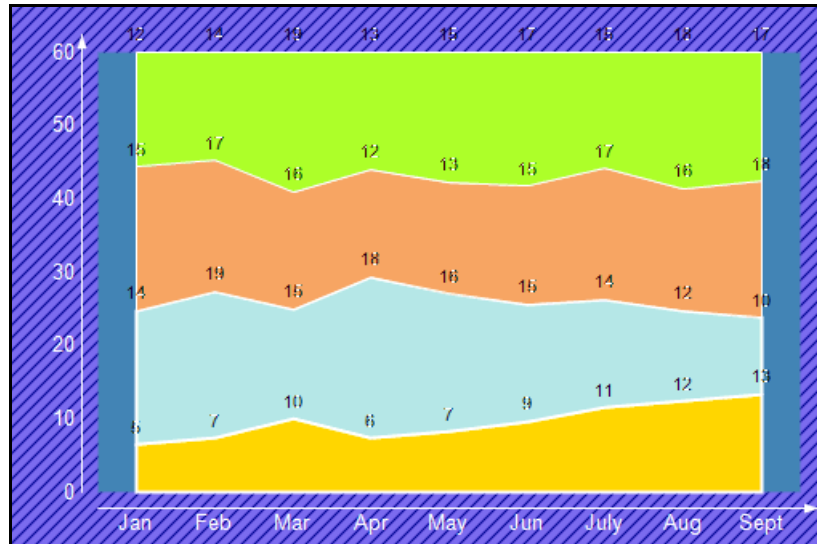
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value

- **StackedArea100Pct Charts**

A stacked area 100 percent chart is an area chart with two or more data series stacked one on top of the other to sum up to 100 percent. Use this chart to show how each value contributes to a total with the relative size of each series representing its contribution to the total.



Number of Y values/data point: 1

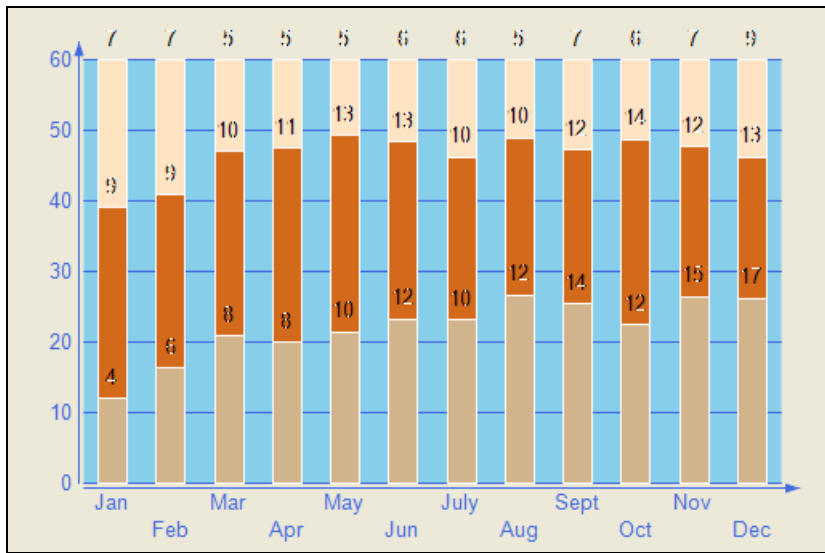
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **StackedBar100Pct Charts**

A StackedBar100Pct chart is a bar chart with two or more data series stacked one on top of the other to sum up to 100 percent. Use this chart to show how each value contributes to a total with the relative size of each series representing its contribution to the total.



Number of Y values/data point: 1

Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: Gap gets or sets the space between the bars of each X axis value

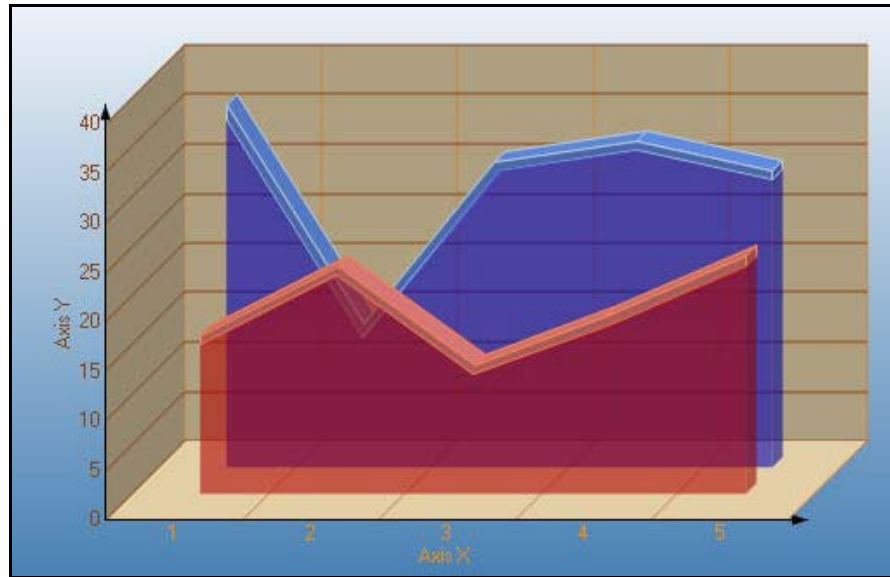
3D Charts

This topic illustrates some of the three dimensional chart types that you can create with the Chart control.

Note: To see a chart in three dimensions, open the *ChartArea Collection* dialog, and in the Projection section, change the *ProjectionType* from *Identical* to *Orthogonal*.

- **Area3D Charts**

Use a 3D area chart to compare trends in two or more data series over a period of time or in specific categories, allowing the data to be viewed side by side.



Number of Y values/data point: 1

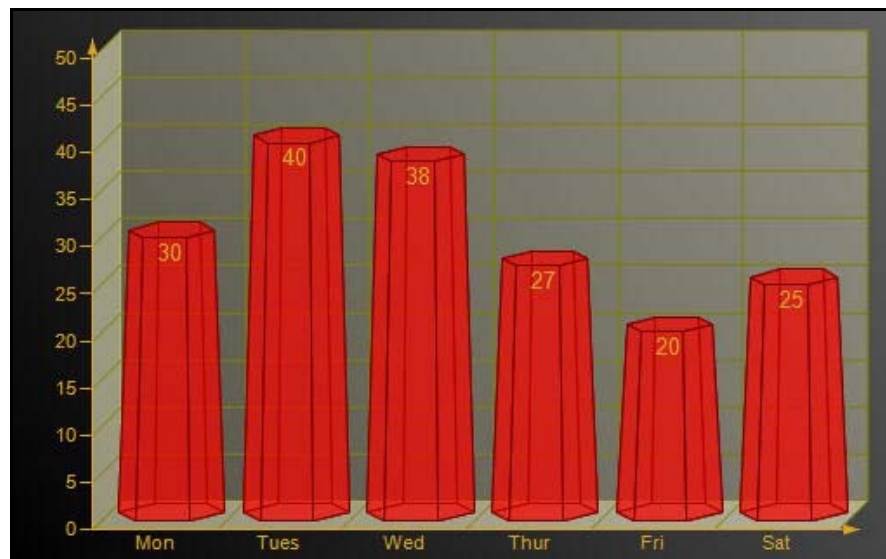
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: LineBackdrop gets or sets the backdrop information for the 3D line. Thickness gets or sets the thickness of the 3D line. Width gets or sets the width of the 3D line.

- **Bar3D Charts**

Use a 3D bar chart to compare values of items across categories, allowing the data to be viewed conveniently in a 3D format.



Number of Y values/data point: 1

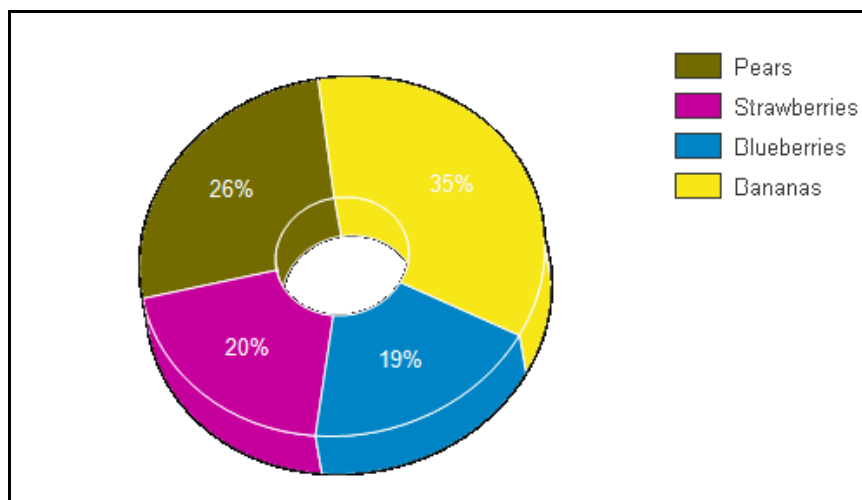
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: BarTopPercent gets or sets the percentage of the top of the bar that is shown for Cone or Custom BarTypes. BarType gets or sets the type of bars that is displayed. Gap gets or sets the space between the bars of each X axis value. RotationAngle gets or sets the starting horizontal angle for custom 3D bar shapes. Can only be used with the Custom BarType. VertexNumber gets or sets the number of vertices for the data point, used to create custom 3D bar shapes. Can only be used with the CustomBarType. Bars must contain 3 or more vertices.

