

# **BIG-IP® Application Security Manager™: Implementations**

Version 11.5





# Table of Contents

<b>Legal Notices.....</b>	<b>15</b>
<b>Acknowledgments.....</b>	<b>17</b>
 <b>Chapter 1: Preventing DoS Attacks for Layer 7 Traffic.....</b>	 <b>21</b>
What is a DoS attack?.....	22
About recognizing DoS attacks.....	22
About configuring TPS-based DoS protection.....	22
About configuring latency-based DoS protection.....	23
About heavy URL protection.....	23
About site-wide DoS mitigation.....	24
Overview: Preventing DoS attacks for applications.....	24
Configuring DoS protection for applications.....	25
Configuring TPS-based DoS protection settings.....	25
Configuring latency-based DoS protection.....	28
Configuring heavy URL protection.....	32
Recording traffic during DoS attacks.....	33
Associating a DoS profile with a virtual server.....	33
Displaying DoS event logs.....	34
Viewing DoS attack statistics.....	34
Viewing URL Latencies reports.....	36
Implementation Result.....	38
 <b>Chapter 2: Configuring DoS Policy Switching.....</b>	 <b>41</b>
About DoS protection and local traffic policies.....	42
Overview: Configuring DoS policy switching.....	42
Creating a DoS profile for Layer 7 traffic.....	43
Modifying the default DoS profile.....	43
Creating a local traffic policy for DoS policy switching.....	44
Creating policy rules for DoS policy switching.....	44
Associating a DoS profile with a virtual server.....	45
Associating a local traffic policy with a virtual server.....	46
Implementation results.....	46
 <b>Chapter 3: Mitigating Brute Force Attacks.....</b>	 <b>47</b>
About mitigation of brute force attacks.....	48
Overview: Mitigating brute force attacks.....	48
Creating login pages.....	48
Configuring brute force protection.....	50
Viewing brute force attack reports.....	52
Displaying brute force event logs.....	52

<b>Chapter 4: Detecting and Preventing Web Scraping</b>	<b>53</b>
Overview: Detecting and preventing web scraping	54
Prerequisites for configuring web scraping	54
Adding allowed search engines	55
Detecting web scraping based on bot detection	55
Detecting web scraping based on session opening	57
Detecting web scraping based on session transactions	59
Using fingerprinting to detect web scraping	60
Displaying web scraping event logs	61
Viewing web scraping statistics	64
Implementation Result	65
<b>Chapter 5: Setting Up IP Address Intelligence Blocking</b>	<b>67</b>
Overview: Setting up IP address intelligence blocking	68
Enabling IP address intelligence	68
Setting up IP address intelligence blocking	69
Reviewing IP address intelligence statistics	70
Creating an iRule to log IP address intelligence information	70
Creating an iRule to reject requests with questionable IP addresses	71
IP address intelligence categories	72
<b>Chapter 6: Managing IP Address Exceptions</b>	<b>73</b>
Overview: Managing IP address exceptions	74
Creating IP address exceptions	74
Deleting IP address exceptions	75
Updating IP address exceptions	75
<b>Chapter 7: Enforcing Application Use at Specific Geolocations</b>	<b>77</b>
Overview: Enforcing application use in certain geolocations	78
Enforcing application use in certain geolocations	78
Setting up geolocation enforcement from a request	79
<b>Chapter 8: Creating Login Pages for Secure Application Access</b>	<b>81</b>
About creating login pages	82
Creating login pages	82
Login page access validation criteria	83
Enforcing login pages	84
<b>Chapter 9: Protecting Sensitive Data with Data Guard</b>	<b>85</b>
About protecting sensitive data with Data Guard	86
Response headers that Data Guard inspects	86
Protecting sensitive data	86

<b>Chapter 10: Masking Credit Card Numbers in Logs.....</b>	<b>89</b>
Overview: Masking credit card numbers in logs.....	90
Masking credit card numbers in request logs.....	90
<b>Chapter 11: Displaying Reports and Monitoring ASM.....</b>	<b>91</b>
ASM Reporting Tools.....	92
Displaying an application security overview report.....	92
Viewing details about requests and violations.....	93
Exporting requests.....	94
<b>Chapter 12: Configuring Application Security Event Logging.....</b>	<b>95</b>
About logging profiles.....	96
Creating a logging profile.....	96
Setting up remote logging.....	97
Associating a logging profile with a security policy.....	98
About logging responses.....	99
About ArcSight log message format.....	99
Filtering logging information.....	99
Viewing application security logs.....	100
<b>Chapter 13: Configuring Application Security Session Tracking.....</b>	<b>101</b>
Overview: Tracking application security sessions using login pages.....	102
Creating login pages.....	102
Enforcing login pages.....	103
Setting up session tracking.....	104
Monitoring user and session information.....	106
Tracking specific user and session information.....	106
<b>Chapter 14: Tracking Application Security Sessions with APM.....</b>	<b>109</b>
Overview: Tracking application security sessions using APM.....	110
Prerequisites for setting up session tracking with APM.....	110
Creating a VLAN.....	110
Creating a self IP address for a VLAN.....	111
Creating a local traffic pool for application security .....	111
Creating a virtual server to manage HTTPS traffic.....	112
Creating a security policy automatically.....	112
Creating an access profile.....	115
Configuring an access policy.....	117
Adding the access profile to the virtual server.....	117
Setting up ASM session tracking with APM.....	118
Monitoring user and session information.....	119

<b>Chapter 15: Mitigating Open Redirects.....</b>	<b>121</b>
Overview: Mitigating open redirects.....	122
Mitigating open redirects.....	122
Configuring how open redirects are learned.....	123
Enforcing redirection domains.....	124
Implementation results.....	124
 <b>Chapter 16: Setting Up Cross-Domain Request Enforcement.....</b>	 <b>127</b>
About cross-domain request enforcement.....	128
Setting up cross-domain request enforcement.....	128
How cross-domain request enforcement works.....	129
 <b>Chapter 17: Implementing Web Services Security.....</b>	 <b>131</b>
Overview: Implementing web services security.....	132
About client and server certificates.....	132
Adding client and server certificates.....	132
Enabling encryption, decryption, signing, and verification of SOAP messages.....	133
Writing XPath queries.....	135
Configuring blocking actions for web services security.....	136
 <b>Chapter 18: Fine-tuning Advanced XML Security Policy Settings.....</b>	 <b>139</b>
Fine-tuning XML defense configuration.....	140
Advanced XML defense configuration settings .....	140
Masking sensitive XML data.....	142
Overriding meta characters based on content.....	143
Managing SOAP methods.....	144
 <b>Chapter 19: Adding JSON Support to an Existing Security Policy.....</b>	 <b>145</b>
Overview: Adding JSON support to existing security policies.....	146
Creating a JSON profile.....	146
Associating a JSON profile with a URL.....	147
Associating a JSON profile with a parameter.....	148
Implementation result.....	148
 <b>Chapter 20: Automatically Creating Security Policies for AJAX Applications.....</b>	 <b>149</b>
Application security for applications that use AJAX.....	150
Overview: Creating a security policy for applications that use AJAX.....	150
Creating a security policy automatically.....	150
Reviewing security policy status.....	153
Implementation result.....	154

<b>Chapter 21: Adding AJAX Blocking Response Behavior to a Security Policy.....</b>	<b>155</b>
Overview: Adding AJAX blocking and login response behavior.....	156
Configuring the blocking response for AJAX applications.....	156
<b>Chapter 22: Securing Web Applications Created with Google Web Toolkit.....</b>	<b>159</b>
Overview: Securing Java web applications created with Google Web Toolkit elements.....	160
Creating a Google Web Toolkit profile.....	160
Associating a Google Web Toolkit profile with a URL.....	161
Implementation result.....	162
<b>Chapter 23: Refining Security Policies with Learning.....</b>	<b>163</b>
About learning.....	164
Learning resources .....	164
About learning suggestions.....	165
Fine-tuning a security policy.....	165
Configuring explicit entities learning.....	166
Viewing requests that caused learning suggestions.....	167
Accepting learning suggestions.....	168
Clearing learning suggestions.....	168
Viewing ignored entities.....	169
About enforcement readiness.....	169
Enforcing entities.....	169
Disabling learning on violations.....	170
<b>Chapter 24: Configuring Security Policy Blocking.....</b>	<b>171</b>
About security policy blocking.....	172
Changing security policy enforcement.....	172
Configuring blocking actions for violations.....	173
About blocking actions.....	174
Configuring HTTP protocol compliance validation.....	174
Configuring blocking actions for web services security.....	175
<b>Chapter 25: Configuring Blocking Responses.....</b>	<b>177</b>
Overview: Configuring blocking responses.....	178
Configuring responses to blocked requests.....	178
Configuring responses to blocked logins.....	179
Customizing responses to blocked XML requests.....	180
<b>Chapter 26: Configuring General Security Policy Building Settings.....</b>	<b>183</b>
About general security policy building settings.....	184
Changing the policy type.....	184

Security policy elements included in each policy type.....	185
Configuring explicit entities learning.....	186
Adjusting the parameter level.....	187
<b>Chapter 27: Configuring Manual Security Policy Settings.....</b>	<b>189</b>
Editing an existing security policy.....	190
Changing security policy enforcement.....	190
Adjusting the enforcement readiness period.....	191
Viewing whether a security policy is case-sensitive.....	191
Differentiating between HTTP and HTTPS URLs.....	192
Specifying the response codes that are allowed.....	192
Activating iRule events.....	193
Application security iRule events.....	193
Configuring trusted XFF headers.....	194
Adding host names.....	194
About adding multiple host names.....	195
Protecting against CSRF.....	195
<b>Chapter 28: Adding File Types to a Security Policy.....</b>	<b>197</b>
About adding file types.....	198
Adding allowed file types.....	198
Wildcard syntax.....	199
Adding disallowed file types.....	200
<b>Chapter 29: Adding Parameters to a Security Policy.....</b>	<b>201</b>
About adding parameters to a security policy.....	202
Creating global parameters.....	202
Creating URL parameters.....	203
Creating flow parameters.....	204
Creating sensitive parameters.....	205
Creating navigation parameters.....	206
Creating parameters with dynamic content.....	206
Creating parameters with dynamic names.....	208
Changing character sets for parameter values .....	208
Changing character sets for parameter names .....	209
Adjusting the parameter level.....	209
Parameter Value Types.....	210
How the system processes parameters.....	211
About path parameters.....	211
Enforcing path parameter security.....	212
<b>Chapter 30: Securing Base64-Encoded Parameters.....</b>	<b>213</b>
Overview: Securing Base64-Encoded Parameters.....	214



Adding base64 decoding to a new user-input parameter.....	214
Adding base64 decoding to an existing user-input parameter.....	214
<b>Chapter 31: Adding URLs to a Security Policy.....</b>	<b>217</b>
About adding URLs.....	218
About referrer URLs.....	218
Adding allowed URLs.....	218
Wildcard syntax.....	220
Allowed URL properties.....	220
Adding disallowed URLs.....	223
Enforcing requests for URLs based on header content.....	224
Specifying characters legal in URLs.....	225
Configuring flows to URLs.....	225
Creating flow parameters.....	226
Configuring dynamic flows to URLs.....	228
Configuring dynamic session IDs in URLs.....	228
<b>Chapter 32: Adding Cookies.....</b>	<b>231</b>
About cookies.....	232
About pure wildcard cookies.....	232
Wildcard syntax.....	233
About cookies and learning.....	233
About adding cookies.....	233
Adding allowed cookies.....	234
Adding enforced cookies.....	235
Changing the order in which wildcard cookies are enforced.....	236
Editing cookies.....	236
Deleting cookies.....	237
Specifying when to add explicit cookies.....	237
Configuring the maximum cookie header length.....	238
<b>Chapter 33: Configuring Advanced Cookie Protection.....</b>	<b>239</b>
Overview: Configuring advanced cookie protection.....	240
Reconfiguring cookie protection.....	240
Importing cookie protection configuration.....	241
Exporting cookie protection configuration.....	242
<b>Chapter 34: Adding Allowed Methods to a Security Policy.....</b>	<b>243</b>
Adding allowed methods.....	244
<b>Chapter 35: Configuring HTTP Headers.....</b>	<b>245</b>
About mandatory headers.....	246
About header normalization.....	246

About default HTTP headers.....	246
Overview: Configuring HTTP headers.....	247
Configuring HTTP headers.....	247
Configuring the maximum HTTP header length.....	248
Implementation Result.....	249
<b>Chapter 36: Configuring How a Security Policy is Automatically Built.....</b>	<b>251</b>
Overview: Configuring automatic policy build settings.....	252
Configuring automatic policy building settings.....	252
About security policy elements.....	253
Modifying security policy elements.....	254
About automatic policy building rules.....	254
About automatic policy building stages.....	255
Modifying security policy rules.....	255
Adding trusted IP addresses to a security policy.....	256
Learning from responses.....	257
Specifying when to add dynamic parameters.....	258
Collapsing entities in a security policy.....	259
Learning based on response codes.....	259
Limiting the maximum number of policy elements.....	260
Specifying the file types for wildcard URLs.....	261
Restoring default values for automatic policy building.....	261
Stopping and starting automatic policy building.....	262
<b>Chapter 37: Configuring General ASM System Options.....</b>	<b>263</b>
Adjusting system preferences.....	264
Incorporating external antivirus protection.....	265
Creating user accounts for application security.....	266
Validating regular expressions.....	266
<b>Chapter 38: Working with Violations.....</b>	<b>269</b>
About violations.....	270
Types of violations.....	270
Viewing descriptions of violations.....	270
Changing severity levels of violations.....	271
Overview: Creating user-defined violations.....	271
Creating user-defined violations.....	271
Enabling user-defined violations.....	272
Sample iRules for user-defined violations.....	273
Deleting user-defined violations.....	278
Exporting and importing user-defined violations.....	278
<b>Chapter 39: Working with Attack Signatures.....</b>	<b>281</b>

About attack signatures.....	282
About attack signature staging.....	282
Types of attacks that attack signatures detect.....	282
Attack signature properties.....	284
Overview: Creating and assigning attack signature sets.....	284
About attack signature sets.....	285
List of attack signature sets.....	285
Creating a set of attack signatures.....	286
Assigning signature sets to a security policy.....	287
Viewing the signature sets in a security policy.....	288
Viewing the attack signatures in a security policy.....	289
Enabling or disabling a specific attack signature.....	289
Enabling or disabling staging for attack signatures.....	289
Overriding attack signatures based on content.....	290
Overview: Managing the attack signature pool.....	291
Updating the attack signature pool .....	291
Getting email about signature updates.....	292
Viewing the attack signature pool and signature details.....	292
Overview: Creating user-defined attack signatures.....	292
Creating a user-defined attack signature.....	293
Importing user-defined attack signatures.....	293
Exporting user-defined attack signatures.....	294
About attack signatures in XML format.....	294
<b>Chapter 40: Maintaining Security Policies.....</b>	<b>297</b>
Overview: Activating and deactivating security policies.....	298
Deactivating security policies.....	298
Activating security policies.....	298
Deleting security policies.....	299
Overview: Importing and exporting security policies .....	299
About security policy export formats.....	300
Exporting security policies.....	300
Importing security policies.....	301
Overview: Comparing security policies.....	301
Comparing security policies.....	302
Overview: Merging security policies.....	303
Merging security policies .....	303
<b>Chapter 41: Configuring ASM with Local Traffic Policies.....</b>	<b>305</b>
About application security and local traffic policies.....	306
About application security and manually adding local traffic policies.....	306
Overview: Configuring ASM with local traffic policies.....	306
Creating a security policy automatically.....	307
Creating local traffic policy rules for ASM.....	309

Implementation results.....	310
<b>Chapter 42: Automatically Synchronizing Application Security Configurations.....</b>	<b>311</b>
Overview: Automatically synchronizing ASM systems.....	312
About device management and synchronizing application security configurations.....	312
Considerations for application security synchronization.....	313
Performing basic network configuration for synchronization.....	313
Specifying an IP address for config sync.....	314
Establishing device trust.....	314
Creating a Sync-Failover device group.....	315
Syncing the BIG-IP configuration to the device group.....	316
Specifying IP addresses for failover communication.....	317
Creating a Sync-Only device group.....	317
Enabling ASM synchronization on a device group.....	318
Synchronizing an ASM-enabled device group.....	319
Implementation result.....	319
<b>Chapter 43: Manually Synchronizing Application Security Configurations.....</b>	<b>321</b>
Overview: Manually synchronizing ASM systems.....	322
About device management and synchronizing application security configurations.....	322
Considerations for application security synchronization.....	323
Performing basic network configuration for synchronization.....	323
Specifying an IP address for config sync.....	324
Establishing device trust.....	324
Creating a Sync-Failover device group.....	325
Syncing the BIG-IP configuration to the device group.....	326
Specifying IP addresses for failover communication.....	327
Enabling ASM synchronization on a device group.....	327
Synchronizing an ASM-enabled device group.....	328
Implementation result.....	329
<b>Chapter 44: Synchronizing Application Security Configurations Across LANs.....</b>	<b>331</b>
Overview: Synchronizing ASM systems across LANs.....	332
About device management and synchronizing application security configurations.....	333
Considerations for application security synchronization.....	333
Performing basic network configuration for synchronization.....	333
Specifying an IP address for config sync.....	334
Establishing device trust.....	334
Creating a Sync-Failover device group.....	335
Syncing the BIG-IP configuration to the device group.....	336
Specifying IP addresses for failover communication.....	337

Creating a Sync-Only device group.....	338
Enabling ASM synchronization on a Sync-Only device group.....	339
Synchronizing an ASM-enabled device group.....	339
Implementation result.....	340
<b>Chapter 45: Integrating ASM with Database Security Products.....</b>	<b>341</b>
Overview: Integrating ASM with database security products.....	342
Creating a security policy automatically.....	343
Creating login pages.....	345
Enforcing login pages.....	346
Configuring a database security server.....	347
Enabling database security integration in a security policy.....	348
Implementation result.....	348
<b>Chapter 46: Integrating ASM and APM with Database Security Products.....</b>	<b>351</b>
Overview: Integrating ASM and APM with database security products.....	352
Prerequisites for integrating ASM and APM with database security.....	352
Creating a VLAN.....	353
Creating a self IP address for a VLAN.....	353
Creating a local traffic pool for application security .....	354
Creating a virtual server to manage HTTPS traffic.....	354
Creating a security policy automatically.....	355
Creating an access profile.....	357
Configuring an access policy.....	359
Adding the access profile to the virtual server.....	360
Configuring a database security server.....	360
Enabling database security integration with ASM and APM.....	361
Implementation result.....	361
<b>Chapter 47: Securing FTP Traffic Using the Default Configuration.....</b>	<b>363</b>
Overview: Securing FTP traffic using default values.....	364
Creating an FTP service profile with security enabled.....	364
Enabling protocol security for an FTP virtual server.....	364
Reviewing violation statistics for security profiles.....	365
<b>Chapter 48: Securing FTP Traffic Using a Custom Configuration.....</b>	<b>367</b>
Overview: Securing FTP traffic using a custom configuration.....	368
Creating a custom FTP profile for protocol security.....	368
Creating a security profile for FTP traffic.....	369
Modifying associations between service profiles and security profiles.....	369
Configuring an FTP virtual server with a server pool.....	369
Reviewing violation statistics for security profiles.....	370

<b>Chapter 49: Securing SMTP Traffic Using the Default Configuration.....</b>	<b>371</b>
Overview: Securing SMTP traffic using system defaults.....	372
Creating an SMTP service profile with security enabled.....	372
Creating an SMTP virtual server with protocol security.....	372
Reviewing violation statistics for security profiles.....	373
 <b>Chapter 50: Securing SMTP Traffic Using a Custom Configuration.....</b>	 <b>375</b>
Overview: Creating a custom SMTP security profile.....	376
Creating a custom SMTP service profile.....	376
Creating a security profile for SMTP traffic.....	377
Enabling anti-virus protection for email.....	377
Modifying associations between service profiles and security profiles.....	378
Creating and securing an SMTP virtual server and pool.....	379
Reviewing violation statistics for security profiles.....	379
 <b>Chapter 51: Configuring Remote High-Speed Logging of Protocol Security Events.....</b>	 <b>381</b>
Overview: Configuring Remote Protocol Security Event Logging.....	382
Creating a pool of remote logging servers.....	383
Creating a remote high-speed log destination.....	384
Creating a formatted remote high-speed log destination.....	384
Creating a publisher .....	385
Creating a custom Protocol Security Logging profile .....	385
Configuring a virtual server for Protocol Security event logging.....	386
Disabling logging .....	387
Implementation result.....	387

# Legal Notices

---

## Publication Date

This document was published on January 27, 2014.

## Publication Number

MAN-0358-06

## Copyright

Copyright © 2013-2014, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

## Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

## Patents

This product may be protected by one or more patents indicated at:

<http://www.f5.com/about/guidelines-policies/patents>

## Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

### **RF Interference Warning**

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

### **FCC Compliance**

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

### **Canadian Regulatory Compliance**

This Class A digital apparatus complies with Canadian ICES-003.

### **Standards Compliance**

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.



# Acknowledgments

---

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, <http://www.and.com>.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler ([bazsi@balabit.hu](mailto:bazsi@balabit.hu)), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller ([nisse@lysator.liu.se](mailto:nisse@lysator.liu.se)), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), [www.gnu.org/copyleft/lgpl.html](http://www.gnu.org/copyleft/lgpl.html).

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at <http://www.perl.com>.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (<http://www.rrdtool.com/index.html>) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (<http://www.nominum.com>).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs ([gerald@wireshark.org](mailto:gerald@wireshark.org)) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,

2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product contains software developed by the RE2 Authors. Copyright ©2009 The RE2 Authors. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes the Zend Engine, freely available at <http://www.zend.com>.

This product includes software developed by Digital Envoy, Inc.

This product contains software developed by NuSphere Corporation, which is protected under the GNU Lesser General Public License.

This product contains software developed by Erik Arvidsson and Emil A Eklund.

This product contains software developed by Aditus Consulting.

## Acknowledgments

This product contains software developed by Dynarch.com, which is protected under the GNU Lesser General Public License, version 2.1 or later.

This product contains software developed by InfoSoft Global (P) Limited.

This product includes software written by Steffen Beyer and licensed under the Perl Artistic License and the GPL.

This product includes software written by Makamaka Hannyaharamitu ©2007-2008.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

---

# Chapter 1

---

## Preventing DoS Attacks for Layer 7 Traffic

---

- *What is a DoS attack?*
- *About recognizing DoS attacks*
- *About configuring TPS-based DoS protection*
- *About configuring latency-based DoS protection*
- *About heavy URL protection*
- *About site-wide DoS mitigation*
- *Overview: Preventing DoS attacks for applications*
- *Implementation Result*

## What is a DoS attack?

---

A *denial-of-service attack* (DoS attack) makes a computer resource unavailable to its intended users, or obstructs the communication media between the intended users and the victim so that they can no longer communicate adequately. Perpetrators of DoS attacks typically target sites or services, such as banks, credit card payment gateways, and e-commerce web sites.

Application Security Manager™ (ASM) helps protect web applications from DoS attacks aimed at the resources that are used for serving the application: the web server, web framework, and the application logic. Advanced Firewall Manager™ (AFM) helps prevent network, SIP, and DNS DoS attacks.

HTTP-GET attacks and page flood attacks are typical examples of application DoS attacks. HTTP-GET attacks are initiated either from a single user (single IP address) or from thousands of computers (distributed DoS attack), which overwhelms the target system. In page flood attacks, the attacker downloads all the resources on the page (images, scripts, and so on) while an HTTP-GET flood repeatedly requests specific URLs regardless of their place in the application.

## About recognizing DoS attacks

---

Application Security Manager™ determines that traffic is a DoS attack based on calculations for transaction rates on the client side (TPS-based) or latency on the server side (latency-based). You can specify the calculations that you want the system to use.

---

**Note:** *You can set up both methods of detection to work independently or you can set them up to work concurrently to detect attacks on both the client side and server side. Whichever method detects the attack handles DoS protection.*

---

In addition, the system can protect web applications against DoS attacks on heavy URLs. Heavy URL protection implies that during a DoS attack, the system protects the heavy URLs using the methods configured in the DoS profile.

You can view details about DoS attacks that the system detected and logged in the event logs and DoS reports. You can also configure remote logging support for DoS attacks when creating a logging profile.

## About configuring TPS-based DoS protection

---

When setting up DoS protection, you can configure the system to prevent DoS attacks based on transaction rates (TPS-based anomaly detection). If you choose TPS-based anomaly protection, the system detects DoS attacks from the client side using the following calculations:

### Transaction rate during detection interval

The average number of requests per second sent for a specific URL, or by a specific IP address. Every second, the system calculates the average TPS for the last minute.

---

**Note:** *The averages for IP address and URL counts are done for each site, that is, for each virtual server and associated DoS profile. If one virtual server has multiple DoS profiles (implemented using a local traffic policy), then each DoS profile has its own statistics within the context of the virtual server.*

---

**Transaction rate during history interval**

The average number of requests per second sent for a specific URL, or by a specific IP address. The system calculates this number every minute.

If the ratio of the transaction rate during the detection interval to the transaction rate during the history interval is greater than the percentage indicated in the **TPS increased by** setting, the system considers the URL to be under attack, or the IP address to be suspicious. In addition, if the transaction rate during the detection interval is absolutely higher than the **TPS reached** setting (regardless of the history interval), then also the respective IP address is suspicious or the URL is being attacked.

Note that TPS-based protection might detect a DoS attack simply because many users are trying to access the server all at once, such as during a busy time or when a new product comes out. In this case, the attack might be a false positive because the users are legitimate. But the advantage of TPS-based DoS protection is that attacks can be detected earlier than when using latency-based protection. So you need to understand the typical maximum peak loads on your system when setting up DoS protection.

## About configuring latency-based DoS protection

---

When setting up DoS protection, you can configure the system to prevent DoS attacks based on the server side (latency-based anomaly detection). In latency-based detection, it takes a latency increase and at least one suspicious IP address, URL, or heavy URL to consider the activity an attack.

***Note:** The average latency is measured for each site, that is, for each virtual server and associated DoS profile. If one virtual server has multiple DoS profiles (implemented using a local traffic policy), then each DoS profile has its own statistics within the context of the virtual server.*

If the ratio of recent versus historical values is greater than the **Latency increased by** setting, then a prerequisite for the presence of an attack is satisfied, but that is not sufficient. It also takes at least one suspicious IP address, one attacked URL based on TPS criteria, or one heavy URL for the system to declare an attack and start mitigation. In addition, if the transaction rate during the detection interval is absolutely higher than the **Latency reached** setting (regardless of the history interval), then also the respective IP address is suspicious or the URL is being attacked.

Latency-based protection is less prone to false positives than TPS-based protection because in a DoS attack, the server is reaching capacity and service/response time is slow: this is impacting all users. Increased latency can be used as a trigger step for detecting an L7 attack. Following the detection of a significant latency increase, it is important to determine whether you need further action. After examining the increase in the requests per second and by comparing these numbers with past activity, you can identify suspicious versus normal latency increases.

## About heavy URL protection

---

*Heavy URLs* are URLs that may consume considerable server resources per request. Heavy URLs respond with low latency most of the time, but can easily reach high latency under specific conditions. Heavy URLs are not necessarily heavy all the time, but tend to get heavy especially during attacks. Therefore, low rate requests to those URLs can cause significant DoS attacks and be hard to distinguish from legitimate clients.

Typically, heavy URLs involve complex database queries; for example, retrieving historical stock quotes. In most cases, users request recent quotes with weekly resolution, and those queries quickly yield responses. However, an attack might involve requesting five years of quotes with day-by-day resolution, which requires retrieval of large amounts of data, and consumes considerably more resources.

Application Security Manager™ allows you to configure protection from heavy URLs in a DoS profile. You can specify a latency threshold for automatically detecting heavy URLs. If some of the web site's URLs could potentially become heavy URLs, you can add them so the system will keep an eye on them, and you can add URLs that should be ignored and not considered heavy.

### About site-wide DoS mitigation

---

In order to mitigate highly distributed DoS attacks, such as those instigated using large scale botnets attacking multiple URLs, you can include site-wide mitigation in a DoS profile. You can use site-wide mitigation as part of the prevention policy for either TPS-based or latency-based DoS protection. In this case, the whole site can be considered suspicious as opposed to a particular URL or IP address. Site-wide mitigation goes into effect when the system determines that the whole site is experiencing high-volume traffic but is not able to pinpoint and handle the problem.

The system implements site-wide mitigation method only as a last resort because it may cause the system to drop legitimate requests. However, it maintains, at least partially, the availability of the web site, even when it is under attack. When the system applies site-wide mitigation, it is because all other active detection methods were unable to stop the attack.

The whole site is considered suspicious when configured thresholds are crossed, and in parallel, specific IP addresses and URLs could also be found to be suspicious. The mitigation continues until the maximum duration elapses or when the whole site stops being suspicious. That is, there are no suspicious URLs, no suspicious IP addresses, and the whole site is no longer suspicious.

### Overview: Preventing DoS attacks for applications

---

You can configure the Application Security Manager™ to protect against DoS attacks on web applications. Depending on your configuration, the system detects DoS attacks based on transactions per second (TPS) on the client side, server latency, or heavy URLs.

You configure DoS protection for Layer 7 by creating a DoS profile with Application Security enabled. You then associate the DoS profile with one or more virtual servers representing applications that you want to protect. DoS protection is not part of a security policy.

#### Task Summary

- Configuring DoS protection for applications*
- Configuring TPS-based DoS protection settings*
- Configuring latency-based DoS protection*
- Configuring heavy URL protection*
- Recording traffic during DoS attacks*
- Associating a DoS profile with a virtual server*
- Displaying DoS event logs*
- Viewing DoS attack statistics*
- Viewing URL Latencies reports*



## Configuring DoS protection for applications

You can configure Application Security Manager™ to protect against and mitigate DoS attacks, and increase system security.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click **Create**.  
The Create New DoS Profile screen opens.
3. In the **Profile Name** field, type the name for the profile.
4. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
5. If you have written an application DoS iRule to specify how the system handles a DoS attack and recovers afterwards, select the **Trigger iRule** setting.
6. If you want to set up DoS protection from the client side, in the TPS-based Anomaly area, select an **Operation Mode** and set up TPS-based DoS protection.  
Another task describes how to configure the settings.
7. If you want to set up DoS protection from the server side, in the Latency-based Anomaly area, select an **Operation Mode** and set up latency-based DoS protection.  
Another task describes how to configure the settings.
8. If you want to set up protection for heavy URLs, in the Heavy URL Protection area, select **Heavy URL Protection** and configure the protection settings.  
Another task describes how to configure the settings.
9. To omit certain addresses, for the **IP Address Whitelist** setting, type IP addresses or subnets that do not need to be examined for DoS attacks, and click **Add**.

---

***Note:** You can add up to 20 IP addresses.*

---

10. To record traffic (perform a TCP dump) during DoS attacks, select the **Record Traffic During Attacks** check box, and specify the options to determine the conditions and how often to perform the dump.  
This option allows you to diagnose the attack vectors and attackers and observe whether it was mitigated.  
If a DoS attack occurs, the system creates a TCP dump in `/shared/dos17/tcpdumps` on the virtual server where the attack was detected.
11. Click **Finished** to save the DoS profile.

You have created a DoS profile.

Next, configure TPS-based, latency-based, or heavy URL DoS protection settings, or all three.

## Configuring TPS-based DoS protection settings

You can configure Application Security Manager™ to mitigate DoS attacks based on transaction rates using TPS-based DoS protection.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one).  
The DoS Profile Properties screen opens.

3. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
4. In the TPS-based Anomaly area, for **Operation Mode**, select an operation mode.

Option	Description
<b>Transparent</b>	Displays information about DoS attacks on the DoS: Application reporting screen but does not block requests.
<b>Blocking</b>	Drops connections coming from an attacking IP address and requests to attacked URLs. Also displays information about DoS attacks on the DoS: Application reporting screen.

The screen refreshes to display additional configuration settings when you select an operation mode.

5. For the **Prevention Policy** setting, select one or more options to determine how the system handles a DoS attack.

---

*Note: If you enable more than one option, the system uses the options in the order in which they are listed.*

---

Option	Description
<b>Source IP-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious IP addresses are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. The default is disabled.
<b>URL-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious URLs are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. This setting enforces strong protection and prevents distributed DoS attacks but affects more clients. The default is disabled.
<b>Site-wide Client-Side Integrity Defense</b>	Determines whether the client is a legal browser or an illegal script by sending a JavaScript challenge to all URLs for each suspicious site and waiting for a response. (Legal browsers are able to respond, while illegal scripts cannot.) The default is disabled.
<b>Source IP-Based Rate Limiting</b>	Drops requests from suspicious IP addresses. The system limits the rate of requests to the average rate prior to the attack, or lower than the absolute threshold specified by the IP detection TPS reached setting. The default is enabled.
<b>URL-Based Rate Limiting</b>	Indicates that when the system detects a URL under attack, Application Security Manager drops connections to limit the rate of requests to the URL to the average rate prior to the attack. The default is enabled.
<b>Site-wide Rate Limiting</b>	Indicates that the system drops transactions for suspicious sites. The system allows requests for that site when the request rate per second is less than the legitimate history interval (before the attack started), or less than the threshold you configure in the TPS reached setting. The default is enabled.

6. For **IP Detection Criteria**, modify the threshold values as needed.

---

*Note: This setting appears only if **Prevention Policy** is set to **Source IP-Based Client Side Integrity Defense** and/or **Source IP-Based Rate Limiting**.*

---

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

Option	Description
<b>TPS increased by</b>	Specifies that the system considers an IP address to be that of an attacker if the transactions sent per second have increased by this percentage, and the detected TPS is greater than the <b>Minimum TPS Threshold for detection</b> . The default value is 500%.
<b>TPS reached</b>	Specifies that the system considers an IP address to be suspicious if the number of transactions sent per second from an IP address equals, or is greater than, this value. This setting provides an absolute value, so, for example, if an attack increases the number of transactions gradually, the increase might not exceed the <b>TPS increased by</b> threshold and would not be detected. If the TPS reaches the <b>TPS reached</b> value, the system considers traffic to be an attack even if it did not meet the <b>TPS increased by</b> value. The default value is 200 TPS.
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers an IP address to be an attacker if the detected TPS for a specific IP address equals, or is greater than, this number, and the <b>TPS increased by</b> number was reached. The default setting is 40 transactions per second.

---

***Tip:** Click the **Set default criteria** link to reset these settings to their default values.*

---

7. For **URL Detection Criteria**, modify the threshold values as needed.

---

***Note:** This setting appears only if **Prevention Policy** is set to **URL-Based Client Side Integrity Defense** and/or **URL-Based Rate Limiting**.*

---

Option	Description
<b>TPS increased by</b>	Specifies that the system considers a URL to be that of an attacker if the transactions sent per second to the URL have increased by this percentage, and the detected TPS is greater than the <b>Minimum TPS Threshold for detection</b> . The default value is 500%.
<b>TPS reached</b>	Specifies that the system considers a URL to be suspicious if the number of transactions sent per second to the URL is equal to or greater than this value. This setting provides an absolute value, so, for example, if an attack increases the number of transactions gradually, the increase might not exceed the <b>TPS increased by</b> threshold and would not be detected. If the TPS reaches the <b>TPS reached</b> value, the system considers traffic to be an attack even if it did not meet the <b>TPS increased by</b> value. The default value is 1000 TPS.
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers a URL to be an attacker if the detected TPS for a specific URL equals, or is greater than, this number, and the <b>TPS increased by</b> number was reached. The default setting is 200 transactions per second.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

8. For **Site-Wide Detection Criteria**, modify the threshold values as needed.

---

***Note:** This setting appears only if using site-wide prevention policies.*

---

Option	Description
<b>TPS increased by</b>	Specifies that the system considers a whole site to be under attack if the transactions sent per second have increased by this percentage, and the detected TPS is greater than the <b>Minimum TPS Threshold for detection</b> . The default value is 500%.

Option	Description
<b>TPS reached</b>	Specifies that the system considers a whole site to be under attack if the number of requests sent per second is equal to or greater than this number. The default value is 10000 TPS.
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers a whole site to be under attack if the detected TPS is equal to or greater than this number, and the <b>TPS increased by</b> number was reached. The default setting is 2000 TPS.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

- For the **Prevention Duration** setting, specify the time spent in each mitigation step until deciding to move to the next mitigation step.

Option	Description
<b>Escalation Period</b>	Specifies the minimum time spent in each mitigation step before the system moves to the next step when preventing attacks against an attacker IP address or attacked URL. During a DoS attack, the system performs attack prevention for the amount of time configured here for methods enabled in the Prevention Policy. If after this period the attack is not stopped, the system enforces the next enabled prevention step. Type a number between 1 and 3600. The default is 120 seconds.
<b>De-escalation Period</b>	Specifies the time spent in the final escalation step until retrying the steps using the methods enabled in the Prevention Policy. Type a number (greater than the escalation period) between 0 (meaning no de-escalation) and 7200 seconds. The default value is 7200 seconds (2 hours).

DoS mitigation is reset after 2 hours even if the detection criteria still hold regardless of the value set for the **De-escalation Period**. If the attack is still taking place, a new attack occurs and mitigation starts over retrying the steps in the Prevention Policy. If you set the **De-escalation Period** to less than 2 hours, the reset occurs more frequently.

- Click **Update** to save the DoS profile.

You have now configured a DoS profile to prevent DoS attacks based on the client side (TPS-based Detection Mode).

Next, you need to associate the DoS profile with the application's virtual server. You also have the option of configuring heavy URL protection.

## Configuring latency-based DoS protection

You can configure Application Security Manager™ to mitigate Layer 7 DoS attacks based on server latency.

- On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
- Click the name of an existing DoS profile (or create a new one).  
The DoS Profile Properties screen opens.
- Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
- In the Latency-based Anomaly area, for **Operation Mode**, select an operation mode.

Option	Description
<b>Transparent</b>	Displays information about DoS attacks on the DoS: Application reporting screen but does not block requests.

Option	Description
--------	-------------

<b>Blocking</b>	Drops connections coming from an attacking IP address and requests to attacked URLs. Also displays information about DoS attacks on the DoS: Application reporting screen.
-----------------	--

The screen refreshes to display additional configuration settings when you select an operation mode.

5. For **Detection Criteria**, modify the threshold values as needed.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

Option	Description
--------	-------------

<b>Latency increased by</b>	Specifies that the system considers traffic to be an attack if the latency has increased by this percentage, and the minimum latency threshold has been reached. The default value is 500%.
-----------------------------	---

<b>Latency reached</b>	Specifies that the system considers traffic to be an attack if the latency is equal to or greater than this value. This setting provides an absolute value, so, for example, if an attack increases latency gradually, the increase might not exceed the <b>Latency Increased by</b> threshold and would not be detected. If server latency reaches the <b>Latency reached</b> value, the system considers traffic to be an attack even if it did not meet the <b>Latency increased by</b> value. The default value is 10000 ms.
------------------------	--

<b>Minimum Latency Threshold for detection</b>	Specifies that the system considers traffic to be an attack if the detection interval for a specific URL equals, or is greater than, this number, and at least one of the <b>Latency increased by</b> numbers was reached. The default setting is 200 ms.
--	---

---

*Tip:* Click the **Set default criteria** link to reset these settings to their default values.

---

6. For the **Prevention Policy** setting, select one or more options to determine how the system handles a DoS attack.

---

*Note:* If you enable more than one option, the system uses the options in the order in which they are listed.

---

Option	Description
--------	-------------

<b>Source IP-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious IP addresses are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. The default is disabled.
--	---

<b>URL-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious URLs are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. This setting enforces strong protection and prevents distributed DoS attacks but affects more clients. The default is disabled.
--	--

<b>Site-wide Client-Side Integrity Defense</b>	Determines whether the client is a legal browser or an illegal script by sending a JavaScript challenge to all URLs for each suspicious site and waiting for a response. (Legal browsers are able to respond, while illegal scripts cannot.) The default is disabled.
--	---

<b>Source IP-Based Rate Limiting</b>	Drops requests from suspicious IP addresses. The system limits the rate of requests to the average rate prior to the attack, or lower than the absolute threshold specified by the IP detection TPS reached setting. The default is enabled.
--------------------------------------	--

Option	Description
<b>URL-Based Rate Limiting</b>	Indicates that when the system detects a URL under attack, Application Security Manager drops connections to limit the rate of requests to the URL to the average rate prior to the attack. The default is enabled.
<b>Site-wide Rate Limiting</b>	Indicates that the system drops transactions for suspicious sites. The system allows requests for that site when the request rate per second is less than the legitimate history interval (before the attack started), or less than the threshold you configure in the TPS reached setting. The default is enabled.

7. For **Suspicious IP Criteria**, modify the threshold values as needed.

---

*Note: This setting appears only if **Prevention Policy** is set to **Source IP-Based Client Side Integrity Defense** and/or **Source IP-Based Rate Limiting**.*

---

Option	Description
<b>TPS increased by</b>	Specifies that the system considers an IP address to be that of an attacker if the transactions sent per second have increased by this percentage, and the detected TPS for a specific IP address is equal to or greater than the <b>Minimum TPS Threshold</b> . The default value is 500%.
<b>TPS reached</b>	Specifies that the system considers an IP address to be suspicious if the number of transactions sent per second from an IP address equals, or is greater than, this value. This setting provides an absolute value, so, for example, if an attack increases the number of transactions gradually, the increase might not exceed the <b>TPS increased by</b> threshold and would not be detected. If the TPS reaches the <b>TPS reached</b> value, the system considers traffic to be an attack even if it did not meet the <b>TPS increased by</b> value. The default value is 200 TPS.
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers an IP address to be an attacker if the detected TPS for a specific IP address equals, or is greater than, this number, and the <b>TPS increased by</b> number was reached. The default setting is 40 transactions per second.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

8. For **Suspicious URL Criteria**, modify the threshold values as needed.

---

*Note: This setting appears only if **Prevention Policy** is set to **URL-Based Client Side Integrity Defense** and/or **URL-Based Rate Limiting**.*

---

Option	Description
<b>TPS increased by</b>	Specifies that the system considers a URL to be an attacker if the transactions sent per second sent to the URL have increased by this percentage, and the detected TPS for a specific IP address is equal to or greater than the <b>Minimum TPS Threshold</b> . The default value is 500%.
<b>TPS reached</b>	Specifies that the system considers a URL to be suspicious if the number of transactions sent per second to the URL is equal to or greater than this value. This setting provides an absolute value, so, for example, if an attack increases the number of transactions gradually, the increase might not exceed the <b>TPS increased by</b> threshold and would not be detected. If the TPS reaches the <b>TPS reached</b> value, the system considers traffic to be an attack even if it did not meet the <b>TPS increased by</b> value. The default value is 1000 TPS.

Option	Description
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers a URL to be an attacker if the detected TPS for a specific URL equals, or is greater than, this number, and the <b>TPS increased by</b> number was reached. The default setting is 40 transactions per second.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

9. For **Suspicious Site-Wide Criteria**, modify the threshold values as needed.

---

*Note: This setting appears only if using site-wide prevention policies.*

---

Option	Description
<b>TPS increased by</b>	Specifies that the system considers a whole site to be under attack if the transactions sent per second have increased by this percentage, and the detected TPS for a specific IP address is equal to or greater than the <b>Minimum TPS Threshold</b> . The default value is 500%.
<b>TPS reached</b>	Specifies that the system considers a whole site to be under attack if the number of requests sent per second is equal to or greater than this number. The default value is 10000 TPS.
<b>Minimum TPS Threshold for detection</b>	Specifies that the system considers a whole site to be under attack if the detected TPS is equal to or greater than this number, and the <b>TPS increased by</b> number was reached. The default setting is 2000 TPS.

If any of these criteria is met, the system handles the attack according to the **Prevention Policy** settings.

10. For the **Prevention Duration** setting, specify the time spent in each mitigation step until deciding to move to the next mitigation step.

Option	Description
<b>Escalation Period</b>	Specifies the minimum time spent in each mitigation step before the system moves to the next step when preventing attacks against an attacker IP address or attacked URL. During a DoS attack, the system performs attack prevention for the amount of time configured here for methods enabled in the Prevention Policy. If after this period the attack is not stopped, the system enforces the next enabled prevention step. Type a number between 1 and 3600. The default is 120 seconds.
<b>De-escalation Period</b>	Specifies the time spent in the final escalation step until retrying the steps using the methods enabled in the Prevention Policy. Type a number (greater than the escalation period) between 0 (meaning no de-escalation) and 7200 seconds. The default value is 7200 seconds (2 hours).

DoS mitigation is reset after 2 hours even if the detection criteria still hold regardless of the value set for the **De-escalation Period**. If the attack is still taking place, a new attack occurs and mitigation starts over retrying the steps in the Prevention Policy. If you set the **De-escalation Period** to less than 2 hours, the reset occurs more frequently.

11. Click **Update** to save the DoS profile.

You have now configured a DoS profile to prevent DoS attacks based on server latency.

Next, associate the DoS profile with the application's virtual server. You also have the option of configuring heavy URL protection.

## Configuring heavy URL protection

To use heavy URL protection, F5 recommends that you configure latency-based anomaly settings in the DoS profile. That way the system can detect low-volume attacks on heavy URLs when no other high-volume attacks are underway. Also, you must enable at least one of the URL-based prevention policy methods in the TPS-based Anomaly or Latency-based Anomaly settings in the DoS profile.

You can configure Application Security Manager™ (ASM) to prevent DoS attacks on heavy URLs. Heavy URLs are URLs on your application web site that may consume considerable resources under certain conditions. By tracking URLs that are potentially heavy, you can mitigate DoS attacks on these URLs before response latency exceeds a specific threshold.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one).  
The DoS Profile Properties screen opens.
3. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
4. Select the **Heavy URL Protection** check box.  
The screen displays additional configuration settings.
5. To automatically detect heavy URLs, select the **Automatic Detection** check box.

---

***Tip:** You may want to hold off selecting this option until after observing normal traffic for a day or two so you can assign a reasonable latency threshold value.*

---

The system detects heavy URLs by measuring the latency tail ratio, which is the number of transactions whose latency is consistently greater than the latency threshold. A URL is considered heavy if its latency tail ratio is considerably above the global average, in the long run (default of 24 hours).

6. In the **Heavy URLs** setting, add the URLs that you expect to be heavy (have high latency) at times in the form `/query.html`.  
If you are not sure which URLs to add, leave this list blank and let the system automatically detect heavy URLs by using automatic detection.
7. In the **Ignored URLs (Wildcards Supported)** setting, add the URLs that you never want the system to consider heavy.  
The URLs in this list may include wildcards.
8. If using automatic detection, in the **Latency Threshold** field, type the number of milliseconds for the system to use as the threshold for automatically detecting heavy URLs.  
The default value is 1000 milliseconds.
9. Click **Update** to save the DoS profile.

You have now configured a DoS profile that includes heavy URL protection. Heavy URLs are detected based on latency. ASM tracks the probability distribution of server latency which is called heavy tailed.

To validate automatic detection, you can view the URL Latencies report periodically to check that the latency threshold that you used is close to the value in the latency histogram column for all traffic. By reviewing the report and sorting the URLs listed by latency, you can make sure that the URLs that you expect to be heavy are listed in the DoS profile. Also, if the system detects too many (or too few) heavy URLs, you can increase (or decrease) the latency threshold.



## Recording traffic during DoS attacks

If you have DoS protection enabled, you can configure the system to record traffic during DoS attacks. By reviewing the recorded traffic in the form of a TCP dump, you can diagnose the attack vectors and attackers, observe whether and how the attack was mitigated, and determine whether you need to change the DoS protection configuration.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one).  
The DoS Profile Properties screen opens.
3. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
4. Toward the bottom of the screen, select the **Record Traffic During Attacks** check box.  
The screen refreshes and displays additional configuration settings.
5. For **Maximum TCP Dump Duration**, type the maximum number of seconds (from 1 - 300) for the system to record traffic during a DoS attack.  
The default value is 30 seconds.
6. For **Maximum TCP Dump Size**, type the maximum size (from 1 - 50) allowed for the TCP dump.  
When the maximum size is reached, the dump is complete. The default value is 10 MB.
7. For **TCP Dump Repetition**, specify how often to perform TCP dumps during a DoS attack:
  - To record traffic once during an attack, select **Dump once per attack**.
  - To record traffic periodically during an attack, select **Repeat dump after** and type the number of seconds (between 1 - 3600) for how long to wait after completing a TCP dump before starting the next one.
8. Click **Update** to save the DoS profile.

When the system detects a DoS attack, it performs a TCP dump to record the traffic on the virtual server where the attack occurred. The files are located on the system in `/shared/dos17/tcpdumps`. The name of the file has the format: `<yyyy_mm_dd_hh:mm:ss>-<attack_ID>-<seq_num>.pcap`, including the time the dump started, the ID of the attack in logs and reports, and the number of the TCP dump since the attack started. If traffic being recorded is SSL traffic, it is recorded encrypted.

If working with F5 support, you can collect the TCP dump files into a QuickView file so that support personnel can help determine the cause of the DoS attack, and recommend ways of preventing future attacks.

## Associating a DoS profile with a virtual server

You must first create a DoS profile separately, to configure denial-of-service protection for applications, the DNS protocol, or the SIP protocol.

You add denial-of-service protection to a virtual server to provide enhanced protection from DoS attacks, and track anomalous activity on the BIG-IP® system.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.

4. From the **Security** menu, choose **Policies**.
5. To enable denial-of-service protection, from the **DoS Protection Profile** list, select **Enabled**, and then, from the **Profile** list, select the DoS profile to associate with the virtual server.
6. Click **Update** to save the changes.

DoS protection is now enabled, and the DoS Protection profile is associated with the virtual server.

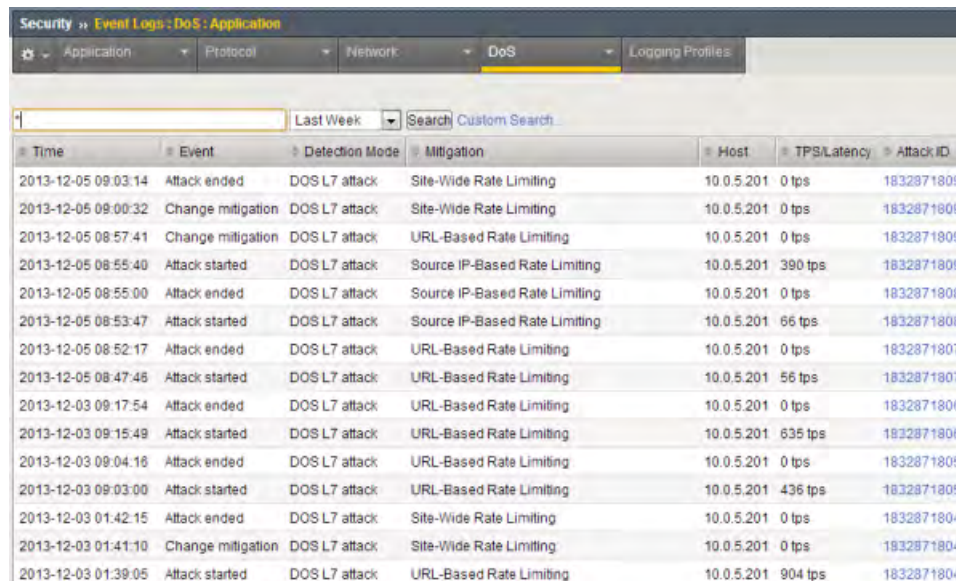
## Displaying DoS event logs

You can display DoS Application event logs to see whether L7 DoS attacks have occurred, and view information about the attacks.

1. On the Main tab, click **Security > Event Logs > DoS > Application**.  
The DoS Application event log opens.
2. Review the list of DoS attacks to see what has occurred, what mitigation is in place, and what caused the attacks.
3. Click the **Attack ID** link for an attack to display additional information in a chart form.

## Sample DoS event log

This figure shows a sample DoS event log for a system (IP address 10.0.5.201) that has had quite a few DoS attacks over the past week. You can see that they have been mitigated using various prevention methods.



Time	Event	Detection Mode	Mitigation	Host	TPS/Latency	Attack ID
2013-12-05 09:03:14	Attack ended	DOS L7 attack	Site-Wide Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871809</a>
2013-12-05 09:00:32	Change mitigation	DOS L7 attack	Site-Wide Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871809</a>
2013-12-05 08:57:41	Change mitigation	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871809</a>
2013-12-05 08:55:40	Attack started	DOS L7 attack	Source IP-Based Rate Limiting	10.0.5.201	390 tps	<a href="#">1832871809</a>
2013-12-05 08:55:00	Attack ended	DOS L7 attack	Source IP-Based Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871808</a>
2013-12-05 08:53:47	Attack started	DOS L7 attack	Source IP-Based Rate Limiting	10.0.5.201	66 tps	<a href="#">1832871808</a>
2013-12-05 08:52:17	Attack ended	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871807</a>
2013-12-05 08:47:45	Attack started	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	56 tps	<a href="#">1832871807</a>
2013-12-03 09:17:54	Attack ended	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871806</a>
2013-12-03 09:15:49	Attack started	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	635 tps	<a href="#">1832871806</a>
2013-12-03 09:04:16	Attack ended	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871805</a>
2013-12-03 09:03:00	Attack started	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	436 tps	<a href="#">1832871805</a>
2013-12-03 01:42:15	Attack ended	DOS L7 attack	Site-Wide Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871804</a>
2013-12-03 01:41:10	Change mitigation	DOS L7 attack	Site-Wide Rate Limiting	10.0.5.201	0 tps	<a href="#">1832871804</a>
2013-12-03 01:39:05	Attack started	DOS L7 attack	URL-Based Rate Limiting	10.0.5.201	904 tps	<a href="#">1832871804</a>

Figure 1: Sample DoS event log

## Viewing DoS attack statistics

Before you can look at the DoS attack statistics, you need to have created a DoS profile so that the system is capturing the analytics on the BIG-IP<sup>®</sup> system. You must associate the DoS profile with one or more virtual servers. If your browser is IE8 or earlier, you need to have Adobe Flash Player installed on the computer where you plan to review the data.

You can display charts that show information about DoS attacks on applications. The charts provide visibility into what caused the attack, IP addresses of the attackers, which applications are being attacked, and how the attacks are being mitigated.

1. On the Main tab, click **Security > Reporting > DoS**.  
The DoS Application Statistics reporting screen opens.
2. From the **View By** list, select the way you want to view information about DoS attacks.  
For example, click **Client IP Addresses** to see the IP addresses from which the attacks are emanating.
3. If you want to filter the information that displays further, click **Expand Advanced Filters** and select the details you want to see.
4. To focus in on the specific details you want more information about, point to the chart or click it.  
The system displays information about the item.

You can continue to review the details about DoS attacks on the reporting screens. As a result, you become more familiar with what caused the attacks, what applications are most vulnerable, and see the mitigation methods that are in place.

If you are recording traffic during attacks, you can view the TCP dumps related to the DoS attacks in `/shared/dos17/tcpdumps`.

### Sample DoS Statistics report

This figure shows a sample DoS Statistics report showing a number of DoS attacks listed by attack ID. The report shows the number of transactions that were dropped during these attacks which were all mitigated using source IP-based rate limiting. With this method of rate limiting, the system noticed a spike in requests coming from certain IP addresses and considered them to be suspicious IP addresses. The system limited the number of requests from these suspicious IP addresses to a reasonable number (before the attack started) or to the threshold configured in the **TPS reached** setting.

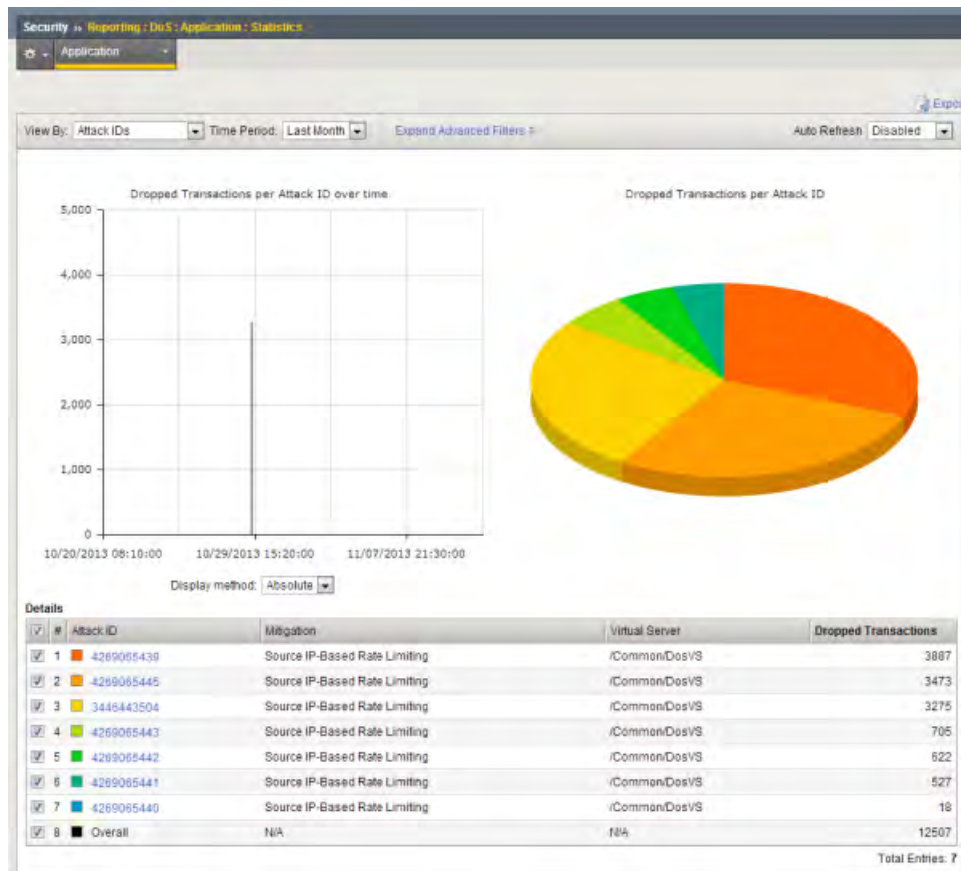


Figure 2: Sample DoS Statistics report

## Viewing URL Latencies reports

For the URL Latencies report to include useful information, you need to have created a DoS profile with heavy URL protection so that the system is capturing the latency statistics. You must associate the DoS profile with one or more virtual servers.

You can display a report that shows information about the latency of traffic to specific web pages in your application. The report lists the latency for each URL separately and one row lists the latency for all URLs combined. You can use this report to check that the latency threshold that you used is close to the value in the latency histogram column for all traffic.

1. On the Main tab, click **Security > Reporting > DoS > Application > URL Latencies**. The URL Latencies reporting screen opens.
2. From the **Time Period** list, select the time period for which you want to view URL latency, or specify a custom time range.
3. If you want to filter the information by DoS profile, virtual server, URL, or detection criteria, specify the ones for which you want to view the URL latency.  
By default, the report displays information for all items.
4. Adjust the chart display options as you want.

### Display Option

### Description

#### Display Mode

Select whether to display the information as **Cumulative** or as related to the respective latency range, **Per Interval**.

Display Option	Description
<b>Unified Scale</b>	Select this check box to display all histograms using a single scale for all URLs, rather than a separate scale for each one.
<b>Order by</b>	Select the order in which to display the statistics: by the average server latency, the number of transactions, the histogram latency ranges (in milliseconds), or by how heavy URLs were detected.

5. Review the latency statistics.

- The report shows the latency for the most active URLs.
- The Aggregated row summarizes the statistics for the URLs not included in the report.
- If there is only one DoS profile or virtual server on the system, the chart does not include these columns.
- The Overall Summary shows the latency of all traffic

6. To focus in on the specific latency details for one row, click the latency histogram.

A magnified view of the histogram is displayed in a separate window. The latency histogram shows the percentage of transactions for each range of latency (0-2 ms, 2-4 ms, and so on up to 10000 ms or 10 seconds).

The URL Latencies report shows how fast your web application returns web pages and can show typical latency for applications (meaning virtual servers associated with a DoS profile) on your system. It can help you to identify slow pages with latency problems that may require additional troubleshooting by application developers.

You can also use the URL Latencies report for the following purposes:

- To determine the threshold latencies, especially the heaviness threshold.

---

**Tip:** Set the heaviness threshold to approximately 90-95% of the latency distribution for the site. Filter the data by site (that is, by virtual server and DoS profile), and check the latency distribution in the histogram of the Total row.

---

- To track the current heavy URLs. You can add or remove manually configured heavy URLs depending on the information in the report.
- To monitor the latency distribution.

## Sample URL Latencies report

This figure shows a sample URL Latencies report for a system with one DoS profile and one virtual server. It shows the latency for three web pages. One page (/) is performing within reasonable ranges displaying pages in 4 to 22 ms. However, two of the URLs, /dos\_1.php and /dos\_5.php, have much higher latency and might require some troubleshooting. While checking into the latency of those URLs, you can add them to the list of heavy URLs in the DoS profile so they do not trigger DoS mitigation.

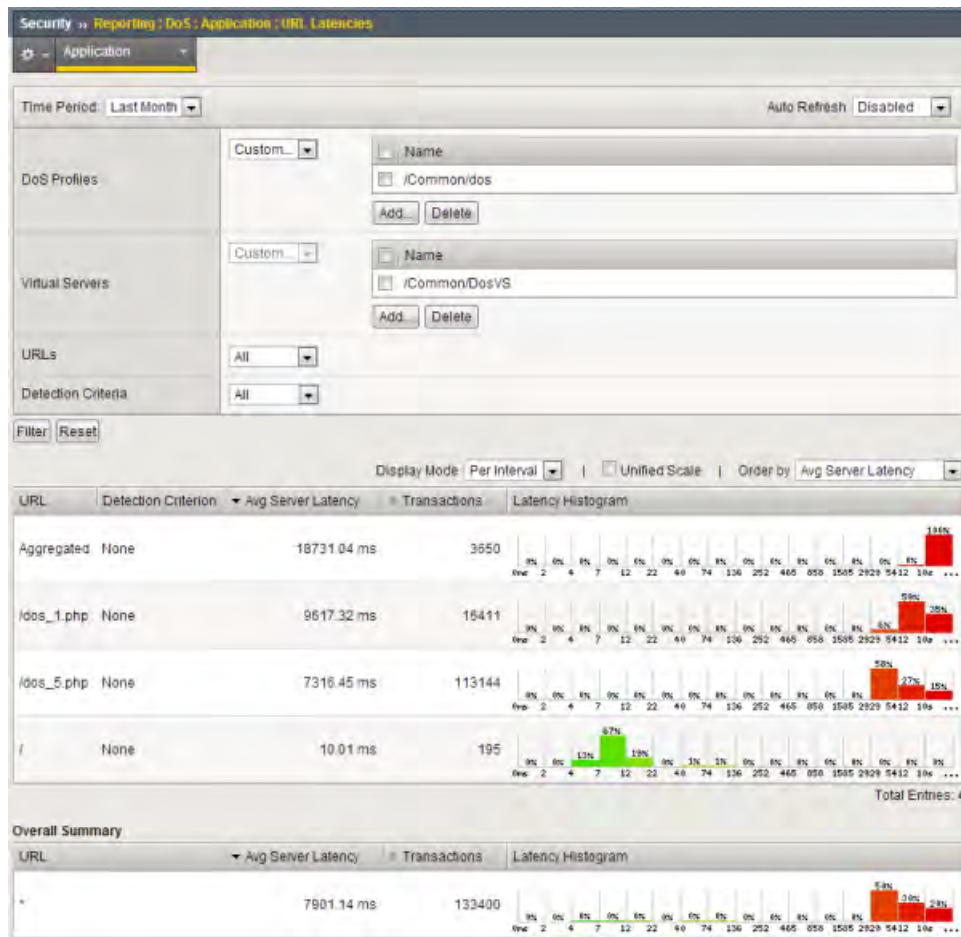


Figure 3: Sample URL Latencies report

## Implementation Result

When you have completed the steps in this implementation, you have configured the Application Security Manager™ to protect against L7 DoS attacks. Depending on your configuration, the system detects DoS attacks based on transactions per second (TPS) on the client side, server latency, or both.

In TPS-based detection mode, if the ratio of the transaction rate during the history interval is greater than the TPS increased by percentage, the system considers the URL to be under attack, the IP address to be suspicious, or possibly the whole site to be suspicious.

In latency-based detection mode, if there is a latency increase and at least one suspicious IP address, URL, or heavy URL, the system considers the URL to be under attack, the IP address to be suspicious, or possibly the whole site to be suspicious.

If you enabled heavy URL protection, the system tracks URLs that consume higher than average resources and mitigates traffic that is going to those URLs.

If you chose the blocking operation mode, the system drops requests from suspicious IP addresses and URLs. If using the transparent operation mode, the system reports DoS attacks but does not block them.

If using iRules®, when the system detects a DoS attack based on the configured conditions, it triggers an iRule and responds to the attack as specified in the iRule code.

After traffic is flowing to the system, you can check whether DoS attacks are being prevented, and investigate them by viewing DoS event logs and reports.





---

# Chapter 2

---

## Configuring DoS Policy Switching

---

- *About DoS protection and local traffic policies*
  - *Overview: Configuring DoS policy switching*
  - *Implementation results*
-

## About DoS protection and local traffic policies

---

To provide additional flexibility for configuring DoS protection, you can use local traffic policies together with DoS protection. The advantage of creating local traffic policies is that you can apply multiple DoS protection policies to different types of traffic, using distinct DoS profiles. However, you need to be aware of certain considerations when using this method.

Local traffic policies can include multiple rules. Each rule consists of a condition and a set of actions to be performed if the respective condition holds. So you can create a local traffic policy that controls Layer 7 DoS protection and includes multiple rules. If you do, every rule must include one of the following Layer 7 DoS actions:

- Enable DoS protection using the default DoS profile (`/Common/dos`)
- Enable DoS protection from a specific DoS profile
- Disable DoS protection

---

**Important:** *Make sure that the local traffic policy with DoS protection includes a default rule with no condition that applies to traffic that does not match any other rule. In addition, be sure that each rule (including the default one), has an L7 DoS action in it, possibly in addition to other actions.*

---

A default rule is required because the local traffic policy action applies not only to the request that matched the condition, but also to the following requests in the same TCP connection, even if they do not match the condition that triggered the action unless subsequent requests on the same connection match a different rule with a different L7 DoS action.

This requirement ensures that every request will match some rule (even the default one), and will trigger a reasonable Layer 7 DoS action. This way a request will not automatically enforce the action of the previous request on the same connection, which can yield unexpected results.

A typical action for the default rule in case of Layer 7 DoS is to create a rule with no condition and simply enable DoS protection. In this case, the action the rule takes is to use the DoS policy attached to the virtual server. In the example of configuring DoS policy switching, the third rule, `others`, is the default rule.

## Overview: Configuring DoS policy switching

---

You can configure the BIG-IP® system to protect against Layer 7 DoS attacks applying unique profiles in different situations, or on different types of traffic.

This implementation provides an example where you configure DoS protection for Layer 7 by creating two DoS profiles with Application Security enabled. You then associate the default DoS profile with a virtual server representing the application that you want to protect. You also create a local traffic policy with rules that assign different DoS protections depending on the traffic. Then you associate the local traffic policy with the virtual server.

This example divides traffic into three categories:

- **Employees:** A unique DoS profile, assigned to employees, reports DoS attacks but does not drop connections when there is an attack.
- **Internal users:** No DoS protection is applied to internal users.
- **Others:** The strictest DoS protection is applied using the default DoS profile for all other users; the system blocks DoS attacks that occur on other traffic.

Many other options are available for configuring DoS policy switching. This is simply one way to illustrate how you can configure multiple DoS protections using a local traffic policy to determine different conditions and actions. By following the steps in this example, you can see the other options that are available on the screens, and can adjust the example for your needs.

### Task Summary

*Creating a DoS profile for Layer 7 traffic*

*Modifying the default DoS profile*

*Creating a local traffic policy for DoS policy switching*

*Creating policy rules for DoS policy switching*

*Associating a DoS profile with a virtual server*

*Associating a local traffic policy with a virtual server*

## Creating a DoS profile for Layer 7 traffic

To define the circumstances under which the system considers traffic to be a Denial of Service (DoS attack), you create a DoS profile. For the DoS policy switching example, you can create a special DoS profile, for employees, that does not block traffic. It only reports the DoS attack.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click **Create**.  
The Create New DoS Profile screen opens.
3. In the **Profile Name** field, type `employee_l7dos_profile` for the profile name in this example.
4. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
5. In the TPS-based Anomaly area, for **Operation Mode**, select **Transparent**.  
When the system detects a DoS attack, it displays the attack data on the Reporting DoS Attacks screen.
6. Use the default values for the other settings.
7. Click **Finished** to save the DoS profile.

You have now created a simple DoS profile to report DoS attacks based on transaction rates using TPS-based DoS protection.

## Modifying the default DoS profile

The BIG-IP® system includes a default DoS profile that you can modify to specify when to use DoS protection. For the DoS policy switching example, you can modify the default DoS profile and use it for people other than employees or internal users who are accessing applications. This example creates a strict default DoS profile that drops requests considered to be an attack.

1. On the Main tab, click **Security > DoS Protection > DoS Profiles**.  
The DoS Profiles list screen opens.
2. Click the profile called **dos**.  
The DoS Profile Properties screen opens.
3. Select the **Application Security** check box.  
The screen refreshes and displays additional configuration settings.
4. In the TPS-based Anomaly area, for **Operation Mode**, select **Blocking**.

5. In the Latency-based Anomaly area, for **Operation Mode**, select **Blocking**.
6. Use the default values for the other settings.
7. Click **Finished** to save the DoS profile.

You have now modified the default DoS profile that will be used for people other than employees or internal users. For these users, the system drops connections from attacking IP addresses, and for requests directed to attacked URLs.

### Creating a local traffic policy for DoS policy switching

You can create a local traffic policy to impose different levels of DoS protection on distinct types of Layer 7 traffic.

1. On the Main tab, click **Local Traffic > Policies**.
2. Click **Create**.  
The New Policy screen opens.
3. In the **Name** field, type a name for the local traffic policy.
4. From the **Strategy** list, select **first-match**.
5. In the **Requires** setting, move **http** from the **Available** to the **Selected** list.
6. In the **Controls** setting, move **l7dos** from the **Available** to the **Selected** list.
7. Click **Finished** to save the local traffic policy.

You have now created a local traffic policy that controls Layer 7 DoS.

Next, you need to add rules to the local traffic policy to specify the DoS protection that should occur for different types of Layer 7 traffic.

### Creating policy rules for DoS policy switching

You can add rules to define conditions and perform specific actions for different types of Layer 7 traffic. This example creates three rules to implement different DoS protection for employees, for internal personnel, and for others.

1. On the Main tab, click **Local Traffic > Policies**.
2. Click the name of the local traffic policy that controls Layer 7 DoS.
3. In the Rules area, click **Add** to create a rule that defines DoS protection for employees.
4. In the **Rule Name** field, type the name `employees`.
5. In the **Actions** setting, define DoS protection to apply to employees: specify the following values, and use the default values for the rest.
  - a) From the **Target** list, select **l7dos**.  
**Event** is set to **request**, **Action** is set to **enable**, and **from\_profile** is set to the default DoS profile, **/Common/dos**.
  - b) To specify a unique DoS profile for employees, from the **Parameters** list, select **from\_profile**; then select **employee\_l7dos\_profile** (or a previously created custom DoS profile), then click the adjacent **Add** button to add the value for the action.
  - c) Above the list of actions, click **Add** to add the action to the list.
6. Click **Finished** to add the rule to the local traffic policy.
7. On the Policy List screen, click the name of the policy that you are working on for Layer 7 DoS.

8. In the Rules area, click **Add** to create a second rule, and call it `internal`.
9. In the **Conditions** setting, define how to handle the internal traffic: specify the following values, and use the default values for the rest.
  - a) From the **Operand** list, select **http-host**.
  - b) From the **Condition** list, select **ends\_with**.
  - c) In the **Values** field, type `internal.my_host.com` and click **Add** to add the value for the condition.
  - d) To add the condition, click **Add**.
10. In the **Actions** setting, disable DoS protection for internal traffic: specify the following values and use the default values for the rest.
  - a) From the **Target** list, select **l7dos**.
  - b) For **Action**, select **disable**.
  - c) Click **Add** to add the action to the list.
11. Click **Finished** to add the rule to the local traffic policy.
12. On the Policy List screen, click the name of the policy that you are working on for Layer 7 DoS.
13. Click **Add** to create a third rule, and call it `others`.
14. In the **Conditions** setting, define how to handle all other traffic for when the first two rules do not apply: use the default values and apply no condition.  
 The **Operand** list is set to **http-basic-auth**, **Event** is set to **request\***, and **Selector** is set to **username**. No special conditions are listed.  
 This last rule is the default rule, which applies if the other two rules do not apply. If you do not include a rule like this and traffic does not match any other rule, the previous rule that was applied is used again.
15. In the **Actions** setting, define the DoS protection to apply to all others: specify the following values, and use the default values for the rest.
  - a) From the **Target** list, select **l7dos**.  
**Event** is set to **request**, **Action** is set to **enable**, and **from\_profile** is set to the default DoS profile, **/Common/dos**.
  - b) Above the list of actions, click **Add** to add the action to the list.
16. Click **Finished** to add the rule to the local traffic policy.
17. Click **Update** to save the local traffic policy with the rules.

You have now created a local traffic policy that defines DoS protection for employees, for internal traffic, and for others.

Next, you need to associate the default DoS profile and the local traffic policy with the virtual server that connects to the application server you are protecting.

## Associating a DoS profile with a virtual server

You must first create a DoS profile separately, to configure denial-of-service protection for applications, the DNS protocol, or the SIP protocol.

You add denial-of-service protection to a virtual server to provide enhanced protection from DoS attacks, and track anomalous activity on the BIG-IP® system.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.

3. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
4. From the **Security** menu, choose **Policies**.
5. To enable denial-of-service protection, from the **DoS Protection Profile** list, select **Enabled**, and then, from the **Profile** list, select the DoS profile to associate with the virtual server.
6. Click **Update** to save the changes.

DoS protection is now enabled, and the DoS Protection profile is associated with the virtual server.

### Associating a local traffic policy with a virtual server

After you create a local traffic policy, you associate that policy with the virtual server created to handle application traffic.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Resources**.
4. In the Policies area, click the **Manage** button.
5. For the **Policies** setting, from the **Available** list, select the local traffic policy you previously created, and move it to the **Enabled** list.
6. Click **Finished**.

## Implementation results

---

When you have completed the steps in this implementation, you have configured the Application Security Manager™ to protect against Layer 7 DoS attacks. By using a local traffic policy, you distinguished between three types of traffic: employees, internal users, and others.

The first rule in the local traffic policy identifies employees by the last line of the host header in the request, which says `employee.my_host.com`. You created a special DoS profile for employees that reports transaction-based DoS attacks but does not drop connections.

The second rule in the local traffic policy identifies internal users by the last line of the host header in the request, which says `internal.my_host.com`. In the policy, you specified that there should be no DoS protection for internal users.

A third rule acts as the default rule and applies to any traffic that was not identified by the first two rules. All other traffic uses the default DoS profile (`dos`) assigned on the Security tab of the virtual server where traffic is directed to the application. You modified the default DoS profile to block transaction-based and server latency-based DoS attacks that the system detects.

After creating the local traffic policy with Layer 7 DoS rules, you also associated it with the virtual server. Different types of traffic directed to the virtual server now has distinct DoS protections assigned to it.

---

# Chapter

# 3

---

## Mitigating Brute Force Attacks

---

- *About mitigation of brute force attacks*
  - *Overview: Mitigating brute force attacks*
-

### About mitigation of brute force attacks

---

*Brute force attacks* are attempts to break in to secured areas of a web application by trying exhaustive, systematic, user name/password combinations to discover legitimate authentication credentials.

To prevent brute force attacks, the Application Security Manager™ tracks the number of failed attempts to reach the configured login URL. The system saves the information in two intervals:

#### History interval

Specifies the number of failed login attempts for the past hour (updated every minute).

#### Detection interval

Specifies the number of failed login attempts for the past minute (updated every second).

You can configure both session-based and dynamic brute force protection.

#### Session-based mitigation

Counts the number of failed login attempts that occur during one session, based on a session cookie. When the number of login attempts during a session exceeds the number specified, the system triggers the Brute Force: Maximum login attempts are exceeded violation, and applies the blocking policy. If the violation is set to block and too many login attempts are made, the client is blocked for a number of seconds.

#### Dynamic mitigation

Detects and mitigates brute force attacks based on statistical analysis of the traffic. You configure dynamic mitigation to determine when the system should consider the login URL to be under attack, and how to react to an attack. The system mitigates attacks when the volume of unsuccessful login attempts is significantly greater than the typical number of failed logins. You activate this method by setting the operation mode to either alarm or alarm and block.

### Overview: Mitigating brute force attacks

---

You can configure the Application Security Manager™ to protect against brute force attacks. The system detects brute force attacks based on failed login rates. Therefore, you need to create login pages for the web applications you want to protect.

#### Task Summary

*Creating login pages*

*Configuring brute force protection*

*Viewing brute force attack reports*

*Displaying brute force event logs*

### Creating login pages

In your security policy, you can create a login page to specify a login URL that presents a site that users must pass through to gain access to the web application. The login URL commonly leads to the login page of the web application.

1. On the Main tab, click **Security > Application Security > Sessions and Logins**.



The Login Pages List screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Login Page screen opens.
4. For the **Login URL** setting, specify a URL that users must pass through to get to the application.
  - a) From the list, select the type of URL: **Explicit** or **Wildcard**.
  - b) Select either **HTTP** or **HTTPS** based on the type of traffic the web application accepts.
  - c) Type an explicit URL or wildcard expression in the field.  
When you click in the field, the system lists URLs that it has seen, and you can select a URL from the list. Or, you can type explicit URLs in the format `/login`, and wildcard URLs without the slash, such as `*.php`.

5. From the **Authentication Type** list, select the method the web server uses to authenticate the login URL's credentials with a web user.

Option	Description
<b>None</b>	The web server does not authenticate users trying to access the web application through the login URL. This is the default setting.
<b>HTML Form</b>	The web application uses a form to collect and authenticate user credentials. If using this option, you also need to type the user name and password parameters written in the code of the HTML form.
<b>HTTP Basic Authentication</b>	The user name and password are transmitted in Base64 and stored on the server in plain text.
<b>HTTP Digest Authentication</b>	The web server performs the authentication; user names and passwords are not transmitted over the network, nor are they stored in plain text.
<b>NTLM</b>	Microsoft LAN Manager authentication (also called Integrated Windows Authentication) does not transmit credentials in plain text, but requires a continuous TCP connection between the server and client.

6. In the Access Validation area, define at least one validation criteria for the login page response.  
If you define more than one validation criteria, the response must meet all the criteria before the system allows the user to access the application login URL.

---

**Note:** The system checks the access validation criteria on the response of the login URL only if the response has one of the following content-types: `text/html`, `text/xml`, `application/sgml`, `application/xml`, `application/html`, `application/xhtml`, `application/x-asp`, and `application/x-aspix`.

---

7. Click **Create** to add the login page to the security policy.  
The new login page is added to the login pages list.
8. Add as many login pages as needed for your web application.
9. In the editing context area, click **Apply Policy** to put the changes into effect.

The security policy now has one or more login pages associated with it.

You can now configure how the login pages are enforced, including the authentication URLs, logout URLs, and whether or not the login pages have time limits.

## Configuring brute force protection

You can add brute force protection to a security policy to prevent hackers from gaining access to a web application by performing multiple login attempts.

1. On the Main tab, click **Security > Application Security > Anomaly Detection > Brute Force Attack Prevention**.

The Brute Force Attack Prevention screen opens where you can specify the login URLs that you want to protect against brute force attacks.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click the **Create** button.  
The New Brute Force Protection Configuration screen opens.
4. For the **Login Page** setting, select a previously created login page from the list (or create a new one).  
The login page specifies the URL that you want to protect against brute force attacks. If you need to create a login page in the security policy, click the **Create** button.
5. For the **IP Address Whitelist** setting, add the IP addresses and subnets from which traffic is known to be safe.

---

**Important:** The system adds any whitelist IP addresses to the centralized IP address exceptions list. The exceptions list is common to both brute force prevention and web scraping detection configurations.

---

6. In the Session-based Brute Force Protection area, for the **Login Attempts From The Same Client** setting, type the number of times a user can attempt to log in before the system blocks the request.  
The default value is 5.

---

**Note:** If you want the system to block brute force attacks, the Maximum login attempts are exceeded violation must be set to block. It is set to block by default. The enforcement mode must also be set to blocking.

---

7. For **Re-enable Login After**, type the number of seconds the user must wait to attempt to log in after they have been blocked.  
The default value is 600 seconds.
8. Above the Session-based Brute Force Protection area, click the **Blocking Settings** link to verify that the Maximum login attempts are exceeded violation is set to block, and the enforcement mode is set to blocking.
9. In the Dynamic Brute Force Protection area, for **Operation Mode**, select how the system handles dynamic brute force attacks.

Option	Description
<b>Off</b>	The system does not check for brute force attacks.
<b>Alarm</b>	The system logs brute force attack data.
<b>Alarm and Block</b>	In addition to logging the attack data, the system drops requests from the offending IP address, or requests to attacked URLs, depending on your configuration.

10. For the **Detection Criteria** setting, specify when to consider login attempts to be an attack.

Option	Description
<b>Minimum Failed Login Attempts</b>	Indicates an attack if, for all IP addresses tracked, the number of login attempts is equal to, or greater than, this number. This setting prevents false positive attack detection. The default value is 20 login attempts per second.
<b>Failed Logins Attempts increased by</b>	Indicates an attack if, for all IP addresses tracked, the ratio between the detection interval and the history interval is greater than this number. The default value is 500 %.
<b>Failed Login Attempts Rate reached</b>	The system considers unsuccessful login attempts to be an attack if, for all IP addresses tracked, the login attempt rate reaches this number. The default value is 100 login attempts per second.

An attack occurs if one of the first two conditions is met, or if the **Failed Login Attempts Rate reached** number is met).

11. For **Suspicious Criteria (per IP address)**, specify how to identify a potential attacker's IP address. If at least one of the criteria is met, the system treats the IP address as an attacker, and prevents the attacker from trying to guess the password. The system also limits the number of login attempts to the normal level.
- a) Type a number for **Failed Login Attempts increased by** criteria. An individual IP address is suspicious if the number of login attempts has increased by this percentage over the normal number of failed logins. The default setting is 500 percent.
  - b) Type a number for **Failed Login Attempts Rate reached**. An individual IP address is suspicious if the number of login attempts per second from that IP address is equal to or greater than this number. The default setting is 20 login attempts per second.

If either of these numbers is reached, the system limits the number of login attempts to the history interval.

12. For the **Prevention Policy** setting, select one or more options to determine how you want the system to handle a brute force attack.

---

*Note: If you enable more than one option, the system uses the options in the order in which they are listed.*

---

Option	Description
<b>Source IP-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious IP addresses are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. The default is disabled.
<b>URL-Based Client-Side Integrity Defense</b>	Determines whether a client is a legal browser or an illegal script by injecting JavaScript into responses when suspicious URLs are requested. Legal browsers can process JavaScript and respond properly, whereas illegal scripts cannot. The default is disabled.
<b>Source IP-Based Rate Limiting</b>	Drops requests from suspicious IP addresses. The system limits the rate of requests to the average rate prior to the attack, or lower than the absolute threshold specified by the IP detection TPS reached setting. The default is enabled.
<b>URL-Based Rate Limiting</b>	Indicates that when the system detects a URL under attack, Application Security Manager™ drops connections to limit the rate of requests to the URL to the average rate prior to the attack. The default is enabled.

13. For **Prevention Duration**, specify how long the system should mitigate brute force attacks.
  - To perform attack prevention until the end of the attack, select **Unlimited**.
  - To limit attack prevention to the amount of time configured here (even if the attack continues) or until the system detects the end of the attack, select **Maximum** and type the number of seconds to perform attack prevention.
14. To add brute force protection to the security policy, click **Create**.  
The screen refreshes, and you see the protected login URL in the list.
15. To put the security policy changes into effect immediately, click **Apply Policy**.

## Viewing brute force attack reports

Before you can look at the brute force attack statistics, you need to have configured session-based or dynamic brute force protection.

You can display charts that show information about brute force attacks. The charts provide visibility into what applications are being attacked, the login URL, and start and end times of an attack.

1. On the Main tab, click **Security > Reporting > Application > Brute Force Attacks**.  
The Brute Force Attacks reporting screen opens.
2. From the **Time Period** list, select the time period for which you want to view information about brute force attacks.
3. To focus in on the specific details you want more information about, point to the chart or click it.  
The system displays information about the item.
4. If you want to export the report to a file or send it by email, click **Export** and select the options.  
To send reports by email, you need to specify an SMTP configuration (**System > Configuration > Device > SMTP**).

You can continue to review the details about brute force attacks on the report screen. As a result, you become more familiar with what caused the attacks and what applications are most vulnerable, and you see the mitigation methods that are in place.

## Displaying brute force event logs

You can display event logs to see whether brute force attacks have occurred, and view information about the attacks.

1. On the Main tab, click **Security > Event Logs > Application > Brute Force Attacks**.  
The Brute Force Attacks event log opens.
2. If the log is long, use the **Security Policy** and/or **Time Period** settings to filter the list and show more specific entries.
3. Review the list of brute force attacks to see which security policy detected the attack, which login URLs were attacked, and the start and end times of the attack.

---

# Chapter 4

---

## Detecting and Preventing Web Scraping

---

- *Overview: Detecting and preventing web scraping*
  - *Implementation Result*
-

### Overview: Detecting and preventing web scraping

---

*Web scraping* is a technique for extracting information from web sites that often uses automated programs, or bots (short for web robots), opening many sessions, or initiating many transactions. You can configure Application Security Manager™ (ASM) to detect and prevent various web scraping activities on web sites that it is protecting.

ASM™ provides the following methods to address web scraping attacks. These methods can work independently of each other, or they can work together to detect and prevent web scraping attacks.

- *Bot detection* investigates whether a web client source is human by limiting the number of page changes allowed within a specified time.
- *Session opening* detects an anomaly when either too many sessions are opened from an IP address or when the number of sessions exceeds a threshold from an IP address. Also, session opening can detect an attack when the number of inconsistencies or session resets exceeds the configured threshold within the defined time period. This method also identifies as an attack an open session that sends requests that do not include an ASM cookie.
- *Session transactions anomaly* captures sessions that request too much traffic, compared to the average amount observed in the web application. This is based on counting the transactions per session and comparing that to the average amount observed in the web application.
- *Fingerprinting* captures information about browser attributes in order to identify a client. It is used when the system fails to detect web scraping anomalies by using IP addresses, ASM cookies, or persistent device identification.
- *Suspicious clients* used together with fingerprinting, specifies how the system identifies and protects against potentially malicious clients; for example, by detecting scraper extensions installed in a browser.

The BIG-IP® system can accurately detect web scraping anomalies only when response caching is turned off.

#### Task Summary

*Adding allowed search engines*

*Detecting web scraping based on bot detection*

*Detecting web scraping based on session opening*

*Detecting web scraping based on session transactions*

*Using fingerprinting to detect web scraping*

*Displaying web scraping event logs*

*Viewing web scraping statistics*

### Prerequisites for configuring web scraping

For web scraping detection to work properly, you should understand the following prerequisites:

- The web scraping mitigation feature requires that the DNS server is on the DNS lookup server list. Go to **System > Configuration > Device > DNS** to see if the DNS lookup server is on the list. If not, add it and restart the system.
- Client browsers need to have JavaScript enabled, and support cookies for anomaly detection to work.
- Consider disabling response caching. If response caching is enabled, the system does not protect cached content against web scraping.
- The Application Security Manager™ does not perform web scraping detection on legitimate search engine traffic. If your web application has its own search engine, we recommend that you add it to the system.

Go to **Security > Options > Application Security > Advanced Configuration > Search Engines**, and add it to the list.

## Adding allowed search engines

The Application Security Manager™ does not perform web scraping detection on traffic from search engines that the system recognizes as being legitimate. You can add other legitimate search engines to the search engines list.

1. On the **Main** tab, click **Security > Options > Application Security > Advanced Configuration > Search Engine**.

The Search Engines screen opens.

2. Click **Create**.

The New Search Engine screen opens.

3. In the **Search Engine** field, type the name.

4. In the **Bot Name** field, type the search engine bot name, such as `googlebot`.

---

**Tip:** You can get this name from the user-agent header of a request that the search engine sends.

---

5. In the **Domain Name** field, type the search engine crawler's domain name; for example, `yahoo.net`.

6. Click **Create**.

---

**Note:** For this feature to work, the DNS server must be on the DNS lookup server list on the BIG-IP® system (**System > Configuration > Device > DNS**). The system uses reverse DNS lookup to verify search engine requests.