- **Doughnut3D Pie Charts**

A 3D doughnut chart shows how the percentage of each data item contributes to a total percentage, allowing the data to be viewed in a 3D format.



A 3D doughnut chart shows how the percentage of each data item contributes to a total percentage, allowing the data to be viewed in a 3D format.

Number of Y values/data point: 1

Number of Series: 1

Marker Support: Series or Data Point

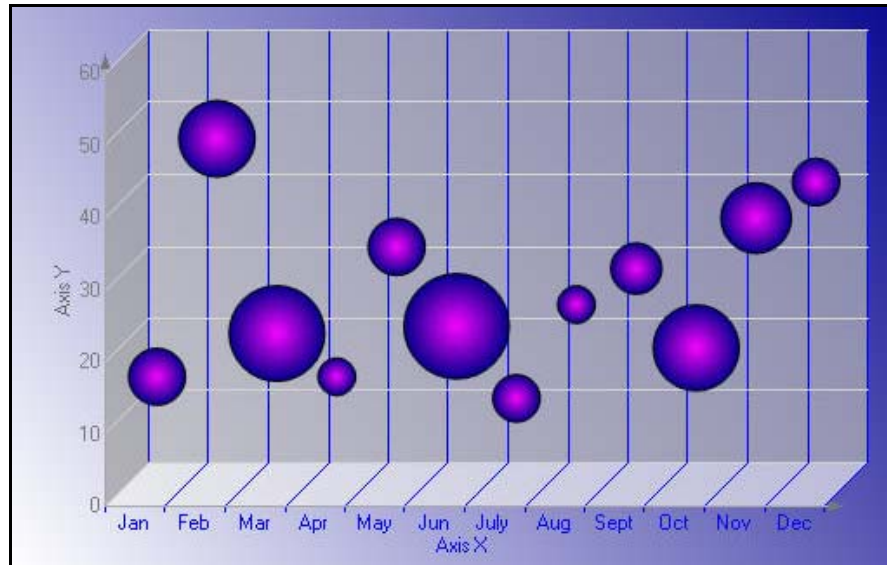
Custom Properties: ExplodeFactor gets or sets the amount of separation between data point values. The value must be less than or equal to 1. To explode one section of the doughnut chart, set ExplodeFactor on the data point instead of on the series. HoleSize gets or sets the inner radius of the chart. If set to 0, the chart will look like a pie chart. The value must be less than or equal to 1. OutsideLabels gets or sets a value indicating whether the data point labels appear outside of the graph. StartAngle gets or sets the horizontal start angle for the series data points.

XY Charts

Some of the XY chart types you can create with the Chart control are described below.

- **Bubble Charts**

The Bubble chart is an XY chart in which bubbles represent data points. The first Y value is used to plot the bubble along the Y axis, and the second Y value is used to set the size of the bubble. The bubble shape can be changed using the series Shape property.



Number of Y values/data point: 2

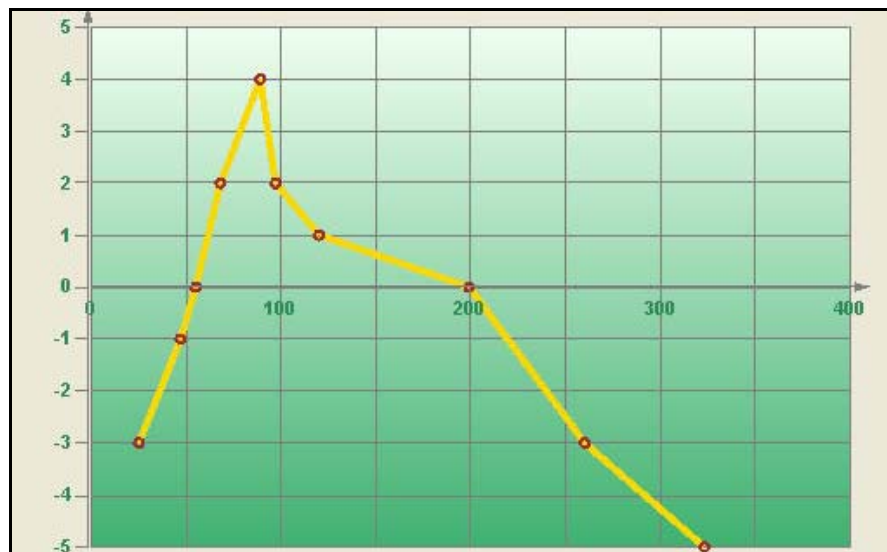
Number of Series: 1 or more

Marker Support: Series or Data Point. Marker labels use the second Y value as the default value.

Custom Properties: MaxSizeFactor gets or sets the maximum size of the bubble radius. Values must be less than or equal to 1. Default is .25. MaxValue gets or sets the bubble size that is used as the maximum. MinValue gets or sets the bubble size that is used as the minimum. Shape gets or sets the shape of the bubbles. Uses or returns a valid MarkerStyle enumeration value.

- **LineXY Charts**

A line XY chart plots points on the X and Y axes as one series and uses a line to connect points to each other.



Number of Y values/data point: 1

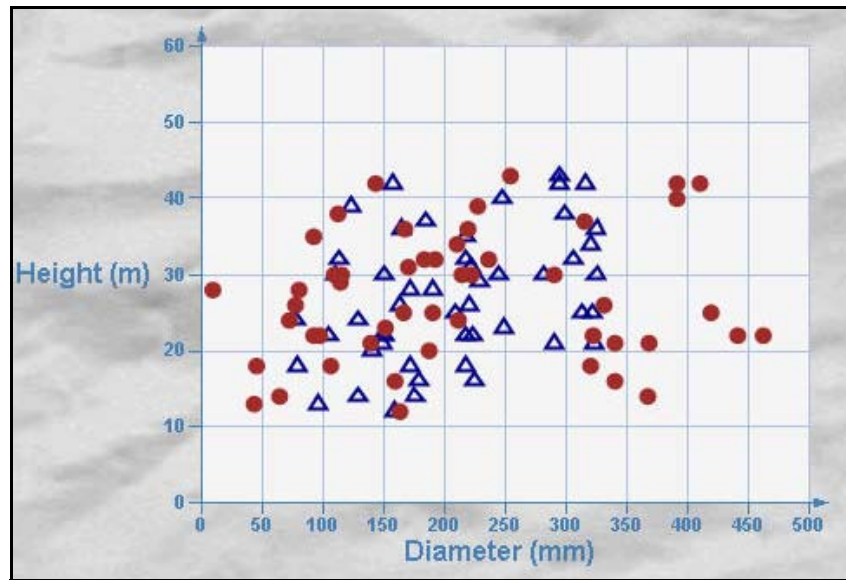
Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

- **PlotXY Charts**

A plot XY chart shows the relationships between numeric values in two or more series sets of XY values.



Number of Y values/data point: 1

Number of Series: 1 or more

Marker Support: Series or Data Point

Custom Properties: None

Chart Data

Data-Bound Charts

The Chart control provides several ways to bind your charts to data at design time.

- Adding Data with the Wizard

To open the Chart Wizard, right-click the chart and select Wizard. In the Chart Wizard, once you have added a series, you can create a data adapter to contain the data for your chart, if needed. When a data source is available, the Value X and Y values can be set for the series in the chart wizard from the expressions and/or data columns retrieved from the data source.

- Adding Data with the Chart Designer

Once a data source is set up, you can easily bind data to a series using the Chart Designer. Choose the Series section on the left, and on the **General** tab, after a series has been added to the chart, set the ValueY property by selecting the name of the data expression you wish to assign to the series.

- Adding Data through the *Chart Data Source* Dialog

To set the data source for the chart through the *Chart Data Source* dialog, click the *DataSource* property.

After the *DataSource* for the chart is set, add a series to the chart. To do this, open the *Series Collection Editor* dialog by clicking the ellipsis button which appears when you click next to the *Series* property in the *Properties* window, then click the **Add** button. To bind the series to an expression or dataset column returned by your data source, set the *ValueMembersY* or *ValueMembersX* property of the series by selecting it from the drop-down list.

Unbound Charts

The Chart control makes it easy to set the data source for a chart control, series, or data points collection at run time.

Below is a list of objects that can be used as data sources.