---

The system adds the search engine to the list.

The system does not perform web scraping detection on traffic originating from the search engines on the search engines list.

## Allowed search engines

By default, Application Security Manager™ allows requests from these well-known search engines and legitimate web robots:

- Ask (\*.ask.com)
- Bing (\*.msn.com)
- Google (\*.googlebot.com)
- Yahoo (\*.yahoo.net)

You can add other search engines to the allowed search engine list; for example, if your web application uses an additional search engine. The list applies globally to all security policies on the system for which web scraping detection is enabled.

## Detecting web scraping based on bot detection

You can mitigate web scraping on the web sites Application Security Manager™ defends by attempting to determine whether a web client source is human or a web robot. The bot detection method also protects web applications against rapid surfing by measuring the amount of time allowed to change a number of web pages before the system suspects a bot.

1. On the Main tab, click **Security > Application Security > Anomaly Detection > Web Scraping**. The Web Scraping screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Bot Detection** setting, select either **Alarm** or **Alarm and Block** to indicate how you want the system to react when it detects that a bot is sending requests to the web application.  
If you choose **Alarm and Block**, the security policy enforcement mode needs to be set to **Blocking** before the system blocks web scraping attacks.

---

***Note:** The system can accurately detect a human user only if clients have JavaScript enabled and support cookies in their browsers.*

---

The screen displays the Bot Detection tab and more settings.

4. If you plan to use fingerprinting to collect browser attributes, select the **Fingerprinting Usage** check box.  
The screen displays additional settings; a separate task explains how to configure fingerprinting.
5. If you want to protect client identification data (when using Bot Detection or Session Opening detection), specify the persistence settings.
  - a) Select the **Persistent Client Identification** check box.
  - b) For **Persistent Data Validity Period**, type how long you want the client data to persist in minutes.  
The default value is 120 minutes.

---

***Note:** This setting enforces persistent storage on the client and prevents easy removal of client data. Be sure that this behavior is compatible with the application privacy policy.*

---

The system maintains client data and prevents removal of this data from persistent storage for the validity period specified.

6. For the **IP Address Whitelist** setting, add the IP addresses and subnets from which traffic is known to be safe.

---

***Important:** The system adds any whitelist IP addresses to the centralized IP address exceptions list. The exceptions list is common to both brute force prevention and web scraping detection configurations.*

---

7. On the Bot Detection tab, for the **Rapid Surfing** setting, specify the maximum number of web pages that can be changed in the specified number of seconds before the system suspects a bot.  
The default value is **Maximum 5 page changes per 1000 milliseconds**.
8. For **Grace Interval**, type the number of requests to allow while determining whether a client is human.  
The default value is 100.
9. For **Unsafe Interval**, type the number of requests that cause the Web Scraping Detected violation if no human activity was detected during the grace period.  
The default value is 100.  
Reaching this interval causes the system to reactivate the grace period.
10. For **Safe Interval**, type the number of requests to allow after human activity is detected, and before reactivating the grace threshold to check again for non-human clients.  
The default value is 2000.
11. Click **Save** to save your settings.
12. To put the security policy changes into effect immediately, click **Apply Policy**.

The system checks for rapid surfing and if too many pages are changed too quickly, it logs Web Scraping detected violations in the event log, and specifies the attack type of bot detection.



After setting up bot detection, you can also set up fingerprinting, session opening and session transactions anomaly detection for the same security policy.

## Detecting web scraping based on session opening

You can configure how the system protects your web application against session opening web scraping violations that result from too many sessions originating from a specific IP address, inconsistencies detected in persistent storage, and when the number of session resets exceeds the threshold.

1. On the Main tab, click **Security > Application Security > Anomaly Detection > Web Scraping**. The Web Scraping screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Session Opening** setting, select either **Alarm** or **Alarm and Block** to indicate how you want the system to react when it detects a large increase in the number of sessions opened from a specific IP address, or when the number of session resets or inconsistencies exceeds the set threshold.  
If you choose **Alarm and Block**, the security policy enforcement mode needs to be set to **Blocking** before the system blocks web scraping attacks.  
The screen displays the Session Opening tab and more settings.
4. If you plan to use fingerprinting to collect browser attributes, select the **Fingerprinting Usage** check box.  
The screen displays additional settings; a separate task explains how to configure fingerprinting.
5. If you want to protect client identification data (when using Bot Detection or Session Opening detection), specify the persistence settings.
  - a) Select the **Persistent Client Identification** check box.
  - b) For **Persistent Data Validity Period**, type how long you want the client data to persist in minutes. The default value is 120 minutes.

---

**Note:** This setting enforces persistent storage on the client and prevents easy removal of client data. Be sure that this behavior is compatible with the application privacy policy.

---

The system maintains client data and prevents removal of this data from persistent storage for the validity period specified.

6. For the **IP Address Whitelist** setting, add the IP addresses and subnets from which traffic is known to be safe.

---

**Important:** The system adds any whitelist IP addresses to the centralized IP address exceptions list. The exceptions list is common to both brute force prevention and web scraping detection configurations.

---

7. To detect session opening anomalies by IP address, on the Session Opening tab, ensure that the **Session Opening Anomaly** check box is selected.
8. For the **Prevention Policy** setting, select one or more options to direct how the system should handle a session opening anomaly attack.

Option	Description
<b>Client Side Integrity Defense</b>	When enabled, the system determines whether a client is a legitimate browser or an illegal script by sending a JavaScript challenge to each new session request. Legitimate browsers can respond to the challenge; scripts cannot.
<b>Rate Limiting</b>	When enabled, the system drops sessions from suspicious IP addresses after determining that the client is an illegal script. If you select this option, the

Option	Description
	screen displays an option for dropping requests from IP addresses with a bad reputation.
<b>Drop IP Addresses with bad reputation</b>	This option is available only if you have enabled rate limiting. When enabled, the system drops requests originating from IP addresses that are in the system's IP address intelligence database when the attack is detected; no rate limiting will occur. (Attacking IP addresses that do not have a bad reputation undergo rate limiting, as usual.) You also need to set up IP address intelligence, and at least one of the IP intelligence categories must have its Alarm or Block flag enabled.

9. For the **Detection Criteria** setting, specify the criteria under which the system considers traffic to be a session opening anomaly attack.

Option	Description
<b>Sessions opened per second increased by</b>	The system considers traffic to be an attack if the number of sessions opened per second increased by this percentage. The default value is 500%.
<b>Sessions opened per second reached</b>	The system considers traffic to be an attack if the number of sessions opened per second is equal to or greater than this number. The default value is 50 sessions opened per second.
<b>Minimum sessions opened per second threshold for detection</b>	The system only considers traffic to be an attack if this value plus one of the sessions opened values is exceeded. The default value is 25 sessions opened per second.

---

***Note:** The **Detection Criteria** values all work together. The minimum sessions value and one of the sessions opened values must be met for traffic to be considered an attack. However, if the minimum sessions value is not reached, traffic is never considered an attack even if the **Sessions opened per second increased by** value is met.*

---

10. For **Prevention Duration**, type a number that indicates how long the system prevents an anomaly attack by logging or blocking requests. The default is 1800 seconds.

If the attack ends before this number of seconds, the system also stops attack prevention.

11. If you enabled **Persistent Client Identification** and you want to detect session opening anomalies based on inconsistencies, select the **Device Identification Integrity** check box, and set the maximum number of integrity faulty events to allow within a specified number of seconds.

The system tracks the number of inconsistent device integrity events within the time specified, and if too many events occurred within the time, a Web scraping detection violation occurs.

12. If you enabled **Persistent Client Identification** and you want to track cookie deletion events, in the **Cookie Deletion Detection** setting, specify how to detect cookie deletion. You can use either one or both options.

- To use persistent device identification to detect cookie deletion events, select the **Enabled by Persistent Device Identification** check box, and set the maximum number of cookie deletions to allow within a specified number of seconds.
- If you enabled **Fingerprinting Usage**, to use fingerprinting to detect cookie deletion events, select the **Enabled by Fingerprinting** check box, and set the maximum number of cookie deletions to allow within a specified number of seconds.

The system tracks the number of cookie deletion events that occur within the time specified, and if too many cookies were deleted within the time, a Web scraping detection violation occurs.

13. For **Prevention Duration**, type a number that indicates how long the system prevents an anomaly attack by logging or blocking requests. The default is 1800 seconds.

If the attack ends before this number of seconds, the system also stops attack prevention.

14. Click **Save** to save your settings.

15. To put the security policy changes into effect immediately, click **Apply Policy**.

The system checks for too many sessions being opened from one IP address, too many cookie deletions, and persistent storage inconsistencies depending on the options you selected. The system logs violations in the web scraping event log along with information about the attack including whether it is a Session Opening Anomaly by IP Address or Session Resets by Persistent Client Identification attack type and when it began and ended. The log also includes the type of violation (Device Identification Integrity or Cookie Deletion Detection) and the violation numbers.

After setting up bot detection, you can also set up fingerprinting, session opening and session transactions anomaly detection for the same security policy.

## Detecting web scraping based on session transactions

You can configure how the system protects your web application against harvesting, which is detected by counting the number of transactions per session and comparing that number to a total average of transactions from all sessions. Harvesting may cause session transaction anomalies.

1. On the Main tab, click **Security > Application Security > Anomaly Detection > Web Scraping**. The Web Scraping screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Session Transactions Anomaly** setting, select either **Alarm** or **Alarm and Block** to indicate how you want the system to react when it detects a large increase in the number of transactions per session.

If you choose **Alarm and Block**, the security policy enforcement mode needs to be set to **Blocking** before the system blocks web scraping attacks.

The screen displays the Session Transactions Anomaly tab and more settings.

4. For the **IP Address Whitelist** setting, add the IP addresses and subnets from which traffic is known to be safe.

---

**Important:** The system adds any whitelist IP addresses to the centralized IP address exceptions list. The exceptions list is common to both brute force prevention and web scraping detection configurations.

---

5. On the Session Transactions Anomaly tab, for the **Detection Criteria** setting, specify the criteria under which the system considers traffic to be a session transactions anomaly attack.

Option	Description
<b>Session transactions above normal by</b>	The system considers traffic in a session to be an attack if the number of transactions in the session is more than normal by this percentage (and minimum session value is met). Normal refers to the average number of transactions per session for the whole site during the last hour. The default value is 500%.
<b>Sessions transactions reached</b>	The system considers traffic to be an attack if the number of transactions per sessions is equal to or greater than this number (and minimum session value is met). The default value is 400 transactions.

Option	Description
<b>Minimum session transactions threshold for detection</b>	The system considers traffic to be an attack only if the number of transactions per session is equal to or greater than this number, and at least one of the sessions transactions numbers was exceeded. The default value is 200 transactions.

---

**Important:** The **Detection Criteria** values all work together. The minimum sessions value and one of the sessions transactions values must be met for traffic to be considered an attack. However, if the **Minimum session transactions threshold** is not reached, traffic is never considered an attack even if the **Sessions transactions above normal by** value is met.

---

- For **Prevention Duration**, type a number that indicates how long the system prevents an anomaly attack by logging or blocking requests. The default is 1800 seconds.  
If the attack ends before this number of seconds, the system also stops attack prevention.
- Click **Save** to save your settings.
- To put the security policy changes into effect immediately, click **Apply Policy**.

When the system detects a session that requests too many transactions (as compared to normal), all transactions from the attacking session cause the **Web Scraping detected** violation to occur until the end of attack or until the prevention duration expires.

After setting up bot detection, you can also set up fingerprinting, session opening and session transactions anomaly detection for the same security policy.

## Using fingerprinting to detect web scraping

Application Security Manager™ (ASM) can identify web scraping attacks on web sites that ASM™ protects by using information gathered about clients through fingerprinting or persistent identification. *Fingerprinting* is collecting browser attributes and saving the information in a special POST data parameter. The system can use the collected information to identify suspicious clients (potential bots) and recognize web scraping attacks more quickly.

- On the Main tab, click **Security > Application Security > Anomaly Detection > Web Scraping**.  
The Web Scraping screen opens.
- In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
- To have the system detect browsers and bots by collecting browser attributes, select the **Fingerprinting Usage** check box.  
The screen enables fingerprinting and displays the **Suspicious Clients** setting, which works together with the fingerprinting feature.
- If you want the system to detect suspicious clients using fingerprinting data, for the **Suspicious Clients** setting, select **Alarm and Block**.  
The system displays a new Suspicious Clients tab.
- To configure how the system determines which clients are suspicious, adjust the setting on the Suspicious Clients tab:
  - For the **Scraping Plugins** setting, select the **Detect browsers with Scraping Extensions** check box, and move the browser extensions you do not want to allow to the **Disallowed Extensions** list.  
If ASM detects a browser with a disallowed extension, the client is considered suspicious, and ASM logs and blocks requests from this client to the web application.

- b) In the **Prevention Duration** field, type the number of seconds for which the system prevents requests from a client after ASM determines it to be suspicious.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The system now collects browser attributes to help with web scraping detection. If you also enabled the **Suspicious Clients** setting, when the system detects clients that may be web scraping attempts using information obtained by fingerprinting, the system records the attack data, and blocks the suspicious requests.

In addition to using fingerprinting, you can also set up bot detection, session opening, and session transactions anomaly detection for the same security policy.

## Displaying web scraping event logs

You can display event logs to see whether web scraping attacks have occurred, and view information about the attacks.

1. On the Main tab, click **Security > Event Logs > Application > Web Scraping Statistics**.  
The Web Scraping Statistics event log opens.
2. If the log is long, you can filter the list by security policy and time period to show more specific entries.
3. Review the list of web scraping attacks to see the web scraping attack type that occurred, the IP address of the client that caused the attack, which security policy detected the attack, and the start and end times of the attack.
4. Examine the web scraping statistics shown, and click the attack type links to see what caused the attack.
5. To learn more about the requests that caused the web scraping attack, click the number of violating requests.  
The Requests screen opens where you can investigate the requests that caused the web scraping attacks.

## Web scraping attack examples

This figure shows a Web Scraping Statistics event log on an Application Security Manager™ (ASM) system where several web scraping attacks, with different attack types, have occurred.

Attack Type	Client IP Address	Security Policy	Start Time	End Time	Rejected Requests	Violating Requests
Bot detected	172.29.71.52	vs_103	2013-11-18 16:27:14	2013-11-18 16:29:58	0	3
Bot detected	172.29.71.52	vs_103	2013-11-18 16:31:01	2013-11-18 16:33:50	0	4
Bot detected	172.29.71.52	vs_103	2013-11-18 16:34:20	2013-11-18 16:38:00	0	9
Bot detected	172.29.71.52	vs_103	2013-11-18 16:44:58	2013-11-18 16:47:21	0	4
Bot detected	172.29.71.52	vs_103	2013-11-18 16:48:47	2013-11-18 16:54:07	0	13
Session Resets by Persistent Client Identification	172.29.71.52	vs_104	2013-11-18 16:53:49	2013-11-18 16:55:54	0	4
Session Resets by Persistent Client Identification	172.29.71.52	vs_104	2013-11-18 16:58:19	2013-11-18 17:00:22	0	7
Suspicious Clients	172.29.71.51	vs_106	2013-11-18 17:03:40	2013-11-18 17:08:30	0	41
Suspicious Clients	172.29.71.51	vs_106	2013-11-18 17:04:57	2013-11-18 17:07:02	1	4
Suspicious Clients	192.168.167.220	vs_106	2013-11-18 17:07:16	2013-11-18 17:09:45	0	4
Suspicious Clients	172.29.71.51	vs_106	2013-11-18 17:08:46	2013-11-18 17:12:34	0	21
Suspicious Clients	192.168.167.220	vs_106	2013-11-18 17:10:05	2013-11-18 17:12:27	0	4
Bot detected	172.29.70.172	vs_103	2013-11-18 17:23:35	2013-11-18 17:27:15	0	21
Bot detected	172.29.70.172	vs_103	2013-11-18 17:28:54	2013-11-18 17:31:31	0	12
Transactions per session anomaly	172.29.70.172	vs_103	2013-11-18 17:29:00	2013-11-18 17:40:00	N/A	54
Bot detected	172.29.70.172	vs_103	2013-11-18 17:59:05	2013-11-18 18:01:07	11	0

**Figure 4: Web scraping statistics event log**

The next figure shows details on a web scraping attack started on November 17 at 7:14PM. The attack type was Session Resets by Persistent Client Identification, and it occurred when the number of cookie deletions detected through the use of fingerprinting exceeded the configured threshold.

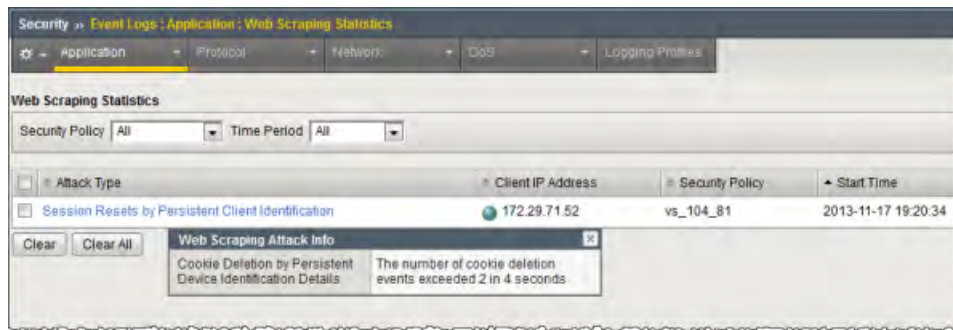
Attack Type	Client IP Address	Security Policy	Start Time
Session Resets by Persistent Client Identification	172.29.71.52	vs_104_81	2013-11-17 19:14:11

Cookie Deletion by Fingerprinting Usage Details	The number of cookie deletion events exceeded 2 in 38 seconds
Scraping Extensions	Scrape
Language	ru
Time Zone	GMT +8:00
Number of restored sessions by Fingerprinting	2

**Figure 5: Example cookie deletion attack (fingerprinting)**

The next figure shows details on a web scraping attack started on November 17 at 7:20PM. The attack type was Session Resets by Persistent Client Identification. It occurred when the number of cookie deletions detected through the use of persistent client identification exceeded the configured threshold (more than 2 in 4 seconds).



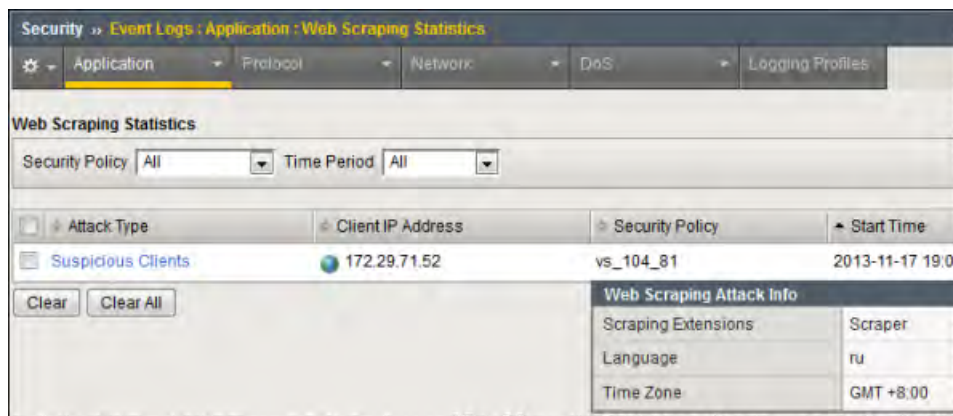
**Figure 6: Example cookie deletion attack (persistent client ID)**

The next figure shows details on a web scraping attack started on November 17 at 7:24PM. The attack type was Session Resets by Persistent Client Identification. It occurred when the number of integrity fault events detected through the use of persistent client identification exceeded the configured threshold (more than 3 in 25 seconds).



**Figure 7: Example device ID integrity attack**

The next figure shows details on a suspicious clients attack that occurred when a client installed the disallowed Scraper browser plug-in.



**Figure 8: Example disallowed plug-in attack**

## Web scraping attack types

Web scraping statistics specify the attack type so you have more information about why the attack occurred. This shows the web scraping attack types that can display in the web scraping event log.

Attack Type	Description
Bot activity detected	Indicates that there are more JavaScript injections than JavaScript replies. Click the attack type link to display the detected injection ratio and the injection ratio threshold.  <i>Note: You cannot configure the Bot activity detected ratio values. This attack type can occur only when the security policy is in Transparent mode.</i>
Bot Detected	Indicates that the system suspects that the web scraping attack was caused by a web robot.
Session Opening Anomaly by IP	Indicates that the web scraping attack was caused by too many sessions being opened from one IP address. Click the attack type link to display the number of sessions opened per second from the IP address, the number of legitimate sessions, and the attack prevention state.
Session Resets by Persistent Client Identification	Indicates that the web scraping attack was caused by too many session resets or inconsistencies occurring within a specified time. Click the attack type link to display the number of resets or inconsistencies that occurred within a number of seconds.
Suspicious Clients	Indicates that the web scraping attack was caused by web scraping extensions on the browser. Click the attack type link to display the scraping extensions found in the browser.
Transactions per session anomaly	Indicates that the web scraping attack was caused by too many transactions being opened during one session. Click the attack type link to display the number of transactions detected on the session.

## Viewing web scraping statistics

Before you can look at the web scraping attack statistics, you need to have configured web scraping protection.

You can display charts that show information about web scraping attacks that have occurred against protected applications.

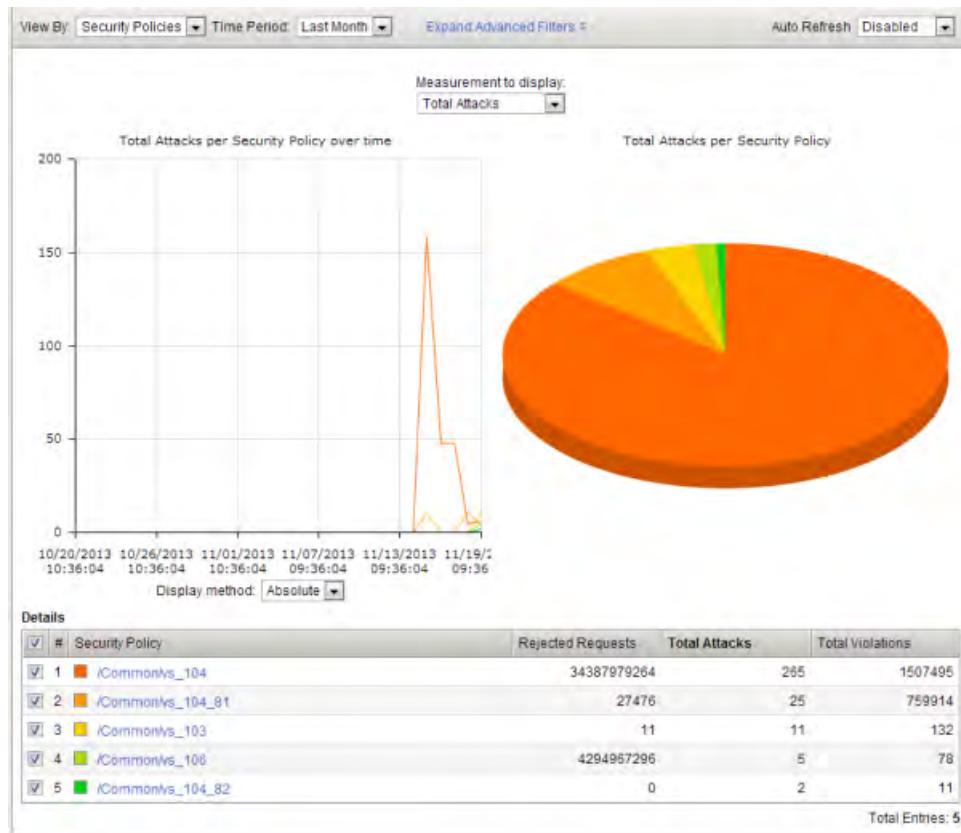
1. On the Main tab, click **Security > Reporting > Application > Web Scraping Statistics**. The Web Scraping Statistics screen opens.
2. From the **Time Period** list, select the time period for which you want to view information about web scraping attacks.
3. If you want to export the report to a file or send it by email, click **Export** and select the options. To send reports by email, you need to specify an SMTP configuration (**System > Configuration > Device > SMTP**).

The statistics show the total number of web scraping attacks, violations and rejected requests that occurred. You can review the details about the attacks and see that mitigation is in place.

## Web scraping statistics chart

This figure shows a Web Scraping Statistics chart on an Application Security Manager™ (ASM) test system where many web scraping attacks occurred during a short period of time.





**Figure 9: Web scraping statistics chart**

You can use this chart to see the number of rejected requests, web scraping attacks, and total violations that occurred on the web applications protected using the five security policies listed at the bottom.

## Implementation Result

When you have completed the steps in this implementation, you have configured the Application Security Manager™ to protect against web scraping. Depending on your configuration, the system detects web scraping attacks based on bot detection, session opening violations, session transaction violations, and fingerprinting.

After traffic is flowing to the system, you can check whether web scraping attacks are being logged or prevented, and investigate them by viewing web scraping event logs and statistics.

If fingerprinting is enabled, the system uses browser attributes to help with detecting web scraping. If using fingerprinting with suspicious clients set to alarm and block, the system collects browser attributes and blocks suspicious requests using information obtained by fingerprinting.

If you chose alarm and block for the web scraping configuration and the security policy is in the blocking operation mode, the system drops requests that cause the Web scraping detected violation. If you chose alarm only (or the policy is in the transparent mode), web scraping attacks are logged only but not blocked.



---

# Chapter

# 5

---

## Setting Up IP Address Intelligence Blocking

---

- *Overview: Setting up IP address intelligence blocking*
- *IP address intelligence categories*

## Overview: Setting up IP address intelligence blocking

---

In Application Security Manager™, you can use IP address intelligence blocking in a security policy to block requests from IP addresses that have questionable reputations. IP addresses from which attacks or spam have originated are included in an IP intelligence database, along with the category describing the problem. The BIG-IP® system must connect to the IP intelligence database before you can use IP address intelligence blocking.

You can configure a security policy to log (alarm) or block requests from IP addresses of questionable reputation, and to perform different actions depending on the categories of problems. For example, you can block requests from IP addresses associated with Windows exploits and log requests from scanners.

You can create a whitelist of IP addresses that might be in the database, and allow them to access the web application regardless of their IP reputation. This is a way to ensure that traffic from known sources is not blocked because of IP address intelligence data.

You can also use iRules to instruct the system how to use IP address intelligence information.

### Task summary

*Enabling IP address intelligence*

*Setting up IP address intelligence blocking*

*Reviewing IP address intelligence statistics*

*Creating an iRule to log IP address intelligence information*

*Creating an iRule to reject requests with questionable IP addresses*

## Enabling IP address intelligence

The requirements for using IP address intelligence are:

- The system must have an IP Intelligence license.
- The system must have an Internet connection either directly or through an HTTP proxy server.
- The system must have DNS configured (go to **System > Configuration > Device > DNS**).

---

**Important:** IP address intelligence is enabled by default. You only need to enable it if it was previously disabled.

---

To enable IP address intelligence on the BIG-IP® system, you enable auto-update to connect the system to the IP intelligence database.

1. Log in to the command line for the BIG-IP® system.
2. To determine whether IP intelligence is enabled, type the following command: `tmsh list sys db iprep.autoupdate`  
If the value of the `iprep.autoupdate` variable is `disable`, IP intelligence is not enabled. If it is `enable`, your task is complete.
3. At the prompt, type `tmsh modify sys db iprep.autoupdate value enable`  
The system downloads the IP intelligence database and stores it in the binary file, `/var/IpRep/F5IpRep.dat`. It is updated every 5 minutes.
4. If the BIG-IP system is behind a firewall, make sure that the BIG-IP system has external access to `vector.brightcloud.com` using port 443.

That is the IP Intelligence server from which the system gets IP Intelligence information.

5. (Optional) If the BIG-IP system connects to the Internet using a forward proxy server, set these system database variables.
  - a) Type `tmsh modify sys db proxy.host value hostname` to specify the host name of the proxy server.
  - b) Type `tmsh modify sys db proxy.port value port_number` to specify the port number of the proxy server.
  - c) Type `tmsh modify sys db proxy.username value username` to specify the user name to log in to the proxy server.
  - d) Type `tmsh modify sys db proxy.password value password` to specify the password to log in to the proxy server.

The IP address intelligence feature remains enabled unless you disable it with the command `tmsh modify sys db iprep.autoupdate value disable`.

You can create iRules® to instruct the system how to handle traffic from IP addresses with questionable reputations, or use Application Security Manager™ to configure IP address intelligence blocking.

## Setting up IP address intelligence blocking

You can configure a security policy to log and block requests from source IP addresses that, according to an IP intelligence database, have a bad reputation and could cause a potential attack.

1. On the Main tab, click **Security > Application Security > IP Addresses > IP Address Intelligence**. The IP Address Intelligence screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select the **IP Address Intelligence** check box. The screen refreshes, and displays additional configuration options.
4. For the **IP Address Whitelist** setting, specify any IP addresses you want to allow, even if they are found in the IP intelligence database.
  - a) Type the **IP Address** and **Subnet Mask** of the address to consider safe.
  - b) Click **Add**.

The system updates the whitelist with the new IP addresses.

5. In the IP Address Intelligence Categories area, select **Alarm** or **Block**, or both, for the categories of IP addresses you are interested in.
  - Select **Alarm** to cause the system to log the IP address intelligence data (IP address intelligence category and status) on the Requests screen whenever a request is from a source IP address in that category.
  - Select **Block** to stop requests sent from a source IP address that matches that category

---

**Tip:** To select all categories at once, click the *Alarm* or *Block* column name check boxes.

---

6. Click **Save**.

The system matches source IP addresses to those in the IP address intelligence database. When a match is found, the violation `Access from malicious IP address` occurs. The system determines what category of reputation the IP address has, then logs or blocks the IP address according to how the IP Address Intelligence categories are set.

### Reviewing IP address intelligence statistics

After you set up IP intelligence blocking on the Application Security Manager™, you can review statistics concerning how many requests were received from IP addresses with questionable reputations. You can also view the requests from those IP addresses.

1. On the Main tab, click **Security > Reporting > Application**.  
The Charts screen opens.
2. In the Charts area, next to **View by**, click **IP Address Intelligence**.  
The chart shows details about IP addresses that were used to send the illegal requests, grouped according to their reputation in the IP intelligence database.
3. Hover over the pie chart or look at the Details table below it to see the categories of IP addresses with questionable reputations.
4. Under Chart Path on the left, click **View Requests** to see the requests from IP addresses in the IP intelligence database.  
The Requests list opens.
5. Click any request to view details about the request.  
The screen expands to show more information about the request. IP address intelligence information is shown in the **Source IP Address** field in the request details. The details include the category of the malicious IP address and information about when the IP intelligence database was last updated.
6. If you have set up remote logging, you can also review IP intelligence data on the remote logger.

Based on the statistics and IP address intelligence categories that the IP addresses fall into, you can adjust what happens (alarm or block) when the system receives requests from IP addresses in different categories.

### Creating an iRule to log IP address intelligence information

Before you can create an iRule to log IP address intelligence information, your system must have IP address intelligence enabled.

You use iRules® to log IP address intelligence categories to the file `/var/log/ltm`. This is an example of the type of iRule you can write.

1. On the Main tab, click **Local Traffic > iRules**.  
The iRule List screen opens, displaying any existing iRules.
2. Click **Create**.  
The New iRule screen opens.
3. In the **Name** field, type a name between 1 and 31 characters, such as `my_iRule`.
4. In the **Definition** field, type the iRule using Tool Command Language (Tcl) syntax.  
For example, to log all IP addresses and any associated IP address intelligence categories, type the following iRule:

```
when CLIENT_ACCEPTED {  
    log local0. "IP Address Intelligence for IP address  
[IP::client_addr]:  
    [IP::reputation [IP::client_addr]]"  
}
```

---

**Tip:** For complete and detailed information iRules syntax, see the F5 Networks DevCentral web site (<http://devcentral.f5.com>).

---

**5. Click **Finished**.**

The new iRule appears in the list of iRules on the system.

When traffic is received from an IP address with a questionable reputation and that is included in the IP intelligence database, the system prints the IP address intelligence information in the `/var/log/ltm` log.

For complete and detailed information about iRules syntax, see the F5 Networks DevCentral web site, <http://devcentral.f5.com>.

## Creating an iRule to reject requests with questionable IP addresses

Before you can create an iRule to reject requests based on an IP address reputation, your system must have IP address intelligence enabled.

You can use iRules® to reject requests from IP addresses that have questionable reputations and are listed in the IP intelligence database. This is an example of the type of iRule you can write.

**1. On the Main tab, click **Local Traffic** > **iRules**.**

The iRule List screen opens, displaying any existing iRules.

**2. Click **Create**.**

The New iRule screen opens.

**3. In the **Name** field, type a name between 1 and 31 characters, such as `my_iRule`.****4. In the **Definition** field, type the iRule using Tool Command Language (Tcl) syntax.**

For example, to reject requests from IP addresses listed in the IP intelligence database because they could be Windows Exploits or Web Attacks, type the following iRule:

```
when HTTP_REQUEST {
    set ip_reputation_categories [IP::reputation [IP::client_addr]]
    set is_reject 0
    if {($ip_reputation_categories contains "Windows Exploits")} {
        set is_reject 1
    }
    if {($ip_reputation_categories contains "Web Attacks")} {
        set is_reject 1
    }
    if {($is_reject)} {
        log local0. "Attempted access from malicious IP address
[IP::client_addr]
($ip_reputation_categories), request was rejected"
        HTTP::respond 200 content
        "<HTML><HEAD><TITLE>Rejected Request</TITLE>
</HEAD><BODY>The request was rejected. <BR>
Attempted access from malicious IP address</BODY></HTML>"
    }
}
```

---

**Tip:** For complete and detailed information about iRules syntax, see the F5 Networks DevCentral web site (<http://devcentral.f5.com>).

---

**5. Click **Finished**.**

The new iRule appears in the list of iRules on the system.

When the system receives traffic from an IP address that is included in the IP intelligence database, the system prints the IP address intelligence information in the `/var/log/ltm` log.

## IP address intelligence categories

Along with the IP address, the IP intelligence database stores the category that explains the reason that the IP address is considered untrustworthy.

Category Name	Description
Botnets	IP addresses of computers that are infected with malicious software (Botnet Command and Control channels, and infected zombie machines) and are controlled as a group by a Bot master, and are now part of a botnet. Hackers can exploit botnets to send spam messages, launch various attacks, or cause target systems to behave in other unpredictable ways.
Cloud Provider Networks	IP addresses and networks that are used by cloud providers.
Denial-of-Service	IP addresses that have launched denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, anomalous SYN flood attacks, or anomalous traffic detection. These attacks are usually requests for legitimate services, but occur at such a fast rate that targeted systems cannot respond quickly enough and become bogged down or unable to service legitimate clients.
Illegal Web sites	IP addresses that contain criminally obscene or potentially criminal internet copyright and intellectual property violations.
Infected Sources	Active IP addresses that issue HTTP requests with a low reputation index score, or that are known malicious web sites offering or distributing malware, shell code, rootkits, worms, or viruses.
Phishing	IP addresses that host phishing sites, and other kinds of fraud activities, such as ad click fraud or gaming fraud.
Proxy/Anonymous Proxies	IP addresses that are associated with web proxies that shield the originator's IP address (such as proxy and anonymization services). This category also includes TOR anonymizer addresses.
Scanners	IP addresses that are involved in reconnaissance, such as probes, host scan, domain scan, and password brute force, typically to identify vulnerabilities for later exploits.
Spam Sources	IP addresses that are known to distribute large amounts of spam email by tunneling spam messages through proxy, anomalous SMTP activities, and forum spam activities.
Web Attacks	IP addresses involved in cross site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force.
Windows Exploits	Active IP addresses that have exercised various exploits against Windows resources by offering or distributing malware, shell code, rootkits, worms, or viruses using browsers, programs, downloaded files, scripts, or operating system vulnerabilities.



---

# Chapter 6

---

## Managing IP Address Exceptions

---

- *Overview: Managing IP address exceptions* |

## Overview: Managing IP address exceptions

---

An *IP address exception* is an IP address that you want the system to treat in a specific way for a security policy. For example, you can specify IP addresses from which the system should always trust traffic, IP addresses for which you do not want the system to generate learning suggestions for the traffic, and IP addresses for which you want to exclude information from the logs. You can use the IP address exception feature to create exceptions for IP addresses of internal tools that your company uses, such as penetration tools, manual or automatic scanners, or web scraping tools. You can add an IP address exception, and instruct the system how to handle traffic coming from that address.

You can view a centralized list of IP address exceptions, and you can add new IP address exceptions to the list. The list of IP address exceptions shows exceptions that you add directly to the list, or those which you add from other locations, as shown by the following examples:

- When creating a security policy, you can specify IP addresses that you want the Policy Builder to always trust.
- When creating a security policy that is integrated with a vulnerability assessment tool, you can configure the scanner IP address as an IP address exception.
- When setting up anomaly detection (such as for DoS, brute force, and web scraping protections), you can specify IP addresses that the system should consider legitimate (called *whitelists*).
- When setting up IP address intelligence, you can add IP addresses that the system should allow even if the IP address is in the IP intelligence database.

The IP Address Exceptions list shows in one location all of the IP exceptions configured for this security policy. You can view or modify IP exceptions both from the centralized IP exception list and from the specific feature screens.

This implementation describes how to create, delete, and update the list of IP address exceptions.

## Creating IP address exceptions

For each security policy, you can create a list of IP address exceptions, and indicate how you want the system to handle the traffic from these IP addresses.

1. On the Main tab, click **Security > Application Security > IP Addresses > IP Address Exceptions**. The IP Address Exceptions screen opens, and displays a centralized list of configured IP address exceptions.
2. Click **Create**. The New IP Address Exception screen opens.
3. In the **IP Address** field, type the IP address that you want the system to trust.

---

***Note:** To add a route domain, type %n after the IP address where n is the route domain identification number.*

---

4. In the **Netmask** field, type the netmask of the IP address exception.  
If you omit the netmask value, the system uses a default value of 255.255.255.255.
5. To consider traffic from this IP address as being safe, for the **Policy Builder trusted IP** setting, select **Enabled**.  
The system adds this IP address to the **Trusted IP Addresses** setting on the Automatic Configuration screen for the Policy Builder.

6. To ignore this IP address when performing DoS, brute force, and web scraping detection, for the **Ignore in Anomaly Detection** setting, select **Enabled**.  
The system adds this IP address to the **IP Address Whitelist** setting on the anomaly detection screens for DoS attacks, brute force, and web scraping.
7. If you do not want the system to generate learning suggestions for traffic sent from this IP address, for the **Ignore in Learning Suggestions** setting, select **Enabled**.

---

***Note:** Application Security Manager does not generate learning suggestions for requests that result in the web server returning HTTP responses with 400 or 404 status codes unless the security policy is configured to learn and block traffic (here both the **Ignore in Learning Suggestions** check box and the **Never block this IP Address** check box need to be disabled).*

---

8. To never block traffic from this IP address, for the **Never block this IP Address** setting, select **Enabled**.  
If the check box is cleared, a system in blocking mode blocks requests sent from this IP address according to the violation settings on the Policy Blocking Settings screen.
9. To prevent the system from logging requests (either legal or illegal) from this IP address, for the **Never log requests from this IP** setting, select **Enabled**.
10. To consider traffic from this IP address to be legitimate even if it is found in the IP Intelligence database, for the **Ignore IP Intelligence** setting, select **Enabled**.  
The system adds this IP address to the **IP Address Whitelist** setting on the IP Address Intelligence screen.
11. Click **Create**.  
The IP Address Exceptions screen opens and shows all of the exceptions configured for the security policy including the one you created.

You can view and manage all of your IP address exceptions from the centralized IP Address Exceptions screen.

## Deleting IP address exceptions

If you no longer want an IP address on the exceptions list, you can delete the IP address exceptions.

1. On the Main tab, click **Security > Application Security > IP Addresses > IP Address Exceptions**.  
The IP Address Exceptions screen opens, and displays a centralized list of configured IP address exceptions.
2. Select the IP address exception you want to delete and click **Delete**.  
The IP address exception is deleted from the list.
3. You can also delete IP address exceptions from the anomaly detection whitelists, the IP address intelligence whitelist, and the policy building configuration. On any of these screens, select the IP address, and click **Delete**.  
The system removes the IP address from the whitelist on the screen. However, the IP address remains on the IP Address Exceptions screen with the related setting changed. For example, if you deleted the IP address from an anomaly detection whitelist, the Anomaly Detection column for that IP address in the exceptions list changes from Ignore IP to say Include IP.
4. In the editing context area, click **Apply Policy** to put the changes into effect.

## Updating IP address exceptions

You can update IP address exceptions from the centralized list of IP address exceptions.

1. On the Main tab, click **Security > Application Security > IP Addresses > IP Address Exceptions**.  
The IP Address Exceptions screen opens, and displays a centralized list of configured IP address exceptions.
2. Click the IP address of the IP address exception you want to modify.  
The IP Address Exception Properties screen opens.
3. Change the settings as needed.
4. Click **Update**.
5. In the editing context area, click **Apply Policy** to put the changes into effect.

---

# Chapter 7

---

## Enforcing Application Use at Specific Geolocations

---

- *Overview: Enforcing application use in certain geolocations*
- *Enforcing application use in certain geolocations*
- *Setting up geolocation enforcement from a request*

### Overview: Enforcing application use in certain geolocations

---

Geolocation software can identify the geographic location of a client or web application user. *Geolocation* refers either to the process of assessing the location, or to the actual assessed location.

For applications protected by Application Security Manager™, you can use geolocation enforcement to restrict or allow application use in specific countries. You adjust the lists of which countries or locations are allowed or disallowed in a security policy. If an application user tries to access the web application from a location that is not allowed, the `Access from disallowed GeoLocation` violation occurs. By default, all locations are allowed, and the violation learn, alarm, and block flags are enabled.

Requests from certain locations, such as RFC-1918 addresses or unassigned global addresses, do not include a valid country code. The geolocation is shown as **N/A** in both the request, and the list of geolocations. You have the option to disallow N/A requests whose country of origination is unknown.

### Enforcing application use in certain geolocations

---

Before you can set up geolocation enforcement, you need to create a security policy. If the BIG-IP® system is deployed behind a proxy, you might need to set the **Trust XFF Header** option in the security policy properties. Then the system identifies the location using the address from the XFF header instead of the source IP address.

You can set up a security policy to allow or disallow access to the web application by users in specific countries, areas, or from anonymous proxies.

1. On the Main tab, click **Security > Application Security > Geolocation Enforcement**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the **Geolocation List** setting, use the move buttons to adjust the lists of allowed and disallowed geolocations. To restrict traffic from anonymous proxies, move **Anonymous Proxy** to the disallowed geolocations list.

If no geolocations are assigned, the list displays the word **None**. The screen shows the value **N/A** in the list of geolocations for cases where a user is in a location that cannot be identified, for example, if using RFC-1918 addresses or unassigned global addresses.

---

**Tip:** *You can approach geolocation enforcement by specifying either which locations you want to disallow or which locations you want to allow.*

---

4. Click **Save** to save your settings.
5. In the editing context area, click **Apply Policy** to put the changes into effect.

Now, if a user in a disallowed location attempts to access the web application, the security policy (if in blocking mode) blocks the user and displays the violation `Access from disallowed Geolocation`.

## Setting up geolocation enforcement from a request

---

You can restrict application use in certain geolocations by using the Requests list. This is an easy way to restrict users in a certain country from accessing the web application. By examining illegal request details, you can disallow the locations from which frequent problems are originating.

1. On the Main tab, expand **Application Security** and click **Reporting**.  
The Requests screen opens and shows all illegal requests that have occurred for this security policy.
2. In the Request List, click anywhere on a request.  
The screen displays details about the request including any violations associated with the request, and other details, such as the geolocation.
3. In the Request Details area, next to **Geolocation**, the country is displayed, and if the country is not on the disallowed geolocation list, you see **Disallow this Geolocation**.  
The system asks you to verify that you want to disallow this geolocation. When you verify that you do, the system adds the country to the geolocation disallowed list.
4. Apply the change to the security policy: on the Main tab, click **Policy**, and then click **Apply Policy**.
5. On the menu bar, click **Geolocation Enforcement**.  
The Geolocation Enforcement screen opens, and you can see that the country was added to the disallowed geolocations list.

Now, if a user in a disallowed location attempts to access the web application, the security policy (if in blocking mode) blocks the user and displays the violation `Access from disallowed Geolocation`.





---

# Chapter 8

---

## Creating Login Pages for Secure Application Access

---

- *About creating login pages*
-

## About creating login pages

---

Your web application may contain URLs that should be accessed only through other URLs. For example, in an online banking application, account holders should be able to access their account information only by logging on through a login screen first. In your security policy, you can create login URLs to limit access to authenticated URLs.

A *login page* is a URL in a web application that requests must pass through to get to the authenticated URLs. Use login pages, for example, to prevent forceful browsing of restricted parts of the web application, by defining access permissions for users. Login pages also allow session tracking of user sessions.

*Authenticated URLs* are URLs that become accessible to users only after they successfully log in to the login URL. A *logout URL* is a URL that, if accessed, forces users to return to the login URL before re-accessing authenticated URLs. System administrators use these special URLs to prevent forceful browsing by causing users to pass through the login URL before viewing the restricted authenticated URLs.

## Creating login pages

In your security policy, you can create a login page to specify a login URL that presents a site that users must pass through to gain access to the web application. The login URL commonly leads to the login page of the web application.

1. On the Main tab, click **Security > Application Security > Sessions and Logins**.  
The Login Pages List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Login Page screen opens.
4. For the **Login URL** setting, specify a URL that users must pass through to get to the application.
  - a) From the list, select the type of URL: **Explicit** or **Wildcard**.
  - b) Select either **HTTP** or **HTTPS** based on the type of traffic the web application accepts.
  - c) Type an explicit URL or wildcard expression in the field.  
When you click in the field, the system lists URLs that it has seen, and you can select a URL from the list. Or, you can type explicit URLs in the format `/login`, and wildcard URLs without the slash, such as `*.php`.
5. From the **Authentication Type** list, select the method the web server uses to authenticate the login URL's credentials with a web user.

Option	Description
<b>None</b>	The web server does not authenticate users trying to access the web application through the login URL. This is the default setting.
<b>HTML Form</b>	The web application uses a form to collect and authenticate user credentials. If using this option, you also need to type the user name and password parameters written in the code of the HTML form.
<b>HTTP Basic Authentication</b>	The user name and password are transmitted in Base64 and stored on the server in plain text.
<b>HTTP Digest Authentication</b>	The web server performs the authentication; user names and passwords are not transmitted over the network, nor are they stored in plain text.

Option	Description
NTLM	Microsoft LAN Manager authentication (also called Integrated Windows Authentication) does not transmit credentials in plain text, but requires a continuous TCP connection between the server and client.

6. In the Access Validation area, define at least one validation criteria for the login page response.  
If you define more than one validation criteria, the response must meet all the criteria before the system allows the user to access the application login URL.

---

***Note:** The system checks the access validation criteria on the response of the login URL only if the response has one of the following content-types: text/html, text/xml, application/sgml, application/xml, application/html, application/xhtml, application/x-asp, and application/x-aspix.*

---

7. Click **Create** to add the login page to the security policy.  
The new login page is added to the login pages list.
8. Add as many login pages as needed for your web application.
9. In the editing context area, click **Apply Policy** to put the changes into effect.

The security policy now has one or more login pages associated with it.

You can now configure how the login pages are enforced, including the authentication URLs, logout URLs, and whether or not the login pages have time limits.

## Login page access validation criteria

Following are descriptions of the access validation criteria for the response to the login URL. You configure one or more of these validations when defining a login page.

Access validation	Define in login page as
A string that should appear in the response	A string that must appear in the response for the system to allow the user to access the authenticated URL; for example, <code>Successful Login</code> .
A string that should NOT appear in the response	A string that indicates a failed login attempt and prohibits user access to the authenticated URL; for example, <code>Authentication failed</code> .
Expected HTTP response status code	An HTTP response code that the server must return to the user to allow access to the authenticated URL; for example, <code>200</code> .
Expected validation header name and value (for example, <code>Location</code> header)	A header name and value that the response to the login URL must match to permit user access to the authenticated URL.
Expected validation domain cookie name	A defined domain cookie name that the response to the login URL must match to permit user access to the authenticated URL.
Expected parameter name (added to URI links in the response)	A parameter that must exist in the login URL's HTML body to allow access to the authenticated URL.

## Enforcing login pages

Login enforcement settings prevent forceful browsing attacks where attackers gain access to restricted parts of the web application by supplying a URL directly. You can use login enforcement to force users to pass through one URL (known as the *login URL*) before being allowed to display a different URL (known as the *target URL*) where they can access restricted pages and resources. Login enforcement settings specify how the security policy enforces login pages including the expiration time, authenticated URLs, and logout URLs. You can also use authenticated URLs to enforce idle time-outs on applications that are missing this functionality.

1. On the Main tab, click **Security > Application Security > Sessions and Logins > Login Enforcement**. The Login Enforcement screen opens.
2. If you want the login URL to be valid for a limited time, set **Expiration Time** to **Enabled**, and type a value, in seconds.
3. For the **Authenticated URLs** setting, specify the target URLs that users can access only by way of the login URL:
  - a) In the **Authenticated URLs** field, type the target URL name in the format `/private.php` (wildcards are allowed).
  - b) Click **Add** to add the URL to the list of authenticated URLs.
  - c) Repeat to add as many authenticated URLs as needed.
4. Optionally, use the **Logout URLs** setting to specify the URLs used to log out of the web application:
  - a) In the **Logout URLs** field, type the URL in the format `/logout.html` (explicit URLs only).
  - b) Click **Add**.
  - c) Repeat to add as many logout URLs as needed.
5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If you specify authenticated URLs and a user tries to bypass them, the system issues the `Login URL bypassed` violation. If a user session is idle and exceeds the expiration time, the system now issues the `Login URL expired` violation, and the user can no longer reach the authenticated URLs. For both login violations, if the enforcement mode is blocking, the system now sends the Login Page Response to the client (see **Application Security > Blocking > Response Pages**).

---

# Chapter

# 9

---

## Protecting Sensitive Data with Data Guard

---

- *About protecting sensitive data with Data Guard*
- *Response headers that Data Guard inspects*
- *Protecting sensitive data*

## About protecting sensitive data with Data Guard

---

In some web applications, a response may contain sensitive user information, such as credit card numbers or social security numbers (U.S. only). The Data Guard feature can prevent responses from exposing sensitive information by masking the data (this is also known as *response scrubbing*).

---

**Note:** When you mask the data, the system replaces the sensitive data with asterisks (\*\*\*\*). F5 Networks recommends that you enable this setting especially when the security policy enforcement mode is transparent. Otherwise, when the system returns a response, sensitive data could be exposed to the client.

---

Using Data Guard, you can configure custom patterns using PCRE regular expressions to protect other forms of sensitive information, and indicate exception patterns not to consider sensitive. You can also specify which URLs you want the system to examine for sensitive data.

The system can examine the content of responses for specific types of files that you do not want to be returned to users, such as ELF binary files or Microsoft Word documents. File content checking causes the system to examine responses for the file content types you select, and to block sensitive file content (depending on the blocking modes), but it does not mask the sensitive file content.

## Response headers that Data Guard inspects

---

Data Guard examines responses that have the following content-type headers:

- "text/..."
- "application/x-shockwave-flash"
- "application/sgml"
- "application/x-javascript"
- "application/xml"
- "application/x-asp"
- "application/x-aspix"
- "application/xhtml+xml"

You can configure one additional user-defined response content-type using the system variable `user_defined_accum_type`. If response logging is enabled, these responses can also be logged.

## Protecting sensitive data

---

You can configure the system to protect sensitive data. If a web server response contains a credit card number, U.S. Social Security number, or pattern that matches a pattern, then the system responds based on the enforcement mode setting.

1. On the Main tab, click **Security > Application Security > Data Guard**.  
The Data Guard screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select the **Data Guard** check box.

4. If you want the system to consider credit card numbers as sensitive data, select the **Credit Card Numbers** check box.
5. If you want the system to consider U.S. social security numbers (in the form `nnn-nn-nnnn`, where `n` is an integer) as sensitive data, select the **U.S. Social Security Numbers** check box.
6. To specify additional sensitive data patterns that occur in the application:
  - a) Select the **Custom Patterns** check box.
  - b) In the **New Pattern** field, type a PCRE regular expression to specify the sensitive data pattern, then click **Add**. For example, `999-[ /d] [ /d] - [ /d] [ /d] [ /d] [ /d]`.

---

**Tip:** You can validate the regular expression using the tool at **Security > Options > Application Security > RegExp Validator**.

---

- c) Add as many custom patterns as needed for the application.
7. To specify data patterns not to consider sensitive:
  - a) Select the **Exception Patterns** check box.
  - b) In the **New Pattern** field, type a PCRE regular expression to specify the sensitive data pattern, then click **Add**.
  - c) Add as many custom patterns as needed for the application.
8. If, in responses (when not blocked), you want the system to replace the sensitive data with asterisks (\*\*\*\*), select the **Mask Data** check box.  
 This setting is not relevant if blocking is enabled for the violation, because the system blocks responses containing sensitive data.
9. To review responses for specific file content (for example, to determine whether someone is trying to download a sensitive type of document):
  - a) For the **File Content Detection** setting, select the **Check File Content** check box.  
 The screen displays a list of available file types.
  - b) Move the file types you want the system to consider sensitive from the **Available** list into the **Members** list.
10. To specify which URLs to examine for sensitive data, use the **Enforcement Mode** setting:
  - To inspect all URLs, use the default value of **Ignore URLs in list**, and do not add any URLs to the list.
  - To inspect all but a few specific URLs, use the default value of **Ignore URLs in list**, and add the exceptions to the list.
  - To inspect only specific URLs, select **Enforce URLs in list**, and add the URLs to check to the list.
 When adding URLs, you can type either explicit (`/index.html`) or wildcard (`*xyz.html`) URLs.

When the system detects sensitive information in a response, it generates the `Data Guard: Information leakage detected` violation (if the violation is set to alarm or block). If the security policy enforcement mode is set to blocking and the violation is set to block, the system does not send the response to the client.





---

# Chapter 10

---

## Masking Credit Card Numbers in Logs

---

- *Overview: Masking credit card numbers in logs*

### Overview: Masking credit card numbers in logs

---

Application Security Manager™ (ASM) can mask credit card numbers in request logs. By default, when you create a security policy, the option to mask credit card numbers is enabled. Wherever credit card numbers appear in logs and violation details, they will be replaced by asterisks.

Keeping the Mask Credit Card Numbers in Request Log option enabled is required for PCI compliance. You must use this option in addition to Data Guard and masking sensitive parameters to comply with the Protect Stored Cardholder Data requirement. Data Guard masks sensitive information, such as credit card numbers and social security numbers, in responses.

Sensitive parameters mask sensitive information that is passed as parameters, such as credit card numbers. Making a parameter sensitive guarantees that its values are always masked in logs. Using sensitive parameters is good for form fields that are designated to contain sensitive data (like credit card numbers). But since a user can include credit card numbers in other places, enabling the Mask Credit Card Numbers in Request Log option looks for them anywhere in the request and masks them, providing an additional layer of security.

### Masking credit card numbers in request logs

You can make sure that a security policy is set up to mask credit card numbers in logs and violations. This protects sensitive information, specifically credit card numbers, more securely.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. Select the **Mask Credit Card Numbers in Request Log** check box if it is not already enabled.
4. Click **Save** to save your settings.

The system now looks for occurrences of credit card numbers in request logs and violations and replaces them with asterisks.

---

# Chapter

# 11

---

## Displaying Reports and Monitoring ASM

---

- *ASM Reporting Tools*
  - *Displaying an application security overview report*
  - *Viewing details about requests and violations*
  - *Exporting requests*
-

## ASM Reporting Tools

You can use several reporting tools in Application Security Manager™ (ASM) to analyze incoming requests, track trends in violations, generate security reports, and evaluate possible attacks. The statistics and monitoring reporting tools are described in this table.

Reporting Tool	Description
Application security overview	Displays a summary of all configured security policies showing the active security policies, attacks that have occurred, anomaly statistics, and networking and traffic statistics. You can save the information or send it as an email attachment.
Requests summary	Summarizes the requested URLs for security policies.
Event correlation	Displays a list of incidents (suspected attacks on the web application). Requests become incidents when at least two illegal requests are sent to the web application within 15 minutes, and the system groups them according to criteria. The criteria concern illegal requests for a specific URL, a specific parameter, or a specific source IP address.
Charts	Displays graphical reports about security policy violations and provides tools that let you view the data by different criteria, drill down for more data, create customized reports, and send or export reports.
Charts scheduler	Allows you to periodically generate specific reports and distribute them using email.
DoS Attacks report	Displays graphic charts about DoS attacks, viewed by selected category, and includes the attack start and end times.
Brute Force Attacks report	Displays graphic charts about brute-force attacks, viewed by selected category, and includes the attack start and end times.
Web Scraping statistics	Displays graphic charts about web scraping attacks, viewed by selected category, and includes the attack start and end times.
Session Tracking status	Displays the users, sessions, and IP addresses that the system is currently tracking, and for which the system is taking action as a result of having triggered one of the violation detection thresholds.
PCI Compliance report	Displays a printable Payment Card Industry (PCI) compliance report for each security policy showing each security measure required for PCI-DSS 1.2, and compliance details.
CPU Utilization report	Displays the amount of the available CPU that the Application Security Manager uses over a period of time.

## Displaying an application security overview report

To view data in the security overview, the system must be logging data internally. Some default logging profiles are already set up on the system but you may want to customize them.

The Application Security Manager™ (ASM) can display a security overview where you can quickly see what is happening on your system. The overview is configurable and can include statistics concerning attack types, violations, and anomalies, traffic summaries, transactions per second, throughput, and top requested

URLs, IP addresses, and request types. You can also export the statistics into a PDF, and email them as an attachment.

1. On the Main tab, click **Security > Overview > Application > Traffic**.  
The Overview Traffic screen opens and summarizes ASM system activity at a glance.
2. To change the default time frame for all widgets, select a time period from the **Override time range to** list.
3. From the **Security Policy** list, select a security policy to narrow down the statistics.  
By default, statistics for all active security policies are shown.
4. Review the summary statistics (organized into areas called *widgets*) to determine what is happening on the system.
5. If you want to create a new area of information customized to your specifications, at the bottom of the screen, click **Add Widget**.  
The Add New Widget popup screen opens.
6. Optionally, for each widget, you can adjust the time range, data measurements, and format of data to display from the **Time Period** list (Last Hour, Last Day, Last Week, Last Month, or Last Year) or the configuration gear settings.  
You can also delete any widget that you do not need on the screen.
7. To save the summary as a PDF file on your computer:
  - a) Click the **Export** link.
  - b) In the popup screen that opens, click **Export** again to save the file on your computer.
8. To send the report as an email attachment, click the **Export** link.

---

***Note:** To send email, you need to configure an SMTP server. If one is not configured, on the Main tab, click **System > Configuration > Device > SMTP**, and then click **Create** to configure one first.*

---

- a) Click **Send the report file via E-Mail as an attachment**.
- b) In the **Target E-Mail Address(es)** field, type the one or more email addresses (separated by commas or semi-colons).
- c) From the **SMTP Server** list, select the SMTP server.
- d) Click **Export**.

The systems sends an email with the PDF to the specified addresses.

You can adjust the overview and create widgets for the information you are interested in.

## Viewing details about requests and violations

---

To review requests related to learning suggestions, you need to have a security policy that is already handling traffic that is causing violations. If no violations have occurred, you will not see any learning suggestions.

You can view details about a request, including viewing the full request itself, and any violations associated with it. You can also drill down to view detailed descriptions of the violations and potential attacks, including violations found for staged entities. When viewing details about an illegal request, if you decide that the request is trusted and you want to allow it, you can accept the violations shown for this specific request.

1. On the Main tab, click **Security > Event Logs > Application > Requests**.  
The Requests screen opens, where, by default, you can view a list of illegal requests for all security policies.

2. In the Requests List, click a request to view information about the request and any violations associated with it.  
You see any violations associated with the request and other details, such as the security policy it relates to, the support ID, severity, and potential attacks that it could cause.
3. To view details about a violation associated with an illegal request:
  - To view details about this specific violation such as the file type, the expected and actual length of the query, or similar relevant information, click the violation name.
  - To display a general description of that type of violation, click the icon to the left of the violation.
4. For violations that you want to allow (false positives), click the **Learn** button.  
If there are learning suggestions, the violation's learning screen opens where you can accept or clear the suggestions one at a time.
5. To view the actual contents of the request, click **HTTP Request** or **HTTP Response**.
6. When you are done looking at the request details, click **Close**.

The Requests List provides information about a request such as: the request category, the time of the request, its severity, the source IP address of the request, the server response code, and the requested URL itself. Icons on each request line provide additional status information such as whether the request is legal or illegal, blocked, truncated, or has a response. By reviewing the request details, you can investigate whether it was an attack or a false positive.

## Exporting requests

---

You can export a list of selected requests in PDF or binary format for troubleshooting purposes.

1. On the Main tab, click **Security > Event Logs > Application > Requests**.  
The Requests screen opens, where, by default, you can view a list of illegal requests for all security policies.
2. If you want to export specific requests, select those requests from the list.  
You can export up to 100 entries in PDF format.
3. Beneath the Requests List, click **Export**.  
The Select Export Method popup screen provides options.
4. Select the export method to use, then click **Export**.
  - To export selected requests into a document, click **Export selected requests in PDF format**.  
You can choose to open or save the file created.
  - To export requests to a document and send it by e-mail, click **Send selected requests in PDF format to your E-mail address**, and type your e-mail address. (Note an SMTP server must be configured on the BIG-IP® system.)
  - To export all requests currently displayed to a tar file, click **Binary export of all requests defined by filter**.  
The system creates a \*.tar.gz file of the requests, and saves it where you specify.

---

# Chapter 12

---

## Configuring Application Security Event Logging

---

- *About logging profiles*
  - *Creating a logging profile*
  - *Setting up remote logging*
  - *Associating a logging profile with a security policy*
  - *About logging responses*
  - *About ArcSight log message format*
  - *Filtering logging information*
  - *Viewing application security logs*
-

## About logging profiles

---

Logging profiles determine where events are logged, and which items (such as which parts of requests, or which type of errors) are logged. Events can be logged either locally on the system and viewed in the Event Logs screens, or remotely by the client's server. The system forwards the log messages to the client's server using the Syslog service.

You can use one logging profile for Application Security, Protocol Security, Advanced Firewall, and DoS Protection. By default, the system includes two logging profiles that log data locally for Application Security: one to log all requests and another to log illegal requests. You can use the system-supplied logging profiles, or you can create a custom logging profile.

The logging profile records requests to the virtual server. By default when you create a security policy using the Deployment wizard, the system associates the log illegal requests profile to the virtual server associated with the policy. You can change which logging profile is associated with the security policy by editing the virtual server.

---

**Note:** *If running Application Security Manager™ on a BIG-IP system using Virtualized Clustered Multiprocessing (vCMP), for best performance, F5 recommends configuring remote logging to store Application Security Manager logs remotely rather than locally.*

---

A logging profile has two parts: the storage configuration and the storage filter. The storage configuration specifies where to store the logs, either locally and/or remotely. The storage filter determines what information gets stored. For remote logging, you can send logging files for storage on a remote system (such as a syslog server), on a reporting server (as key/value pairs), or on an ArcSight server (in CEF format). Note that configuring external logging servers is not the responsibility of F5 Networks.

## Creating a logging profile

---

You can create a custom logging profile to log application security events.

1. On the Main tab, click **Security > Event Logs > Logging Profiles**.  
The Logging Profiles list screen opens.
2. Click **Create**.  
The New Logging Profile screen opens.
3. In the **Profile Name** field, type a unique name for the profile.
4. Select the **Application Security** check box.  
The screen displays additional fields.
5. On the Application Security tab, for **Configuration**, select **Advanced**.
6. By default, logs are stored locally. The **Local Storage** check box is selected and cannot be cleared unless you enable **Remote Storage** to store logs remotely.  
This prevents you from creating a logging profile that does not log any traffic.
  - To store logs locally only, leave the **Local Storage** check box selected.
  - To store logs remotely, select the **Remote Storage** check box.
  - To store logs both places, select both check boxes.
7. Optional for local logging: To ensure that the system logs requests for the security policy, even when the logging utility is competing for system resources, select the **Guarantee Local Logging** check box.
8. From the **Response Logging** list, select one of the following options.



Option	Description
<b>Off</b>	Do not log responses.
<b>For Illegal Requests Only</b>	Log responses for illegal requests.
<b>For All Requests</b>	Log responses for all requests. when the Storage Filter <b>Request Type</b> is set to All Requests. (Otherwise, logs only illegal requests.)

By default, the system logs the first 10000 bytes of responses, up to 10 responses per second. You can change the limits by using the response logging system variables.

- By default, the system logs all requests. To limit the type of requests that the system or server logs, set up the **Storage Filter**.
- If setting up local event logging only, click **Finished**. To set up remote logging, continue to set up remote logging.

When you store the logs locally, the logging utility may compete for system resources. Using the **Guarantee Logging** setting ensures that the system logs the requests in this situation but may result in a performance reduction in high-volume traffic applications.

## Setting up remote logging

---

To set up remote logging, you need to have created a logging profile.

You can configure a custom logging profile to log application security events remotely on syslog or reporting servers.

- On the Main tab, click **Security > Event Logs > Logging Profiles**.  
The Logging Profiles list screen opens.
- Click the name of the logging profile for which you want to set up remote logging.
- Select the **Remote Storage** checkbox.
- From the **Remote Storage Type** list, select the appropriate type:
  - To store traffic on a remote logging server like syslog, select **Remote**. Messages are in syslog format.
  - To store traffic on a reporting server (for example, Splunk) using a pre-configured storage format, select **Reporting Server**. Key/value pairs are used in the log messages.
  - If your network uses ArcSight logs, select **ArcSight**. Log messages are in Common Event Format (CEF).
- For the Protocol setting, select the protocol that the remote storage server uses: **TCP** (the default setting), **TCP-RFC3195**, or **UDP**.
- If setting up local event logging only, click **Finished**. To set up remote logging, continue to set up remote logging.  
The selected protocol applies to all remote server settings on this screen, including all server IP addresses.
- For **Server Addresses**, specify one or more remote servers, reporting servers, or ArcSight servers on which to log traffic. Type the **IP Address**, **Port Number** (default is 514), and click **Add**.
- If using the Remote storage type, for **Facility**, select the facility category of the logged traffic. The possible values are **LOG\_LOCAL0** through **LOG\_LOCAL7**.

---

**Tip:** If you have more than one security policy you can use the same remote logging server for both applications, and use the facility filter to sort the data for each.

---

9. If using the Remote storage type, in the Storage Format setting, you can specify how the log displays information, which traffic items the server logs, and what order it logs them:
  - a) To determine how the log appears, select **Field-List** to display the items in the Selected Items list in CSV format with a delimiter you specify; select **User-Defined** to display the items in the Selected Items list in addition to any free text you type in the Selected Items list.
  - b) To specify which items appear in the log, move items from the Available Items list into the Selected Items list.
  - c) To control the order in which predefined items appear in the server logs, select an item in the Selected Items list, and click the **Up** or **Down** button.
10. For **Maximum Query String Size**, specify how much of a request the server logs.
  - To log the entire request, select **Any**.
  - To limit the number of bytes that are logged per request, select **Length** and type the maximum number of bytes to log.
11. For **Maximum Entry Length**, specify how much of the entry length the server logs. The default length is 1K for remote servers that support UDP, and 2K for remote servers that support TCP and TCP-RFC3195. You can change the default maximum entry length for remote servers that support TCP.
12. If you want the system to send a report string to the remote system log when a brute force attack or web scraping attack starts and ends, select **Report Detected Anomalies**
13. In the Storage Filter area, make any changes as required.
14. Click **Update** (or **Finished**, whichever is appropriate).

When you create a logging profile for remote storage, the system stores the data for the associated security policy on one or more remote systems. The system stores the data in Comma Separated Value (CSV) format or another format that you defined.

## Associating a logging profile with a security policy

---

A logging profile records requests to the virtual server. By default when you create a security policy, the system associates the Log Illegal Requests profile with the virtual server used by the policy. You can change which logging profile is associated with the security policy or assign a new one by editing the virtual server.

1. Click **Local Traffic > Virtual Servers**
2. Click the name of the virtual server used by the security policy.  
The system displays the general properties of the virtual server.
3. From the **Security** menu, select **Policies**.  
The system displays the policy settings for the virtual server.
4. Ensure that the **Application Security Policy** setting is **Enabled** and that **Policy** is set to the security policy you want.
5. For **Log Profile**,
  - a) Check that it is set to **Enabled**.
  - b) From the **Available** list, select the profile to use for the security policy, and move it into the **Selected** list.
6. Click **Update**.

Information related to traffic controlled by the security policy is logged using the logging profile or profiles specified in the virtual server.

## About logging responses

---

If you enable response logging in the logging profile, the system can log only responses that include the following content headers:

- "text/..."
- "application/x-shockwave-flash"
- "application/sgml"
- "application/x-javascript"
- "application/xml"
- "application/x-asp"
- "application/x-aspix"
- "application/xhtml+xml"
- "application/soap+xml"
- "application/json"

The system cannot log other responses.

## About ArcSight log message format

---

If your network uses ArcSight logs, you can create a logging profile so that the log information is saved using the appropriate format. Application Security Manager stores all logs on a remote logging server using the predefined ArcSight settings for the logs. The log messages are in Common Event Format (CEF).

The basic format is:

```
CEF:Version|Device Vendor|Device Product|Device Version
|Device Event Class ID|Name|Severity|Extension
```

## Filtering logging information

---

The storage filter of an application security logging profile determines the type of requests the system or server logs. By default, the system logs illegal requests only. You can create a custom storage filter for a logging profile so that the event logs include the exact information you want to see.

1. On the Main tab, click **Security > Event Logs > Logging Profiles**.  
The Logging Profiles list screen opens.
2. In the Profile Name column, click the logging profile name for which you want to set up the filter.

***Note:** This profile must be one that you created and not one of the system-supplied profiles, which cannot be edited.*

The Edit Logging Profile screen opens.

3. From the **Storage Filter** list, select **Advanced**.  
The screen displays additional settings.

4. For the **Logic Operation** setting, specify the filter criteria to use.

Option	Description
<b>OR</b>	Select this operator to log the data that meets one or more of the criteria.
<b>AND</b>	Select this operator to log the data that meets all of the criteria.

5. For the **Request Type** setting, select the requests that you want the system to store in the log, **All Requests** or **Illegal Requests Only**.
6. For the **Protocols** setting, select whether logging occurs for both HTTP and HTTPS protocols or a specific protocol.
7. For the **Response Status Codes** setting, select whether logging occurs for all response status codes or only for specific ones.
8. For the **HTTP Methods** setting, select whether logging occurs for all methods or only for specific ones.
9. For the **Request Containing String** setting, select whether the request logging is for any string or dependent on a specific string that you specify.
10. Click **Update**.

The system logs application security data that meets the criteria specified in the storage filter.

## Viewing application security logs

---

You can view locally stored system logs for the Application Security Manager™ on the BIG-IP® system. These are the logs that include general system events and user activity.

---

**Tip:** *If you prefer to review the log data from the command line, you can find the application security log data in the `/var/log/asmfile`.*

---

1. Click **System > Logs**
2. Click **Application Security**.

The system displays application security data that meets the criteria specified in the logging profile.

---

# Chapter 13

---

## Configuring Application Security Session Tracking

---

- *Overview: Tracking application security sessions using login pages*
-

## Overview: Tracking application security sessions using login pages

---

You can track sessions using login pages configured from within Application Security Manager™ (ASM™), or have the policy retrieve the user names from Access Policy Manager® (APM®). This implementation describes how to set up session tracking for a security policy using login pages. The advantage of using session tracking is that you are able to identify the user, session, or IP address that instigated an attack.

When creating login pages for the application, you define the URLs, parameters, and validation criteria required for users to log in to the application. User and session information is included in the system logs so you can track a particular session or user. The system can log activity, or block a user or session if either generates too many violations.

If you configure session awareness, you can view the user and session information in the application security charts.

### Task Summary

*Creating login pages*

*Enforcing login pages*

*Setting up session tracking*

*Monitoring user and session information*

*Tracking specific user and session information*

## Creating login pages

In your security policy, you can create a login page to specify a login URL that presents a site that users must pass through to gain access to the web application. The login URL commonly leads to the login page of the web application.

1. On the Main tab, click **Security > Application Security > Sessions and Logins**.  
The Login Pages List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Login Page screen opens.
4. For the **Login URL** setting, specify a URL that users must pass through to get to the application.
  - a) From the list, select the type of URL: **Explicit** or **Wildcard**.
  - b) Select either **HTTP** or **HTTPS** based on the type of traffic the web application accepts.
  - c) Type an explicit URL or wildcard expression in the field.  
When you click in the field, the system lists URLs that it has seen, and you can select a URL from the list. Or, you can type explicit URLs in the format `/login`, and wildcard URLs without the slash, such as `*.php`.
5. From the **Authentication Type** list, select the method the web server uses to authenticate the login URL's credentials with a web user.

Option	Description
None	The web server does not authenticate users trying to access the web application through the login URL. This is the default setting.

Option	Description
<b>HTML Form</b>	The web application uses a form to collect and authenticate user credentials. If using this option, you also need to type the user name and password parameters written in the code of the HTML form.
<b>HTTP Basic Authentication</b>	The user name and password are transmitted in Base64 and stored on the server in plain text.
<b>HTTP Digest Authentication</b>	The web server performs the authentication; user names and passwords are not transmitted over the network, nor are they stored in plain text.
<b>NTLM</b>	Microsoft LAN Manager authentication (also called Integrated Windows Authentication) does not transmit credentials in plain text, but requires a continuous TCP connection between the server and client.

6. In the Access Validation area, define at least one validation criteria for the login page response.  
If you define more than one validation criteria, the response must meet all the criteria before the system allows the user to access the application login URL.

---

***Note:** The system checks the access validation criteria on the response of the login URL only if the response has one of the following content-types: text/html, text/xml, application/sgml, application/xml, application/html, application/xhtml, application/x-asp, and application/x-asp.*

---

7. Click **Create** to add the login page to the security policy.  
The new login page is added to the login pages list.
8. Add as many login pages as needed for your web application.
9. In the editing context area, click **Apply Policy** to put the changes into effect.

The security policy now has one or more login pages associated with it.

You can now configure how the login pages are enforced, including the authentication URLs, logout URLs, and whether or not the login pages have time limits.

## Enforcing login pages

Login enforcement settings prevent forceful browsing attacks where attackers gain access to restricted parts of the web application by supplying a URL directly. You can use login enforcement to force users to pass through one URL (known as the *login URL*) before being allowed to display a different URL (known as the *target URL*) where they can access restricted pages and resources. Login enforcement settings specify how the security policy enforces login pages including the expiration time, authenticated URLs, and logout URLs. You can also use authenticated URLs to enforce idle time-outs on applications that are missing this functionality.

1. On the Main tab, click **Security > Application Security > Sessions and Logins > Login Enforcement**. The Login Enforcement screen opens.
2. If you want the login URL to be valid for a limited time, set **Expiration Time** to **Enabled**, and type a value, in seconds.
3. For the **Authenticated URLs** setting, specify the target URLs that users can access only by way of the login URL:
  - a) In the **Authenticated URLs** field, type the target URL name in the format `/private.php` (wildcards are allowed).
  - b) Click **Add** to add the URL to the list of authenticated URLs.

- c) Repeat to add as many authenticated URLs as needed.
4. Optionally, use the **Logout URLs** setting to specify the URLs used to log out of the web application:
  - a) In the **Logout URLs** field, type the URL in the format `/logout.html` (explicit URLs only).
  - b) Click **Add**.
  - c) Repeat to add as many logout URLs as needed.
5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If you specify authenticated URLs and a user tries to bypass them, the system issues the `Login URL bypassed` violation. If a user session is idle and exceeds the expiration time, the system now issues the `Login URL expired` violation, and the user can no longer reach the authenticated URLs. For both login violations, if the enforcement mode is blocking, the system now sends the Login Page Response to the client (see **Application Security > Blocking > Response Pages**).

## Setting up session tracking

You can use session tracking to track, enforce, and report on user sessions and IP addresses. To perform tracking, you enable session awareness and indicate how to associate the application user name with the session. You can also determine whether to track violations and perform logging or blocking actions based on the number of violations per user, session, and IP address.

1. On the Main tab, click **Security > Application Security > Sessions and Logins > Session Tracking**. The Session Tracking screen opens.
2. In the Session Tracking Configuration area, for **Session Awareness**, select the **Enabled** check box.
3. Use the **Application Username** setting to specify the login pages for the application:
  - a) From the list, select **Use Login Pages**.
  - b) Move the login pages for the application from the Available list to the Selected list.  
If the login page is not listed, click **Add** to create it.
4. In the Violation Detection Actions area, select the **Track Violations and Perform Actions**, check box.
5. In the **Violation Detection Period** field, type the number of seconds that indicates the sliding time period to count violations for violation thresholds.  
The default is 900 seconds.
6. If you want the system to block all activity for a user, session, or IP address when the number of violations exceeds the threshold, specify one or more of the following settings on the Block All tab.

---

**Note:** For the system to block requests, the security policy Enforcement Mode must be set to blocking (see **Security > Application Security > Blocking > Settings**) and some violations must be set to block.

---

Option	Description
<b>Blocked URLs</b>	Specify which URLs to block after the number of violations exceeds the enabled thresholds. To block all URLs, select <b>Block all URLs</b> . To block authenticated URLs protected by login pages, select <b>Block Authenticated URLs</b> .
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block this user's activity.



Option	Description
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block activity for this HTTP session.
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block the activity of this IP address.
<b>Block All Period</b>	Specify how long to block users, sessions, or IP addresses if the number of violations exceeds the threshold. To block the user, session, or IP address indefinitely, click <b>Infinite</b> . Otherwise, click <b>User-defined</b> and type the number of seconds to block the traffic. The default is 600 seconds.

7. If you want the system to log activity when the number of user, session, or IP address violations exceeds the threshold during the violation detection period, specify one or more of the following settings on the Log All Requests tab.

Option	Description
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging this user's activity for the log all requests period.
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging activity for this HTTP session for the log all requests period.
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging the activity of this IP address for the log all requests period.
<b>Log All Requests Period</b>	Specify how long the system should log all requests when any of the enabled thresholds is reached. Type the number of seconds in the field.

8. If you want more tolerant blocking for selected violations, such as those prone to false positives, specify one or more of the following settings on the Delay Blocking tab.

---

***Note:** For the system to block requests, the security policy Enforcement Mode must be set to blocking (see **Security > Application Security > Blocking > Settings**) and the specified violations must be set to block.*

---

Option	Description
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations a user must cause before the system begins blocking this user for the delay blocking period.
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations users must cause (during the violation detection period) before the system begins blocking this HTTP session for the delay blocking period.
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system begins blocking this IP address for the delay blocking period.
<b>Delay Blocking Period</b>	Type the number of seconds that the system should block the user, session, or IP address when any of the enabled thresholds is reached.
<b>Associated Violations</b>	Move the violations for which you want delay blocking from the <b>Available</b> list into the <b>Selected</b> list. If the selected violations occur, the system does not block traffic until one of the enabled thresholds is reached. At that point, the system blocks traffic causing those violations for the user, session, or IP address, but allows other transactions to pass.

9. Click **Save** to save your settings.

After you set up session tracking, if any enabled threshold exceeds the number of violations during the detection period, the system starts the configured actions (block all, log all requests, or delay blocking).

### Monitoring user and session information

To monitor user and session information, you first need to set up session tracking for the security policy.

You can use the reporting tools in Application Security Manager™ to monitor user and session details, especially when you need to investigate suspicious activity that is occurring with certain users, sessions, or IP addresses.

1. On the Main tab, click **SecurityReporting ApplicationSession Tracking Status**.  
The Session Tracking Status screen opens and shows the users, sessions, and IP addresses that the system is currently tracking for this security policy.

2. From the **Action** list, select the action by which to filter the data.

Action	Description
All	Specifies that the screen displays all entries. This is the default value.
Block All	Specifies that the system displays sessions whose requests the system blocks after the configured threshold was reached.
Log All Requests	Specifies that the system displays sessions whose requests the system logs after the configured threshold was reached.
Delay Blocking	Specifies that the system displays sessions whose requests the system delayed blocking until the configured threshold was reached.

3. From the **Scope** list, specify the scope (username, session, or IP address) by which to filter the data.

Option	Description
Alt	Specifies that the screen displays all entries. This is the default value.
Username	Specifies that the system displays usernames whose illegal requests exceeded the security policy's threshold values.
Session	Specifies that the system displays identification numbers of illegal sessions that exceeded the security policy's threshold values.
IP Address	Specifies that the system displays IP addresses where illegal requests from these IP addresses exceeded the security policy's threshold values.

4. If you want to filter the information by value, in the **Value** field, type the username, session identification number, IP address, or string. If empty, the screen displays all entries.
5. When you finish specifying the filter details, click **Go**.  
The Session Tracking Status list now shows the information specified in the Filter setting.

After you set up session tracking, you can monitor the specific requests that cause violations by examining each request and reviewing graphical charts.

### Tracking specific user and session information

To monitor user and session information, you first need to set up session tracking for the security policy.

You can configure Application Security Manager™ to log, block, or delay blocking requests from a specific username, session, or source IP address.

1. On the Main tab, click **Security > Reporting > Application > Session Tracking Status**.  
The Session Tracking Status screen opens and shows the users, sessions, and IP addresses that the system is currently tracking for this security policy.
2. Next to the Session Tracking Status list, click **Add**.  
The Add Session to Tracking screen opens.
3. From the **Action** list, select the action that the system will take if it detects the specified username, session, or IP address.

Action	Description
<b>Block All</b>	Specifies that the system blocks all requests from a specific username, session, or IP address for the configured period of time.
<b>Log All Requests</b>	Specifies that the system blocks all requests from a specific username, session, or IP address for the configured period of time.
<b>Delay Blocking</b>	Specifies that the system will delay blocking the associated violations from a specific username, session, or IP address until the threshold is reached; then they will be blocked for the configured period of time.

4. From the **Scope** list, specify whether the system is tracking a specific Username (the default value), Session, or IP Address.
5. In the **Value** field, type the unique username, session identification number, or IP address that you want to track, based on what you selected in the **Scope** option.
6. Click **Add**.  
The system adds the entry to the Session Tracking list and immediately begins to enforce it.

If the system detects the specific username, session, or IP address, it takes that action you configured for it.



---

# Chapter 14

---

## Tracking Application Security Sessions with APM

---

- *Overview: Tracking application security sessions using APM*
  - *Prerequisites for setting up session tracking with APM*
-

## Overview: Tracking application security sessions using APM

---

You can track sessions using login pages configured from within Application Security Manager™ (ASM™), or have the policy retrieve the user names from Access Policy Manager® (APM®). This implementation describes how to set up session tracking for a security policy using APM to verify user credentials. Then, you can set up session awareness from within ASM to identify the user, session, or IP address that instigated an attack.

If you configure session tracking, you can view the user and session information in the application security charts.

## Prerequisites for setting up session tracking with APM

---

In order to set up session tracking from within Application Security Manager™ (ASM™) so that the security policy retrieves the user names from Access Policy Manager® (APM®), you need to perform basic these system configuration tasks according to the needs of your networking configuration:

- Run the setup utility and create a management IP address.
- License and provision ASM, APM, and Local Traffic Manager™ (LTM™).
- Configure a DNS address (**System > Configuration > Device > DNS**).
- Configure an NTP server (**System > Configuration > Device > NTP**).
- Restart ASM (at the command line, type `tmsh restart /sys service asm`).

### Task summary

Use the following tasks to set up application security session tracking with APM authentication integrated.

*Creating a VLAN*

*Creating a self IP address for a VLAN*

*Creating a local traffic pool for application security*

*Creating a virtual server to manage HTTPS traffic*

*Creating a security policy automatically*

*Creating an access profile*

*Configuring an access policy*

*Adding the access profile to the virtual server*

*Setting up ASM session tracking with APM*

*Monitoring user and session information*

## Creating a VLAN

VLANs represent a collection of hosts that can share network resources, regardless of their physical location on the network. You create a VLAN to associate physical interfaces with that VLAN.

1. On the Main tab, click **Network > VLANs**.  
The VLAN List screen opens.
2. Click **Create**.  
The New VLAN screen opens.

3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting, click an interface number from the **Available** list, and use the Move button to add the selected interface to the **Untagged** list. Repeat this step as necessary.
5. Click **Finished**.  
The screen refreshes, and displays the new VLAN from the list.

## Creating a self IP address for a VLAN

Ensure that you have at least one VLAN configured before you create a self IP address.

Self IP addresses enable the BIG-IP® system, and other devices on the network, to route application traffic through the associated VLAN.

1. On the Main tab, click **Network > Self IPs**.  
The Self IPs screen opens.
2. Click **Create**.  
The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type an IPv4 or IPv6 address.  
This IP address should represent the address space of the VLAN that you specify with the **VLAN/Tunnel** setting.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address.
  - On the internal network, select the VLAN that is associated with an internal interface or trunk.
  - On the external network, select the VLAN that is associated with an external interface or trunk.
7. Use the default values for all remaining settings.
8. Click **Finished**.  
The screen refreshes, and displays the new self IP address.

The BIG-IP system can now send and receive TCP/IP traffic through the specified VLAN.

## Creating a local traffic pool for application security

You can use a local traffic pool with Application Security Manager™ system to forward traffic to the appropriate resources.

---

**Note:** You can optionally create a pool as part of creating a security policy using the Deployment wizard.

---

1. On the Main tab, click **Local Traffic > Pools**.  
The Pool List screen opens.
2. Click **Create**.  
The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, for the **New Members** setting, add to the pool the application servers that host the web application:
  - a) Type an IP address in the **Address** field.

- b) In the **Service Port** field, type a port number (for example, type 80 for the HTTP service), or select a service name from the list.
- c) Click **Add**.

5. Click **Finished**.

The BIG-IP® system configuration now includes a local traffic pool containing the resources that you want to protect using Application Security Manager™.

## Creating a virtual server to manage HTTPS traffic

You can create a virtual server to manage HTTPS traffic.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the **Create** button.  
The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type 443 or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select **clientssl**, and using the Move button, move the name to the **Selected** list.
9. (Optional) From the **SSL Profile (Server)** list, select **serverssl**.

---

***Note:** This setting ensures that there is an SSL connection between the HTTP virtual server and the external HTTPS server.*

---

10. From the **Source Address Translation** list, select **Auto Map**.
11. From the **Default Pool** list, select the pool that is configured for application security.
12. Click **Finished**.

The HTTPS virtual server appears in the Virtual Server List screen.

## Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the **Create** button.  
The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.



3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
  - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
  - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
  - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
  - If creating a new virtual server, specify the protocol, name, IP address and port, pool IP address, and port.
  - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy.
  - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

The name of the new or existing virtual server becomes the name of the security policy.

The Select Deployment Scenario screen opens.

5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.  
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

---

**Important:** You cannot change this setting after you have created the security policy.

---

7. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

---

**Important:** You cannot change this setting after you have created the security policy.

---

8. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.

9. Click **Next**.  
The Configure Attack Signatures screen opens.

10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.

The system adds the attack signatures needed to protect the selected systems.

11. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

---

**Note:** Because the Real Traffic Policy Builder® begins building the security policy in Blocking mode, you can keep signature staging enabled to make sure that false positives do not occur.

---

New and updated attack signatures remain in staging for 7 days, and are not enforced (according to the learn, alarm, and block flags) during that time.

12. Click **Next**.  
The Configure Automatic Policy Building screen opens.

13. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
<b>Fundamental</b>	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
<b>Enhanced</b>	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, Explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles.
<b>Comprehensive</b>	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

14. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

15. For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
<b>All</b>	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted, the policy is created faster when you select this option.
<b>Address List</b>	Specifies networks to consider safe. Fill in the <b>IP Address</b> and <b>Netmask</b> fields, then click <b>Add</b> . This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

16. If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.

17. If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.

18. Click **Next**.

The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.

19. Click **Finish** to create the security policy.

The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM™ creates the virtual server with an HTTP profile, and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

---

***Tip:** This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.*

---

## Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy > Access Profiles**.  
The Access Profiles List screen opens.
2. Click **Create**.  
The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.
4. From the **Profile Type** list, select one:
  - **APM-LTM** - Select for a web access management configuration.
  - **SSO** - Select only when you do not need to configure an access policy.
  - **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
  - **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
  - **SSL-VPN** - Select for other types of access, such as network access, portal access, application access. (Most access policy items are available for this type.)
  - **ALL** - Select for any type of access.