- dataset
- dataset Column
- Data Table
- SqlCommand/OleDbCommand
- SqlDataAdapter/OleDbDataAdapter
- Array

Below are some examples of binding to different data sources at run time.

dataset

The Chart control's *DataSource* property can be set to a dataset at run time. The following code demonstrates setting up a dataset, setting the *DataSource* property to the dataset, creating a series, and setting the *ValueMembersY* property to the dataset expression at run time.

```
// C#
// create the series
DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist
Security Info=False";

System.Data.OleDb.OleDbConnection m_cnn = new
System.Data.OleDb.OleDbConnection(m_cnnString);

System.Data.OleDb.OleDbDataAdapter oDBAdapter;

// create the dataset
System.Data.DataSet oDS;

oDBAdapter = new System.Data.OleDb.OleDbDataAdapter("SELECT ShipCountry,
SUM(Freight) AS
Expr1 FROM Orders GROUP BY ShipCountry", m_cnnString);

oDS = new System.Data.DataSet();

oDBAdapter.Fill(oDS, "Expr1");
```

```
// set the DataSource and ValueMembersY properties
this.ChartControl1.DataSource = oDS;
s.ValueMembersY = "Expr1";
this.ChartControl1.Series.Add(s);
```

dataset Column

In the Chart control, the ValueMembersX and ValueMembersY properties of a series can be set to a dataset column. The following code demonstrates creating a series, setting up a dataset, setting the DataSource property to the dataset, and setting the ValueMembersY and ValueMembersX properties to dataset columns at run time.

```
// C#

// create the series
DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist
    Security Info=False";

System.Data.OleDb.OleDbConnection m_cnn = new
System.Data.OleDb.OleDbConnection(m_cnnString);

System.Data.OleDb.OleDbDataAdapter oDBAdapter;

// create the dataset
System.Data.DataSet oDS;

oDBAdapter = new System.Data.OleDb.OleDbDataAdapter("SELECT * from Orders
WHERE OrderDate
    < #08/17/1994#", m_cnnString);

oDS = new System.Data.DataSet();
oDBAdapter.Fill(oDS, "Orders");

// set the DataSource, ValueMembersY, and ValueMembersX properties
this.ChartControl1.DataSource = oDS;
this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].ValueMembersY =
oDS.Tables["Orders"].Columns[7].ColumnName;

this.ChartControl1.Series[0].ValueMemberX =
oDS.Tables["Orders"].Columns[8].ColumnName;
```

Data Command

A chart's data source can be set to a SqlCommand or OleDbCommand. The following code demonstrates creating a series, creating an OleDbCommand, setting the DataSource property to the data command, and setting the ValueMembersY property for the series at run time.

```
// C#

// create the series
```

```

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

string m_cnnString = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:/
Northwind.mdb;Persist

    Security Info=False";

System.Data.OleDb.OleDbConnection m_cnn = new
System.Data.OleDb.OleDbConnection(m_cnnString);

string query = "SELECT ShipCountry, SUM(Freight) AS Expr1 FROM Orders GROUP
BY ShipCountry";

// create the OleDbCommand and open the connection
System.Data.OleDb.OleDbCommand command = new
System.Data.OleDb.OleDbCommand(query, m_cnn);

command.Connection.Open();

// set the DataSource and ValueMembersY properties
this.ChartControl1.DataSource = command;
this.ChartControl1.Series.Add(s);
this.ChartControl1.Series[0].ValueMembersY = "Expr1";

// close the connection
m_cnn.Close();

```

Array

The Chart control allows the data source for the data points collection to be set to an array. The following code demonstrates creating a series, creating an array, and using the DataBindY method to set the data source for the data points collection at run time.

```

// C#

// create the series

DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

// create the array
double [] a = {1,4,2,6,3,3,4,7};

// set the data source for the data points collection
this.ChartControl1.Series.Add(s);
this.ChartControl1.Series[0].Points.DataBindY(a);

```

Calculated and Sequence Series Charts

The Chart control allows you to bind a formula to the ValueMembersY property of a series to create a calculated or sequence series for your chart.

Calculated Series

You can easily create a calculated series based on the values of one or more series by setting the ValueMembersY property of a series to a formula. To reference a series in the formula, use the name of the series. The following code demonstrates creating two series, one bound to a data array and the other bound to a formula based on the Y values of the first series.

```
// C#
DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

DataDynamics.ActiveReports.Chart.Series cS = new
DataDynamics.ActiveReports.Chart.Series();

double [] a = { 1,4,2,6,3,3,4,7};

this.ChartControl1.Series.AddRange(new DataDynamics.SharpGraph.Windows.Series[]
{s, cS});

this.ChartControl1.Series[0].Name = "Series1";
this.ChartControl1.Series[0].Points.DataBindY(a);
this.ChartControl1.Series[1].ValueMembersY = "Series1.Y[0]+10";
```

Sequence Series

Set a sequence series by specifying the minimum value, maximum value, and step for the series. The following code shows how to set the ValueMembersY property at run time to create a sequence series.

```
// C#
DataDynamics.ActiveReports.Chart.Series s = new
DataDynamics.ActiveReports.Chart.Series();

this.ChartControl1.Series.Add(s);

this.ChartControl1.Series[0].ValueMembersY = "sequence(12,48,4)";
```

Chart Effects

Colors

In the Chart control, colors can be used in different ways to enhance the chart's appearance, distinguish different series, point out or draw attention to data information such as averages, and more.

Color Palettes

The Chart control includes several pre-defined color palettes that can be used to automatically set the colors for data values in a series. The pre-defined palettes are as follows:

- Cascade (default) A cascade of eight cool colors ranging from deep teal down through pale orchid.
- Confetti A sprinkling of bright and pastel colors.
- Iceberg A range of the soft blues and greys found in an iceberg.
- Springtime The colors of spring, in deep green, two vivid colors and five pastels.
- None All data is drawn using the same teal color.

These enumerated values are accessed through the Series class with code like the following.

```
// C#
this.ChartControl1.Series[0].ColorPalette = DataDynamics.ActiveReports.Chart.
ColorPalette.Iceburg;
```

Gradients

Gradients can be used in object backdrops to enhance the visual appearance of various chart items. Gradients can be used in the following chart sections:

- Chart backdrop
- Chart area backdrops
- Wall backdrops
- Title backdrops
- Legend backdrops
- Legend item backdrops (for custom legend items)
- WallRange backdrops
- Series backdrops
- Data point backdrops
- Marker backdrops
- Marker label backdrops
- Annotation TextBar backdrops

3D Effects

Using the projection and viewpoint settings, you have the ability to display your 3D chart at or from any angle needed to provide the desired view or call attention to a specific chart section.

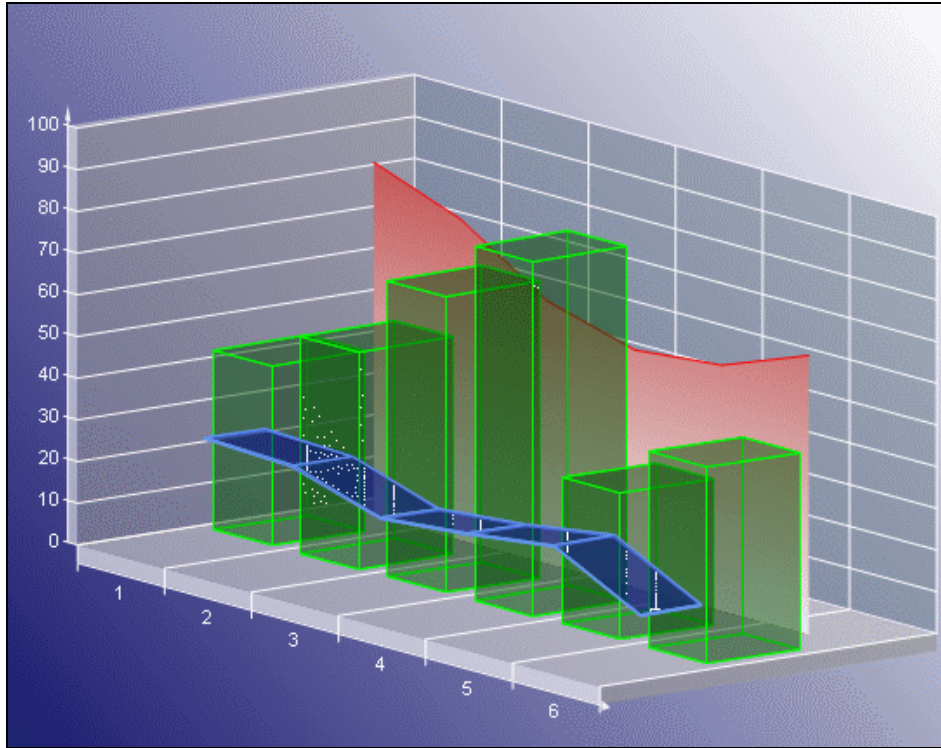
Projection

Determine the projection for a 3D chart using three factors: the ZDepth ratio, the projection type, and the projection DX and DY values.

- **ZDepth ratio** The Z depth ratio is the level of depth the Z axis has in the chart. Values range from 0 (for a 2D chart) to 1.0.
- **ProjectionType** The type of projection used for the chart. In order to show charts three dimensionally, the ProjectionType in the ChartArea Collection editor must be set to Orthogonal. To access this dialog box, click the ellipsis button next to the ChartAreas (Collection) property in the *Properties* window.
- **ProjectionDX** The origin position of the Z axis in relation to the X axis. This property is valid only when the ProjectionType is Orthogonal.
- **ProjectionDY** The origin position of the Z axis in relation to the Y axis. This property is valid only when the ProjectionType is Orthogonal.
- **HorizontalRotation** The HorizontalRotation property allows you to set the degree (-90° to 90°) of horizontal rotation from which the chart is seen.
- **VerticalRotation** The VerticalRotation property allows you to set the degree (-90° to 90°) of vertical rotation from which the chart is seen.

Lighting

The Chart control provides the ability to completely customize lighting options for 3D charts.



Directional Light Ratio

Using the `DirectionalLightRatio` property, you can control the directional or ambient intensity ratio.

Light Type

By setting the `Type` property to one of the enumerated `LightType` values, you can control the type of lighting used in the chart. The settings are as follows:

- **Ambient** An ambient light source is used. It is equal to `DirectionalLightRatio = 0`.
- **InfiniteDirectional** An infinite directional light source (like the sun) is used.
- **FiniteDirectional** A point light source is used.

Light Source

You can also set the `Source` property to a `Point3d` object, which controls the location of the light source.