Additional settings display.

5. To configure timeout and session settings, select the **Custom** check box.
6. In the **Inactivity Timeout** field, type the number of seconds that should pass before the access policy times out. Type 0 to set no timeout.  
If there is no activity (defined by the **Session Update Threshold** and **Session Update Window** settings in the Network Access configuration) between the client and server within the specified threshold time, the system closes the current session.
7. In the **Access Policy Timeout** field, type the number of seconds that should pass before the access profile times out because of inactivity.  
Type 0 to set no timeout.
8. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.  
Type 0 to set no timeout.

9. In the **Max Concurrent Users** field, type the maximum number of users that can use this access profile at the same time.  
Type 0 to set no maximum.
10. In the **Max Sessions Per User** field, type the maximum number of concurrent sessions that one user can start.  
Type 0 to set no maximum.
11. In the **Max In Progress Sessions Per Client IP** field, type the maximum number of concurrent sessions that one client IP address can support.  
Type 0 to set no maximum.
12. Select the **Restrict to Single Client IP** check box to restrict the current session to a single IP address.  
This setting associates the session ID with the IP address.  
Upon a request to the session, if the IP address has changed the request is redirected to a logout page, the session ID is deleted, and a log entry is written to indicate that a session hijacking attempt was detected. If such a redirect is not possible, the request is denied and the same events occur.
13. To configure logout URIs, in the Configurations area, type each logout URI in the **URI** field, and then click **Add**.
14. In the **Logout URI Timeout** field, type the delay in seconds before logout occurs for the customized logout URIs defined in the **Logout URI Include** list.
15. To configure SSO:
  - For users to log in to multiple domains using one SSO configuration, skip the settings in the SSO Across Authentication Domains (Single Domain mode) area. You can configure SSO for multiple domains only after you finish the initial access profile configuration.
  - For users to log in to a single domain using an SSO configuration, configure settings in the SSO Across Authentication Domains (Single Domain mode) area, or you can configure SSO settings after you finish the initial access profile configuration.
16. In the **Domain Cookie** field, specify a domain cookie, if the application access control connection uses a cookie.
17. In the **Cookie Options** setting, specify whether to use a secure cookie.
  - If the policy requires a secure cookie, select the **Secure** check box to add the **secure** keyword to the session cookie.
  - If you are configuring an LTM access scenario that uses an HTTPS virtual server to authenticate the user and then sends the user to an existing HTTP virtual server to use applications, clear this check box.
18. If the access policy requires a persistent cookie, in the **Cookie Options** setting, select the **Persistent** check box.  
This sets cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent; but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value will be used to set the persistent cookie expiration.
19. From the **SSO Configurations** list, select an SSO configuration.
20. In the Language Settings area, add and remove accepted languages, and set the default language.  
A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
21. Click **Finished**.

The access profile appears in the Access Profiles List.

To add an SSO configuration for multiple domains, click **SSO / Auth Domains** on the menu bar. To provide functionality with an access profile, you must configure the access policy. The default access policy for a profile denies all traffic and contains no actions. Click **Edit** in the **Access Policy** column to edit the access policy.

## Configuring an access policy

You configure an access policy to provide authentication, endpoint checks, and resources for an access profile. This procedure configures a simple access policy that adds a logon page, gets user credentials, submits them to an authentication type of your choice, then allows authenticated users, and denies others.

1. On the Main tab, click **Access Policy > Access Profiles**.  
The Access Profiles List screen opens.
2. Click the name of the access profile you want to edit.
3. On the menu bar, click **Access Policy**.
4. For the **Visual Policy Editor** setting, click the **Edit access policy for Profile *policy\_name*** link.  
The visual policy editor opens the access policy in a separate window or tab.
5. Click the (+) icon anywhere in the access policy to add a new action item.  
A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. On the Logon tab, select **Logon Page** and click the **Add Item** button.  
The Logon Page Agent properties screen opens.
7. Click **Save**.  
The Access Policy screen reopens.
8. On the rule branch, click the plus sign (+) between **Logon Page** and **Deny**.
9. Set up the appropriate authentication and client-side checks required for application access at your company, and click **Add Item**.
10. Change the Successful rule branch from **Deny** to **Allow** and click the **Save** button.
11. If needed, configure further actions on the successful and fallback rule branches of this access policy item, and save the changes.
12. At the top of the screen, click the **Apply Access Policy** link to apply and activate your changes to this access policy.
13. Click the **Close** button to close the visual policy editor.

## Adding the access profile to the virtual server

Before you can perform this task, you need to create an access profile using Access Policy Manager™.

You associate the access profile with the virtual server created for the web application that Application Security Manager™ is protecting.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server that manages the network resources for the web application you are securing.
3. In the Access Policy area, from the **Access Profile** list, select the access profile.
4. Click **Update**.

Your access policy is now associated with the virtual server.

## Setting up ASM session tracking with APM

You can use session tracking to track, enforce, and report on user sessions and IP addresses. To perform tracking, you enable session awareness and indicate how to associate the application user name with the session.

1. On the Main tab, click **Security > Application Security > Sessions and Logins > Session Tracking**. The Session Tracking screen opens.
2. In the Session Tracking Configuration area, for **Session Awareness**, select the **Enabled** check box.
3. From the **Application Username** list, select **Use APM Usernames and Session ID**.
4. In the Violation Detection Actions area, select the **Track Violations and Perform Actions**, check box.
5. In the **Violation Detection Period** field, type the number of seconds that indicates the sliding time period to count violations for violation thresholds.  
The default is 900 seconds.
6. If you want the system to block all activity for a user, session, or IP address when the number of violations exceeds the threshold, specify one or more of the following settings on the Block All tab.

---

***Note:** For the system to block requests, the security policy Enforcement Mode must be set to blocking (see **Security > Application Security > Blocking > Settings**) and some violations must be set to block.*

---

Option	Description
<b>Blocked URLs</b>	Specify which URLs to block after the number of violations exceeds the enabled thresholds. To block all URLs, select <b>Block all URLs</b> . To block authenticated URLs protected by login pages, select <b>Block Authenticated URLs</b> .
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block this user's activity.
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block activity for this HTTP session.
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts to block the activity of this IP address.
<b>Block All Period</b>	Specify how long to block users, sessions, or IP addresses if the number of violations exceeds the threshold. To block the user, session, or IP address indefinitely, click <b>Infinite</b> . Otherwise, click <b>User-defined</b> and type the number of seconds to block the traffic. The default is 600 seconds.

7. If you want the system to log activity when the number of user, session, or IP address violations exceeds the threshold during the violation detection period, specify one or more of the following settings on the Log All Requests tab.

Option	Description
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging this user's activity for the log all requests period.
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging activity for this HTTP session for the log all requests period.

Option	Description
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system starts logging the activity of this IP address for the log all requests period.
<b>Log All Requests Period</b>	Specify how long the system should log all requests when any of the enabled thresholds is reached. Type the number of seconds in the field.

8. If you want more tolerant blocking for selected violations, such as those prone to false positives, specify one or more of the following settings on the Delay Blocking tab.

---

***Note:** For the system to block requests, the security policy Enforcement Mode must be set to blocking (see **Security > Application Security > Blocking > Settings**) and the specified violations must be set to block.*

---

Option	Description
<b>Username Threshold</b>	Select <b>Enable</b> and specify the number of violations a user must cause before the system begins blocking this user for the delay blocking period.
<b>Session Threshold</b>	Select <b>Enable</b> and specify the number of violations users must cause (during the violation detection period) before the system begins blocking this HTTP session for the delay blocking period.
<b>IP Address Threshold</b>	Select <b>Enable</b> and specify the number of violations allowed before the system begins blocking this IP address for the delay blocking period.
<b>Delay Blocking Period</b>	Type the number of seconds that the system should block the user, session, or IP address when any of the enabled thresholds is reached.
<b>Associated Violations</b>	Move the violations for which you want delay blocking from the <b>Available</b> list into the <b>Selected</b> list. If the selected violations occur, the system does not block traffic until one of the enabled thresholds is reached. At that point, the system blocks traffic causing those violations for the user, session, or IP address, but allows other transactions to pass.

9. Click **Save** to save your settings.

After you set up session tracking, if any enabled threshold exceeds the number of violations during the detection period, the system starts the configured actions for block all, log all requests, and delay blocking.

Test that you can log in to the web application through the Access Policy Manager™ logon page. You can also test that the security policy works by generating violations and reviewing the application security logs.

## Monitoring user and session information

To monitor user and session information, you first need to set up session tracking for the security policy.

You can use the reporting tools in Application Security Manager™ to monitor user and session details, especially when you need to investigate suspicious activity that is occurring with certain users, sessions, or IP addresses.

1. On the Main tab, click **SecurityReporting ApplicationSession Tracking Status**.  
The Session Tracking Status screen opens and shows the users, sessions, and IP addresses that the system is currently tracking for this security policy.
2. From the **Action** list, select the action by which to filter the data.

Action	Description
All	Specifies that the screen displays all entries. This is the default value.
Block All	Specifies that the system displays sessions whose requests the system blocks after the configured threshold was reached.
Log All Requests	Specifies that the system displays sessions whose requests the system logs after the configured threshold was reached.
Delay Blocking	Specifies that the system displays sessions whose requests the system delayed blocking until the configured threshold was reached.

3. From the **Scope** list, specify the scope (username, session, or IP address) by which to filter the data.

Option	Description
Alt	Specifies that the screen displays all entries. This is the default value.
Username	Specifies that the system displays usernames whose illegal requests exceeded the security policy's threshold values.
Session	Specifies that the system displays identification numbers of illegal sessions that exceeded the security policy's threshold values.
IP Address	Specifies that the system displays IP addresses where illegal requests from these IP addresses exceeded the security policy's threshold values.

4. If you want to filter the information by value, in the **Value** field, type the username, session identification number, IP address, or string. If empty, the screen displays all entries.
5. When you finish specifying the filter details, click **Go**.  
The Session Tracking Status list now shows the information specified in the Filter setting.

After you set up session tracking, you can monitor the specific requests that cause violations by examining each request and reviewing graphical charts.



---

# Chapter

# 15

---

## Mitigating Open Redirects

---

- *Overview: Mitigating open redirects*
  - *Implementation results*
-

## Overview: Mitigating open redirects

Application Security Manager™ (ASM) can protect users from open redirects. An *open redirect* is a vulnerability where the server tries to redirect the user to a target domain that is not defined in the security policy. This vulnerability is one of the OWASP top ten application security risks.

Spammers use open redirects in phishing attacks to get users to visit malicious sites without knowing it. Often, the request includes a parameter, which contains a URL that redirects a user to an external web application without any validation. An example of this vulnerability is a request such as:

```
https://www.good.com/redirect.php?url=http://www.evil.com.
```

This type of request may result in a response containing a Location header that points to a new target. For example:

```
HTTP/1.1 200 OK
Location: http://www.evil.com
```

You can configure redirection protection and the domains where users are permitted to be redirected on a response header in an existing security policy. By default, redirection protection is enabled in ASM with a pure wildcard configured as an allowed domain (effectively providing no enforcement). You can adjust the settings so that the security policy allows redirect to specific domains, and protects against unvalidated redirects.

This feature does not affect internal redirection, which is always allowed. For example, the following example would be allowed even if redirection protection is enabled on the system.

```
Location: /<anotherpage>/<onthisserver>/internal_redirect.php
```

### Task Summary

*Mitigating open redirects*

*Configuring how open redirects are learned*

*Enforcing redirection domains*

## Mitigating open redirects

You can configure an existing security policy in Application Security Manager™ (ASM) to protect users from being redirected by unvalidated redirects. By enabling redirection protection, you can help prevent users from being redirected to questionable phishing or malware web sites.

1. On the Main tab, click **Security > Application Security > Headers > Redirection Protection**. The Redirection Protection screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Make sure that the **Redirection Protection** check box is selected.
4. In the **Allowed Redirection Domains** setting, configure the domains where users can be redirected.
  - a) In the **Domain Name** field, type the name of the domain (in English-only, such as `yahoo.com`), or its IP address.

If protection is enabled and no domains are configured, then only relative URIs are allowed (for example, `/login.php`).

- b) If you want users to be able to be redirected to sub-domains of the specified domain, select **Include Sub-domains**.

If this check box is selected for `f5.com`, for example, then redirects to `www.f5.com`, `mail.f5.com`, and `websupport.f5.com` are also allowed. If it is not selected, redirection to sub-domains, such as `www.f5.com`, is not allowed. You need to add all allowed domains and sub-domains explicitly in that case.

- c) Click **Add**.

The system adds the domain to the security policy's list of allowed redirection domains.

You can add up to 100 redirection domains. If you are using the Policy Builder for automatic policy building, you can leave the \* wildcard configured to **Add All Entities** in the policy. When the tightening period is over and the policy is stable, the system will have added the redirection domains occurring within the traffic that it saw (if any), and then the system deletes the wildcard. If not using the Policy Builder, consider removing the \* wildcard.

5. In the **Allowed Redirection Domains** setting, select the \* wildcard and click the **Enforce** button to delete it.
6. Click **Save** to save your settings.

If ASM™ receives a request that attempts to redirect the user to a domain other than one that is listed in the redirection protection, the system issues an `Illegal redirection attempt` violation, which is an attack type of Open/Unvalidated Redirects. The violation is set to Learn, Alarm, and Block, by default. If the policy is in transparent mode, responses are always forwarded to the client. If the policy is in blocking mode, illegal redirection attempts are blocked.

## Configuring how open redirects are learned

You can adjust the explicit entities learning settings for redirection domains. Explicit learning settings specify when Real Traffic Policy Builder® adds, or suggests you add, explicit redirection domains to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**. The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings area, for the **Explicit Entities Learning** setting, for **Redirection Domains**, select the option for which Learning suggestions (based on real traffic) to use.

Option	Description
<b>Never (wildcard only)</b>	Specifies that when false positives occur, the system suggests relaxing the settings of the wildcard. If Policy Builder is running, it does not add domains to the list of allowed redirection domains, and does not remove the wildcard.
<b>Add All Entities</b>	Creates a comprehensive whitelist policy that includes all observed domains to the list of allowed redirection domains. If Policy Builder is running, it adds explicit domains to the security policy. When the security policy is stable, the * wildcard is removed. If Policy Builder is not running, the system suggests adding explicit domains. This is the default value.

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now learns new redirection domains according to the explicit learning setting you specified.

### Enforcing redirection domains

After you create a security policy and traffic is sent to the web application, the system adds domains where users are redirected by means of learning explicit entities. Redirection protection is enabled by default with a pure wildcard. You can review the redirection domains that are ready to be enforced, and add them to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Enforcement Readiness**. The Enforcement Readiness summary screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. To enforce all entities that are ready to be enforced, click **Enforce Ready**.  
If you click this button, you are done. Continue only if you want to review learning suggestions for redirection domains.
4. In the Enforcement Readiness Summary, check to see if a number appears in the Have Suggestions column next to redirection domains.  
A number greater than zero indicates that an Illegal Redirection Attempt occurred, and the system made a learning suggestion.
5. Click the number in the Have Suggestions column.
6. Select the domains to which you want the security policy to allow users to be redirected, and click **Accept**.
7. Click **Security > Application Security > Blocking** and check to be sure that the Learn, Alarm, and Block settings for the Illegal Redirection Attempt violation are selected.

The system adds selected redirection domains to the security policy and allows users to be redirected to them. Attempts at redirection to other domains will be blocked when the system is in blocking mode.

On the Policy Building Status (Automatic) screen, you can review the status of the security policy, see the policy elements that were added including the redirection domains, and view details about them.

### Implementation results

---

When you configure redirection protection, Application Security Manager™ (ASM) protects users from being redirected to a web site that is not listed in the allowed redirection domains. If the pure wildcard is listed as an allowed domain, ASM™ allows redirection to all domains. If you want to check whether users are redirected by the application, you can leave the wildcard as an allowed domain and let the system learn the redirect domains.

For the allowed domains, the system does not enforce protocol differences: HTTPS and HTTP are treated the same.

ASM sets the explicit entities learning for redirection domains in the general policy building settings. The security policy learns, by default, all domains (Add All Entities) where users are redirected. If you are using automatic policy building, the system adds to the security policy the redirect domains that match the pure wildcard, and lists how many it added, in the policy elements learned table on the Status screen. When the security policy is stable, the Policy Builder removes the wildcard redirect domain from the security policy, and allows users to be redirected only to the redirect domains that were added to the policy.

If you are building the security policy manually, the system learns and suggests that you add the redirect domains that it detects. You can determine whether there are redirection domains with learning suggestions by looking at the Enforcement Readiness Summary. After you add the legitimate redirect domains to the security policy, you can consider removing the wildcard redirect domain from the security policy. As a result, the policy on redirects becomes more strictly enforced.



---

# Chapter 16

---

## Setting Up Cross-Domain Request Enforcement

---

- *About cross-domain request enforcement* |

## About cross-domain request enforcement

---

Cross-Origin Resource Sharing (CORS) is an HTML5 feature that enables one website to access the resources of another website using JavaScript within the browser. On occasion, your web application might need to share resources with another external website that is hosted on a different domain. Using Application Security Manager™, you can safely allow CORS by specifying the conditions that state when a foreign web application is allowed to access your web application, after making a cross-domain request. This feature is called *cross-domain request enforcement*.

You enable cross-domain request enforcement as part of the Allowed URL properties within a security policy. Then you can specify which domains can access the response generated by requesting this URL (the “resource”), and also configure how to overwrite CORS response headers that are returned by the web server.

This feature does not affect internal redirection, which is always allowed. For example, `Location: /anotherpage/onthisserver/internal_redirect.php` would be allowed even if cross-domain request enforcement is enabled on the system.

## Setting up cross-domain request enforcement

For this task, you must have already created a URL in a security policy.

If you want to allow one website to access the resources of another website, you can add cross-domain request enforcement to an existing URL.

1. On the Main tab, click **Security > Application Security > URLs**.  
The Allowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Allowed URLs List, click the name of the URL you want to modify.  
The Allowed URL Properties screen opens.
4. From the **Allowed URL Properties** list, select **Advanced**.
5. Select the **HTML5 Cross-Domain Request Enforcement** check box.  
The screen now includes an additional tab in the next area.
6. On the HTML5 Cross-Domain Request Enforcement tab, select the **Allow HTML5 Cross-Origin Requests** check box.  
The tab now includes additional settings where you define which domains can access the response generated by a request to this URL, and how to overwrite CORS response headers returned by the web server.
7. In the **Allowed Origins** setting, add the origins that are allowed to share data returned by this URL.  
If you select **Unmodified**, the system leaves the response header as set by the server. If you select **Replace with**, specify the origin names:
  - a) For **Protocol**, select the appropriate protocol for the allowed origin.
  - b) For **Origin Name**, type the domain name or IP address that you want to allow to share your data with.  
  
Wildcards are allowed in the names. For example: `*.f5.com` will match `b.f5.com`; however it will not match `a.b.f5.com`.
  - c) For **Port**, select the port that other web applications can use to request data from your web application, or use the `*` wildcard for all ports.



- d) If you want to allow sub-domains to receive data, select the **Include Sub-Domains** check box.
- e) Click **Add** to add the origins.  
The origins that can share data with the URL are included in the list.

8. For **Allowed Methods**, specify which methods other applications may use when requesting this URL from another domain.

Move the methods to allow from the **Available Methods** to the **Allowed Methods** list.

---

**Important:** Any method you allow here must also be in the *Allowed Methods* list in the security policy (*Security > Application Security > Headers > Methods*).

---

9. For **Allowed Headers**, type the headers to allow other applications to use when requesting this URL from another domain.  
Allowed headers are request headers sent by clients. For example, to allow clients to send Ajax requests, type `X-Requested-With`, and to allow XML requests, type `Content-Type`.
10. For **Exposed Headers**, specify the headers that can be exposed in JavaScript and shared with other applications to use when requesting this URL from another domain.  
Exposed headers are the headers returned by the server in the response. For example, To discover server side web application technology, type `X-Powered-By`.
11. For **Allow Credentials**, specify whether requests from applications in another domains can include user credentials.
12. For **Maximum Age**, specify the number of seconds that the results of a preflight request can be cached or use the default.
13. Click **Update**.
14. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy allows requests for the URL to access the resources of other websites hosted in a different domain according to the enforcement conditions that you configured.

## How cross-domain request enforcement works

If you enable cross-domain request enforcement, the system must authorize requests (typically AJAX requests) made from one domain to another. When a client makes a request to another origin, the browser sends a *preflight request* to determine whether JavaScript from another domain may access your resource. The preflight request consists of an OPTIONS HTTP method and CORS-related headers.

The CORS-related headers that are included in a preflight request are:

Header	Description
Origin	Determines requesting origin.
Access-Control-Request-Method	Indicates which methods are used in the actual request (other than simple methods).
Access-Control-Request-Headers	Indicates which headers are used in the actual request (other than simple headers).

In response to the preflight request, the system uses these CORS response headers:

Header	Description
Access-Control-Allow-Origin	List of origins the resource may be shared among (support wildcard).

Header	Description
Access-Control-Allow-Credentials	Indicates whether actual request may include user credentials (true/false).
Access-Control-Allow-Methods	Indicates which methods can be used during the actual request.
Access-Control-Allow-Headers	Indicates which request headers can be used during the actual request.
Access-Control-Max-Age	Indicates how long (in seconds) to cache the results of a preflight request in the browser.
Access-Control-Expose-Headers	Indicates which response headers are safe to expose to JavaScript.

The browser uses the response to determine whether to allow the JavaScript to make the actual request. If the cross-domain request is authorized, the server processes the actual requests by rechecking the origin and including another response header:

Header	Description
Access-Control-Expose-Headers	Indicates which response headers are safe to expose to JavaScript.

The browser then allows the foreign domain to send its original requests.

If you do not enable cross-domain request enforcement, the system removes all cross-origin request headers and CORS is not allowed for the URL.

---

# Chapter 17

---

## Implementing Web Services Security

---

- *Overview: Implementing web services security*
-

### Overview: Implementing web services security

---

Web services security adds another level of protection to XML-based web applications by embedding security-related data within SOAP messages. For web services that Application Security Manager™ protects, you can use web services security to do the following:

- Encrypt and decrypt parts of SOAP messages
- Digitally sign parts of SOAP messages
- Verify parts of SOAP messages using digital signatures

If you want to use features such as encryption, you can add web services security to an existing security policy that has an associated XML profile. You can enforce web services security only for URLs.

#### Task Summary

*Adding client and server certificates*

*Enabling encryption, decryption, signing, and verification of SOAP messages*

*Writing XPath queries*

*Configuring blocking actions for web services security*

### About client and server certificates

Client and server certificates are XML digital signatures that ensure the integrity of the message data, and can authenticate the identity of the document signer. By importing client and server certificates, the system can perform encryption and decryption of SOAP messages.

The system uses client and server certificates differently:

#### Server Certificates

Decrypt SOAP messages from a web client to a web service, or sign SOAP messages from a web service back to a web client.

#### Client Certificates

Encrypt SOAP messages from a web service to a web client, or verify SOAP messages from a web client to a web service.

### Adding client and server certificates

To use web services security for encryption, decryption, and digital signature signing and verification, you must upload client and server certificates onto the Application Security Manager™. The system uses these certificates to process Web Services Security markup in SOAP messages within requests and responses to and from web services.

You must import both client and server certificates to perform encryption and decryption on the Application Security Manager.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Certificates Pool**.  
The Certificates Pool screen opens.
2. Add one server certificate, and a client certificate for each client that you want to access the XML application. For each certificate you want to add, perform these steps:

---

***Note:** The server and client certificates must be PEM files in x509v3 format. Also, the server certificate should contain the server's private key.*

---

- a) Click **Add**.  
The Create New Certificate screen opens.
- b) For **Name**, type a name for the certificate
- c) For **Type**, select **Client** or **Server**, as appropriate.
- d) For the **.PEM File** setting, either select **Upload File** from the list, then browse to and upload a certificate, or select **Paste text** to paste a copy of the certificate in the field.
- e) To store the certificate even if it is expired or untrusted, enable the **Save Expired/Untrusted Certificate** setting
- f) Click **Add**.

The system adds the certificate to the certificates pool.

You have added client or server certificates to the system's database. You can configure a security policy to use these certificates in an associated XML profile. The certificates in the pool can be used for any web applications.

## Enabling encryption, decryption, signing, and verification of SOAP messages

Before you can complete this task, you first must have created a security policy using the option **Create a policy for XML and web services manually**, created and associated an XML profile with the policy, and uploaded security certificates onto the system.

You can use the web services security features of Application Security Manager™ to off load encryption and decryption of SOAP messages from the application server. Web services security can also handle verification of digital signatures and digital signing of SOAP messages.

1. On the Main tab, click **Security > Application Security > Content Profiles > XML Profiles**.  
The XML Profiles screen opens.
2. Click the name of the XML profile for which you want to configure web services security, or create a new profile.  
The XML Profile Properties screen opens.
3. For the **Web Services Security** setting, select **Enabled**.
4. Click **Web Services Security Configuration**.  
The XML Profile Properties screen displays Web Services Security Configuration options.
5. For **Server Certificate**, select one server certificate from the list, or click **Create** to add a new certificate to the configuration.  
A Request area appears after you specify the certificate.  
The system uses the server certificate to decrypt SOAP messages from a web client to a web service, or sign SOAP messages from a web service back to a web client.
6. For **Client Certificates**, select names from the **Available** list and then move them into the **Members** list.  
The system uses the client certificates to encrypt SOAP messages from a web service to a web client, or to verify SOAP messages from a web client to a web service.
7. In the Request area, for **Action**, select the action you want the system to perform in SOAP message requests.
  - Select **Verify and Decrypt** to decrypt and verify digitally signed SOAP messages. F5 recommends that you use this value.
  - Select **Decrypt** to decode encrypted SOAP messages.

- Select **Verify** to validate digitally signed SOAP messages. This option is available only if you imported client certificates, but no server certificate.

8. For **Role/Actor**, select a role to determine which security headers you want the system to process in SOAP message requests.

Role	Description
<b>Do not check role/actor</b>	Process all security headers regardless of the role. This is the default setting.
<b>Custom role/actor</b>	Process security headers that contain the role you type in the adjacent box.
<b>next</b>	Process security headers that contain the role <b>next</b> or <code>http://www.w3.org/2003/05/soap-envelope/role/next</code> .
<b>none</b>	Process security headers that contain the role <b>none</b> or <code>http://www.w3.org/2003/05/soap-envelope/role/none</code> .
<b>ultimateReceiver</b>	Process security headers that contain the role <b>ultimateReceiver</b> or <code>http://www.w3.org/2003/05/soap-envelope/role/ultimateReceiver</code> .

9. Select the **Enforce And Verify Defined Elements** check box to confirm that elements defined in the Namespaces and Elements area of the screen and contained in the request are signed and verified. This setting also enforces the options **SOAP Body in Request Must Be Signed and Verified** and **Enforce Timestamp In Request**.

10. In the Response area, for **Action**, select the action you want the system to perform on the elements defined in the Namespaces and Elements area of the screen for SOAP message responses.

- Select **Encrypt** to encrypt the elements.
- Select **Sign** to digitally sign the elements.
- Select **Sign, Then Encrypt** to first digitally sign and then encrypt the elements. F5 recommends that you use this value.
- Select **Encrypt, Then Sign** to first encrypt, then digitally sign the elements.

---

***Note:** For the action to occur, you must also select **Apply Action To Defined Elements**.*

---

11. To limit how long a security header is valid:

- a) Enable the **Add Timestamp** setting.
- b) Type the length of time (in seconds) the timestamp should be valid. The default is 300 seconds. If you want the timestamp to be valid for an unlimited amount of time, enter 0. The maximum value is 134217728 seconds.

12. For **Role/Actor**, select a role to insert into the security header of SOAP messages.

Role	Description
<b>Do not assign role/actor</b>	If the document contains a security header without a role, the system inserts the cryptographic information into the security header. This is the default setting.
<b>Assign custom role/actor</b>	If the document contains a security header with a custom role, the system inserts the cryptographic information into the existing security header. In the field, type the custom role/actor attribute.
<b>next</b>	If the document contains a security header with the <b>next</b> role, the system inserts the cryptographic information into that security header.

Role	Description
<b>none</b>	If the document contains a security header with the <b>none</b> role, the system inserts the cryptographic information into that security header.
<b>ultimateReceiver</b>	If the document contains a security header with the <b>ultimateReceiver</b> role, the system inserts the cryptographic information into that security header.

13. If the response action includes signing, for **Signature Algorithm**, select the type of signature algorithm used to sign parts of SOAP messages in responses that match the response elements that you configure in the Namespaces and Elements area of the screen.

- Select **RSA-SHA-1** (the default value) to use the RSA public cryptosystem for encryption and authentication.
- Select **HMAC-SHA-1** to use secret-key hashing.

---

*Tip: Be sure your clients support this type of encryption.*

---

14. If the response action includes encryption, for **Encryption Algorithm** and **Key Transport Algorithm**, select the types of encryption to use for the elements and keys.

15. Select the **Apply Action To Defined Elements** check box to perform the action you selected.

16. In the Namespaces and Elements area of the Web Services Security Configuration, configure these settings to specify how to process the XML document:

- For **Namespace Mappings**, add the namespace mappings (prefix and URLs) the system uses for XPath queries:
- Select the **SOAP Body In Request Must Be Signed And Verified** check box to verify that requests contain a SOAP body that is digitally signed and verified.  
If not, the system issues a `Verification Error` violation.
- Select the **Enforce Timestamp In Request** check box to verify that the SOAP request contains a valid timestamp.  
If the request has no timestamp, the `Missing Timestamp` violation occurs. If the timestamp is expired, the system issues the `Expired Timestamp` violation.

17. Specify which parts of the XML document you want the system to process:

- If you want the response action to apply to the whole SOAP message (`/soapenv:Envelope/soapenv:Body`), select the **Apply Action to Entire Response Body Value** check box.
- To specify which parts of requests and responses you want the system to process, use the **Elements** setting to add XPath expressions to define the parts of the SOAP message to encrypt.

18. If you are updating an existing profile, click **Update**. If you are creating a new profile, click **Create**.

The security policy that is associated with the XML profile now includes web services security for the XML application.

## Writing XPath queries

You can write up to three XPath queries to define the content that you are looking for in XML documents. When writing XPath queries, you use a subset of the XPath syntax described in the XML Path Language (XPath) standard at <http://www.w3.org/TR/xpath>.

These are the rules for writing XPath queries for XML content-based routing.

1. Express the queries in abbreviated form.
2. Map all prefixes to namespaces.
3. Use only ASCII characters in queries.
4. Write queries to match elements and attributes.
5. Use wildcards as needed for elements and namespaces; for example, `//emp:employee/*`.
6. Do not use predicates in queries.

### Syntax for XPath expressions

This table shows the syntax to use for XPath expressions.

Expression	Description
Nodename	Selects all child nodes of the named node.
@Attname	Selects all attribute nodes of the named node.
/	Indicates XPath step.
//	Selects nodes that match the selection no matter where they are in the document.

### XPath query examples

This table shows examples of XPath queries.

Query	Description
/a	Selects the root element a.
//b	Selects all b elements wherever they appear in the document.
/a/b:*	Selects any element in a namespace bound to prefix b, which is a child of the root element a.
//a/b:c	Selects elements in the namespace of element c, which is bound to prefix b, and is a child of element a.

## Configuring blocking actions for web services security

You can select which web services security errors must occur for the system to learn, log, or block requests that trigger the errors. These errors are sub-violations of the parent violation, `Web Services Security failure`.

1. On the Main tab, click **Security > Application Security > Blocking**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Adjust the **Enforcement Mode** setting if needed.
  - To block traffic that causes violations, select **Blocking**.
  - To not block traffic even if it causes violations (allowing you to make sure that legitimate traffic would not be blocked), select **Transparent**.

You can only configure the Block flag if the enforcement mode is set to **Blocking**.



4. Review the **Web Services Security failure** violation and adjust the **Learn**, **Alarm**, and **Block** flags as required.
5. Click the **Web Services Security failure** violation link.  
The web services subviolations are displayed.
6. Enable or disable the web services subviolations, as required.
7. Click **Save** to save your settings.
8. To put the security policy changes into effect immediately, click **Apply Policy**.

If a request causes one of the enabled errors to occur, web services security stops parsing the document. How the system reacts depends on how you configured the blocking settings for the `Web Services Security failure` violation:

- If configured to **Learn** or **Alarm** when the violation occurs, the system does not encrypt or decrypt the SOAP message, and sends the original document to the web service.
- If configured to **Block** when the violation occurs, the system blocks the traffic and prevents the document from reaching its intended destination.



---

# Chapter 18

---

## Fine-tuning Advanced XML Security Policy Settings

---

- *Fine-tuning XML defense configuration*
- *Advanced XML defense configuration settings*
- *Masking sensitive XML data*
- *Overriding meta characters based on content*
- *Managing SOAP methods*

## Fine-tuning XML defense configuration

---

Before you can perform this task, you must have created a security policy using the option **Create a policy for XML and web services manually**, and created and associated an XML profile with the policy.

The defense configuration in an XML profile provides formatting and attack pattern checks for the XML data. The defense configuration complements the validation configuration to provide comprehensive security for XML data and web services applications. If your XML application has special requirements, you can adjust the defense configuration settings. This is an advanced task that is not required when creating a security policy for an XML application.

1. On the Main tab, click **Security > Application Security > Content Profiles > XML Profiles**.  
The XML Profiles screen opens.
2. Click the name of the XML profile for which you want to modify the advanced defense configuration settings.  
The XML Profile Properties screen opens.
3. Optionally, modify the attack signatures, meta characters, or sensitive data for this XML profile on the appropriate tabs.
4. On the XML Firewall Configuration tab, from the **Defense Configuration** list, select **Advanced**.  
The screen displays additional defense configuration settings.
5. For the **Defense Level** setting, select the protection level you want for the application.  
The defense level determines the granularity of the security inspection for the XML application. You can choose **High**, **Medium**, or **Low** and let the system determine the defense level settings. Or you can set the level, then adjust any of the settings to create a **Custom** defense level.
6. Adjust the defense configuration settings as required by your application and traffic.
7. Click **Update** to update the XML profile.
8. To put the security policy changes into effect immediately, click **Apply Policy**.

A trade-off occurs between ease of configuration and defense level. The higher the defense level, the more you may need to refine the security policy. For example, if you use the default defense level of **High**, the XML security is optimal; however, when you initially apply the security policy, the system may generate false-positives for some XML violations. However, a **Low** defense level may not protect the application as strictly but may cause fewer false positives.

The system checks requests that contain XML data to be sure that the data complies with the various document limits defined in the defense configuration of the security policy's XML profile. The system generally examines the message for compliance to boundaries such as the message's size, maximum depth, and maximum number of children. When the system detects a problem in an XML document, it causes the XML data does not comply with format settings violation, if the violation is set to Alarm or Block.

## Advanced XML defense configuration settings

---

This table describes the defense configuration settings. The **Defense Level** setting in an XML profile determines the default values for the setting, or you can adjust them. A value of **Any** indicates unlimited; that is, up to the boundaries of an integer type.

Setting	Description	Default Values
<b>Defense Level</b>	Specifies the level of protection that the system applies to XML documents, applications, and services. If you change any of the default settings, the system automatically changes the defense level to <b>Custom</b> .	High, Medium, Low
<b>Allow DTDs</b>	Specifies, when enabled, that the XML document can contain Document Type Definitions (DTDs).	High: Disabled, Medium: Enabled, Low: Enabled
<b>Allow External References</b>	Specifies, when enabled, that the XML document is allowed to list external references using operators, such as schemaLocation and SYSTEM.	High: Disabled, Medium: Disabled, Low: Enabled
<b>Tolerate Leading White Space</b>	Specifies, when enabled, that leading white spaces at the beginning of an XML document are acceptable.	High: Disabled, Medium: Disabled, Low: Enabled
<b>Tolerate Close Tag Shorthand</b>	Specifies, when enabled, that the close tag format <code>&lt;/&gt;</code> , which is used in the XML encoding for Microsoft Office Outlook Web Access, is acceptable.	High: Disabled, Medium: Disabled, Low: Enabled
<b>Tolerate Numeric Names</b>	Specifies, when enabled, that the entity and namespace names can start with an integer (0-9). Note that this is a compatibility option for use with Microsoft Office Outlook Web Access.	High: Disabled, Medium: Disabled, Low: Enabled
<b>Allow Processing Instructions</b>	Specifies, when enabled, that the system allows processing instructions in the XML request. If you upload a WSDL file that references valid SOAP methods, this setting is inactive.	High: Enabled, Medium: Enabled, Low: Enabled
<b>Allow CDATA</b>	Specifies, when enabled, that the system permits the existence of character data (CDATA) sections in the XML document part of a request.	High: Disabled, Medium: Enabled, Low: Enabled
<b>Maximum Document Size</b>	Specifies, in bytes, the largest acceptable document size.	High: 1024000, Medium: 10240000, Low: Any
<b>Maximum Elements</b>	Specifies the maximum number of elements that can be in a single document.	High: 65536, Medium: 512000, Low: Any

Setting	Description	Default Values
<b>Maximum Name Length</b>	Specifies, in bytes, the maximum acceptable length for element and attribute names.	High: 256, Medium: 1024, Low: Any
<b>Maximum Attribute Value Length</b>	Specifies, in bytes, the maximum acceptable length for attribute values.	High: 1024, Medium: 4096, Low: Any
<b>Maximum Document Depth</b>	Specifies the maximum depth of nested elements.	High: 32, Medium: 128, Low: Any
<b>Maximum Children Per Element</b>	Specifies the maximum acceptable number of child elements for each parent element.	High: 1024, Medium: 4096, Low: Any
<b>Maximum Attributes Per Element</b>	Specifies the maximum number of attributes for each element.	High: 16, Medium: 64, Low: Any
<b>Maximum NS Declarations</b>	Specifies the maximum number of namespace declarations allowed in a single document.	High: 64, Medium: 256, Low: Any
<b>Maximum Namespace Length</b>	Specifies the largest allowed size, in bytes, for a namespace prefix in the XML part of a request.	High: 256, Medium: 1024, Low: Any

## Masking sensitive XML data

Before you can perform this task, you must have created a security policy using the option **Create a policy for XML and web services manually**, and created and associated an XML profile with the policy.

You can mask sensitive XML data so that it does not appear in the interface or logs. You set this up in the XML profile of a security policy.

1. On the Main tab, click **Security > Application Security > Content Profiles > XML Profiles**.  
The XML Profiles screen opens.
2. Click the name of the XML profile for which you want to mask sensitive data.  
The XML Profile Properties screen opens.
3. Click the Sensitive Data Configuration tab.  
The screen displays Sensitive Data Configuration settings.
4. On the XML Firewall Configuration tab, from the **Defense Configuration** list, select **Advanced**.  
The screen displays additional defense configuration settings.
5. For **Namespace**, select one of the options:

Option	Use
<b>Any Namespace</b>	When the sensitive data can appear in an element or attribute in any namespace.
<b>Custom</b>	When the sensitive data appears in an element or attribute in a particular namespace. Type the namespace prefix that can contain sensitive data.
<b>No Namespace</b>	When no namespace in the XML document has an element or attribute with a value that contains sensitive data.

6. For **Name**:
  - a) Select **Element** or **Attribute** to indicate whether the sensitive data appears as a value of either an XML element or an attribute.
  - b) In the field, type the XML element or attribute whose value can contain sensitive data. Entries in this field are case-sensitive.
7. Click **Add** to add the information you entered in the **Namespace** and **Name** fields to the Sensitive Data table and the XML profile.
8. Click **Update** to update the XML profile.
9. To put the security policy changes into effect immediately, click **Apply Policy**.

The system checks requests that contain XML data and if they contain sensitive data, that data is masked in logs and in request content shown in the Application Security Manager™.

## Overriding meta characters based on content

---

Before you can perform this task, you must have previously created a JSON, XML, or Google Web Toolkit (GWT) content profile.

You can have the system check for allowed or disallowed meta characters based on the content of a request as defined in content profiles (XML, JSON, or GWT). In addition, you can override the security policy settings so that the system avoids checking for meta characters in particular content.

1. On the Main tab, point to **Security > Application Security > Content Profiles** and click a content profile type (**XML**, **JSON**, or **GWT**).
2. In the profiles list, click the name of the content profile for which you want to override meta character checks.  
The profile properties screen opens.
3. Click the Meta Characters tab (for XML) or Value Meta Characters (for JSON or GWT).
4. Select the appropriate check box:
  - For JSON or GWT profiles, select the **Check characters** check box to have the system check for meta characters in JSON data.
  - For XML profiles, select **Check element value characters** to check meta characters in XML elements, and select **Check attribute value characters** to check meta characters in XML attributes.
5. In the **Global Security Policy Settings** list, review the meta characters that are assigned to the security policy, and which are allowed or disallowed in the content profile.
6. From the **Global Security Policy Settings** list, move any meta characters that you want to override for this content profile into the **Overridden Security Policy Settings** list.
7. Set the meta character to **Allow** or **Disallow** in the overridden settings list (the opposite from the global setting).
8. Click **Update** to update the content profile.
9. To put the security policy changes into effect immediately, click **Apply Policy**.

If the content matches that defined in the content profile, meta characters are allowed or disallowed according to the overridden meta character settings in the content profile.

## Managing SOAP methods

---

Before you can perform this task, you must have created a security policy using the option **Create a policy for XML and web services manually**, and created and associated an XML profile with the policy. You must have already uploaded a WSDL document in the XML profile.

When using a WSDL document in the XML profile, the system includes the relevant SOAP methods in the validation configuration. You can enable or disable the SOAP methods, as needed.

1. On the Main tab, click **Security > Application Security > Content Profiles > XML Profiles**.  
The XML Profiles screen opens.
2. Click the name of the XML profile for which you want to enable or disable one or more SOAP methods.  
The XML Profile Properties screen opens.
3. In the Validation Configuration area, the **Valid SOAP Methods** table lists the SOAP methods used by the WSDL file you uploaded previously. Select or clear the **Enabled** check box for each method that you want to enable (allow) or disable (not allow).
4. Click **Update** to update the XML profile.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The XML profile is updated if you changed which SOAP methods are allowed by the security policy. If you disable a SOAP method, and a request contains that method, the system issues the `SOAP method not allowed violation`, and blocks the request if the enforcement mode is set to blocking.



---

# Chapter 19

---

## Adding JSON Support to an Existing Security Policy

---

- *Overview: Adding JSON support to existing security policies*
  - *Implementation result*
-

## Overview: Adding JSON support to existing security policies

---

This implementation describes how to add JSON (JavaScript® Object Notation) support to an existing security policy for an application that uses JSON for data transfer. You create a JSON profile to define what the security policy enforces and considers legal when it detects traffic that contains JSON data.

You can add JSON support to a security policy by completing these tasks.

### Task Summary

*Creating a JSON profile*

*Associating a JSON profile with a URL*

*Associating a JSON profile with a parameter*

## Creating a JSON profile

Before you can complete this task, you need to have already created a security policy for your application.

This task describes how to create a JSON profile that defines the properties that the security policy enforces for an application sending JSON payloads.

---

**Note:** The system supports JSON in UTF-8 and UTF-16 encoding.

---

1. On the Main tab, click **Security > Application Security > Content Profiles > JSON Profiles**.
2. Click **Create**.  
The Create New JSON Profile screen opens.
3. Type the name of the profile.
4. Adjust the maximum values that define the JSON data for the AJAX application, or use the default values.
5. In the Attack Signatures tab, in the **Global Security Policy Settings** list, select any attack signatures that you want to apply to this profile, and then move them into the **Overridden Security Policy Settings** list.

---

**Tip:** If no attack signatures are listed in the **Global Security Policy Settings** list, create the profile, update the attack signatures, then edit the profile.

---

6. Once you have moved any applicable attack signatures to the **Overridden Security Policy Settings** list, enable or disable each them as needed:

Option	Description
<b>Enabled</b>	Enforces the attack signature for this JSON profile, although the signature might be disabled in general. The system reports the violation <code>Attack Signature Detected</code> when the JSON in a request matches the attack signature.
<b>Disabled</b>	Disables the attack signature for this JSON profile, although the signature might be enabled in general.

7. To allow or disallow specific meta characters in JSON data (and thus override the global meta character settings), click the Value Meta Characters tab.
  - Select the **Check characters** check box, if it is not already selected.