Alpha Blending

The `Backdrop` class in the Chart control has an `Alpha` property which employs GDI+, and is used to set the transparency level of each object's backdrop. GDI+ uses 32 bits overall and 8 bits per alpha, red, green, and blue channels respectively to indicate the transparency and color of an object. Like a color channel's levels of color, the alpha channel represents 256 levels of transparency.

The default value of the `Alpha` property is 255, which represents a fully opaque color. For a fully transparent color, set this value to 0. To blend the color of the object's backdrop with the background color, use a setting between 0 and 255.

In the Chart control, you can use the `Color.FromArgb` method to set the alpha and color levels for a particular chart element. The following example shows how you can use the method to set the alpha and color values for the chart backdrop.

```
// C#
```

```
this.ChartControl1.Backdrop = new DataDynamics.ActiveReports.Chart.
```

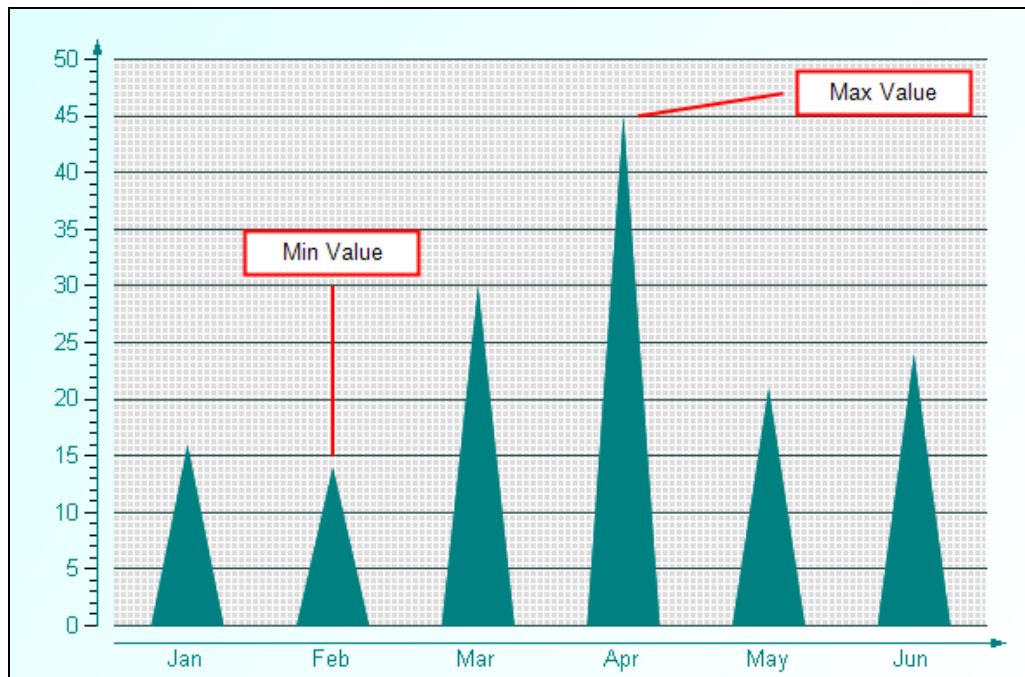
```
BackdropItem(Color.FromArgb(100, 0, 11, 220));
```

Changing the alpha level of a chart element reveals other items that are beneath the object. Because you can set the alpha level for any chart element that supports color, you can create custom effects for any chart. For example, you can use alpha blending to combine background images with a semi-transparent chart backdrop to create a watermark look.

Chart Control Items

Annotations

The Chart control offers a built-in annotation tool to allow you to include floating text bars or images in your charts or call attention to specific items or values in your charts using the line and text bar controls included in the Annotation Collection Editor.

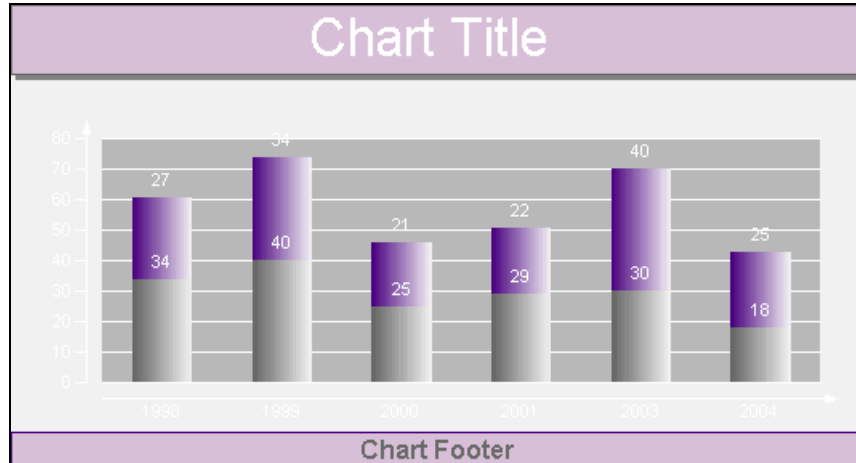


The following properties are important when setting up annotations for your chart:

- **Start Point:** sets the starting point (X and Y axis values) for an annotation line.
- **End Point:** sets the end point (X and Y axis values) for an annotation line.
- **Anchor Placement:** sets the position of the anchor point for the text bar on the chart surface.
- **Anchor Point:** sets the point (X and Y axis values) where the text bar will be anchored based on the anchor placement selected.

Titles and Footers

The Chart control allows you to add custom titles to your charts. The Titles collection is accessible from the SharpGraph object. With the ability to add as many titles as needed, dock them to any side of a chart area, change all of the font properties, add borders and shadows, make the background look the way you want it, and change the location of the text, you can easily make your titles look the way you want them to look.

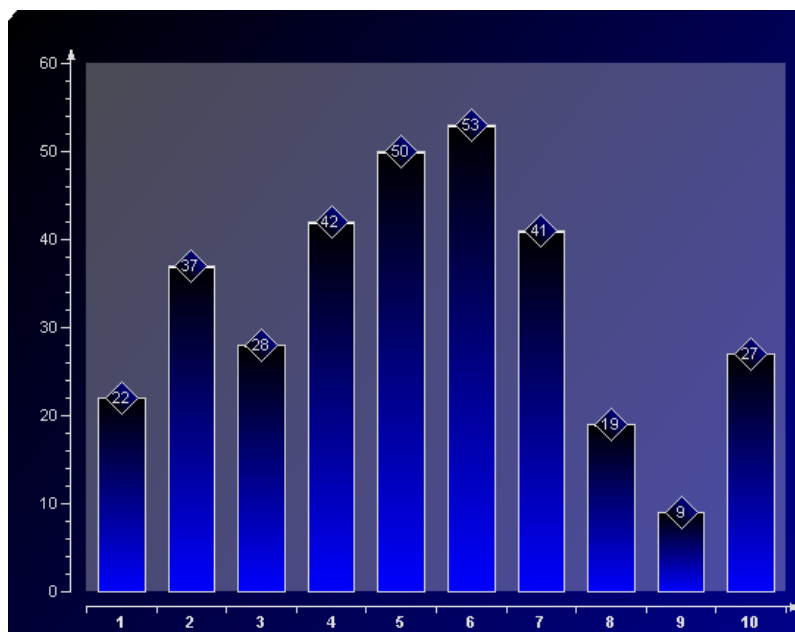


Legends

The Chart control automatically creates a legend item for each series added to a chart at design time and sets the Legend property for each series by default. However, the legend's Visible property must be set to True for the legend to show with the chart. The text for each default legend entry is taken from the Name property on the series. Each Series to be shown in the Legend must have a Name. If the Name property is not set, the Series does not show up in the Legend.

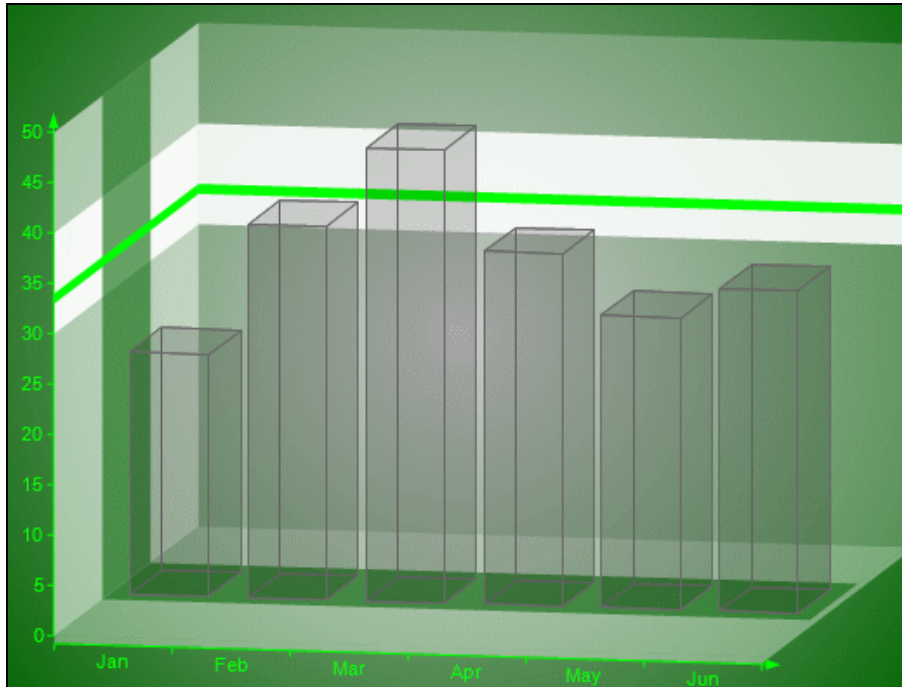
Markers

Markers are used to show specific data series values in a chart.