- Move any meta characters that you want allow or disallow from the **Global Security Policy Settings** list into the **Overridden Security Policy Settings** list.
  - In the **Overridden Security Policy Settings** list, change the meta character state to **Allow** or **Disallow**.
8. To mask sensitive JSON data (replacing it with asterisks), click the Sensitive Data Configuration tab.
- In the **Element Name** field, type the JSON element whose values you want the system to consider sensitive.
  - Click **Add**.

---

**Important:** *If the JSON data causes violations and the system stops parsing the data part way through a transaction, the system masks only the sensitive data that was fully parsed.*

---

Add any other elements that could contain sensitive data that you want to mask.

9. Click **Create**.  
The system creates the profile and displays it in the JSON Profiles list.

This creates a JSON profile which does not affect the security policy until you associate the profile with a URL or parameter.

Next, you need to associate the JSON profile with any URLs or parameters that might include JSON data.

## Associating a JSON profile with a URL

Before you can associate a JSON profile with a URL, you need to have created a security policy with policy elements including application URLs, and the JSON profile.

You can associate a JSON profile with one or more explicit or wildcard URLs.

1. On the Main tab, click **Security > Application Security > URLs**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. From the Allowed URLs List, click the name of a URL that might contain JSON data.  
The Allowed URL Properties screen opens.
4. Next to **Allowed URL Properties**, select **Advanced**.  
The screen refreshes to display additional configuration options.
5. For the **Header-Based Content Profiles** setting, in the **Request Header Name** field, type the explicit string or header name that defines when the request is treated as the **Parsed As** type; for example, `content-type`.  
This field is not case sensitive.

---

**Note:** *If the URL always contains JSON data, just change the default header-based content profile to be **Parsed As JSON**, then you do not have to specify the header name and value here.*

---

6. For the **Header-Based Content Profiles** setting, in the **Request Header Value** field, type the wildcard (including \*, ?, or [chars]) for the header value that must be matched in the **Request Header Name** field; for example, `*json*`.  
This field is case sensitive.
7. From the **Parsed As** list, select **JSON**.
8. From the **Profile Name** list, either select the JSON profile appropriate for this URL, or click **Create** to quickly add a new profile to the configuration.
9. Click **Add**.

Add as many header types as you need to secure this URL, clicking **Add** after specifying each one.

10. To override the global meta character settings for this URL, adjust the meta character policy settings:
  - In the Meta Characters tab, select the **Check characters on this URL** check box, if it is not already selected.
  - Move any meta characters that you want allow or disallow from the **Global Security Policy Settings** list into the **Overridden Security Policy Settings** list.
  - In the **Overridden Security Policy Settings** list, change the meta character state to **Allow** or **Disallow**.
11. Click **Update**.
12. To put the security policy changes into effect immediately, click **Apply Policy**.

The JSON profile is associated with the URL.

Continue to associate JSON profiles with any URLs in the application that might contain JSON data.

### Associating a JSON profile with a parameter

You need to have created a security policy with policy elements including parameters and a JSON profile before starting this procedure.

You can associate a JSON profile with a parameter.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Parameters List area, click the name of a parameter to which to assign a JSON profile. The Parameter Properties screen opens.
4. For the **Parameter Value Type** setting, select **JSON value**.
5. From the **JSON Profile** list, select the JSON profile to use for this parameter.
6. Click **Update**.  
The system associates the JSON profile with the parameter.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

Continue to associate JSON profiles with any parameters in the application that might contain JSON data.

### Implementation result

---

You have manually added JSON support to the active security policy. The policy can now secure applications that use JSON for data transfer between the client and the server. If web application traffic includes JSON data, the system checks that it meets the requirements that you specified in the JSON profile.

---

# Chapter

# 20

---

## Automatically Creating Security Policies for AJAX Applications

---

- *Application security for applications that use AJAX*
- *Overview: Creating a security policy for applications that use AJAX*
- *Implementation result*

## Application security for applications that use AJAX

---

Application Security Manager™ can protect AJAX applications including those that use JSON or XML for data transfer between the client and the server. If the AJAX application uses XML for data transfer, the security policy requires that an XML profile be associated with a URL or parameter. If the AJAX application uses JSON for data transfer, the security policy requires that a JSON profile be associated with a URL or parameter. If the AJAX application uses HTTP for data transfer, no profile is needed.

You can also set up AJAX blocking response behavior for applications so that if a violation occurs during AJAX-generated traffic, the system displays a message or redirects the application user to another location.

## Overview: Creating a security policy for applications that use AJAX

---

AJAX (Asynchronous JavaScript and XML) applications make requests to the server and send responses to the client formatted using XML or JavaScript Object Notation (JSON). You can create a security policy automatically for applications that use AJAX.

### Task Summary

*Creating a security policy automatically*

*Reviewing security policy status*

## Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the **Create** button.  
The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
  - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
  - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
  - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
  - If creating a new virtual server, specify the protocol, name, IP address and port, pool IP address, and port.
  - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy.
  - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

The name of the new or existing virtual server becomes the name of the security policy.

The Select Deployment Scenario screen opens.

5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.  
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

---

**Important:** You cannot change this setting after you have created the security policy.

---

7. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

---

**Important:** You cannot change this setting after you have created the security policy.

---

8. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.

9. Click **Next**.

The Configure Attack Signatures screen opens.

10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.  
The system adds the attack signatures needed to protect the selected systems.

11. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

---

**Note:** Because the Real Traffic Policy Builder® begins building the security policy in Blocking mode, you can keep signature staging enabled to make sure that false positives do not occur.

---

New and updated attack signatures remain in staging for 7 days, and are not enforced (according to the learn, alarm, and block flags) during that time.

12. Click **Next**.

The Configure Automatic Policy Building screen opens.

13. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
<b>Fundamental</b>	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
<b>Enhanced</b>	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, Explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles.

Option	Description
<b>Comprehensive</b>	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

- For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

- For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
<b>All</b>	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted, the policy is created faster when you select this option.
<b>Address List</b>	Specifies networks to consider safe. Fill in the <b>IP Address</b> and <b>Netmask</b> fields, then click <b>Add</b> . This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

- If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.

- If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.

- Click **Next**.

The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.

- Click **Finish** to create the security policy.

The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM<sup>™</sup> creates the virtual server with an HTTP profile, and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not



block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

---

**Tip:** *This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.*

---

## Reviewing security policy status

You can monitor the general progress of the Real Traffic Policy Builder®, see what policy elements the system has learned, and view additional details on the Automatic Policy Building Status screen.

1. On the Main tab, click **Security > Application Security > Policy Building > Status (Automatic)**. The Status (Automatic) screen opens where you can see the automatic policy building status, file types, URLs, parameters, and cookies that were added to the security policy.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Review any messages in the identification and messages area to learn what is currently happening on the system.

For example, messages say when the Policy Builder is enabled, when the security policy was last updated, and the number of elements that were learned.

4. Review the status of the Real Traffic Policy Builder.

Option	Description
<b>Enabled</b>	The system is configured to automatically build a security policy, and the Policy Builder is processing traffic.
<b>Disabled</b>	The system is not processing traffic. Check the automatic policy building configuration. If you did not associate a virtual server, you need to do that to process traffic.
<b>Detecting Language</b>	The system is still configuring the language after analyzing responses to identify the language of the web application. The Policy Builder is enabled, but it cannot add elements to the security policy until the language is set.

5. Examine the **General Progress** of the security policy.

A progress bar indicates the stability level of the security policy. The progress bar reaches 100% when the policy is stable, no new policy elements need to be added, and time and traffic thresholds have been reached.

6. In the Policy Elements Learned table, review the number of elements that the Policy Builder has analyzed and added to the security policy, and the attributes that need to be updated.

---

**Tip:** *Click the number in the Elements column to see the specific elements that were added.*

---

7. Optionally, in the Details tree view, click the expand button for any item to learn more about that security policy element, what the system has seen so far, and what it will take to stabilize the element.

When enough traffic from unique sessions occurs over a period of time, the system starts to enforce the file types and other elements in the security policy. When enforced as part of a stable policy, the files types and other elements are removed from staging.

## Implementation result

---

The Real Traffic Policy Builder<sup>®</sup> creates a security policy that can protect applications that use AJAX with JSON or XML for data transfer between the client and the server. The system examines the traffic and creates an appropriate profile. If the application uses XML, the security policy includes one or more XML profiles associated with URLs or parameters. If the application uses JSON, the security policy includes one or more JSON profiles associated with URLs or parameters.

---

# Chapter

# 21

---

## Adding AJAX Blocking Response Behavior to a Security Policy

---

- *Overview: Adding AJAX blocking and login response behavior*
- *Configuring the blocking response for AJAX applications*

### Overview: Adding AJAX blocking and login response behavior

---

Normal policy blocking and login response behavior could interfere with applications that use AJAX. If you want to display a message or redirect traffic without interfering with the user experience while browsing to an AJAX-featured web application, you need to enable AJAX blocking behavior (JavaScript injection). You can implement blocking and login response behavior for applications that use AJAX with JSON or XML for data transfer.

---

**Important:** *You can implement AJAX blocking behavior only for applications developed using one of the following frameworks:*

- Microsoft® ASP.NET
- jQuery
- Prototype®
- MooTools

---

By default, if you enable AJAX blocking behavior, when an AJAX request results in a violation that is set to **Block**, Application Security Manager performs the default AJAX response page action. The system presents a login response if the application user sends an AJAX request that attempts to directly access a URL that should only be accessed after logging in.

---

**Note:** *Enabling AJAX blocking behavior has performance implications.*

---

### Configuring the blocking response for AJAX applications

---

Before you can complete this task, you need to have already created a security policy for your web application. The application needs to have been developed using ASP.NET, jQuery, Prototype®, or MooTools to use AJAX blocking behavior.

When the enforcement mode of the security policy is set to blocking and a request triggers a violation (that is set to block), the system displays the AJAX blocking response according to the action set that you define. If a login violation occurs when requesting the login URL, the system sends a login response page, or redirects the user.

1. On the Main tab, click **Security > Application Security > Blocking > Response Pages**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click the AJAX Response Page tab.
4. Select the **Enable AJAX blocking behavior (JavaScript injection)** check box.  
The system displays the default blocking response and login response actions for AJAX.
5. For the **Default Response Page action** setting, select the type of response you want the application user to receive when they are blocked from the application:
  - **Custom Response** lets you specify HTML text or upload a file to use as a replacement for the frame or browser page that generated the AJAX request. Include the text, then click **Show** to preview the response.
  - **Popup message** displays text in a popup window (default text is included).

- **Redirect URL** redirects the user to the URL you specify. You can also include the support ID. For example:

`http://www.example.com/blocking_page.php?support_id=<%TS.request.ID()%>.`

6. For the **Login Page Response action**, select the type of response (types are the same as for default response page in Step 5).
7. Click **Save**.
8. To put the security policy changes into effect immediately, click **Apply Policy**.



---

# Chapter

# 22

---

## Securing Web Applications Created with Google Web Toolkit

---

- *Overview: Securing Java web applications created with Google Web Toolkit elements*
  - *Implementation result*
-

## Overview: Securing Java web applications created with Google Web Toolkit elements

---

*Google Web Toolkit (GWT)* is a Java framework that is used to create AJAX applications. When you add GWT enforcement to a security policy, the Security Enforcer can detect malformed GWT data, request payloads and parameter values that exceed length limits, attack signatures, and illegal meta characters in parameter values. This implementation describes how to add GWT support to an existing security policy for a Java web application created with GWT elements.

### Task summary

*Creating a Google Web Toolkit profile*

*Associating a Google Web Toolkit profile with a URL*

## Creating a Google Web Toolkit profile

Before you can begin this task, you need to create a security policy for the web application that you are creating using Google Web Toolkit (GWT).

A GWT profile defines what the security policy enforces and considers legal when it detects traffic that contains GWT data.

---

**Note:** *The system supports GWT in UTF-8 and UTF-16 encoding.*

---

1. On the Main tab, click **Security > Application Security > Content Profiles > GWT Profiles**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.

The Create New GWT Profile screen opens.

Option	Description
<b>Any</b>	Specifies that there are no length restrictions.
<b>Length</b>	Specifies, in bytes, the maximum data length that is acceptable.

4. Type a name and optional description for the profile.
5. For the **Maximum Total Length of GWT Data** setting, specify the maximum byte length for the request payload or parameter value that contains GWT data.

The default is 10000 bytes.

Option	Description
<b>Any</b>	Specifies that there are no length restrictions.
<b>Length</b>	Specifies, in bytes, the maximum acceptable length.

6. For the **Maximum Value Length** setting, specify the longest acceptable value for a GWT element that occurs in a document that the security policy allows.

The default is 100 bytes.

Option	Description
<b>Any</b>	Specifies that there are no length restrictions.
<b>Length</b>	Specifies, in bytes, the maximum acceptable length.

7. Clear the **Tolerate GWT Parsing Warnings** check box if you want the system to report warnings about parsing errors in GWT content.



8. To change the security policy settings for specific attack signatures for this GWT profile, from the **Global Security Policy Settings** list, select the attack signatures and then move them into the **Overridden Security Policy Settings** list.

---

*Note:* If no attack signatures are listed in the **Global Security Policy Settings** list, create the profile, update the attack signatures, then edit the profile.

---

9. In the **Overridden Security Policy Settings** list, enable or disable each attack signature as needed:

Option	Description
<b>Enabled</b>	Enforces the attack signature for this GWT profile, although the signature might be disabled in general. The system reports the Attack Signature Detected violation when the GWT data in a request matches the attack signature.
<b>Disabled</b>	Deactivates the attack signature for this GWT profile, although the signature might be enabled in general.

10. To allow or disallow specific meta characters in GWT data (and thus override the global meta character settings), click the Value Meta Characters tab.
  - a) Select the **Check characters** check box, if it is not already selected.
  - b) Move any meta characters that you want allow or disallow from the **Global Security Policy Settings** list into the **Overridden Security Policy Settings** list.
  - c) In the **Overridden Security Policy Settings** list, change the meta character state to **Allow** or **Disallow**.

11. Click **Create**.

The system creates the profile and displays it in the GWT Profiles list.

The security policy does not enforce the GWT profile settings until you associate the GWT profile with any URLs that might include GWT data.

## Associating a Google Web Toolkit profile with a URL

Before you can associate a Google Web Toolkit (GWT) profile with a URL, you need to create a security policy with policy elements, including application URLs and the GWT profile.

When you associate a GWT profile with a URL in a security policy, the Security Enforcer can apply specific GWT checks to the associated requests.

1. On the Main tab, click **Security > Application Security > URLs**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Allowed URLs List area, click the name of a URL that might contain GWT data. The Allowed URL Properties screen opens.
4. From the **Allowed URL Properties** list, select **Advanced**.
5. For the **Header-Based Content Profiles** setting, specify the characteristics of the traffic to which the GWT profile applies.
  - a) In the **Request Header Name** field, type the explicit string or header name that defines when the request is treated as the **Parsed As** type; for example, `Content-Type`.  
This field is not case-sensitive.
  - b) In the **Request Header Value** field, type a wildcard character (including `*`, `?`, or `[chars]`) for the header value; for example, `*gwt*`.

This field is case-sensitive.

- c) For the **Parsed As** setting, select **GWT**.
- d) For the **Profile Name** setting, select the GWT profile that you created from the list.
- e) Click **Add**.

The system adds the header and profile information to the list.

- 6. (Optional) If you have multiple headers and profiles defined, you can adjust the order of processing.
- 7. Click **Update**.
- 8. To put the security policy changes into effect immediately, click **Apply Policy**.

When the system receives traffic that contains the specified URLs, the Security Enforcer applies the checks you established in the GWT profile, and takes action according to the corresponding blocking policy.

## Implementation result

---

You have now added Google Web Toolkit (GWT) support to a security policy. When the Security Enforcer detects GWT traffic that matches the URLs defined in the security policy, the selected parameters are enforced as you have indicated.

---

# Chapter

# 23

---

## Refining Security Policies with Learning

---

- *About learning*
- *Learning resources*
- *About learning suggestions*
- *Fine-tuning a security policy*
- *Configuring explicit entities learning*
- *Viewing requests that caused learning suggestions*
- *Accepting learning suggestions*
- *Clearing learning suggestions*
- *Viewing ignored entities*
- *About enforcement readiness*
- *Enforcing entities*
- *Disabling learning on violations*

## About learning

---

You can use learning resources to help build a security policy, particularly if you are building a security policy manually. When you send client traffic through the Application Security Manager™ (ASM), the learning data provides information on requests or responses that do not comply with the current security policy and have triggered a violation. The reason for triggering a violation can be either a false positive (typically seen during the process of building a policy), or an actual attack on the site.

ASM™ generates learning suggestions for requests that cause violations and do not pass the security policy checks. You can examine the requests that cause learning suggestions, and then use the suggestions to refine the security policy. In some cases, learning suggestions may contain recommendations to relax the security policy. When dealing with learning suggestions, make sure to relax the policy only where false positives occurred, and not in cases where a real attack caused a violation.

If you are generating a security policy automatically, ASM handles all learning for you, adjusting the security policy based on traffic characteristics. In that case, the learning screens show only the elements the security policy is in the process of learning.

## Learning resources

---

This table describes the screens in Application Security Manager™ (ASM) where you can view and handle learning suggestions.

Resource	Description
Manual Traffic Learning screen	Displays learning suggestions that the system generates. The learning suggestions are categorized by violation type, and can represent actual threats or false-positives. Learning suggestions are for the currently active security policy. When you accept a learning suggestion, you are updating the currently active security policy.
Enforcement Readiness screen	Summarizes the security policy entities in staging or with learn explicit entities enabled, that may have learning suggestions, and may be ready to be enforced. For file types, parameters, URLs, cookies, and signatures, you can review the entities, and decide whether to add them to the security policy.
Ignored Entities screen	Lists the file types, URLs, and flows that you have instructed the system to disregard, that is, to stop generating learning suggestions for. Typically, the ignored entities are items that you do not want to be a part of the security policy.
IP Address Exceptions screen	Lists IP address exceptions with specific characteristics that you can configure. You can instruct the system not to generate learning suggestions for traffic sent from any of these IP addresses.
View Full Request Information screen	Displays any violations and details associated with a request. You can review this information, and then if you want to accept the learning suggestion, click the <b>Learn</b> button to update the active security policy. To display the View Full Request Information screen, from the Event Logs > Application > Requests screen, click a Requested URL in the Requests List.

## About learning suggestions

---

Application Security Manager™ (ASM) generates learning suggestions for violations if the Learn flag is enabled for the violations on the Blocking Settings screen. When the system receives a request that triggers a violation, the system updates the Manual Traffic Learning screen with learning suggestions based on the violating request information. From this screen, you can review the learning suggestions to determine whether the request triggered a legitimate security policy violation, or if the violation represents a need to update the security policy.

Making decisions about which learning suggestions to use requires some general understanding of application security, and specific knowledge of the protected application (for example, recognizing valid traffic). Often, you should consider accepting a learning suggestion when you see that it has occurred multiple times, from many different source IP addresses. Repeated learning suggestions typically indicate valid traffic behavior that warrants relaxing the security policy.

The Manual Traffic Learning screen also displays violations for which the system does not generate learning suggestions. Typically, these violations are related to RFC compliance and system resources; the resolution for these violations may be to disable the violation or sub-violation rather than to perform any specific configuration. The system displays these violations along with the learning suggestions to ease the security policy management tasks.

## Fine-tuning a security policy

---

After you create a security policy, the system provides learning suggestions concerning additions to the security policy based on the traffic that is accessing the application. For example, you can have users or testers browse the web application. By analyzing the traffic to and from the application, Application Security Manager™ generates learning suggestions or ways to fine-tune the security policy to better suit the traffic and secure the application.

---

***Note:** If you are using the Policy Builder to add elements to the security policy, you can skip this task.*

---

1. On the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made based on real traffic.
2. In the Traffic Learning area, click each violation hyperlink, then review and handle learning suggestions:

Option	Description
<b>Accept</b>	Select a learning suggestion, click <b>Accept</b> , and then click <b>Apply Policy</b> . The system updates the security policy to allow the file type, URL, parameter, or other element.
<b>Clear</b>	Select a learning suggestion, and click <b>Clear</b> . The system removes the learning suggestion and continues to generate suggestions for that violation.
<b>Cancel</b>	Click <b>Cancel</b> to return to the Manual Traffic Learning screen.

By default, a security policy is put into a staging-tightening period for seven days. During this time, you can examine learning suggestions and adjust the security policy without blocking traffic.

3. On the Manual Traffic Learning screen, review the violations and consider whether you want to permit any of them (for example, if a violation is causing false positives). Select any violations you do not want the system to trigger, and click **Disable Violation**.

A popup screen opens, and you can verify that you want to disable the violations or cancel the action.

4. To put the security policy changes into effect immediately, click **Apply Policy**.
5. On the Main tab, click **Security > Overview > Application > Action Items**.  
The Action Items screen opens.
6. Examine the Action Items screen for information about recommended actions that you need to complete.
  - a) Review the Suggested Action Items area, which lists system tasks and security policy tasks that should be completed.
  - b) Click the links in the Suggested Action Items area to go to the screen where you can perform the recommended action.
  - c) In the Quick Links area, click any of the links to gain access to common configuration and reporting screens.

The security policy now includes elements unique to your web application.

It is a good idea to periodically review the learning suggestions on the Manual Traffic Learning screen to determine whether the violations are legitimate, or if they are false positives that indicate a need to update the security policy.

## Configuring explicit entities learning

---

You can adjust the explicit entities learning settings for file types, URLs, parameters, cookies, and redirection domains. Explicit learning settings specify when Real Traffic Policy Builder® adds, or suggests you add, explicit entities to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings area, for **Explicit Entities Learning**, for each type of entity (**File Types**, **URLs**, **Parameters**, **Cookies**, and **Redirection Domains**), select the option that determines which Learning suggestions are provided by the system (based on real traffic).

Option	Description
<b>Never (wildcard only)</b>	Specifies that when false positives occur, the system suggests relaxing the settings of the wildcard. This option results in a security policy that is easy to manage, but is not as strict. If Policy Builder is running, it does not add explicit entities that match a wildcard to the security policy. The wildcard entity remains in the security policy. The Policy Builder changes the attributes of any matched wildcard. If not running, Policy Builder suggests changing the attributes of matched wildcard entities, but does not suggest you add explicit entities that match the wildcard entity.
<b>Selective</b>	Applies only to * wildcard entity. When false positives occur, adds an explicit entity with relaxed settings. This option serves as a good balance between security, policy size, and ease of maintenance. If Policy Builder is running, it adds explicit entities that do not match the attributes of the * wildcard, and does not remove the * wildcard. If Policy Builder is not running, the system suggests adding explicit entities that match the * wildcard. (Option not applicable to Redirection Domains.)
<b>Add All Entities</b>	Creates a comprehensive whitelist policy that includes all web site entities. This option results in a large, more granular configuration with stricter security. If Policy Builder is running, it adds explicit entities that match a wildcard to the security policy. When

Option	Description
--------	-------------

	the security policy is stable, the * wildcard is removed. If Policy Builder is not running, the system suggests adding explicit entities that match the wildcard.
--	---

Changing the explicit entities learning settings may change the **Policy Type** to **Custom**.

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now learns new file types, parameters, URLs, cookies, and redirection domains according to the explicit learning settings you specified.

## Viewing requests that caused learning suggestions

---

To review requests related to learning suggestions, you need to have a security policy that is already handling traffic that is causing violations. If no violations have occurred, you will not see any learning suggestions.

Before you process a learning suggestion, it is very helpful to examine the details of the request that caused the learning suggestion. By viewing the request, you can determine whether the violation was caused by an attack or if it is a false positive.

1. On the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made based on real traffic.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Traffic Learning area, click a violation hyperlink to view either the Requests List, or the specific elements in the request that triggered the security policy violation and the corresponding learning suggestion.
4. In the Occurrences column, click the number.  
The Requests List popup screen opens, and displays all of the requests that triggered the learning suggestion. Close the popup when you are done.
5. In the Recent Incidents column (if attack signatures were detected), click the number.  
The Requests List popup screen displays the requests that contained an item that triggered the learning suggestion.
6. In the Requests List area of the popup screen, in the URL column, click a URL link.  
The View Full Request Information screen or View Request Information opens in the popup screen, where you can review the request that triggered the learning suggestion.
7. For each violation with a **Learn** button, click **Learn** to go back to the violation learning screen where you can accept or clear the learning suggestions for the security policy one value at a time.
8. To view the actual contents of the request, click **Full Request** (on the View Request Information screen) or HTTP Request (on the View Full Request Information screen). and when you are done looking at the request details, click Close.
9. On the screen showing learning suggestions for the violation, to accept the suggestion and change the security policy, click **Accept**.
10. To remove learning suggestions without changing the security policy, select the ones to remove, and then click the **Clear** button.
11. On the Manual Traffic Learning screen, continue to review the violations and associated learning suggestions.

When you accept a learning suggestion, the system updates the current edited security policy to accept the request entity that triggered the violation. When you clear a learning suggestion, the system deletes the learning suggestion, and does not update the security policy; the system continues to generate learning suggestions for future instances of the violation.

### Accepting learning suggestions

---

If you have reviewed a learning suggestion and want to make the suggested change to the security policy, you can accept the suggestion.

1. On the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made based on real traffic.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Traffic Learning area, click a violation hyperlink.  
The screens vary for different violations.  
The learning suggestions properties screen opens.
4. Select one or more learning suggestions, and then click the **Accept**, **Apply**, or **Allow** button, depending on the violation.  
The system updates the security policy, applies the learning suggestions, and opens the Requests List popup screen.

### Clearing learning suggestions

---

If you want to ignore a learning suggestion and remove it from the screen, you can clear it, or you can clear all learning suggestions for a violation.

1. On the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made based on real traffic.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. To clear all learning suggestions for a violation:
  - a) Select one or more violations, and then click **Clear**.
  - b) Click **OK**.

The system deletes all of the learning suggestions and removes the violation from the list without changing the security policy.

4. To clear specific learning suggestions for a violation:
  - a) Click a violation hyperlink.
  - b) Select one or more learning suggestions, and then click **Clear**.
  - c) For URLs, file types, or flows, if you want to stop generating learning suggestions, select the **Move to ignored entities** check box
  - d) Click **OK**.

The system deletes the learning suggestion without changing the security policy.



Although the learning suggestions are cleared, the system continues to generate learning suggestions for future instances of the violation unless you added the entity to the Ignored Entities list. When the system receives subsequent requests for those items on the Ignored Entities list, the system no longer generates learning suggestions for them. The system does continue to log the requests.

## Viewing ignored entities

---

You can view file types, URL, or flows that are on the Ignored Entities list and for which the system is not generating learning suggestions. You can also delete items from the list.

1. On the Main tab, click **Security > Application Security > Policy Building > Ignored Entities**. The Ignored Entities screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. On the Ignored Entities screen, if ignored entities exist for an entity type, that type becomes a link; click one of the links to view a list of all entities logged within that category. The Ignored File Types screen, Ignored URLs screen, or Ignored Flows screen opens.
4. If you want to remove an entity from the list, select it, then click **Delete**, and click **OK** to confirm. The system removes the selected item from the Ignored Entities list.

## About enforcement readiness

---

When you are creating a security policy, you specify an enforcement readiness period that indicates a staging period for entities and attack signatures (typically 7 days). When entities or attack signatures are in staging, the system does not enforce them. Instead, the system posts learning suggestions for staged entities in the Violations Found for Staged Entities table in the request details.

When the enforcement readiness period is over and no learning suggestions are added for the staging period duration (the default is 7 days), the file type, URL, parameter, cookie, signature, or redirection domain is considered ready to be enforced. You can delve into the details to see if you want to enforce these entities in the security policy. From the Enforcement Readiness summary, you can add selected entities to the security policy, or you can enforce all of the entities and signatures that are ready to be enforced.

## Enforcing entities

---

After you create a security policy and traffic is sent to the web application, new entities are added by means of learning explicit entities, and existing entities are modified through staging. You can review the entities and signatures that are in staging or that are ready to be enforced, and add them to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Enforcement Readiness**. The Enforcement Readiness summary screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. To enforce all entities that are ready to be enforced, click **Enforce Ready**.  
If you select this option, you are done. Continue only if you want to enforce selected entities or signatures.

4. In the Enforcement Readiness Summary, check to see if a number appears in the Not Enforced column. A number greater than zero indicates that entities of that type are in staging or with learn explicit entities enabled.
5. Click the number in the Not Enforced column. The allowed file types, URLs, parameters, cookies, signatures or redirection protection list opens showing the entities that you can enforce.
6. Select the entities you want the security policy to enforce, and click **Enforce**.

The system removes the selected entities or signatures from staging. If any of the entities are wildcards that are learning explicit entities, the wildcards are deleted.

## Disabling learning on violations

---

F5 recommends that you review the violations that occur, and consider whether they represent legitimate violations or false-positives. You can disable learning on violations that are not applicable to your web application.

---

***Note:** Be sure that you understand the ramifications of disabling a violation before doing it.*

---

1. On the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning**. The Manual Traffic Learning screen opens, and lists violations and learning suggestions that the system has made based on real traffic.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Traffic Learning area, select the box next to the violation name that you want to disable.
4. Click the **Disable Violation** button, and click **OK** to confirm. The screen refreshes, and you no longer see the violation in the Traffic Learning area.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

Disabling a violation turns off the blocking policy so that you are no longer notified of requests that trigger the violation. The system then ignores future instances of the violation, and passes the requests on to the web application resources. Alternately, you can clear the learning suggestions, and the system continues to issue learning suggestions for the requests.

---

# Chapter 24

---

## Configuring Security Policy Blocking

---

- *About security policy blocking*
-

## About security policy blocking

You can configure how Application Security Manager™ handles requests that violate the security policy in several ways.

Method	Description
Blocking actions	Blocking actions for each of the security policy violations, along with the enforcement mode, determine the action that will be taken when the violation occurs.
Evasion techniques	Sophisticated hackers have figured out coding methods that normal attack signatures do not detect. These methods are known as <i>evasion techniques</i> . Application Security Manager can detect the evasion techniques, and you can configure blocking properties for them.
HTTP Protocol Compliance	The system performs validation checks on HTTP requests to ensure that the requests are formatted properly. You can configure which validation checks are enforced by the security policy.
Web Services Security	You can configure which web services security errors must occur for the system to learn, log, or block requests that trigger the errors.
Response pages	When the enforcement mode of the security policy is blocking, and a request (or response) triggers a violation for which the Block action is enabled, the system returns the response page to the client. If you configure login pages, you can also configure a response page for blocked access.

## Changing security policy enforcement

An *enforcement mode* specifies how the system processes a request that triggers a security policy violation. Security policies can be in one of two enforcement modes: transparent or blocking. You can manually change the enforcement mode for a security policy depending on how you want the system to handle traffic that causes violations.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. In the Configuration area, for the **Enforcement Mode** setting, specify how to treat traffic that causes violations.
  - To block traffic that causes violations, select **Blocking**.
  - To stop traffic from being blocked and review the violations, select **Transparent**.
4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

When the enforcement mode is set to *transparent*, traffic is not blocked even if a violation is triggered. The system typically logs the violation event (if the Learn flag is set on the violation). You can use this mode along with an enforcement readiness period when you first put a security policy into effect to make sure that no false positives occur that would stop legitimate traffic.

When the enforcement mode is set to *blocking*, traffic is blocked if it causes a violation (configured for blocking), and the enforcement readiness period is over. You use this mode when you are ready to enforce a security policy.

## Configuring blocking actions for violations

You can configure the Learn, Alarm, and Block flags, or blocking actions, for each violation. The blocking actions (along with the enforcement mode) determine how the system processes requests that trigger the corresponding violation.

1. On the Main tab, click **Security > Application Security > Blocking**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Adjust the **Enforcement Mode** setting if needed.
  - To block traffic that causes violations, select **Blocking**.
  - To not block traffic even if it causes violations (allowing you to make sure that legitimate traffic would not be blocked), select **Transparent**.

You can only configure the Block flag if the enforcement mode is set to **Blocking**.

4. For each violation, review the settings so you understand how the security policy handles requests that cause the violation, and adjust if necessary.

Option	Description
<b>Learn</b>	If selected, the system generates learning suggestions for requests that trigger the violation.
<b>Alarm</b>	If selected, the system records requests that trigger the violation in the Charts screen, the system log ( <code>/var/log/asm</code> ), and possibly in local or remote logs (depending on the settings of the logging profile).
<b>Block</b>	If selected (and the enforcement mode is set to <b>Blocking</b> ), the system blocks requests that trigger the violation.

---

**Tip:** Click the information icon preceding a violation for a description of it.

---

5. Click the violations that are links to display more granular details or subviolations for which you can enable blocking properties.  
You can enable or disable blocking subviolations for evasion techniques, HTTP protocol compliance, and web services security.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

Entities in staging and wildcards set to add all entities do not cause violations, and consequently are not blocked. But if the enforcement mode is blocking and violations are set to Block, traffic causing those violations is blocked. If violations are set to Alarm, the system logs the violations. For violations set to Learn, the system generates learning suggestions if the violation occurs.

You can now configure the response that the system sends when a request is blocked.

## About blocking actions

The system takes the following actions when the blocking actions are enabled.

Blocking Action	Description
<b>Learn</b>	When the Learn flag is enabled for a violation, and a request triggers the violation, the system logs the request and generates learning suggestions. The system takes this action when the security policy is in either the transparent or blocking enforcement mode.
<b>Alarm</b>	When the Alarm flag is enabled for a violation, and a request triggers the violation, the system logs the request, and also logs a security event. The system takes this action when the security policy is in either the transparent or blocking enforcement mode.
<b>Block</b>	The Block flag blocks traffic when (1) the security policy is in the blocking enforcement mode, (2) a violation occurs, (3) the Block flag is enabled for the violation, and (4) the entity is enforced. The system sends the blocking response page (containing a Support ID to identify the request) to the client.

## Configuring HTTP protocol compliance validation

The first security checks that Application Security Manager™ performs are those for RFC compliance with the HTTP protocol. The system validates HTTP requests to ensure that the requests are formatted properly. For each security policy, you can configure which HTTP protocol checks the system performs, and specify what happens if requests are not compliant.

1. On the Main tab, click **Security > Application Security > Blocking**.  
The Settings screen opens.
2. In the RFC Violations area, for the **HTTP protocol compliance failed** violation, set the blocking settings as needed.

Select this Option	When You Want to
<b>Learn</b>	Generate learning suggestions for requests that trigger the violation.
<b>Alarm</b>	Record requests that trigger the violation in ASM Charts, the system log (/var/log/asm), and possibly in local or remote logs (depending on the logging profile settings).
<b>Block</b>	Block requests that trigger the violation (the enforcement mode must be set to <b>Blocking</b> ).

3. Click the **HTTP protocol compliance failed** violation link.  
The HTTP subviolations are displayed.
4. Select or clear the HTTP protocol checks, as required.

---

**Tip:** For an explanation of the individual HTTP validations, click the Info icon preceding each one.

---

5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If the `HTTP protocol compliance failed violation` is set to **Learn**, **Alarm**, or **Block**, the system performs the protocol compliance checks. If the **Enforcement Mode** is set to **Blocking** and the violation is set to block, the system blocks requests that are not compliant with the selected HTTP protocol validations.

If you use automatic policy building, the system immediately enables the **Learn**, **Alarm**, and **Block** settings for the `HTTP protocol compliance failed violation`; also, the security policy immediately enables one of the HTTP protocol checks: `Bad HTTP version` (version 1.0 or later is required). After the system processes sufficient traffic from different users over a period of time, it enables other appropriate HTTP protocol checks.

If a request is too long and causes the `Request length exceeds defined buffer size violation`, the system stops validating protocol compliance for that request.

## Configuring blocking actions for web services security

You can select which web services security errors must occur for the system to learn, log, or block requests that trigger the errors. These errors are sub-violations of the parent violation, `Web Services Security failure`.

1. On the Main tab, click **Security > Application Security > Blocking**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Adjust the **Enforcement Mode** setting if needed.
  - To block traffic that causes violations, select **Blocking**.
  - To not block traffic even if it causes violations (allowing you to make sure that legitimate traffic would not be blocked), select **Transparent**.

You can only configure the Block flag if the enforcement mode is set to **Blocking**.

4. Review the **Web Services Security failure** violation and adjust the **Learn**, **Alarm**, and **Block** flags as required.
5. Click the **Web Services Security failure** violation link.  
The web services subviolations are displayed.
6. Enable or disable the web services subviolations, as required.
7. Click **Save** to save your settings.
8. To put the security policy changes into effect immediately, click **Apply Policy**.

If a request causes one of the enabled errors to occur, web services security stops parsing the document. How the system reacts depends on how you configured the blocking settings for the `Web Services Security failure` violation:

- If configured to **Learn** or **Alarm** when the violation occurs, the system does not encrypt or decrypt the SOAP message, and sends the original document to the web service.
- If configured to **Block** when the violation occurs, the system blocks the traffic and prevents the document from reaching its intended destination.





---

# Chapter

# 25

---

## Configuring Blocking Responses

---

- *Overview: Configuring blocking responses* |

## Overview: Configuring blocking responses

The Application Security Manager™ has a default blocking response page that it returns to the client when the client request, or the web server response, is blocked by the security policy. The system also has a login response page for login violations. You can change the way the system responds to blocked logins or blocked requests.

---

**Note:** *The system issues response pages only when the enforcement mode is set to **Blocking**.*

---

A security policy can respond to blocked requests in these ways:

- Default response
- Custom response
- Redirect URL
- SOAP fault

The system uses default pages in response to a blocked request or blocked login. If the default pages are acceptable, you do not need to change them and they work automatically. However, if you want to customize the response, or include XML or AJAX formatting in the blocking responses, you need to enable the blocking behavior first. You enable XML blocking on the XML profile, and AJAX blocking on the AJAX response page.

All default response pages contain a variable, `<%TS.request.ID()%>`, that the system replaces with a support ID number when it issues the page. Customers can use the support ID to identify the request when making inquiries.

## Configuring responses to blocked requests

You can configure the blocking response that the system sends to the user when the security policy blocks a client request.

1. On the Main tab, click **Security > Application Security > Blocking > Response Pages**.  
The Response Pages screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. On the Default Response Page tab, for the **Response Type** setting, select one of the following options.

Option	System Response to Blocked Request
<b>Default Response</b>	The system returns the system-supplied response page in HTML. No further configuration is needed.
<b>Custom Response</b>	The system returns a response page with HTML code that you define.
<b>Redirect URL</b>	The system redirects the user to a specified web page.
<b>SOAP Fault</b>	The system returns the system-supplied blocking response page in XML format. You cannot edit the text, but you need to select <b>Use XML Blocking Response Page</b> on the XML profile.

The settings on the screen change depending on the selection that you make for the **Response Type** setting.

4. If you selected the **Custom Response** option, you can either modify the default text or upload an HTML file.

To modify the default text:

- a) For the **Response Headers** setting, type the response header you want the system to send.
- b) For the **Response Body** setting, type the text you want to send to a client in response to an illegal blocked request. Use standard HTTP syntax.
- c) Click **Show** to see what the response will look like.

To upload a file containing the response:

- a) For the **Upload File** setting, specify an HTML file that contains the response you want to send to blocked requests.
- b) Click **Upload** to upload the file into the response body.

5. If you selected the **Redirect URL** option, then in the **Redirect URL** field, type the URL to which the system redirects the user, for example, `http://www.myredirectpage.com`.

The URL should be for a page that is not within the web application itself.

For example, to redirect the blocking page to a URL with a support ID in the query string, type the URL and the support ID in the following format:

```
http://www.myredirectpage.com/block_pg.php?support_id= <%TS.request.ID()%>
```

The system replaces `<%TS.request.ID%>` with the relevant support ID so that the blocked request is redirected to the URL with the relevant support ID.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If the enforcement mode is blocking and a request is blocked, the system displays the selected response page or redirects the user to another URL depending on the option you selected.

## Configuring responses to blocked logins

You can configure the blocking response that the system sends to the user when the security policy blocks a client attempt to log in to the application.

1. On the Main tab, click **Security > Application Security > Blocking > Response Pages**. The Response Pages screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. On the Default Response Page tab, for the **Response Type** setting, select one of the following options.

Option	System Response to Blocked Request
<b>Default Response</b>	The system returns the system-supplied response page in HTML. No further configuration is needed.
<b>Custom Response</b>	The system returns a response page with HTML code that you define.
<b>Redirect URL</b>	The system redirects the user to a specified web page.
<b>SOAP Fault</b>	The system returns the system-supplied blocking response page in XML format. You cannot edit the text, but you need to select <b>Use XML Blocking Response Page</b> on the XML profile.

The settings on the screen change depending on the selection that you make for the **Response Type** setting.

4. If you selected the **Custom Response** option, you can either modify the default text or upload an HTML file.

To modify the default text:

- a) For the **Response Headers** setting, type the response header you want the system to send.
- b) For the **Response Body** setting, type the text you want to send to a client in response to an illegal blocked request. Use standard HTTP syntax.
- c) Click **Show** to see what the response will look like.

To upload a file containing the response:

- a) For the **Upload File** setting, specify an HTML file that contains the response you want to send to blocked requests.
- b) Click **Upload** to upload the file into the response body.

5. If you selected the **Redirect URL** option, then in the **Redirect URL** field, type the URL to which the system redirects the user, for example, `http://www.myredirectpage.com`.

The URL should be for a page that is not within the web application itself.

For example, to redirect the blocking page to a URL with a support ID in the query string, type the URL and the support ID in the following format:

```
http://www.myredirectpage.com/block_pg.php?support_id= <%TS.request.ID()%>
```

The system replaces `<%TS.request.ID%>` with the relevant support ID so that the blocked request is redirected to the URL with the relevant support ID.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If a user violates one of the preconditions when requesting the target URL of a configured login page, the system displays the selected response page or redirect URL depending on the option you selected.

## Customizing responses to blocked XML requests

You can configure the blocking response that the system sends to the user when the security policy blocks a client request that contains XML content, which does not comply with the settings of an XML profile in the security policy.

---

**Note:** If you want to use the default SOAP response (SOAP Fault), you only need to enable XML blocking on the profile.

---

1. On the Main tab, click **Security > Application Security > Blocking > Response Pages**. The Response Pages screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click the **XML Response Page** tab.
4. For the **Response Type** setting, select **Custom Response**.
5. In the **Response Headers** field, type the response header you want the system to send.

---

**Tip:** Paste the default response header to use the system response that you can then edit.

---

6. In the **Response Body** field:
  - If you want to specify the content to send the client in response to an illegal blocked request, type the text using XML syntax.
  - To upload a file containing the XML response, specify an XML file and click **Upload** to upload the file into the response body.

Click **Show** to see what the response will look like.

7. Click **Save** to save your settings.
8. Make sure that the XML profile the application is using has blocking enabled:
  - a) On the Main tab, click **Security > Application Security > Content Profiles > XML Profiles**.
  - b) Click name of the XML profile used by the application.
  - c) Make sure that the **Use XML Blocking Response Page** check box is selected.
  - d) Click **Update**.
9. To put the security policy changes into effect immediately, click **Apply Policy**.



---

# Chapter

# 26

---

## Configuring General Security Policy Building Settings

---

- *About general security policy building settings*
  - *Changing the policy type*
  - *Configuring explicit entities learning*
  - *Adjusting the parameter level*
-

## About general security policy building settings

---

General policy building settings determine how a security policy is built for both automatic policy building and manual policy building. The settings define the type of policy to create, and what level of Learning suggestions to provide based on real traffic. You can specify the circumstances under which the system adds or suggests that you add explicit entities to the security policy. The settings also let you determine at which level (global or URL) to add parameters to the policy.

## Changing the policy type

---

The *policy type* determines which security policy elements are included in the security policy. If you have an existing security policy and want to change which elements are included in the policy from now on, you can change the policy type.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings, for **Policy Type**, select the type that defines how you want the security policy built.

Option	Description
<b>Fundamental</b>	Provides security at a level that is appropriate for most organizations, creating a robust security policy, which is highly maintainable and quick to configure. This is the default setting.
<b>Enhanced</b>	Provides extra customization, creating a security policy with more granularity.
<b>Comprehensive</b>	Provides the highest level of customization, creating a security policy with more granularity, but it may take longer to configure.
<b>Vulnerability Assessment</b>	Specifies a security policy that is built using the recommendations from a vulnerability assessment tool. By default, the system does not add explicit entities, leaving that to the tool. (Only available if a vulnerability assessment tool is selected on the Vulnerability Assessments Settings screen.)
<b>Custom</b>	Provides the level of security that you specify when you adjust settings such as which security policy elements are included in the security policy. The policy type changes to <b>Custom</b> if you change any of the default settings for a policy type.