Constant Lines and Stripes

The Chart control supports constant lines and stripes through the use of the WallRanges collection. It allows you to display horizontal or vertical lines or stripes in a chart to highlight certain areas. For example, you could draw a stripe in a chart to draw attention to a high level in the data or draw a line to show the average value of the data presented.



Important properties

- EndValue--Sets the end value on the primary axis for the wall range.
- StartValue --Sets the start value on the primary axis for the wall range.
- PrimaryAxis--Sets the axis on which the wall range should appear.

Chart Axes and Walls

Standard Axes

The Chart control provides the means to change axis settings at design time or run time. Chart axes make it possible to view and understand the data plotted in a graph.

Axis Types

Most 2D charts contain a numerical axis (AxisY) and a categorical axis (AxisX). 3D charts include another numerical axis (AxisZ). These axes are accessible at run time from the ChartArea object and allow you to control the settings for each, including scaling, labels, and various formatting properties. For any of the scaling or labeling properties you set to show up at run time, you will need to set the Visible property of the axis to True.

Changing Axis Settings

Axis settings can be changed at design time by clicking on a Chart control and using the *Properties* window or at run time in code from the chart's ChartArea object.

Scaling

For normal linear scaling on a numeric axis, you will need to set the Max and Min properties for the axis, which correspond to the numerical values in the chart's data series. You will also need to set the Step property of the MajorTick to show the major numerical unit values. The Step property controls where labels and/or tick marks are shown on the numerical axis.

```
// C#
```

```
this.ChartControl1.ChartAreas[0].Axes["AxisY"].Max = 100;
```

```
this.ChartControl1.ChartAreas[0].Axes["AxisY"].Min = 0;
```

```
this.ChartControl1.ChartAreas[0].Axes["AxisY"].MajorTick.Step = 10;
```

The Chart control also supports logarithmic scaling which allows you to show the vertical spacing between two points that corresponds to the percentage of change between those numbers. You can set your numeric axis to scale logarithmically by setting the IsLogarithmic property on the axis to True and setting the Max and Min properties of the axis.

Labeling

To show labels on an axis, you will need to specify the value for the LabelsGap property, set your LabelsFont properties, and set LabelsVisible to True. These properties can be set in the AxisBase Collection editor, which is accessed at design time by clicking the ellipsis button next to the ChartAreas (Collection) property, then the Axes (Collection) property of the ChartArea.

NOTE: Labels render first, and then the chart fills in the remaining area, so be sure to make the chart large enough if you use angled labels.

You can specify strings to be used for the labels instead of numerical values on an axis by using the Labels collection property at design time or assigning a string array to the Labels property at run time. You can also specify whether you want your axis labels to appear on the outside or inside of the axis line using the LabelsInside property. By default, labels appear outside the axis line.

Secondary Axes

By default, a Chart object includes secondary X and Y axes (AxisX2 and AxisY2). At design time or run time, you can specify a secondary axis to plot data against by setting all of the appropriate properties for AxisX2 or AxisY2, including the Visible property.

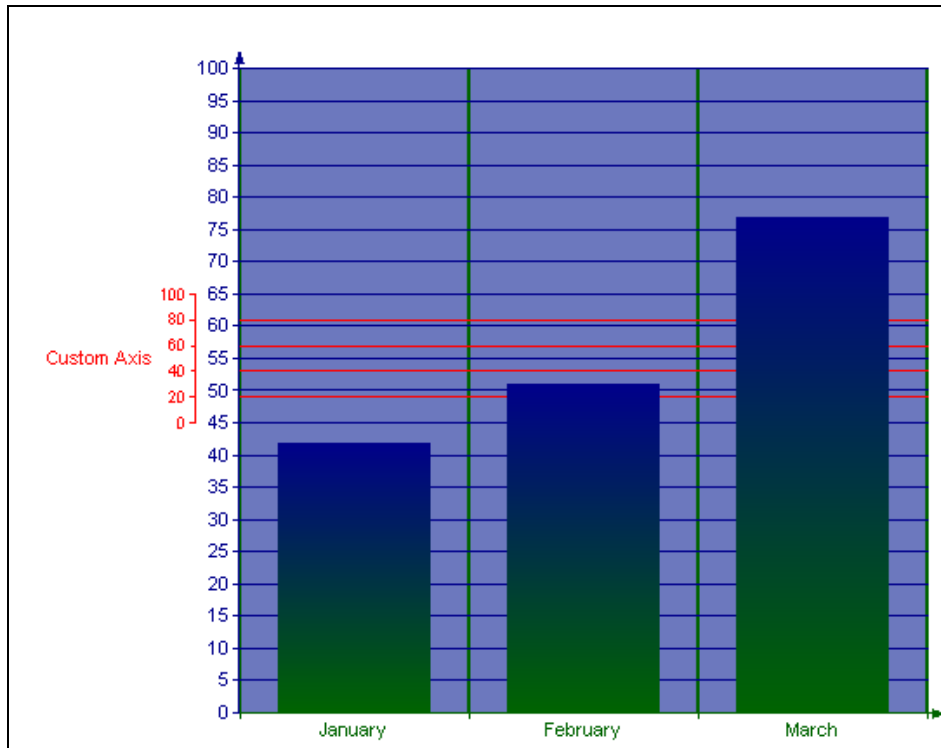
If you want to use two axes to show the same data as it appears on two different scales, you can set the primary axis to show the actual data value scale, for example, and set the secondary axis to show a logarithmic scale.

Custom Axes

The Chart control supports the creation of additional custom axes through the use of the chart's CustomAxes collection. Once a custom axis has been added to the collection, in addition to setting the normal axis properties, you will need to set the following properties:

- **Parent**—The Parent property allows you to choose the primary or secondary axis on which your custom axis resides.
- **PlacementLength**—The PlacementLength property allows you to set the length of the custom axis in proportion to the Min and Max property values you have already set for the parent axis.

- **PlacementLocation**—The PlacementLocation property allows you to set the starting location value for the custom axis to appear in relation to the parent axis.



Gridlines and Tick Marks

Gridlines and tick marks are generally used to help increase the readability of a chart.

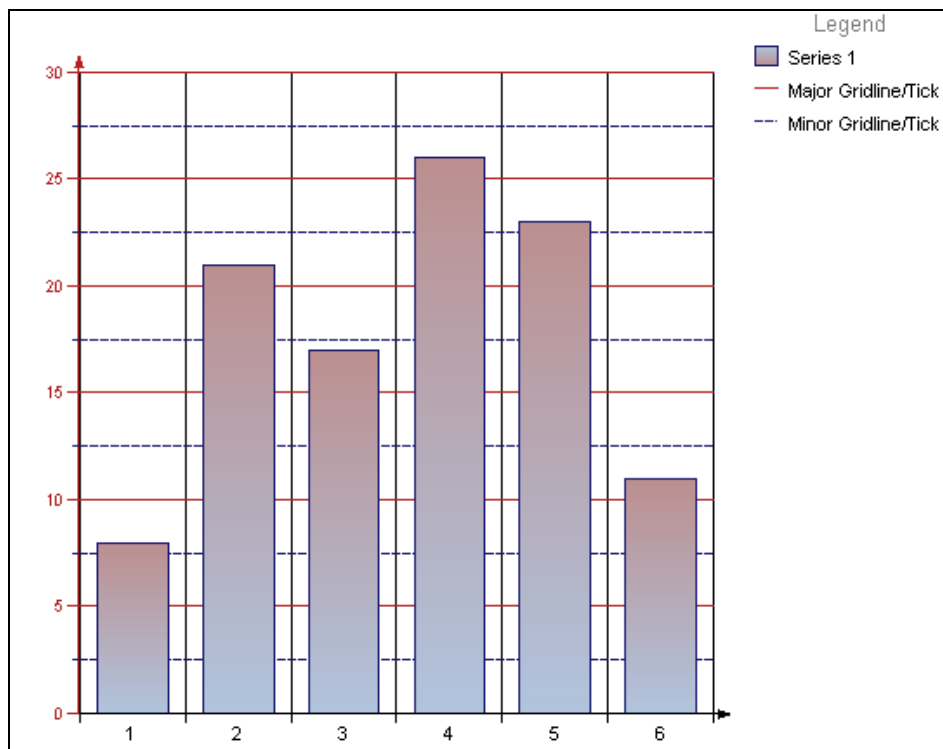


Chart-Specific Properties

Each chart type in the Chart control contains specific properties that apply to it. Set the chart type and chart-specific properties in the *Series Collection Editor* dialog box accessed through the Series property in the property grid and in the *DataPoint Collection* dialog box accessed through the Points property in the *Series* dialog box.