The selected security policy elements and other options on the screen change depending on the policy type you choose.

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The elements that are currently in the security policy remain in the policy. From this point on, the security policy is built according to the new policy type you have selected.



## Security policy elements included in each policy type

The elements that the system adds to a security policy depend on the policy type you select for automatic policy building. You can set the policy type when creating the security policy in the Deployment wizard or later by modifying the policy settings (**Security > Application Security > Policy Building > Settings >** ). When the policy type is set or modified, the Application Security Manager™ (ASM) assigns the Explicit Entities Learning settings as follows.

**Table 1: Explicit Entities Learning Settings for Each Policy Type**

Security policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
<b>File Types</b>	Add All Entities	Add All Entities	Add All Entities	Never (wildcard only)
<b>URLs</b>	Never (wildcard only)	Selective	Add All Entities	Never (wildcard only)
<b>Parameters</b>	Selective (wildcard only)	Selective	Add All Entities	Never (wildcard only)
<b>Cookies</b>	Never (wildcard only)	Selective	Selective	Never (wildcard only)
<b>Redirection Domains</b>	Add All Entities	Add All Entities	Add All Entities	Add All Entities

**Table 2: Explicit Entities Learning Settings**

Setting	Description
<b>Add All Entities</b>	The Policy Builder includes all of the website entities. This option creates a large set of security policy entities with a granular object level configuration and high security level.
<b>Selective</b>	This option applies only to the * wildcard. When false positives occur, the system adds or suggests adding an explicit entity with relaxed settings. This option provides a good balance between security, policy size, and ease of maintenance.
<b>Never (Wildcard Only)</b>	When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option creates a security policy that is easy to manage but may result in overall relaxed application security.

Depending on which policy type you select, ASM™ includes a different set of policy elements in the Automatic Policy Building Settings.

**Table 3: Policy Elements**

Security Policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
<b>HTTP Protocol Compliance</b>	Yes	Yes	Yes	Yes
<b>Evasion Techniques Detected</b>	Yes	Yes	Yes	Yes
<b>File Type Lengths</b>	Yes	Yes	Yes	No

Security Policy element	Fundamental	Enhanced	Comprehensive	Vulnerability Assessment
<b>Attack Signatures</b> (Applies to policy, parameter, content profile, and cookie signatures)	Yes	Yes	Yes	Yes
<b>URL Meta Characters</b>	No	Yes	Yes	No
<b>Parameter Name Meta Characters</b>	No	No	Yes	No
<b>Parameter Value Lengths</b>	No	Yes	Yes	No
<b>Value Meta Characters</b> (for Parameters and Content Profiles)	No	No	Yes	No
<b>Allowed Methods</b>	No	Yes	Yes	Yes
<b>Request Length Exceeds Defined Buffer Size</b>	Yes	Yes	Yes	No
<b>Header Length</b>	Yes	Yes	Yes	No
<b>Cookie Length</b>	Yes	Yes	Yes	No
<b>Failed to Convert Character</b>	Yes	Yes	Yes	Yes
<b>Content Profiles</b>	No	Yes	Yes	No
<b>Automatically detect advanced protocols</b>	No	No; but Yes if JSON/XML payload detection selected	No; but Yes if JSON/XML payload detection selected	No
<b>Host Names</b>	Yes	Yes	Yes	Yes
<b>CSRF URLs</b>	No	No	Yes	Yes

**Note:** In the table, Yes means the element is automatically included in the policy type; No means it is not included.

## Configuring explicit entities learning

You can adjust the explicit entities learning settings for file types, URLs, parameters, cookies, and redirection domains. Explicit learning settings specify when Real Traffic Policy Builder® adds, or suggests you add, explicit entities to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**. The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings area, for **Explicit Entities Learning**, for each type of entity (**File Types**, **URLs**, **Parameters**, **Cookies**, and **Redirection Domains**), select the option that determines which Learning suggestions are provided by the system (based on real traffic).

Option	Description
<b>Never (wildcard only)</b>	Specifies that when false positives occur, the system suggests relaxing the settings of the wildcard. This option results in a security policy that is easy to manage, but is not as strict. If Policy Builder is running, it does not add explicit entities that match a wildcard to the security policy. The wildcard entity remains in the security policy. The Policy Builder changes the attributes of any matched wildcard. If not running, Policy Builder suggests changing the attributes of matched wildcard entities, but does not suggest you add explicit entities that match the wildcard entity.
<b>Selective</b>	Applies only to * wildcard entity. When false positives occur, adds an explicit entity with relaxed settings. This option serves as a good balance between security, policy size, and ease of maintenance. If Policy Builder is running, it adds explicit entities that do not match the attributes of the * wildcard, and does not remove the * wildcard. If Policy Builder is not running, the system suggests adding explicit entities that match the * wildcard. (Option not applicable to Redirection Domains.)
<b>Add All Entities</b>	Creates a comprehensive whitelist policy that includes all web site entities. This option results in a large, more granular configuration with stricter security. If Policy Builder is running, it adds explicit entities that match a wildcard to the security policy. When the security policy is stable, the * wildcard is removed. If Policy Builder is not running, the system suggests adding explicit entities that match the wildcard.

Changing the explicit entities learning settings may change the **Policy Type** to **Custom**.

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now learns new file types, parameters, URLs, cookies, and redirection domains according to the explicit learning settings you specified.

## Adjusting the parameter level

You can adjust how the system determines what parameters it adds (automatic policy building) or suggests you add (manual policy building) to the security policy. In most cases, you do not need to change the default values of these settings.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**. The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings area, for the **Parameter Level** setting, select the level of parameter to add.

Option	Description
<b>Global</b>	Add parameters at the global level for all URLs in the security policy. Make learning suggestions based on the properties of entities that already exist in the security policy. Default value for <b>Fundamental</b> and <b>Enhanced</b> policy types.
<b>URL</b>	Add parameters at the URL level, only for specific URLs. Make learning suggestions based on real traffic. Default value for <b>Comprehensive</b> policy type.

---

**Note:** This option applies only to the attack signature and illegal meta character violations.

---

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now adds parameters according to the level you specified.

---

# Chapter

# 27

---

## Configuring Manual Security Policy Settings

---

- *Editing an existing security policy*
- *Changing security policy enforcement*
- *Adjusting the enforcement readiness period*
- *Viewing whether a security policy is case-sensitive*
- *Differentiating between HTTP and HTTPS URLs*
- *Specifying the response codes that are allowed*
- *Activating iRule events*
- *Configuring trusted XFF headers*
- *Adding host names*
- *Protecting against CSRF*

## Editing an existing security policy

---

When you create a security policy using the Deployment wizard, the system uses default values. If you are manually building the security policy rather than using the Policy Builder, you can edit the security policy. You can access a security policy for editing either from the Active Policies screen or from the editing context area. The editing context area appears at the top of almost every security policy component screen throughout Application Security Manager™.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. Make any changes that are required for that security policy, such as to URLs, parameters, and so on.
4. To quickly access the Properties screen for a security policy, click the **Current edited policy** link in the editing context area.
5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.
7. To edit other security policies, for **Current edited policy**, select the security policy you want to edit.

## Changing security policy enforcement

---

An *enforcement mode* specifies how the system processes a request that triggers a security policy violation. Security policies can be in one of two enforcement modes: transparent or blocking. You can manually change the enforcement mode for a security policy depending on how you want the system to handle traffic that causes violations.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. In the Configuration area, for the **Enforcement Mode** setting, specify how to treat traffic that causes violations.
  - To block traffic that causes violations, select **Blocking**.
  - To stop traffic from being blocked and review the violations, select **Transparent**.
4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

When the enforcement mode is set to *transparent*, traffic is not blocked even if a violation is triggered. The system typically logs the violation event (if the Learn flag is set on the violation). You can use this mode along with an enforcement readiness period when you first put a security policy into effect to make sure that no false positives occur that would stop legitimate traffic.

When the enforcement mode is set to *blocking*, traffic is blocked if it causes a violation (configured for blocking), and the enforcement readiness period is over. You use this mode when you are ready to enforce a security policy.

## Adjusting the enforcement readiness period

---

For each security policy, you can configure the number of days used as the *enforcement readiness period*. Security policy entities and attack signatures remain in staging for this period of time before the system suggests that you enforce them. Staging allows you to test security policy entities and attack signatures for false positives without enforcing them. The default value of 7 days works for most situations so you typically do not need to change it.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. For the **Enforcement Readiness Period**, type the number of days you want the entities or signatures to be in staging; this is also how long you want the security policy to learn explicit entities for wildcards (in **Add All Entities** mode).  
The default value is 7 days.
4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

During the enforcement readiness period, the system does not block traffic, even if requests trigger violations against the security policy. The security policy provides suggestions when requests match the attack signatures or do not adhere to the security policy entity's settings.

If you enable the option to learn explicit entities on the wildcard entities, the system learns the explicit file types, parameters, or URLs that the web application uses. You can review the new entities and decide which are legitimate entities for the web application, and accept them into the security policy.

If you are using automatic policy building and the system has processed sufficient traffic, after the enforcement readiness period is over, the Real Traffic Policy Builder® automatically enables the security policy entities and the attack signatures that did not cause violations during the period.

## Viewing whether a security policy is case-sensitive

---

When you first create a security policy using the Deployment wizard, you have the option of making a security policy case-sensitive. By default, the option **Security Policy is case sensitive** is selected, and the security policy treats file types, URLs, and parameters as case-sensitive. You cannot change this setting after the security policy is created, but you can view what the setting is.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. Review the **Security Policy is case sensitive** setting.  
If the value is **Yes**, the security policy is case-sensitive; if the value is **No**, the policy is not case-sensitive.
4. Click **Cancel** when you are done.

## Differentiating between HTTP and HTTPS URLs

---

When creating a security policy, you can determine whether a security policy differentiates between HTTP and HTTPS URLs. Later, you can view the setting, but you can change it only if the security policy contains no URLs that have the same name and use different protocols.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. Review the **Differentiate between HTTP and HTTPS URLs** setting.  
If the **Enabled** check box is selected, the security policy differentiates between HTTP and HTTPS URLs. Otherwise, it does not, and creates protocol-independent URLs.
4. Click **Cancel** when you are done.

If the **Differentiate between HTTP and HTTPS URLs** setting is disabled, the security policy configures URLs without specifying a specific protocol. This is useful for applications that behave the same for HTTP and HTTPS, and it keeps the security policy from including the same URL twice.

## Specifying the response codes that are allowed

---

You can specify which responses a security policy permits. By default, the Application Security Manager™ accepts all response codes from 100 to 399 as valid responses. Response codes from 400 to 599 are considered invalid unless added to the Allowed Response Status Codes list. By default, 400, 401, 404, 407, 417, and 503 are on the list as allowed HTTP response status codes.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. If you want to allow additional responses for the **Allowed Response Status Codes** setting, in the **New Allowed Response Status Code** field, type the HTTP response status code, between 400 and 599, that the security policy should consider a legal response, and click **Add**.
5. If you do not want to allow any response codes between 400 and 599, click **Remove All**.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy considers legal responses that return response codes that are listed as allowed response codes. If a response contains a response status code from 400 to 599 that is not on the list, the system issues the violation, *Illegal HTTP status in response*. If you configured the security policy to block this violation, the system blocks the response.



## Activating iRule events

An iRule is a script that lets you customize how you manage traffic on the BIG-IP® system. You can write iRules® to modify a request or response, or to cause an action to occur. For detailed information on iRules, see the F5 Networks DevCentral web site, <http://devcentral.f5.com>. If you are using iRules to perform actions based on Application Security Manager™ iRule events, you must instruct ASM™ to trigger iRule events. By default, the trigger iRule event setting is disabled.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. If you have written iRules to process application security events, for the **Trigger ASM iRule Events** setting, select the **Enabled** check box.  
Leave this option disabled if you have not written any ASM iRules, or you have written iRules not for ASM (triggered by the Local Traffic Manager™).
5. For the **ASM iRules Event Mode** setting, select the mode to use.
  - Recommended: If you are writing new iRules, such as those that perform a specific action after handling requests, select **Normal Mode**. Whenever ASM processes a request, it triggers an `ASM_REQUEST_DONE` event.
  - Not recommended: If you are using iRules that use `ASM_REQUEST_VIOLATION`, select **Compatibility Mode**. Whenever ASM processes a request with a violation, it triggers an `ASM_REQUEST_VIOLATION` event. F5 recommends that you rewrite the iRules using `ASM_REQUEST_DONE` in the **Normal Mode**.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If you write iRules that process ASM iRule events and assign them to a specific virtual server, when the trigger iRules setting is enabled, ASM triggers iRule events for requests. If the trigger iRules setting is not enabled, no iRule events occur for ASM iRule events.

## Application security iRule events

These are the events that iRules® can subscribe to in Application Security Manager™.

Application Security iRule Event	Description
<code>ASM_REQUEST_DONE</code>	Occurs when Application Security Manager finishes processing a request in Normal mode (regardless of whether a violation occurred or not). The system triggers this event after deciding what to do with the request, block it or forward it, but before actually executing that action, so you can specify a change to that action.
<code>ASM_REQUEST_BLOCKING</code>	Occurs when Application Security Manager is generating an error response to the request that caused a violation, and gives the iRule a chance to modify the response before it is sent. Allows you to modify the blocking page.

Application Security iRule Event	Description
ASM_RESPONSE_VIOLATION	Occurs when Application Security Manager detects a response that violates a security policy.
ASM_REQUEST_VIOLATION	Deprecated. Use ASM_REQUEST_DONE instead. Occurs when Application Security Manager detects a request that violates a security policy when using Compatibility mode only.

## Configuring trusted XFF headers

You can configure Application Security Manager™ (ASM™) to trust XFF (X-Forwarded-For) headers or customized XFF headers in requests. For example, you could do this if ASM is deployed behind an internal or other trusted proxy. Then, the system uses the IP address that initiated the connection to the proxy instead of the internal proxy's IP address. This option is useful for logging, web scraping, anomaly detection, and the geolocation feature.

You should not configure trusted XFF headers if you think the HTTP header may be spoofed, or crafted, by a malicious client.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. For the **Trust XFF Header** setting, select the **Enabled** check box.  
The screen displays the **Custom XFF Headers** configuration option.
5. If your web application uses custom XFF headers, in the **Custom XFF Headers** setting, add them as follows:
  - a) In the **New Custom XFF Header** field, type the XFF header that the system should trust.
  - b) Click **Add**.

You can add up to five custom XFF headers.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

When you trust XFF headers, the system has confidence in XFF headers in the request. If you added custom XFF headers, the system recognizes and trusts them. If deployed behind a proxy, ASM uses the initiating IP address rather than the address of the proxy.

## Adding host names

You can manually add legitimate host names to a security policy, for example, if users can access the application from multiple host names. If you are using automatic policy building, the system automatically adds domain names to the security policy so adding them in that case is optional.

1. On the Main tab, click **Security > Application Security > Headers > Host Names**.  
The Host Names screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Above the list of host names, click the **Create** button.  
The New Host Name screen opens.
4. In the **Host Name** field, type the host name that is used to access the web application (either a domain name or an IP address).
5. To include all sub-domains of the specified host name, select the **Include Sub-domains** check box.
6. Click **Create**.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The host name is added to the list of host names that can legitimately be used to access the web application that the security policy is protecting.

## About adding multiple host names

If users can access a web application using multiple host names or IP addresses, you can add the multiple host names or IP addresses to the security policy that protects the application. The system uses this list of host names as follows:

- The Policy Builder considers the host names in the list to be legitimate internal links and forms, and learns security policy entities from them, and also from relative URLs that do not contain a domain name.
- The CSRF feature uses the list to distinguish between internal and external links and forms, and the system inserts the CSRF token only into internal links and forms.

The Application Security Manager™ (ASM) identifies web application-related host names as fully qualified domain names (FQDNs) in requests or responses. If you include sub-domains with the host name, the system matches all sub-domains when evaluating FQDNs, and inserts ASM™ cookies into responses from the sub-domains of the host name. When an application uses several sub-domains, ASM cookie-based features (like CSRF protection, Login Pages, and Dynamic Sessions ID in URL) require ASM cookies to be inserted from the correct domain.

## Protecting against CSRF

---

Cross-site request forgery (CSRF) is an attack where a user is forced to execute unauthorized actions (such as a bank transfer) within a web application where the user is currently authenticated. You can configure a security policy to protect against CSRF attacks, including specifying which URLs you want the system to examine.

1. On the Main tab, click **Security > Application Security > CSRF Protection**.  
The CSRF Protection screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select the **CSRF Protection** check box.
4. Specify which part of the application you want to protect against CSRF attacks: check box.
  - To protect SSL requests only in the secured part of the application, select the **SSL Only** check box.
  - To protect the entire web application, leave the **SSL Only** check box cleared.
5. If you want the CSRF session cookie (which is injected into responses) to expire:

- a) For **Expiration Time**, select **Enabled**.
- b) In the field, type the amount of time, in seconds (1 to 99999), after which the cookie should expire. The default is 600 seconds.

**6.** In the **URLs List** setting, specify the URLs you want the system to examine.

The system considers all URLs not on the list safe unless another problem is discovered.

- a) Type the URL in the format `/index.html`.

You can also use wildcards for URLs; for example `/myaccount/*.html`, `/*/index.php`, or `/index.?html`.

- b) Click **Add**.
- c) Add all of the potentially unsafe URLs that you want the system to examine.

**7.** Click **Save** to save your settings.

**8.** To put the security policy changes into effect immediately, click **Apply Policy**.

If the system detects a CSRF attack, it issues a `CSRF attack detected` violation. The system inserts an Application Security Manager™ token to prevent CSRF attacks. To prevent token hijacking, the system reviews the token expiration date. If the token is expired, the system issues the `CSRF authentication expired` violation.

If you want to block requests suspected of being CSRF attacks, in addition to enabling CSRF protection, you also need to set the security policy enforcement mode to Blocking. Also, one or both of the CSRF violations must have the Block flag enabled. Though these violations are set to block by default, CSRF protection must be enabled for this feature to work.

---

# Chapter

# 28

---

## Adding File Types to a Security Policy

---

- *About adding file types*
  - *Adding allowed file types*
  - *Adding disallowed file types*
-

## About adding file types

---

In a security policy, you can manually specify the file types that are allowed (or disallowed) in traffic to the web application being protected. This is only if you are not using the recommended automatic policy building. When you are using automatic policy building, Application Security Manager™ determines which file types to add, based on legitimate traffic.

When you create a security policy, a wildcard file type of \*, representing all file types, is added to the file type list. During the enforcement readiness period, the system examines the file types in the traffic and makes learning suggestions that you can review and add the file types to the policy as needed. This way, the security policy includes the file types that are typically used. When you think all the file types are included in the security policy, you can remove the \* wildcard from the allowed file types list.

## Adding allowed file types

---

You can manually add allowed file types, which are file types that the security policy accepts in traffic to the web application being protected.

1. On the Main tab, click **Security > Application Security > File Types**.  
The Allowed File Types screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The Add Allowed File Type screen opens.
4. For **File Type**, choose a type:

Option	Description
<b>Explicit</b>	Specifies a unique file type, such as JPG or HTML. Type the file type (from 1 to 8 characters) in the adjacent box.
<b>No Extension</b>	Specifies that the web application has a URL with no file type. The system automatically assigns this file type the name <b>no_ext</b> . The slash character (/) is an example of a <b>no_ext</b> file type.
<b>Wildcard</b>	Specifies that the file type is a wildcard expression. Any file type that matches the wildcard expression is considered legal. The pure wildcard (*) is automatically added to the security policy so you do not need to add it. But you can add other wildcards such as <code>htm*</code> . Type a wildcard expression in the adjacent box.

5. For the length settings, adjust the values as needed. This is optional.

Option	Specifies
<b>URL Length</b>	The maximum acceptable length, in bytes, for a URL in the context of an HTTP request containing this file type. The default is 100 bytes.
<b>Request Length</b>	The maximum acceptable length, in bytes, for the whole HTTP request that applies to this file type. The default is 5000 bytes.
<b>Query String Length</b>	The maximum acceptable length, in bytes, for the query string portion of a URL that contains the file type. The default is 1000 bytes.

Option	Specifies
<b>POST Data Length</b>	The maximum acceptable length, in bytes, for the POST data of an HTTP request that contains the file type. The default is 1000 bytes

- By default, the **Perform Staging** check box is selected. We recommend that you keep it selected unless you are creating a wildcard file type for which you plan to **Add All Entities** in the **Learn Explicit Entities** setting. In that case, clear it.
- If you are creating a wildcard file type, from the **Learn Explicit Entities** list, specify whether the system adds explicit file types that match a wildcard to the security policy.

Option	Description
<b>Never (wildcard only)</b>	The system does not add or suggest that you add entities that match the wildcard to the policy. When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option results in a security policy that is easy to manage but may not be as strict.
<b>Add All Entities</b>	The system creates a comprehensive whitelist policy that includes all of the website entities. This option will form a large set of security policy entities, which will produce a granular object-level configuration and high security level, it may take more time to maintain such a policy.

---

***Note:** Do not enable both staging and **Add All Entities** on the same wildcard entity.*

---

- If you want the system to validate responses for this file type, select the **Apply Response Signatures** check box.  
Selecting this option enables attack signatures (that are designed to inspect server responses) to filter responses.
- Click **Create**.  
The Allowed File Types screen opens and lists the new file type.
- To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy allows the file type that you added. If the file type is in staging, the system informs you when learning suggestions are available or when it is ready to be enforced.

## Wildcard syntax

The syntax for wildcard entities is based on shell-style wildcard characters. This table lists the wildcard characters that you can use in the names of file types, URLs, parameters, or cookies so that the entity name can match multiple objects.

Wildcard Character	Matches
*	All characters
?	Any single character
[abcde]	Exactly one of the characters listed
[!abcde]	Any character not listed
[a-e]	Exactly one character in the range
[!a-e]	Any character not in the range

### Adding disallowed file types

---

For some web applications, you may want to deny requests for certain file types. In this case, you can create a set of disallowed file types. Adding disallowed file types is useful for file types that you know should never appear on your site (such as .exe files), or for files on your site that you never want users from the outside to reach (such as .bak files).

1. On the Main tab, click **Security > Application Security > File Types > Disallowed File Types**. The Disallowed File Types screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**. The New Disallowed File Type screen opens.
4. In the **File Type (Explicit only)** field, type the file type that the security policy does not allow (for example, jpg or exe).

---

***Note:** File types are case-sensitive unless you cleared **Security Policy is case sensitive** when you created the policy.*

---

5. Click **Create**. The Disallowed File Types screen opens and lists the new file type.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

The system categorizes both disallowed file types, and requested file types not configured in the security policy as illegal file types. When the Application Security Manager™ receives a request with a disallowed file type, the system ignores, learns, logs, or blocks the request depending on the settings you configure for the Illegal File Type violation on the Application Security: Blocking: Settings screen.



---

# Chapter 29

---

## Adding Parameters to a Security Policy

---

- *About adding parameters to a security policy* |

## About adding parameters to a security policy

---

Parameters are an integral part of any web application, and they need to be protected so clients cannot access them, modify them, or view sensitive data. When you define parameters in a security policy, you increase the security of the web application and prevent web parameter tampering.

Application Security Manager™ evaluates parameters, meta characters, query string lengths, and POST data lengths as part of a positive security logic check. When the security policy includes known parameters, you are creating a whitelist of acceptable parameters. The system allows traffic that includes the parameters that you configure in a security policy.

Security policies can include parameters defined as global parameters, URL parameters, and flow parameters. You can further specify parameters as being particular value types: static content, dynamic content, dynamic parameter name, user-input, JSON, or XML. You can also create parameters for which the system does not check or verify the value.

### Creating global parameters

*Global parameters* are parameters that are not associated with specific URLs or application flows. The advantage of using global parameters is that you can configure a global parameter once, and the system enforces the parameter wherever it occurs. You create a global parameter to address these conditions:

- The web application has a parameter that appears in several URLs or flows.
  - You want the Application Security Manager™ to enforce the same parameter attributes on all parameters.
1. On the Main tab, click **Security > Application Security > Parameters**.
  2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
  3. Click **Create**.  
The Add Parameter screen opens.
  4. In the Create New Parameter area, for the **Parameter Name** setting, specify the type of parameter you want to create.
    - To create a named parameter, select **Explicit**, then type the name.
    - To use pattern matching, select **Wildcard**, then type a wildcard expression. Any parameter name that matches the wildcard expression is permitted by the security policy.
    - To create an unnamed parameter, select **No Name**. The system creates a parameter with the label, UNNAMED.
  5. For the **Parameter Level** setting, select **Global**.  
The parameter can occur anywhere and is not associated with a specific URL or flow.
  6. Leave the **Perform Staging** check box selected if you want the system to evaluate traffic before enforcing this parameter.  
Staging helps reduce the occurrence of false positives.
  7. If you are creating a wildcard parameter and you want the system to display explicit parameters that match the wildcard entity pattern that you specify, for the **Learn Explicit Entities** setting, select **Add All Entities**.
  8. Specify whether the parameter requires a value:
    - If the parameter is acceptable without a value, leave the **Allow Empty Value** setting enabled.
    - If the parameter must always include a value, clear the **Allow Empty Value** check box.

9. To allow users to send a request that contains multiple parameters with the same name, select the **Allow Repeated Occurrences** check box.

---

**Important:** Before enabling this check box, consider that requests containing multiple parameters of the same name could indicate an attack on the web application (HTTP Parameter Pollution).

---

10. If you want to treat the parameter you are creating as a sensitive parameter (data not visible in logs or the user interface), enable the **Sensitive Parameter** setting.
11. For the **Parameter Value Type** setting, select the format of the parameter value.  
Depending on the value type you select, the screen refreshes to display additional configuration options.
12. Click **Create** to add the new parameter to the security policy.
13. To put the security policy changes into effect immediately, click **Apply Policy**.

When you first create a global parameter, the system places the parameter in staging by default and does not block requests even if a violation occurs and the system is configured to block the violation. The system makes learning suggestions that you can accept or clear.

## Creating URL parameters

*URL parameters* are parameters that are defined in the context of a URL. You can use a URL parameter when it does not matter where users were before they accessed this URL, or whether the parameter was in a GET or POST request. You can create a parameter that goes with a URL that already exists in the security policy.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The Add Parameter screen opens.
4. In the Create New Parameter area, for the **Parameter Name** setting, specify the type of parameter you want to create.
  - To create a named parameter, select **Explicit**, then type the name.
  - To use pattern matching, select **Wildcard**, then type a wildcard expression. Any parameter name that matches the wildcard expression is permitted by the security policy.
  - To create an unnamed parameter, select **No Name**. The system creates a parameter with the label, UNNAMED.
5. For the **Parameter Level** setting, select **URL**, then for the **URL Path** setting, select a protocol from the list, and then type the URL in this format: `/url_name.ext`.  
When you begin to type the URL, the system lists all URLs that include the character you typed, and you can select the URL from the list.
6. Leave the **Perform Staging** check box selected if you want the system to evaluate traffic before enforcing this parameter.  
Staging helps reduce the occurrence of false positives.
7. If you are creating a wildcard parameter and you want the system to display explicit parameters that match the wildcard entity pattern that you specify, for the **Learn Explicit Entities** setting, select **Add All Entities**.
8. Specify whether the parameter requires a value:
  - If the parameter is acceptable without a value, leave the **Allow Empty Value** setting enabled.

- If the parameter must always include a value, clear the **Allow Empty Value** check box.
9. To allow users to send a request that contains multiple parameters with the same name, select the **Allow Repeated Occurrences** check box.

---

**Important:** Before enabling this check box, consider that requests containing multiple parameters of the same name could indicate an attack on the web application (HTTP Parameter Pollution).

---

10. If you want to treat the parameter you are creating as a sensitive parameter (data not visible in logs or the user interface), enable the **Sensitive Parameter** setting.
11. For the **Parameter Value Type** setting, select the format of the parameter value.  
Depending on the value type you select, the screen refreshes to display additional configuration options.
12. Click **Create** to add the new parameter to the security policy.
13. To put the security policy changes into effect immediately, click **Apply Policy**.

When you define a URL parameter, the system applies the security policy to the parameter attributes in the context of the associated URL, and ignores the flow information. When you first create a URL parameter, the system places the parameter in staging by default and does not block requests even if a violation occurs and the system is configured to block the violation. The system makes learning suggestions that you can accept or clear.

## Creating flow parameters

Before you can create a flow parameter, you need to first have created the flow to which the parameter applies. If the source URL is a referrer URL, that URL must already be defined in the security policy as well.

You define parameters in the context of a flow when it is important to enforce that the target URL receives a parameter only from a specific referrer URL. Flow parameters provide very tight, flow-specific security for web applications. With this increased protection comes an increase in maintenance and configuration time. Note that if your application uses dynamic parameters, you need to manually add those to the security policy.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The Add Parameter screen opens.
4. In the Create New Parameter area, for the **Parameter Name** setting, specify the type of parameter you want to create.
  - To create a named parameter, select **Explicit**, then type the name.
  - To use pattern matching, select **Wildcard**, then type a wildcard expression. Any parameter name that matches the wildcard expression is permitted by the security policy.
  - To create an unnamed parameter, select **No Name**. The system creates a parameter with the label, UNNAMED.
5. In the **Parameter Level** setting, select **Flow**, and then for **From URL** define where the flow must come from:
  - If the source URL is an entry point, click **Entry Point**.
  - If the source URL is a referrer URL (already defined in the policy), click **URL Path**, select the protocol used for the URL, then type the referrer URL associated with the flow.

When you begin to type the URL, the system lists all referrer URLs that include the character you typed, and you can select the URL from the list.

6. In the **Parameter Level** setting, for **Method**, select the HTTP method (**GET** or **POST**) that applies to the target referrer URL (already defined in the policy).
7. In the **Parameter Level** setting, for **To URL**, select the protocol used for the URL, then type the target URL.
8. Leave the **Perform Staging** check box selected if you want the system to evaluate traffic before enforcing this parameter.  
Staging helps reduce the occurrence of false positives.
9. If you are creating a wildcard parameter and you want the system to display explicit parameters that match the wildcard entity pattern that you specify, for the **Learn Explicit Entities** setting, select **Add All Entities**.
10. If the parameter is required in the context of the flow, select the **Is Mandatory Parameter** check box.  
Note that only flows can have mandatory parameters.
11. Specify whether the parameter requires a value:
  - If the parameter is acceptable without a value, leave the **Allow Empty Value** setting enabled.
  - If the parameter must always include a value, clear the **Allow Empty Value** check box.
12. To allow users to send a request that contains multiple parameters with the same name, select the **Allow Repeated Occurrences** check box.

---

**Important:** Before enabling this check box, consider that requests containing multiple parameters of the same name could indicate an attack on the web application (HTTP Parameter Pollution).

---

13. If you want to treat the parameter you are creating as a sensitive parameter (data not visible in logs or the user interface), enable the **Sensitive Parameter** setting.
14. For the **Parameter Value Type** setting, select the format of the parameter value.  
Depending on the value type you select, the screen refreshes to display additional configuration options.
15. Click **Create** to add the new parameter to the security policy.
16. To put the security policy changes into effect immediately, click **Apply Policy**.

When you create a parameter that is associated with a flow, the system verifies the parameter in the context of the flow. For example, if you define a parameter in the context of a GET request, and a client sends a POST request that contains the parameter, the system generates an `Illegal Parameter` violation.

## Creating sensitive parameters

The Application Security Manager™ stores incoming requests in plain text format. Some requests include sensitive data in parameters, such as an account number, that you want to hide from system users. You can create sensitive parameters as described in the procedure, following, or by enabling the **Sensitive Parameter** setting when creating or editing any parameter. All parameters defined as sensitive, regardless of how you configured them, appear in the Sensitive Parameters list.

1. On the Main tab, click **Security > Application Security > Parameters > Sensitive Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Sensitive Parameter screen opens.

4. In the **Parameter Name** field, type the name of the user-input parameter, exactly as it occurs in the HTTP request, for which you do not want the system to store the actual value.

In this example, `account` is the sensitive parameter:

```
http://www.siterequest.com/bank.php?account=12345
```

---

**Tip:** *If a parameter of this name already exists in the security policy, click it in the parameter list, and enable the **Sensitive Parameter** setting instead of creating a new sensitive parameter.*

---

5. Click **Create** to add the new parameter to the security policy.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

When you create sensitive parameters, the system replaces the sensitive data, in the stored request and in logs, with asterisks (\*\*\*).

## Creating navigation parameters

If you want the security policy to differentiate between pages in the web application that are generated by requests with the same URL name but with different parameter and value pairs, and to build the appropriate flows, you must specify the exact names of the parameters that trigger the creation of the pages in the web application. These parameters are called *navigation parameters*. A navigation parameter cannot be a wildcard.

1. On the Main tab, click **Security > Application Security > Parameters > Navigation Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Navigation Parameter screen opens.
- 4.
5. In the **Navigation Parameter** field, type the name of the parameter passed to the web server for dynamic page-building purposes.
6. Click **Create** to add the new parameter to the security policy.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

## Creating parameters with dynamic content

*Dynamic content value (DCV) parameters* are parameters where the web application sets the value on the server side (so, for example, the content can change depending on who the user is). When you create a DCV parameter, you also specify where and how to get the dynamic information. For example, in an auction application, you can configure the price parameter as a DCV parameter to keep users from tampering with the price.

You can also use DCV parameters for user identities in web applications that use sessions. As an example, user identity is often passed between pages as a hidden parameter, which could be exploited by malicious users, unless protected.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The Add Parameter screen opens.

4. In the Create New Parameter area, for the **Parameter Name** setting, specify the type of parameter you want to create.
  - To create a named parameter, select **Explicit**, then type the name.
  - To use pattern matching, select **Wildcard**, then type a wildcard expression. Any parameter name that matches the wildcard expression is permitted by the security policy.
  - To create an unnamed parameter, select **No Name**. The system creates a parameter with the label, `UNNAMED`.
5. For the **Parameter Level** setting, select the appropriate type, typically **Global** or **URL**.
6. For the **Parameter Value Type** setting, select **Dynamic content value**.
7. Click **Create**.

---

***Note:** You should define the extractions for a DCV parameter before you apply the security policy that includes the parameters. Otherwise, the system warns you that the security policy contains dynamic parameters with no extractions defined.*

---

A popup screen opens asking if you want to define extractions.

8. Click **OK**.  
The Create New Extraction screen opens. The **Name** field shows the name of the parameter you created.
9. From the **Extracted Items Configuration** list, select **Advanced**.
10. Use the **Extract From** setting to specify which items the system searches for dynamic parameter values.

Use This Option	When
<b>File Types</b>	You want the system to extract dynamic parameters from responses to requests for certain file types that exist in the security policy. Select the file type and click <b>Add</b> .
<b>URLs</b>	You want the system to extract dynamic parameters from responses to requests for the listed URLs. To add the URLs, select the protocol, type the URL and click <b>Add</b> . If the URL is not in the security policy, it is added.
<b>RegExp</b>	You want the system to extract dynamic parameters from responses to requests that match a regular expression pattern.
<b>Extract From All Items</b>	You want the system to extract dynamic parameters from all text-based URLs and file types.

11. From the **Extracted Methods Configuration** list, select **Advanced**.
12. Select the appropriate check boxes to specify how to get the dynamic parameter values.

Select This Option	When
<b>Search in Links</b>	You want the system to extract dynamic parameter values from links (href tags) within the server response to a URL.
<b>Search Entire Form</b>	You want the system to extract dynamic parameter values from all parameters in a form in the HTML response to a requested URL.
<b>Search Within Form</b>	You want the system to extract dynamic parameter values from a specific parameter within in a form. Also specify the <b>Form Index</b> and the <b>Parameter Index</b> .
<b>Search in XML</b>	You want the system to extract dynamic parameter values from within XML entities. Type the XPath specification in the <b>XPath</b> field.
<b>Search in Response Body</b>	You want the system to search for dynamic parameter values in the body of the response. You can also specify how many incidents the system should find, a prefix, a RegExp value, or a prefix to search for.

13. Click **Create** to add the extraction properties to the parameter.
14. Click **Update** to save the changes.
15. To put the security policy changes into effect immediately, click **Apply Policy**.

When the Application Security Manager receives a request that contains an entity (for example, a file extension or URL) with a dynamic content value parameter, the system extracts the parameter value from the web application response and stores it away. The next time the system receives a request containing that parameter, it uses the stored value to validate the dynamic content value parameter. The system verifies that the client is not changing the parameter value that the server sets from one request to the next, or using the values from a different user.

By default, the system saves up to 950 values that it finds for a dynamic content value parameter. If the number of values exceeds 950, the system replaces the first-extracted values with the new values.

## Creating parameters with dynamic names

Before you can make a parameter with a dynamic name, you must have created a flow parameter.

In some web applications, flow parameters have dynamic names. When you create a parameter with a dynamic name, you also specify the manner in which Application Security Manager™ discovers the parameter names.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. In the Parameters List, click the name of the flow parameter that you want to have a dynamic name. The Parameter Properties screen opens where you can edit the flow parameter.
3. For the **Parameter Value Type** setting, select **Dynamic parameter name**.
4. On the Dynamic Parameter Properties tab, for the **Extract Parameter from URL** setting, select the protocol to use and type the URL from which you want the system to extract the dynamic parameter.
5. Specify whether the system searches for the parameter name in a form or the response body:
  - To search in forms, select **Search Within Form**, and specify values for **Form Index** and **Parameter Index**.
  - To search in the response body, select **Search parameters in response body (in form elements names only)**. In the **By Pattern** field, type a regular expression to search for parameter names in input elements in the forms. Select **Check parameter value** to verify the parameter value in addition to the name matched in the **By Pattern** field.
6. Click **Update** to save the changes.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The system extracts the parameters from the web server responses and then uses the extracted parameters to enforce the dynamic parameter associated with the flow.

## Changing character sets for parameter values

The character sets for parameter values are the characters and meta characters that the security policy accepts in a parameter value. You can view and modify the character set that is allowed in a parameter value.

1. On the Main tab, click **Security > Application Security > Parameters > Character Sets > Parameter Value**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.



3. Use the **View** option to filter the character set.
4. For each character or meta character, change the state, as required.

State	Description
<b>Allow</b>	The security policy permits this character or meta character in parameter values.
<b>Disallow</b>	The security policy does not permit this character or meta character in parameter values.

5. Click **Save** to save the changes.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If a request includes a parameter with a disallowed character, the system generates an `Illegal parameter` violation (if that violation is set to Alarm or Block).

## Changing character sets for parameter names

The character sets for parameter names are the characters and meta characters that the security policy accepts in a parameter name. You can view and modify the character set that is allowed in a parameter name.

1. On the Main tab, click **Security > Application Security > Parameters > Character Sets > Parameter Name**.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Use the **View** option to filter the character set.
4. For each character or meta character, change the state, as required.

State	Description
<b>Allow</b>	The security policy permits this character or meta character in parameter names.
<b>Disallow</b>	The security policy does not permit this character or meta character in parameter names.

5. Click **Save** to save the changes.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If a request includes a parameter name with a disallowed character, the system generates an `Illegal parameter` violation (if that violation is set to Alarm or Block).

## Adjusting the parameter level

You can adjust how the system determines what parameters it adds (automatic policy building) or suggests you add (manual policy building) to the security policy. In most cases, you do not need to change the default values of these settings.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.

3. In the General Policy Building Settings area, for the **Parameter Level** setting, select the level of parameter to add.

Option	Description
<b>Global</b>	Add parameters at the global level for all URLs in the security policy. Make learning suggestions based on the properties of entities that already exist in the security policy. Default value for <b>Fundamental</b> and <b>Enhanced</b> policy types.
<b>URL</b>	Add parameters at the URL level, only for specific URLs. Make learning suggestions based on real traffic. Default value for <b>Comprehensive</b> policy type.

---

***Note:** This option applies only to the attack signature and illegal meta character violations.*

---

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now adds parameters according to the level you specified.

## Parameter Value Types

When you add a parameter to the security policy, you specify its parameter value type. The parameter value type indicates the format of the parameter. You can configure global, URL, and flow parameters as any value type, except the dynamic parameter name type. You can configure only flow parameters as dynamic parameter names.

Parameter Value Type	Description
<b>Dynamic content value</b>	<i>Dynamic parameters</i> are parameters whose values can change, and are often linked to a user session. When you create a new parameter of this type, you must also define dynamic parameter extraction properties. The server sets the value for dynamic content value (DCV) parameters. DCV parameters are often associated with applications that use session IDs for client sessions.
<b>Dynamic parameter name</b>	If using flow parameters with names that change dynamically, you can use this parameter type. If you select this type, you also need to specify the URL from which the system can extract dynamic parameter name parameters.
<b>Ignore value</b>	If you do not want the system to perform validity checks on the parameter value, select this value type. Regarding signatures, this value type prevents the system from performing parameter-based signature checks on the parameter value, but it does perform other relevant signature checks.
<b>JSON value</b>	The JSON value type is for parameters that contain JSON data that is validated according to a JSON profile that defines the format of the data. Select an existing JSON profile or create a new one.
<b>Static content value</b>	Static parameters are those that have a known set of values. A list of country names or a yes/no form field are both examples of static parameters. If you select this type, you also need to specify the static values for the parameter in the Parameter Static Values list. For example, a credit card payment parameter in a shopping application may be static and have the static values MasterCard®, Visa®, and American Express®.
<b>User-input value</b>	User-input parameters are those that require users to enter or provide some sort of data. This is the most commonly used parameter value type.

Parameter Value Type	Description
	Comment, name, and phone number fields on an online form are all examples of user-input parameters. You can also configure user-input parameters even if the parameter is not really user input. For example, if a parameter has a wide range of values or many static values, you may want to configure the parameter as a user-input parameter instead of as a static content parameter. By default, the system looks for attack patterns within all alpha-numeric user-input parameters. For each parameter, you can enable or disable a specific attack signature.
<b>XML value</b>	XML parameters are those whose parameter value contains XML data that is validated according to an XML profile that defines the format of the data. Select an existing XML profile or create a new one.

## How the system processes parameters

When you create any type of parameter, the system automatically places the parameter in staging and does not block requests even if a violation occurs and the system is configured to block that violation. Based on examining traffic, the system makes learning suggestions that you can accept or clear. If you create wildcard parameters, you also have the option of enabling learning for explicit entities.

The system enforces parameters in the following order:

- Flow parameters
- URL parameters
- Global parameters

If a parameter is defined more than once in the request context, the system applies only the more specific definition. For example, parameter `param_1` is defined as a static content global parameter, and also defined as a user-input URL parameter. When the Application Security Manager™ receives a request for the parameter in a URL that matches a URL defined in the security policy, and the parameter is defined on both the global and URL level, the system generates any violations based on the URL parameter definition.

## About path parameters

Path parameters are parameters that are attached to path segments in the URI. You can configure Application Security Manager™ (ASM) to enforce path parameters as needed in your organization. Path parameters can be ignored, or treated as parameters, or as an integral part of URLs.

Although path parameters are not widely used, they could serve as covert back doors to potential attacks even for server applications that do not use path parameters. For example, an application could copy a URI with path parameters containing attack signatures to the body of the response.

Path parameters can have multiple parameters in the same path segment separated by semicolons. A semicolon also separates the path segment from the parameters; for example, `/path/name;param1;p2;p3`. Each parameter can optionally equal a value; for example, `param=value;p2`. If a path parameter has more than one value, the values are separated by commas, such as `param=val1,val2,val3`.

Path parameters are extracted from requests, but not from responses.

## Enforcing path parameter security

A URI path parameter is the part of a path segment that occurs after its name. You can configure how a security policy handles path parameters that are attached to path segments in URIs. You can enforce different levels of security based on your needs.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. Scroll down to **Handle Path Parameters**, and select how you want to treat path parameters in URIs.

Option	Description
<b>As Parameter</b>	The system normalizes and enforces path parameters. For each path parameter, the system removes it from the URL as part of the normalization process, finds a corresponding parameter in the security policy (first at the matching URL level, and if not found, then at the Global level), and enforces it according to its attributes like any other parameter.
<b>As URL</b>	The system does not normalize or enforce path parameters, and treats them as an integral part of the URL.
<b>Ignore</b>	The system removes path parameters from URLs as part of the normalization process, but does not enforce them.