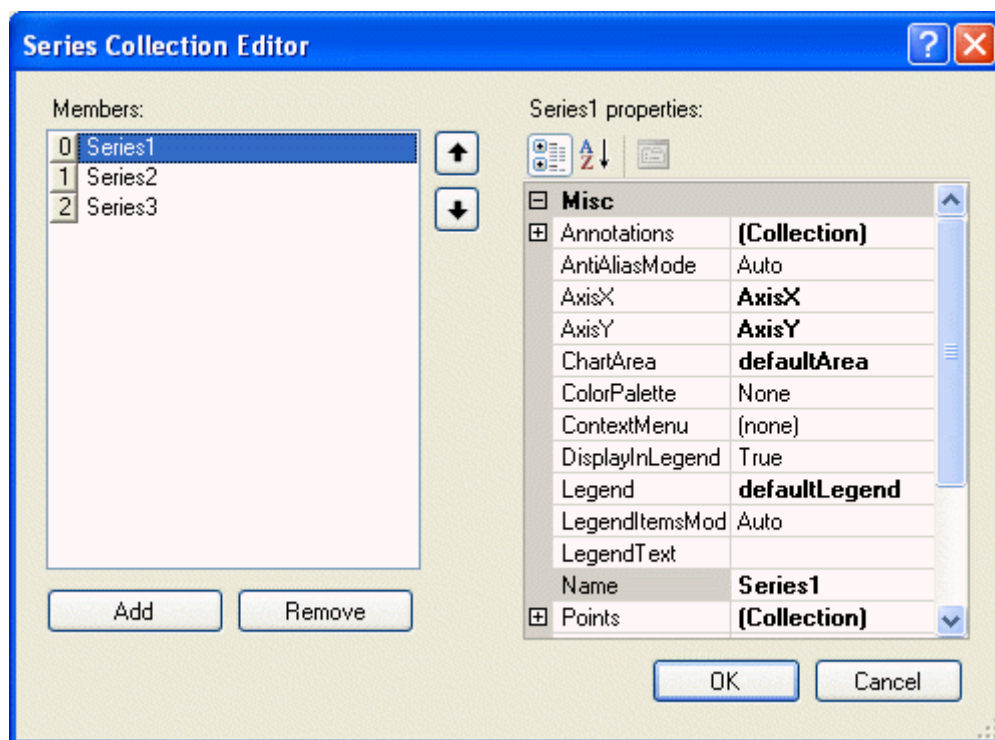
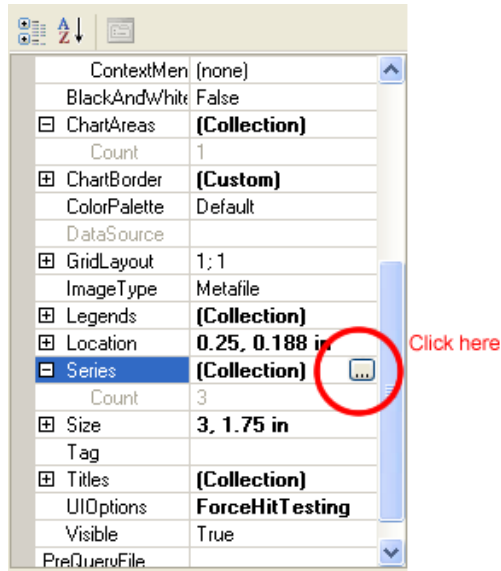
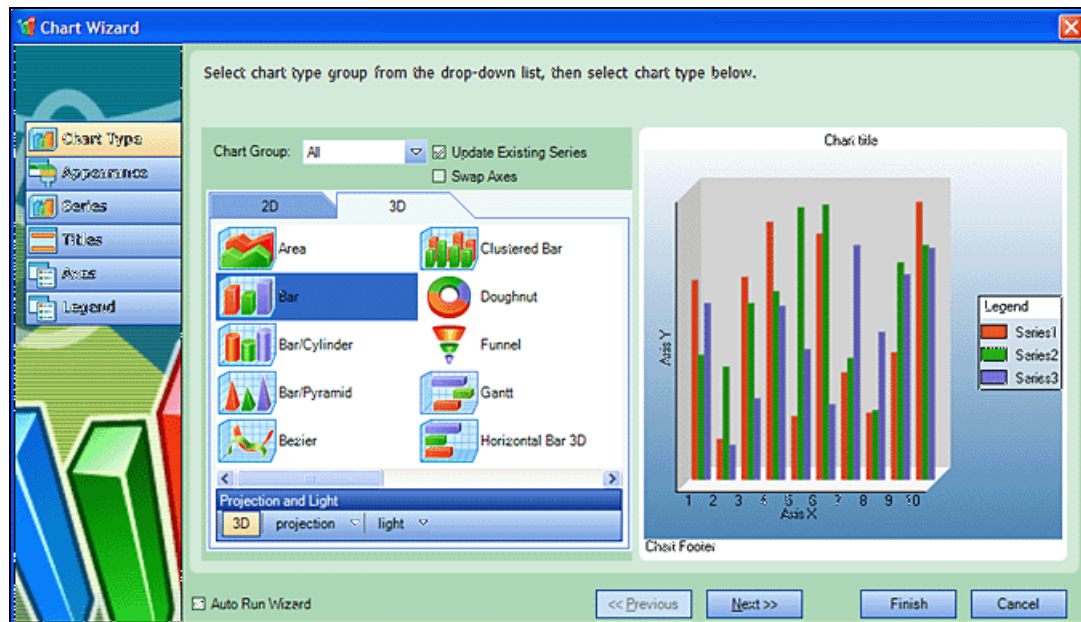


Chart Wizard

The chart control features an easy-to-use wizard. The chart wizard automatically runs when you first add a chart control to a report. If you prefer not to have the wizard run automatically, uncheck the Auto Run Wizard check box at the bottom of the wizard..



Walk-Through: Creating a Report

In this exercise, you will build a report similar to the vulnerability (classic) report, but not as intricate.

Task 1: Build the master report.

- 1 Click **File** → **New**.
- 2 On the *Create Report Definition* window, enter the following:
Name: My vulnerability report
Description: Sample report
- 3 In the Context list, select **Scan**.
- 4 Select **Exposed in Product**.
- 5 In the **View Name** list, select **Basic - Server Information**.
- 6 Click **OK**.
- 7 Right-click the PageHeader caption and select Delete.
- 8 Right-click the Detail caption and select **Insert** → **Report Header/Footer**.
- 9 In the toolbox, drag **LinkedSubReportControl** into the ReportHeader section.
- 10 On the *Choose a Report* dialog, expand the Vulnerability (classic) group, select **ScanHeader**, and click **OK**.
- 11 Position the element and extend it to the right margin.

- 12 Click the ReportHeader caption.
- 13 In the Properties grid, set CanShrink = True.
- 14 Click the Detail caption.
- 15 In the Properties grid, set CanShrink = True.

Task 2: Add a Link to a Subreport

- 1 In the toolbox, drag a LinkedSubReportControl into the Detail section.
- 2 On the *Choose a Report* dialog, expand the Vulnerability (classic) group, select **ServerHeader**, and click **OK**.
- 3 Position the element and extend it to the right margin.
- 4 With the ServerHeader selected, in the Properties grid under Associated Fields, click **@ServerID** and select ServerID.
- 5 Click the **Preview** tab.
- 6 When prompted to design parameters, select **No**.
- 7 Select a scan and click **Next**.
- 8 When prompted to select a report, click **Finish**.
- 9 Click **File** → **Save**.

Task 3: Create a Subreport

- 1 Click **File** → **New**.
- 2 On the *Create Report Definition* window, enter or select the following:
 - a For the Name, enter “My vulnerability by server.”
 - b For the Description, enter “Sample report.”
- 3 From the **Context** list, select **Scan**.
- 4 Clear the **Exposed in Product** check mark.
- 5 In the **View Name** list, select *Basic - Vulnerability by Session*.
- 6 Click **OK**.
- 7 Delete the PageHeader caption (right-click the caption and select **Delete**).
- 8 In the Properties grid, set CanShrink = True.
- 9 Right-click the Detail caption and select **Insert** → **Group Header/Footer**.
- 10 In the Properties grid:
 - a Set CanShrink = True.
 - b Change the name to GroupServer.
 - c For the DataField, select Server.
- 11 Drag a BookmarkControl to the GroupServer area.
- 12 In the Properties grid, select BookmarkText and enter the following:


```
{=MainReportName}\{=Server}
```


Task 4: Add a chart to the report

- 1 Click **Edit** → **Modify/Create Report**.
- 2 Select **Aggregate - Severity Summary by Server** and click **OK**. This query will be used to generate a chart.
- 3 Drag a ChartControl onto the design area.
- 4 On the Chart Wizard, click the **2D** tab and select **Bar**.
- 5 Click **Finish**.
- 6 Resize the chart and arrange it to your liking.
- 7 With the chart selected, go to the Properties grid, click **AssociatedQuery**, and select the query you just added: Aggregate - Severity Summary by Server.
- 8 Right-click the chart and select Wizard.
- 9 Select **Series** from the list in the left-hand pane.
- 10 Assign a series to each severity category: critical, high, medium, low, informational, and best practice.
 - a Select **Series1**, and in the Series Properties area and enter “Critical” for the Name.
 - b In the Data Binding area, select the Y axis and select **Critical** from the drop-down list.
 - c Repeat this process for each series; click **Add New Item** where necessary.
- 11 Click **Finish**.
- 12 With the chart selected, go to the Properties grid and click **@ServerID** under AssociatedFields and select VulnerabilityCount.

Task 5: Add a section for the Check ID, Check Severity, and Check Name, and Summary

- 1 Right-click the Detail caption and select **Insert** → **Group Header/Footer**.
- 2 Collapse the footer.
- 3 Click the GroupHeader.
- 4 In the Properties grid:
 - a Change the name to “groupCheck.”
 - b Set CanShrink = True
 - c For the DataField, select “checkid.”
- 5 Drag a TextBox to the groupCheck section.
- 6 In the Properties grid:
 - a For Name, enter txtSeverity
 - b For DataField, select “checkseverity.”
- 7 Drag another TextBox into the groupCheck section and place it to the right of the first TextBox.
- 8 In the Properties grid:
 - a Change the name to “txtCheckName.”
 - b Set CanShrink = True
 - c For the DataField, select “checkname.”

- d For ClassName, select Normal Bold.
- 9 Drag a Label into the area.
- 10 In the Properties grid:
 - a Change the name to lblSummary.
 - b For Text, enter Summary.
- 11 Drag a RichTextBox onto the canvas; place it below the summary label and extend it to the right.
- 12 In the Properties grid:
 - a Change the name to txtSummary.
 - b For the DataField, select ReportSection_Summary.
- 13 Drag a BookmarkControl and place it anywhere on the groupCheck canvas
- 14 On the Properties grid:
 - a For BookMarkText, enter {=MainReportName}\Checks\{=Checkid}.
 - b For the Name, enter BookmarkChecks.

Task 6: Add an area for the HTTP Request

- 1 Right-click on the Detail caption and select **Insert** → **Group Header/Footer**.
- 2 Collapse the group footer.
- 3 On the Properties grid:
 - a Set CanShrink =True.
 - b For the Name, enter groupRequest.
- 4 Drag a RichTextBox to the groupRequest canvas. Size it and extend it to the right margin.
- 5 On the Properties grid:
 - a Set CanShrink =True.
 - b For the Name, enter txtRequest.
 - c For the DataField, select RequestText.
 - d For TruncateVulnerability, select True.
 - e For HighlightVulnerability, select True

Task 7: Add an area for the HTTP Response

- 1 Drag a RichTextBox to the groupRequest canvas. Size it and extend it to the right margin.
- 2 On the Properties grid:
 - a Set CanShrink =True.
 - b For the Name, enter txtResponse.
 - c For the DataField, select ResponseText.
 - d For TruncateVulnerability, select True.
 - e For HighlightVulnerability, select True

Task 8: Populate the Detail section.

- 1 Drag the bound field “fullURL” to the Detail section.
- 2 Click the Parameter Designer icon on the toolbar.
- 3 In the Parameter Designer Canvas area, delete all parameters (click in the area, press Ctrl + a, and then press **Delete**).
- 4 Click **Save and Close**.

Task 9: Add/Modify the script

- 1 Click the **Script** tab on the Report Designer.
- 2 Change the method name “myEventHandler” to “onGroupCheckFormat.”
- 3 Delete all the script and replace with the following:

```
using System;
using DataDynamics.ActiveReports;
using HP.AppSec.Reporting.ReportScript;
namespace Script.Events
{
    public class MyEventClass
    {
        /*
         * You can declare fields, events and methods just like in c#...
         * in fact this is C#!
         */
        /*
         * Script event handlers, MUST have this method signature
         */
        public void OnGroupCheckFormat(ScriptReportObject report, EventArgs
ea)
        {
            int nSeverity = (int)report.Fields["checkseverity"];
            TextBox txtSeverity =
report.CurrentSection.Controls["txtSeverity"] as TextBox;
            if (nSeverity <= 10)
            {
                txtSeverity.Text = "Informational";
            }
            else if( 10 < nSeverity && nSeverity <= 25)
            {
                txtSeverity.Text = "Low";
            }
            else if( 25 < nSeverity && nSeverity <= 50)
            {
                txtSeverity.Text = "Medium";
            }
            else if( 50 < nSeverity && nSeverity <= 75)
            {
                txtSeverity.Text = "High";
            }
            else if( 75 < nSeverity && nSeverity <= 100)
            {
                txtSeverity.Text = "Critical";
            }
        }
    }
}
```

```

    }
}
}

```

- 4 After entering the script, click the **Report Events** tab (in the lower right) and select **groupCheck** from the drop-down list.
- 5 For the Section Format Event, select `Script.Events.MyEventClass.onGroupCheckFormat`.
- 6 Save the report.

Task 10: Add a pre-query to the master report

- 1 Open MyVulnerability report (listed under Custom Reports on the *Open a Report* dialog).
- 2 Click **Edit** → **Modify/Create Report**.
- 3 From the **View Name** list, select **PreQuery - Vulnerability**.
A pre-query improves performance by first determining if any data is available for the report.
- 4 Drag a `LinkedSubReportControl` onto the Detail area.
- 5 From the *Choose a Report* dialog, select My vulnerability by server and click **OK**.
- 6 Position the control and extend it to the right margin.
- 7 On the Properties grid:
 - a Under `AssociatedFields`, click **@serverID** and select `serverID`.
 - b For `PreQueryFile`, select `PreQuery - Vulnerability`.
- 8 Click **Save**.
- 9 Click the **Preview** tab.
- 10 Note and correct any improperly positioned controls, then save your work.

B Policies and Components

Introduction

A policy is a collection of vulnerability checks and attack methodologies that HP scanners deploy against a Web application. All policies contain all possible audit engines and agents, but each policy has a different subset of these components enabled. Although your environment may also include custom policies designed by your developers, the standard installation contains the prepackaged policies described in the following section.

Policies

- **All Checks**—An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the check database. This scan includes all checks that are listed in the compliance reports that are available in HP's Web application and Web services vulnerability assessment products. This includes checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers.
- **Application Only**—The Application Only policy performs a security assessment of your Web application by submitting known and unknown Web application attacks, and only submits specific attacks that assess the application layer. When performing assessments of enterprise level Web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your assessment in terms of speed and memory usage.
- **Assault**—An assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server, and Web application layers. An assault scan includes checks that can create denial-of-service conditions.



You are strongly advised to use assault scans in test environments only.

- **Blank**—This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Criticals and Highs**—Use the Criticals and Highs policy to quickly scan your Web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It 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 assessment of your Web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a Web site to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **Dev**—A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web application layer only. The Developer policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **DevInspectEclipse**—The DevInspectEclipse policy is the standard policy for use by DevInspect Java Eclipse. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **DevInspectVS**—The DevInspect VS policy is the standard policy for use by DevInspect VS. It performs both a crawl and audit, and tests the application for known and unknown vulnerabilities.
- **OWASP Top Ten**—Many government agencies suggest testing for the Open Web Application Security Project (OWASP) Top Ten Web application vulnerabilities as a best practice in ensuring the security of your Web application.
- **Passive Scan**—The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **Platform Only**—The Platform Only policy performs a security assessment of your Web application platform by submitting attacks specifically against the Web server and known Web applications. When performing assessments of enterprise-level Web applications, use the Platform Only policy in conjunction with the Application Only policy to optimize your assessment in terms of speed and memory usage
- **QA**—The QA policy is designed to help QA professionals make project release decisions in terms of Web application security. It performs checks for both known and unknown Web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
- **Quick**—A quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the Web server, Web application server and Web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **Safe**—A safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown vulnerabilities at the Web server, Web application server and Web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.
- **SQL Injection**—The SQL Injection policy performs a security assessment of your Web application for SQL injection vulnerabilities. SQL injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the Web application for execution by a backend database.
- **Standard**—A Standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the Web server, Web application server and Web application layers. A Standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

Policy Components

A policy is a collection of audit engines and attack agents that WebInspect uses when scanning or crawling your Web application. These components are organized into the following groups:

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

For detailed information about all the possible agents, open the Policy Manager, select the Attack Groups category, and click on any agent name.

Audit Engines

WebInspect uses the following audit engines.

Audit Options—These include Robots.txt Parser, WebInspect Scan Signature, Ws_ftp.log Parser, and CVS Entries Parser.

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, WebInspect continuously applies appropriate assessment resources that adapt to the specification application environment.

- **Comment Checks**—The comment audit examines each session for filenames 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 runs the cross-site scripting parameter injections attacks. Cross-site scripting is caused by insufficient filtering of client-supplied data that is returned to Web users by the Web application.
- **Directory Enumeration**—Directory enumeration finds all directory paths and possibilities on the application server, including hidden directories that could possibly contain sensitive information. This helps WebInspect create a full and accurate map of the targeted site.
- **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. Data extension checking involves adding file extensions to find old renamed files left on the server. For example, an attacker might find hi.asp, and then search for hi.asp.bak or hi.asp.old. WebInspect will attempt to locate all files left on your server that could be used by an attacker.

- **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. For example, an attacker who finds `hi.asp` might search for *copy of hi.asp* and retrieve the script's source code.
- **Fixed Checks**—This audit performs checks for files with known vulnerabilities. The Fixed Checks audit does not probe the directory structure before sending the attacks.
- **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 Web site 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 Web site.
- **Known Vulnerabilities**—This audit engine examines your Web site 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.
- **Logic Checks**—This audit performs checks based on previously discovered vulnerabilities.
- **Postdata Injection, 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. WebInspect will determine your application's susceptibility to attacks that rely on the POST method of parameter manipulation.
- **Query Injection, 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, WebInspect 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.

- **Request Inspect**—During the crawl of a Web application to map its internal structure, the Request Inspect engine applies the regular expressions that are associated with checks to the requests being sent.

- **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.
- **Server Side Include**—During the course of normal operations, many Web applications will accept a full URL as an expected and returned parameter value. This audit engine will manipulate that process and determine if an attacker could exploit any vulnerabilities within the application by including commands and other functions within the URL accepted by the application.
- **Site Search**—This can be considered the information-gathering stage, employing the same tactics an intruder would use 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 reveal confidential data, information about internal server and application configurations and settings, administrative access to the site, and 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

General Application Testing

This group of agents, used mainly by the Directory Enumeration engine, searches the site's tree structure for commonly occurring directories. 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).

General Text Searching

This group of agents searches for a wide variety of text strings, such as database connection strings, error messages, Social Security numbers, credit card numbers, and debug applications.

Third-Party Web Applications

This group of agents looks for known vulnerabilities associated with hundreds of 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 specific Web servers.

Web Site Discovery

This group of agents searches for commonly used files, account information, backup files, CVS files, Include files, core dumps, statistics, logs, and various other files that could be used to infiltrate and exploit the Web site.

Custom Checks

A custom check is a user-defined probe for a specific vulnerability that the standard WebInspect repertoire does not address. Use the Policy Manager to create custom checks and integrate them into your policies. See [Creating a Custom Check](#) on page 167 for more information.

Index

A

- Abnormal Input, 166
- Activation ID, 12
- ActiveX, 261
- Activity Log, 49
- Adaptive Agents, 329
- Administration, 48
- AJAX, 261
- AMP console, 37
- AMP Web console, 7
- Application Lifecycle Management, 8
- Archive, 83, 85, 87, 89, 90
- Assessment, 132
- Assessments, 5, 78, 79, 80, 83, 84
- attack agents, 170
- Audit Engines, 160, 329
- Audit Inputs Editor, 172
- Audit Options, 160
- Authentication, 180, 188, 218
- Authentication methods
 - Automatic, 123, 192, 231, 245
 - Basic, 123
 - Digest, 123
 - HTTP Basic, 192, 231, 245
 - Kerberos, 123
 - NTLM, 123, 192, 231, 245
- Auto-archive, 83, 89, 90
- Automatic, 123
- Automatic authentication, 192, 231, 245

B

- Base64, 197, 198
- Basic, 123
- Blowfish, 198, 199

C

- CAPTCHA, 255

- character frequency, 228
- Check Inputs, 173
- Command execution check, 164
- Compliance Manager, 247
- Compliance templates, 41
- Connected users, 49
- Console, 37
- Console options, 34
- cookie, 225
- Cookie Cruncher, 225
- Cookie Cruncher settings, 230
- Cross-Site Scripting, 165
- Custom Checks, 160, 169
 - creating, 162
 - definition, 332
- custom policy, 162

D

- Dependencies, 82, 97, 98, 99, 101
- DES, 198
- DevInspect, 7
- Digest, 123
- Directory Enumeration, 160, 163
- Directory Traversal, 165

E

- EBCDIC, 198
- E-Mail Alerts, 52
- Encoder/Decoder, 197
- Engine Inputs, 172

- Evasions, 220
 - Case Sensitivity, 222
 - DOS/Win Directory Syntax, 222
 - Double Slashes, 220
 - HTTP Misformatting, 221
 - Long URLs, 222
 - Method Matching, 220
 - NULL Method Processing, 222
 - Parameter Hiding, 221
 - Reverse Traversal, 221
 - Self-Reference Directories, 221
 - URL Encoding, 220

- Excluded URLs, 31

- export
 - Web Brute list, 190

- Export Paths, 52

F

- File extension addition, 163
- File extension replacement, 164
- Filters, 220
- Finding Details, 86
- Flash, 261
- Flash files, 217
- Fuzzer filters, 234
- Fuzzer generators, 233

G

- generator, 233
- Generators, Web Fuzzer, 233
- global form entry, 180
- Greenwich Mean Time, 29
- Group, 137
- GZIP, 208

H

- hexadecimal, 198
- HP Fortify, 86, 89
- HTTP Basic authentication, 192, 231, 245
- HTTP Editor, 190, 198, 201, 204, 216, 259
- HTTP Editor settings, 208

I

- icons, 171
- IIS, 162, 173, 231, 245
- IIS Virtual Directory, 15

- import
 - check input modifications, 172
 - list of proxy servers, 218
 - proxy server information, 192, 240
 - Web Brute list, 190
 - Web form file, 184

- Installation
 - AMP console, 26
 - Sensor, 28
 - Server/Manager, 11

- Interactive mode, 210, 217, 222, 223

J

- Japanese, 241
- Java, 199
- JavaScript, 31, 165, 184, 208
- JRun, 329

K

- Kerberos, 123
- Keyword search, 164, 169, 330
- Known Vulnerabilities, 330

L

- Launch Interactive, 255
- Licensing, 50
- List-Driven Scan, 109, 134
- Listener Configuration, 217
- Logging on, 33
- Login macro, 213

M

- Macro
 - Web, 215
- MD5, 197, 198
- Microsoft Internet Explorer 6.0., 8
- Microsoft Windows 2000, 8

N

- NTLM, 123
- NTLM authentication, 192, 231, 245

O

- Oracle, 99
- Organization Roles, 55

- Organization roles, 59
- Organizations, 34
- Organizations, creating, 57

P

- Parameter injection, 164
- passwords, 187
- Phase, 83, 137
- policy
 - editing, 162
- Policy Manager, 160
- postdata, 238
- postdata injection, 330
- Project Roles, 56
- Project roles, 63
- Projects, 34
- Projects, creatinig, 63
- proxy server, 213
- Proxy Settings, 185, 205, 209, 211, 212, 213, 215, 231, 232, 240, 244, 246, 253, 261, 284, 285

Q

- QAInspect, 7
- query string, 174, 236, 237, 257

R

- randomness, 228
- RC2, 198
- RC4, 198
- Regular Expression Editor, 200
- Regular Expressions, 201
- Report
 - Generating, 151
 - Viewing, 156
- Report Designer, 286
- Report templates, 151
- Report Viewer, 156
- Roles, 55
- ROT13, 198

S

- Scanning policies, 327
- Scan policies, 40
- Scan queue, 40

- Secure Hash Algorithm, 199
- Sensors, 47
- Sensor Users, 54
- Server Analyzer, 283
- Server Analyzer settings, 283
- Session Editor, 236
- session ID, 225
- SHA, 199
- SHA-256, 199
- SHA-384, 199
- SHA-512, 199
- Simple attack, 166
- Site search, 166
- Smart Update, 51
- Smart Update Approval, 51
- SMTP Settings, 53
- SNMP Alerts, 53
- SNMP settings, 54
- Source Code, 86
- Source Code Analysis, 86
- SQL injection, 165, 241
- SQL Injector, 241
- SQL Injector settings, 243
- SQL Server, 7, 13, 16, 41, 241
- Startup macro, 213, 244
- subcookies, 226
- System Requirements, 8
- System roles, 57

T

- Time Stamping, 29
- Time Zones, 29
- ToLower, 199

Tools

- Audit Inputs Editor, 172
- Compliance Manager, 247
- Cookie Cruncher, 225
- Encoder/Decoder, 197
- HTTP Editor, 204
- Options, 160
- Policy Manager, 160
- Regular Expression Editor, 200
- Report Designer, 286
- Server Analyzer, 283
- Smart Update, 224
- SQL Injector, 241
- Web Brute, 187
- Web Discovery, 194
- Web Form Editor, 180
- Web Fuzzer, 233
- Web Macro Recorder (Event-Based), 264
- Web Macro Recorder (Session-Based), 253
- Web Proxy, 213
- Web Service Test Designer, 276

Tool settings

- Cookie Cruncher, 230
- HTTP Editor, 208
- Server Analyzer, 283
- SQL Injector, 243
- Web Brute, 191
- Web Discovery, 195
- Web Form Editor, 185
- Web Fuzzer, 239
- Web Macro Recorder (Event-Based), 273
- Web Macro Recorder (Session-Based), 260
- Web Proxy, 217

ToUpper, 199

TwoFish, 199

U

Unicode, 197, 199

Universal Time, 29

Upgrading, 10

URL encoding, 199

W

Web Brute, 187

Web Brute settings, 191

Web console, 7

Web Discovery, 194

Web Discovery settings, 195

Web Form Editor, 180

Web Form Editor settings, 185

Web Form list

- creating manually, 180
- recording, 182

Web Fuzzer, 233

Web Fuzzer settings, 239

WebInspect, 1, 7, 10, 28, 48, 51, 52, 54, 76, 78, 159

Web macro, 215

Web Macro Recorder (Session-Based), 253

Web Macro Recorder (Session-Based) settings, 260

Web Proxy, 213

- interactive mode, 222

Web Proxy settings, 217

Web Service operations, 280

Web Service Test Designer, 276

windows

- Add Check By ID, 250
- Add User-Defined Input, 181
- Compliance Manager, 248
- Convert Web Form Values, 184
- Create Web Macro, 215
- Export Dictionary, 191
- Export File, 285
- Filters, 235
- Find in Request, 208
- Find in Response, 208
- Import/Export Dictionary, 190
- Import Dictionary, 190
- LAN Settings, 213, 217
- Modify Input, 181
- Regular Expression Editor, 200
- Save As, 191
- Select Data Dictionary, 189
- Settings, 180
- Settings Properties, 195
- WebForm Editor, 181
- Web Fuzzer, 236
- Web Fuzzer Request, 234
- Web Proxy, 213
- Web Proxy Settings, 223

Windows XP, 8

Workflow-Driven Scan, 109, 135

X

XML, 331

XOR, 199

Z

zero.webappsecurity.com, 180

zlib, 208

Zulu time, 29