5. Click **Save**.
6. In the editing context area, click **Apply Policy** to put the changes into effect.

Path parameters in URIs are handled as specified in the security policy properties

---

**Note:** The maximum number of path parameters collected in one URI path is 10. All the rest of the parameters (from the eleventh on, counting from left to right) are ignored as parameters, but are still stripped from the URI as part of the normalization process.

---

---

# Chapter

# 30

---

## Securing Base64-Encoded Parameters

---

- *Overview: Securing Base64-Encoded Parameters*
- *Adding base64 decoding to a new user-input parameter*
- *Adding base64 decoding to an existing user-input parameter*

## Overview: Securing Base64-Encoded Parameters

---

*Base64 encoding* is a convenient encoding method that uses a compact presentation, and is relatively unreadable to the casual observer. Many applications apply base64 encoding to binary data, for inclusion in URLs or in hidden web form fields. Unfortunately, it is also possible to mask application attacks in base64-encoded data. To provide better security for applications that use base64 encoding, Application Security Manager™ can decode user-input parameter values that are base64-encoded.

## Adding base64 decoding to a new user-input parameter

---

If your application uses base64 encoding, the system can apply base64 decoding to a user-input parameter. When the decoding is successful, the system applies the parameter checks specified in the security policy. When the decoding is not successful, the system issues the `Illegal base64 encoded value` violation and responds to the offending request according the associated blocking policy.

1. On the Main tab, click **Security > Application Security > Parameters**.
2. Type the name for the new explicit parameter.
3. For the **Parameter Level** setting, select where in a request the parameter is located.

Option	Description
<b>Global</b>	The parameter can occur anywhere and is not associated with a specific URL or flow.
<b>URL</b>	The parameter occurs in the specific URL that you provide.
<b>Flow</b>	The parameter occurs in the specific entry point URL or referrer URL that you provide.

4. Leave the **Perform Staging** check box selected if you want the system to evaluate traffic before enforcing this parameter.  
Staging helps reduce the occurrence of false positives.
5. For the **Parameter Value Type** setting, select **User-input value**.
6. On the Data Type tab, for the **Data Type** setting, select either **Alpha-Numeric** or **File Upload**.
7. Select the **Base64 Decoding** check box if you want the system to apply base64 decoding to values for this parameter.
8. Configure any other properties that apply to this new parameter.
9. Click **Create**.  
The screen refreshes, and the new parameter appears in the parameters list.
10. To put the security policy changes into effect immediately, click **Apply Policy**.

## Adding base64 decoding to an existing user-input parameter

---

When enabled, the system can decode base64 encoding in a user-input parameter. If the decoding is successful, the system applies the parameter checks specified in the security policy. If the decoding is not successful,

the system issues the `Illegal base64 encoded value` violation and responds to the offending request according to the associated blocking policy.

1. On the Main tab, click **Security > Application Security > Parameters > Parameters List**.
2. In the Parameters List filter, select **Parameter Value Type** in the left list, **User-input value** in right list, and click **Go**.  
The screen refreshes and lists only user-input parameters.
3. In the Parameter Name column, click the name of the parameter to which you want to add base64 decoding.  
The Parameter Properties screen opens.
4. On the Data Type tab, select the **Base64 Decoding** check box so the system applies base64 decoding to values for this parameter.

---

***Note:** The base64 decoding setting is available only for user-input parameters of the alpha-numeric or file upload data type.*

---

5. Click **Update**.  
The screen refreshes, and displays the parameters list.
6. To put the security policy changes into effect immediately, click **Apply Policy**.





---

# Chapter

# 31

---

## Adding URLs to a Security Policy

---

- *About adding URLs*
- *About referrer URLs*
- *Adding allowed URLs*
- *Adding disallowed URLs*
- *Enforcing requests for URLs based on header content*
- *Specifying characters legal in URLs*
- *Configuring flows to URLs*
- *Creating flow parameters*
- *Configuring dynamic flows to URLs*
- *Configuring dynamic session IDs in URLs*

## About adding URLs

---

In a security policy, you can manually specify the file types that are allowed (or disallowed) in traffic to the web application being protected. This is only if you are not using automatic policy building which F5 recommends doing. When using automatic policy building, Application Security Manager™ determines which file types to add, based on legitimate traffic.

When you create a security policy, a wildcard file type of \*, representing all file types, is added to the file type list. During the enforcement readiness period, the system examines the file types in the traffic and makes learning suggestions that you can review and add the file types to the policy as needed. This way, the security policy includes the file types that are typically used. When you think all the file types are included in the security policy, you can remove the \* wildcard from the allowed file types list.

## About referrer URLs

---

*Referrer URLs* are web pages that request other URLs within a web application. For example, an HTML page can request a GIF, JPG, or PNG image file. The HTML page is the referrer, and the GIF, JPG, and PNG files are non-referrers. In lists of URLs, non-referrer URLs appear in blue and referrer URLs appear in gold.

A referrer in Application Security Manager™ is similar to the HTTP Referer header. Use referrers for complex objects, such as HTML pages, but not for embedded objects, such as GIF files.

## Adding allowed URLs

---

You can manually add *allowed URLs*, which are URLs that the security policy accepts in traffic to the web application being protected.

1. On the Main tab, click **Security > Application Security > URLs**.  
The Allowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Allowed URL screen opens.
4. For **URL**, choose a type and protocol, and then type the URL name or wildcard.

Option	Description
<b>Explicit</b>	Specifies a unique URL, such as <code>/index.html</code> . Choose <b>HTTP</b> or <b>HTTPS</b> , and type the URL in the adjacent field.
<b>Wildcard</b>	Specifies that the URL is a wildcard expression. Any URL that matches the wildcard expression is considered legal. The pure wildcard (*) is automatically added to the security policy so you do not need to add it. But you can add other wildcards such as <code>/main/*</code> . Select <b>HTTP</b> or <b>HTTPS</b> , and type a wildcard expression in the adjacent field.

5. By default, the **Perform Staging** check box is selected. F5 recommends that you keep it selected unless you are creating a wildcard URL for which you plan to **Add All Entities** in the **Learn Explicit Entities** setting. In that case, clear it.
6. If you are creating a wildcard URL, using the **Learn Explicit Entities** list, specify whether the system adds explicit URLs that match a wildcard to the security policy.

Option	Description
<b>Never (wildcard only)</b>	The system does not add or suggest that you add entities that match the wildcard to the policy. When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option results in a security policy that is easy to manage but may not be as strict.
<b>Add All Entities</b>	The system creates a comprehensive whitelist policy that includes all of the website entities. This option will form a large set of security policy entities, which produce a granular object-level configuration and high security level; it may take more time to maintain such a policy.

---

***Note:** Do not enable both staging and **Add All Entities** on the same wildcard entity.*

---

7. If you want to view more options, next to **Create New Allowed URL**, select **Advanced**.
8. To process requests for this URL according to the header content, create header-based content profiles. Another task provides details on how to do this.
9. To protect the application from being able to harbor illegitimate frames and iframes with malicious code in the application, set up protection from clickjacking:
  - a) For **Clickjacking Protection**, select the **Enabled** check box.
  - b) From the **Allow Rendering in Frames** list, select an option to determine whether to allow this URL to be rendered in a frame or iframe.
10. For wildcard URLs, leave **Wildcard Match Includes Slashes** selected.
 

When this option is selected, an asterisk in a wildcard matches any number of path segments (separated by slashes); when cleared, an asterisk matches at most one segment.
11. For wildcard URLs, in the Meta Characters tab, you can specify whether to check for meta characters in the URL, and which ones to allow or disallow.
  - a) The **Check characters on this URL** setting is enabled by default so that the system verifies meta characters in the URL. (If you do not want to check for meta characters, clear the check box and skip to the next step.)
  - b) To specify which meta characters to allow or disallow, from the **Global Security Policy Settings** list, select any meta characters that you want to specifically allow or disallow, and move them to the **Overridden Security Policy Settings** list.
  - c) For each meta character that you moved, set the state to **Allow** or **Disallow**.

---

***Note:** The **Overridden Security Policy Settings** take precedence over the global settings for the web application character set.*

---

12. Click **Create**.
 

The Allowed URLs screen opens and lists the new URL.
13. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy allows requests for the URL or URLs matching the wildcard that you added. If the URL is in staging, the system informs you when learning suggestions are available or when it is ready to be enforced.

## Wildcard syntax

The syntax for wildcard entities is based on shell-style wildcard characters. This table lists the wildcard characters that you can use in the names of file types, URLs, parameters, or cookies so that the entity name can match multiple objects.

Wildcard Character	Matches
*	All characters
?	Any single character
[abcde]	Exactly one of the characters listed
[!abcde]	Any character not listed
[a-e]	Exactly one character in the range
[!a-e]	Any character not in the range

## Allowed URL properties

These tables describe the allowed URL properties (both Basic and Advanced settings) that appear on different parts of the screen.

### Create New Allowed URL properties

Property	Description
<b>URL</b>	Specifies a URL that the security policy allows. The available types are: <ul style="list-style-type: none"> <li><b>Explicit:</b> Specifies that the URL is a unique URL. Type the URL in the adjacent field using the format <code>/index.html</code>.</li> <li><b>Wildcard:</b> Specifies a wildcard expression. Any URL that matches is considered legal. For example, typing <code>*</code> specifies that any URL is allowed by the security policy. Type a wildcard expression in the adjacent field.</li> </ul>
<b>Protocol</b>	Specifies whether the protocol for the URL is HTTP or HTTPS.
<b>Perform Staging</b>	Specifies that the system places this URL in staging. Learning suggestions produced by requesting staged URLs are logged in the Learning screens. Review staging status on the URL List screen. If a URL is in staging, point to the icon to display staging information. When you are no longer getting learning suggestions, you can disable this setting. If you enforce a URL, this setting is cleared.
<b>Learn Explicit Entities</b>	Specifies how to add or suggests you add URLs to the security policy if you are creating a wildcard URL. <ul style="list-style-type: none"> <li><b>Add All Entities:</b> The system suggests you add explicit URLs that match the wildcard to the security policy creating a comprehensive whitelist of all the URLs on the web site. You can review suggestions on the Traffic Learning screen.</li> <li><b>Never (wildcard only):</b> The system does not add URLs that match the wildcard to the security policy, and suggests changing the attributes of matched wildcard entities.</li> </ul>

Property	Description
<b>Check Flows to this URL</b>	Specifies that the security policy validates flows to the URL (if configured). If this setting is disabled, the system ignores the flows to the URL. When you select this check box, additional settings appear.
<b>URL is Entry Point</b>	(Visible when <b>Check Flows to this URL</b> is selected.) Specifies that this URL is a page through which a visitor can enter the web application.
<b>URL is Referrer</b>	(Visible when <b>Check Flows to this URL</b> is selected.) Specifies that the URL is a URL from which a user can access other URLs in the web application.
<b>URL can change Domain Cookie</b>	Specifies that the security policy does not block an HTTP request where the domain cookie was modified on the client side. Note that this setting is applicable only if the URL is a referrer.
<b>URL with Navigation Parameter</b>	Specifies that you want to associate a navigation parameter with this URL. You must have a navigation parameter defined in the security policy to view this option.
<b>Select Navigation Parameter</b>	Specifies a list of navigation parameters that you can associate with this URL.
<b>Navigation Parameter Value</b>	Indicates the value of the navigation parameter.
<b>Clickjacking Protection</b>	Specifies that the system adds the X-Frame-Options header to the domain cookie's response header. This is done to protect the web application against clickjacking. <i>Clickjacking</i> occurs when attacker lures a user to click illegitimate frames and iframes because the attacker hid them on legitimate visible website buttons. Therefore, enabling this option protects the web application from other web sites hiding malicious code behind them. The default is disabled. After you enable this option, you can select whether, and under what conditions, the browser should allow this URL to be rendered in a frame or iframe.
<b>Allow Rendering in Frames</b>	Specifies the conditions for when the browser should allow this URL to be rendered in a frame or iframe. <ul style="list-style-type: none"> <li>• <b>Never:</b> Specifies that this URL must never be rendered in a frame or iframe. The web application instructs browsers to hide, or disable, frame and iframe parts of this URL.</li> <li>• <b>Same Origin Only:</b> Specifies that the browser may load the frame or iframe if the referring page is from the same protocol, port, and domain as this URL. This limits the user to navigate only within the same web application.</li> <li>• <b>Only From URL:</b> Specifies that the browser may load the frame or iframe from a specified domain. Type the protocol and domain in URL format - for example, <code>http://www.mywebsite.com</code>. Do not enter a sub-URL, such as <code>http://www.mywebsite.com/index</code>.</li> </ul>
<b>Wildcard Match Includes Slashes</b>	Specifies that an asterisk in a wildcard URL matches any number of path segments (separated by slashes); when cleared, specifies that an asterisk matches at most one segment. For example: the wildcard <code>/art/*</code> matches <code>/art/abc/index.html</code> if the wildcard match includes slashes (default value), but does not match it if the check box is cleared. In that case, it matches <code>/art/go.html</code> (only one segment below <code>/art</code> ).
<b>HTML5 Cross-Domain Request Enforcement</b>	CORS (Cross-Origin Resource Sharing) lets one website access the resources of another website using JavaScript (within the browser). Web applications may share resources with other websites hosted on a different domain. When the option is selected, the system protects a specific URL in your web application from cross-origin resource sharing. You can configure which domains can access the

Property	Description
	response generated by requesting this URL (the resource), and how to overwrite CORS response headers returned by the web server.
<b>URL Description</b>	Describes the URL (optional).

### Header-Based Content Profiles

Property	Description
<b>Request Header Name</b>	Specifies an explicit header name that must appear in requests for this URL. This field is not case-sensitive.
<b>Request Header Value</b>	Specifies a simple pattern string (glob pattern matching) for the header value that must appear in legal requests for this URL; for example, <code>*json*</code> , <code>xml_method?</code> , or <code>method[0-9]</code> . If the header includes this pattern, the system assumes the request contains the type of data you select in the <b>Request Body Handling</b> setting. This field is case-sensitive.
<b>Request Body Handling</b>	<p>Indicates how the system parses the content of requests for the allowed URL:</p> <ul style="list-style-type: none"> <li>• <b>Apply Content Signatures:</b> Do not parse the content; scan the entire payload with full-content attack signatures.</li> <li>• <b>Apply Value and Content Signatures:</b> Do not parse the content or extract parameters; process the entire payload with value and full-content attack signatures.</li> <li>• <b>Disallow:</b> Block requests for an URL containing this header content. Log the Illegal Request Content Type violation.</li> <li>• <b>Do Nothing:</b> Do not inspect or parse the content. Handle the header of the request as specified by the security policy.</li> <li>• <b>Form Data:</b> Parse content as posted form data in either URL-encoded or multi-part formats. Enforce the form parameters according to the policy.</li> <li>• <b>GWT:</b> Perform checks for data in requests, based on the configuration of the GWT (Google Web Toolkit) profile associated with this URL.</li> <li>• <b>JSON:</b> Review JSON data using an associated JSON profile, and use value attack signatures to scan the element values.</li> <li>• <b>XML:</b> Review XML data using an associated XML profile.</li> </ul>
<b>Profile Name</b>	Specifies the XML, JSON, or GWT profile the security policy uses when examining requests for this URL if the header content is parsed as XML, JSON, or GWT. You can also create or view the XML, JSON, or GWT profile from this option.

### HTML5 Cross-Domain Request Enforcement

Property	Description
<b>Allow HTML5 Cross-Origin Requests</b>	Allows all CORS requests to this URL, and displays additional settings.
<b>Allowed Origins</b>	Allows you to specify a list of origins allowed to share data returned by this URL.
<b>Allowed Methods</b>	Allows you to specify a list of methods that other web applications hosted in different domains can use when requesting this URL.
<b>Allowed Headers</b>	Allows you to specify a list of request headers that other web applications hosted in different domains can use when requesting this URL. Or you can delete non-simple headers returned in response to requests.

Property	Description
<b>Exposed Headers</b>	Allows you to specify a list of response headers that are safe to expose to JavaScript, and can be shared with web applications hosted in different domains. Or you can allow only simple headers to be exposed.
<b>Allow Credentials</b>	Specifies whether requests from other web applications hosted in different domains may include user credentials.
<b>Maximum Age</b>	Specifies how long (in seconds) to cache in the browser the results of a preflight request (a special request that the browser sends to your web application to determine if JavaScript from another domain may access your resource).

### Meta Characters

Property	Description
<b>Check characters on this URL</b>	Specifies that the system verifies meta characters on this URL. You can change which meta characters are allowed or disallowed.

## Adding disallowed URLs

For some web applications, you may want to deny requests for certain URLs. In this case, you can create a set of disallowed URLs. Adding disallowed URLs is useful, for example, to prevent access to an administrative interface to the web application such as `/admin/config.php`.

1. On the Main tab, click **Security > Application Security > URLs > Disallowed URLs**.  
The Disallowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Disallowed URL screen opens.
4. For the **URL (Explicit only)** setting, select **HTTP** or **HTTPS** as the protocol for the URL, and type the URL that the security policy considers illegal; for example, `/index.html`.

---

***Note:** URLs are case-sensitive unless you cleared the **Security Policy is case sensitive** option when you created the policy.*

---

5. Click **Create**.  
The Disallowed URLs screen opens and lists the URL.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If a requested URL is on the disallowed URLs list, the system ignores, learns, logs, or blocks the request depending on the settings you configure for the **Illegal URL** violation on the Application Security: Blocking: Settings screen. You can view learning suggestions for disallowed URLs on the Illegal URL learning screen.

## Enforcing requests for URLs based on header content

Before you can enforce requests for URLs using header content, you need to have added an allowed URL.

When you manually create a new allowed URL, the system reviews requests for the URL using HTTP parsing. The system automatically creates a default header-based content profile for HTTP, and you cannot delete it. However, requests for an URL may contain other types of content, such as JSON, XML, or other proprietary formats.

You can use header-based content profiles to configure how the system recognizes and enforces requests for this URL according to the header content in the request. You can also use header-based content profiles to block traffic based on the type of header and header value in requests for a URL.

1. On the Main tab, click **Security > Application Security > URLs**.  
The Allowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Allowed URLs List, click the name of the URL for which you want to specify legal header content.  
The Allowed URL Properties screen opens where you can modify the properties of the URL.
4. From the **Allowed URL Properties** list, select **Advanced**.
5. In the Header-Based Content Profiles area, specify the header and value as follows:
  - a) In the **Request Header Name** field, type the explicit header name that must appear in requests for this URL. This field is not case-sensitive.
  - b) In the **Request Header Value** field, type the pattern string for the header value to find in legal requests for this URL, for example, `*json*`, `xml_method?`, or `method[0-9]`. This field is case-sensitive.  
If a header value includes this pattern, the system assumes that the request contains the type of data you select in the **Request Body Handling** setting.
- c) From the **Request Body Handling** list, specify how the system recognizes and enforces requests for this URL according to the requests' header content:

Option	Result
<b>Apply Content Signatures</b>	Do not parse the content; scan the entire payload with full-content attack signatures.
<b>Apply Value and Content Signatures</b>	Do not parse the content or extract parameters; process the entire payload with value and full-content attack signatures. This option provides basic security for protocols other than HTTP, XML, JSON, and GWT; for example, use <code>*amf*</code> as the header value for a content-type of Action Message Format.
<b>Disallow</b>	Block requests for an URL containing this header content. The system logs the <code>Illegal Request Content Type</code> violation.
<b>Do Nothing</b>	Do not inspect or parse the content. Handle the header of the request as specified by the security policy.
<b>Form Data</b>	Parse content as posted form data in either URL-encoded or multi-part formats. Enforce the form parameters according to the policy.
<b>GWT</b>	Examine data in requests, based on the configuration of a GWT (Google Web Toolkit) profile associated with this URL.



Option	Result
JSON	Examine JSON data using an associated JSON profile, and use value attack signatures to scan the element values.
XML	Examine XML data using an associated XML profile.

- d) If the content is GWT, JSON, or XML, select an existing profile or click the create (+) button to create one. (The other options do not require special profiles.)
- e) Click **Add**.

6. Click **Update**.

7. To put the security policy changes into effect immediately, click **Apply Policy**.

If the system detects a request for a URL, which contains header content that is disallowed in the URL's Header-Based Content Profile, the `Illegal request content type` violation occurs.

## Specifying characters legal in URLs

When you create a security policy, you select a language encoding (or let the system determine it automatically) that determines the characters that can be used in URLs. You can view or modify which characters the security policy allows or disallows in URLs.

1. On the Main tab, click **Security > Application Security > URLs > Character Set**.  
The URLs Character Set screen opens, where you can view the character set, and state of each character.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Use the **View** option to display the characters that you want to see.

---

**Tip:** To restore the default character set definitions, you can click the **Restore Defaults** button at any time.

---

4. To modify which characters the system should permit or prohibit in the name of a wildcard URL, click **Allow** or **Disallow** next to the character.
5. Click **Save** to save the changes.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy checks that URLs in requests do not include any disallowed characters. For example, by disallowing the characters `<`, `>`, `'`, and `|`, a security policy protects against many cross-site scripting attacks and injection attacks.

## Configuring flows to URLs

Before you can configure a flow, should have created the explicit URL for which you want to add the flow.

A *flow* defines the access path leading from one explicit URL to another, between a referrer URL and a target URL in a web application. For example, a basic web page may include a graphic and hyperlinks to other pages in the application. The calls from the basic page to the other pages make up the flow. You can configure flows to a URL.

---

**Note:** Configuring flows is an optional task. Unless you need the enhanced security of configured flows, F5 Networks recommends that you do not configure flow-based security policies due to their complexity.

---

1. On the Main tab, click **Security > Application Security > URLs**.  
The Allowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Allowed URLs List, click the name of the URL you want to modify.  
The Allowed URL Properties screen opens.
4. On the menu bar, click **Flows to URL**.  
The Flows to URL screen opens and shows the flows to that specific URL.
5. Above the Flows to URL area, click **Create**.  
The Create a New Flow popup screen opens.
6. For the **Referrer URL** setting, specify how the client enters the application.
  - If you want the client to enter the application from this URL, select **Entry Point**.
  - To specify the path of a referrer URL that refers to other URLs in the application, select **URL Path**; for example, type `/index.html`.
7. From the **Protocol** list, select the appropriate protocol, **HTTP** or **HTTPS**.
8. From the **Method** list, select the HTTP method that the URL expects a visitor to use to access the authenticated URL, for example, **GET** or **POST**.
9. In the **Frame Target** field, type the index (0-29, or 99) of the HTML frame in which the URL belongs, if the web application uses frames.

---

**Tip:** If your web application does not use frames, type the value `1`.

---

10. If this flow can contain a query strings or POST data, select the **Allow QS/PD** check box.
11. If you want the system to verify query strings or POST data for this flow, select the **Check QS/PD** check box.
12. Click **OK**.  
The popup screen closes, and on the Flows to URL screen, you see the URLs from which the URL can be accessed.
13. To view the flow or modify the flow properties, click the URL in the Flows list.
14. To view the entire application flow, click **Security > Application Security > URLs > Flows List**
15. To put the security policy changes into effect immediately, click **Apply Policy**.

You now have the option of creating parameters that are associated with the flow.

---

## Creating flow parameters

---

Before you can create a flow parameter, you need to first have created the flow to which the parameter applies. If the source URL is a referrer URL, that URL must already be defined in the security policy as well.

You define parameters in the context of a flow when it is important to enforce that the target URL receives a parameter only from a specific referrer URL. Flow parameters provide very tight, flow-specific security for web applications. With this increased protection comes an increase in maintenance and configuration time. Note that if your application uses dynamic parameters, you need to manually add those to the security policy.

1. On the Main tab, click **Security > Application Security > Parameters**.
  2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
  3. Click **Create**.  
The Add Parameter screen opens.
  4. In the Create New Parameter area, for the **Parameter Name** setting, specify the type of parameter you want to create.
    - To create a named parameter, select **Explicit**, then type the name.
    - To use pattern matching, select **Wildcard**, then type a wildcard expression. Any parameter name that matches the wildcard expression is permitted by the security policy.
    - To create an unnamed parameter, select **No Name**. The system creates a parameter with the label, UNNAMED.
  5. In the **Parameter Level** setting, select **Flow**, and then for **From URL** define where the flow must come from:
    - If the source URL is an entry point, click **Entry Point**.
    - If the source URL is a referrer URL (already defined in the policy), click **URL Path**, select the protocol used for the URL, then type the referrer URL associated with the flow.

When you begin to type the URL, the system lists all referrer URLs that include the character you typed, and you can select the URL from the list.
  6. In the **Parameter Level** setting, for **Method**, select the HTTP method (**GET** or **POST**) that applies to the target referrer URL (already defined in the policy).
  7. In the **Parameter Level** setting, for **To URL**, select the protocol used for the URL, then type the target URL.
  8. Leave the **Perform Staging** check box selected if you want the system to evaluate traffic before enforcing this parameter.  
Staging helps reduce the occurrence of false positives.
  9. If you are creating a wildcard parameter and you want the system to display explicit parameters that match the wildcard entity pattern that you specify, for the **Learn Explicit Entities** setting, select **Add All Entities**.
  10. If the parameter is required in the context of the flow, select the **Is Mandatory Parameter** check box.  
Note that only flows can have mandatory parameters.
  11. Specify whether the parameter requires a value:
    - If the parameter is acceptable without a value, leave the **Allow Empty Value** setting enabled.
    - If the parameter must always include a value, clear the **Allow Empty Value** check box.
  12. To allow users to send a request that contains multiple parameters with the same name, select the **Allow Repeated Occurrences** check box.
- 
- Important:** Before enabling this check box, consider that requests containing multiple parameters of the same name could indicate an attack on the web application (HTTP Parameter Pollution).
- 
13. If you want to treat the parameter you are creating as a sensitive parameter (data not visible in logs or the user interface), enable the **Sensitive Parameter** setting.
  14. For the **Parameter Value Type** setting, select the format of the parameter value.  
Depending on the value type you select, the screen refreshes to display additional configuration options.
  15. Click **Create** to add the new parameter to the security policy.
  16. To put the security policy changes into effect immediately, click **Apply Policy**.

When you create a parameter that is associated with a flow, the system verifies the parameter in the context of the flow. For example, if you define a parameter in the context of a GET request, and a client sends a POST request that contains the parameter, the system generates an `Illegal Parameter` violation.

## Configuring dynamic flows to URLs

---

Before you can configure a dynamic flow, you must have created the explicit URL for which you want to add the dynamic flow.

Some web applications contain URLs with dynamic names, for example, the links to a server location for file downloads, where the file name may be unique to each user. You can configure the system to detect these URLs by creating a dynamic flow. For the dynamic flow, you specify a regular expression that describes the dynamic name, and associate the flow with the URL.

1. On the Main tab, click **Security > Application Security > URLs**.  
The Allowed URLs screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Allowed URLs List, click the name of the URL you want to modify.  
The Allowed URL Properties screen opens.
4. On the menu bar, click **Dynamic Flows from URL**.  
The Flows to URL screen opens and shows the flows to that specific URL.
5. Above the Dynamic Flows to URL area, click **Create**.  
The Create a New Dynamic Flow popup screen opens.
6. In the **Prefix** field, type a fixed substring that appears near the top of the HTML source page before the dynamic URL.  
The prefix may be the name of a section in combination with HTML tags, for example, `<title>Online Banking</title>`.
7. For the **RegExpValue** setting, type a regular expression that specifies the set of URLs that make up the dynamic flow, for example, a set of archive files.
8. For the **Suffix** setting, type a fixed string that occurs in the referring URL's source code, and is physically located after the reference to the dynamic name URL.
9. Click **OK**.  
The popup screen closes, and on the Dynamic Flows from URL screen, you see the dynamic flow extraction properties.
10. To put the security policy changes into effect immediately, click **Apply Policy**.

The regular expression describes the dynamic URL name. The Application Security Manager extracts dynamic URL names from the URL responses associated with the dynamic flow.

## Configuring dynamic session IDs in URLs

---

If an application uses dynamic information in URLs (for example, user names), the Application Security Manager™ cannot use its normal functions to extract and enforce URLs or flows because the URI contains a dynamic element. If the web application that you are securing could contain dynamic information in a URL, you can allow dynamic session IDs in URLs. (You only need to configure this setting if you know that your application works this way.)

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. For the **Dynamic Session ID in URL** setting, specify how the security policy should process URLs that use dynamic sessions.

Use this option	When
<b>Custom pattern</b>	The security policy uses a user-defined regular expression to recognize a dynamic session ID in URLs. Type a regular expression in the <b>Value</b> field, and a description in the <b>Description</b> field.
<b>Default pattern</b>	The security policy uses the default regular expression <code>(\sap\[^\]+)</code> for recognizing a dynamic session ID in URL.
<b>Disabled</b>	The security policy does not enforce dynamic session IDs in URLs. This is the default value.

5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

Normally, if the system receives a request in which the dynamic session information does not match the settings in the security policy, the system issues the `Illegal session ID in URL` violation. When you allow dynamic session IDs in URLs, ASM extracts the dynamic session information from requests or responses, based on the pattern that you configure. For requests, the system applies the pattern to the URI up to, but not including, the question mark (?) character in a query string.

---

**Note:** The system can extract dynamic information only from illegal URLs.

---



---

# Chapter

# 32

---

## Adding Cookies

---

- *About cookies*
  - *About adding cookies*
-

### About cookies

---

Many web-based applications use cookies to help users navigate the web site efficiently and perform certain functions. For example, web servers may use cookies to authenticate users logging in to secure applications, or an application can use cookies to store user preferences. Whether using automatic policy building or manually creating a security policy, you may want to add cookies that the web application uses.

You may want a security policy to ignore certain known and recognized cookie headers that are included in HTTP requests. For example, if cookies can change on the client side legitimately, you can create *allowed cookies*.

You may also want a security policy to prevent changes to specific cookies, such as session-related cookies that are set by the application. If so, you can create *enforced cookies*. The cookie in the request must not be modified, or it generates the Modified Domain Cookie violation.

In addition, some PHP applications treat cookies as parameters and use the value of the cookie as input to the application. For that reason, you can have the system check attack signatures on the cookie (as you can for parameters). You can apply attack signatures only to allowed cookies, because enforced cookies are set by the server, and therefore, are considered to be secure.

Both allowed and enforced cookies can be put in staging when they are created so that you can make sure that they do not cause false positives during the staging period.

If you are using automatic policy building, the security policy adds cookies automatically. If manually building a security policy, the manual traffic learning screens suggest cookies to add.

### About pure wildcard cookies

When you create a security policy, it includes a pure wildcard (\*) and it is created as an allowed cookie in the Allowed Cookies list. You cannot delete the pure wildcard from the security policy but you can change its type from allowed to enforced. The allowed cookie wildcard allows all cookies, and you can specify which cookies the users cannot change in the enforced cookies list. This is considered a negative security model, because you allow all cookies except the ones you specify.

However, new cookies are added to the security policy (or not) based on the Learn Explicit Entities value of the matched wildcard. The value can be Never (do not add cookies) or Selective (add cookies that match the wildcard). The default value differs depending on the deployment scenario you use to create the policy.

The following deployments create pure wildcard cookies using the value **Never**, thus they do not add (or suggest to add) explicit cookies to the security policy:

- All templates (including Rapid Deployment policy)
- Automatic policy building with Fundamental policy type
- Vulnerability assessment

All other deployment scenarios create the pure wildcard cookie with Learn Explicit Entities set to Selective. So it adds (if building the policy automatically) or suggests to add (if building the policy manually) explicit cookies encountered in the traffic to the security policy.

In Selective mode, the system learns cookies that violate the settings of the wildcard. In particular, cookies that do not change are learned as enforced cookies. Most cookies are added to the security policy as allowed cookies, and are checked for the configured signature set. These are captured by the \* pure wildcard. The exceptions are the enforced cookies and cookies that need to be exempted from some of the signature checks. These are whitelisted.



## Wildcard syntax

The syntax for wildcard entities is based on shell-style wildcard characters. This table lists the wildcard characters that you can use in the names of file types, URLs, parameters, or cookies so that the entity name can match multiple objects.

Wildcard Character	Matches
*	All characters
?	Any single character
[abcde]	Exactly one of the characters listed
[!abcde]	Any character not listed
[a-e]	Exactly one character in the range
[!a-e]	Any character not in the range

## About cookies and learning

When you create a security policy that includes cookies, the system adds new cookies (or suggests that you add them) to the security policy (or not) based on the Learn Explicit Entities value of the matched wildcard. The value can be Never (do not add cookies) or Selective (add cookies that match the wildcard). The default value differs depending on the deployment scenario you use to create the policy.

The following deployments create pure wildcard cookies using the value Never, thus they do not add (or suggest to add) explicit cookies to the security policy by default:

- Rapid Deployment policy
- Automatic policy building with Fundamental policy type
- Vulnerability assessment

All other deployment scenarios create the pure wildcard cookie with Learn Explicit Entities set to Selective. So the system adds (if building the policy automatically) or suggests to add (if building the policy manually) explicit cookies encountered in the traffic to the security policy.

You could start by having the wildcard set to selective in the allowed cookies, get a list of all the cookies that your web application uses, then move them to the enforced list. This would make it easier to add the cookies that your web application uses and that you want to enforce to the security policy.

## About adding cookies

Application Security Manager™ (ASM) allows you to add cookies with different characteristics to security policies.

You can specify the cookies that you want to allow, and the ones you want to enforce in a security policy:

- Allowed cookies: The system allows these cookies and clients can change them.
- Enforced cookies: The system enforces the cookies in the list (not allowing clients to change them) and allows clients to change all others.

If the cookies in the web application change, you can edit or delete the cookies.

## Adding allowed cookies

You manually add allowed cookies to a security policy when you want a security policy to ignore those cookies. You may want to add allowed cookies for certain known and recognized cookie headers that are often included in HTTP requests. For example, if clients can change certain cookies legitimately and they are not session-related (like cookies assigned by single sign-on servers), you can specify these cookies as allowed in the security policy.

1. On the Main tab, click **Security > Application Security > Headers**.  
The Cookies List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Cookie screen opens.
4. For **Cookie Name** identify the cookie.
  - a) From the list, select whether the system identifies the cookie by a specific name (**Explicit**), or by a regular expression (**Wildcard**).  
The pure wildcard (\*) is automatically added to the security policy so you do not need to add it. But you can add other wildcards such as `*site.com`.
  - b) In the field, type either the name of the cookie, or the pattern string for the wildcard to match cookie names.
5. For **Cookie Type**, select **Allowed**.
6. Leave the **Perform Staging** check box selected if you want the security policy to evaluate traffic before enforcing this entity.  
Staging helps reduce the occurrence of false positives.
7. For wildcard cookies, from the **Learn Explicit Entities** list, select whether the system adds explicit entities that match a wildcard entity to the security policy.

Option	Description
<b>Never (wildcard only)</b>	The system does not add or suggest that you add entities that match the wildcard to the policy. When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option results in a security policy that is easy to manage but may not be as strict.
<b>Selective</b>	The system adds or suggests that you add entities that match the wildcard to the policy. When false positives occur, the system adds or suggests that you add an explicit entity with relaxed settings that avoid the false positive. This option provides a good balance between security, policy size, and ease of maintenance.

For pure wildcard cookies (\*), you specify **Explicit Entities Learning** on the Policy Building Settings screen.

8. If you want the system to add the HttpOnly attribute to the response header of the domain cookie, select the **Insert HttpOnly attribute** check box.  
This attribute prevents the cookie from being modified or intercepted on the client side, by unwanted third parties that run scripts on the web page. The client's browser allows only pure HTTP or HTTPS traffic to access the protected cookie.
9. If you want the system to add the Secure attribute to the response header of the domain cookie, select the **Insert Secure attribute** check box.  
This attribute ensures that cookies are returned to the server only over SSL, which prevents the cookie from being intercepted. It does not, however, guarantee the integrity of the returned cookie.

10. If this is a custom cookie that may include base64 encoding, select the **Base64 Decoding** check box.  
If the cookie contains a Base64 encoded string, the system decodes the string and continues with its security checks.
11. To adjust the attack signature settings for this cookie, use the Attack Signatures tab. Tip: The most common action you perform here is to disable a specific attack signature for a specific cookie.
  - a) If you want to override the attack signature settings for this cookie, select the **Check attack signatures on this cookie** check box.  
When this option is selected, the system displays a list of attack signatures.
  - b) From the **Global Security Policy Settings** list, move any attack signatures whose global settings you want to override into the **Overridden Security Policy Settings** and adjust the state as needed.
12. Click **Create**.  
The new cookie is created and added to the list.
13. To put the security policy changes into effect immediately, click **Apply Policy**.

The system ignores allowed cookies in requests, and allows clients to change allowed cookies in the list.

## Adding enforced cookies

You manually add enforced cookies to a security policy when you want a security policy to prevent clients from changing those cookies.

1. On the Main tab, click **Security > Application Security > Headers**.  
The Cookies List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Cookie screen opens.
4. For **Cookie Name** identify the cookie.
  - a) From the list, select whether the system identifies the cookie by a specific name (**Explicit**), or by a regular expression (**Wildcard**).  
The pure wildcard (\*) is automatically added to the security policy so you do not need to add it. But you can add other wildcards such as `*site.com`.
  - b) In the field, type either the name of the cookie, or the pattern string for the wildcard to match cookie names.
5. For **Cookie Type**, select **Enforced**.
6. Leave the **Perform Staging** check box selected if you want the security policy to evaluate traffic before enforcing this entity.  
Staging helps reduce the occurrence of false positives.
7. For wildcard cookies, from the **Learn Explicit Entities** list, select whether the system adds explicit entities that match a wildcard entity to the security policy.

Option	Description
<b>Never (wildcard only)</b>	The system does not add or suggest that you add entities that match the wildcard to the policy. When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option results in a security policy that is easy to manage but may not be as strict.
<b>Selective</b>	The system adds or suggests that you add entities that match the wildcard to the policy. When false positives occur, the system adds or suggests that you add an

Option	Description
	explicit entity with relaxed settings that avoid the false positive. This option provides a good balance between security, policy size, and ease of maintenance.

For pure wildcard cookies (\*), you specify **Explicit Entities Learning** on the Policy Building Settings screen.

8. If you want the system to add the HttpOnly attribute to the response header of the domain cookie, select the **Insert HttpOnly attribute** check box.

This attribute prevents the cookie from being modified or intercepted on the client side, by unwanted third parties that run scripts on the web page. The client's browser allows only pure HTTP or HTTPS traffic to access the protected cookie.

9. If you want the system to add the Secure attribute to the response header of the domain cookie, select the **Insert Secure attribute** check box.

This attribute ensures that cookies are returned to the server only over SSL, which prevents the cookie from being intercepted. It does not, however, guarantee the integrity of the returned cookie.

10. Click **Create**.

The new cookie is created and added to the list.

11. To put the security policy changes into effect immediately, click **Apply Policy**.

If a request contains a modified or unsigned enforced cookie header and the Modified domain cookie(s) violation is set to alarm or block, the system logs and/or blocks the request (when the system is in blocking mode). Note that the request is not blocked if the enforced cookie is in staging, or if the security policy is in transparent mode.

## Changing the order in which wildcard cookies are enforced

If you create several wildcard cookies, the security policy adds each new one to the top of the wildcard cookies list. The cookie wildcards are enforced from the top of the list down. You can change the order in which a security policy enforces wildcard cookies.

1. On the Main tab, click **Security > Application Security > Headers > Cookie Wildcards Order**. The Cookie Wildcards Order screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select either the Enforced Cookies or Allowed Cookies tab to locate the cookie you want to edit.
4. In the **Wildcard Cookies** list, adjust the order of the cookie wildcards by using the Up and Down buttons putting the cookies you want to enforce first at the top of the list.
5. Click **Save** to save the changes.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

The system enforces the cookie wildcards from the top down.

## Editing cookies

You can edit cookies as required by changes in the web application that the security policy is protecting.

1. On the Main tab, click **Security > Application Security > Headers**. The Cookies List screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select either the Enforced Cookies or Allowed Cookies tab to locate the cookie you want to edit.
4. In the Cookie Name column, click the cookie name.  
The Edit Cookie screen opens.
5. In the Cookie Properties area, make the required changes to the cookie.
6. Click **Update** to save the changes.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

## Deleting cookies

You can delete cookies that are no longer needed in your security policy. If a cookie changes in your application, you may want to delete the old cookie and let Application Security Manager™ add the new cookie (or suggest adding it).

1. On the Main tab, click **Security > Application Security > Headers**.  
The Cookies List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select either the Enforced Cookies or Allowed Cookies tab to locate the cookie you want to edit.
4. In the Enforced Cookies or Allowed Cookies list, select the check box next to the cookie you want to delete.
5. Click **Delete** to delete the entity, and click **OK** when asked to confirm.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

## Specifying when to add explicit cookies

You can specify the circumstances under which Application Security Manager™ adds, or suggests you add, explicit cookies to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the **Explicit Entities Learning** setting, for **Cookies**, select the option you want.

Option	Description
<b>Never (wildcard only)</b>	The system does not add or suggest that you add cookies that match the wildcard to the policy. When false positives occur, the system suggests relaxing the settings of the wildcard entity. This option results in a security policy that is easy to manage but may not be as strict.
<b>Selective</b>	The system adds or suggests that you add cookies that match the wildcard to the policy. When false positives occur, the system adds or suggests that you add an explicit entity with relaxed settings that avoid the false positive. This option provides a good balance between security, policy size, and ease of maintenance.

4. Click **Save** to save the changes.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

## Configuring the maximum cookie header length

You specify a maximum cookie header length so that the system knows the acceptable maximum length for the cookie header in an incoming request. This setting is useful primarily in preventing buffer overflow attacks.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the name of the security policy you want to work on.  
The Properties screen opens.
3. From the **Configuration** list, select **Advanced**.
4. For the **Maximum Cookie Header Length** setting, select one of the options.

Option	Description
<b>Any</b>	Specifies that the system accepts requests with cookie headers of any length.
<b>Length with a value in bytes</b>	Specifies that the system accepts cookie headers up to that length. The default maximum length is <b>8192</b> bytes.

5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

The system calculates and enforces the cookie header length based on the sum of the length of the cookie header name and value. Requests with headers that are longer than the maximum length cause an Illegal header length violation.

---

# Chapter

# 33

---

## Configuring Advanced Cookie Protection

---

- *Overview: Configuring advanced cookie protection*
-

## Overview: Configuring advanced cookie protection

---

Many of the Application Security Manager™ (ASM) security features store ASM™ cookies on clients as part of the traffic security enforcement. Examples of security features that use cookies for validation are cookie enforcement, parameter enforcement, CSRF protection, login enforcement, session tracking, and anomaly detection. Cookie enforcement is also called *domain cookies*; cookies for the other features are called *other ASM cookies*.

The system applies a random security key unique to each deployment and uses it in conjunction with an encryption algorithm. The combination of the randomly generated key and the selected algorithms is called the *security context*. Normally, you do not have to change the cookie protection settings. However, in cases where you suspect a security breach has occurred, or if you want a different balance between speed and security, you can reconfigure cookie protection.

By default, when you initially start the system, it automatically generates a security key and sets the cookie security level to secure. You can change the encryption schema to provide faster cookie protection by reconfiguring cookie protection.

If you want to use the same security context on other systems, you can set up advanced cookie configuration settings on one BIG-IP® system and export them. You can then import the settings on the other systems. You can configure all your systems to use the same cookie protection, or apply different settings to the systems. However, if you have multiple ASM-enabled devices that share traffic (and are not synchronized using device groups), it is recommended that those systems should all use the same cookie protection settings.

If synchronizing multiple ASM systems using device groups, you can configure the settings you want to use for all systems on one and then synchronize the systems.

## Reconfiguring cookie protection

Application Security Manager™ (ASM) automatically configures cookie protection. If you need to adjust cookie protection due to a security breach or because you want to change the current protection level, you can reconfigure cookie protection.

---

**Note:** *This is an advanced configuration task that is required only in special circumstances.*

---

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Cookie Protection**.  
The Cookie Protection screen opens.
2. Review the data and time specified in the **Latest Generation/Import Configuration Time** setting to see when cookie protection was last configured.
3. To review the details of the cookie protection, click **View Algorithms Configuration**.  
The screen shows the specific algorithms the system uses to protect domain and other ASM cookies.
4. If you decide that you want to change the cookie configuration, click **Reconfigure Cookie Protection**.  
The Reconfigure Cookie Protection screen opens.
5. For **Grace Period Until signing with new Security Context**, type the amount of time in minutes that must pass before the system begins signing ASM cookies with the new key and algorithm that you are configuring.  
The default value is 30 minutes. Initially when you start the system, this is the period the system waits to apply the new security context for the new release.
6. For **Grace Period To Accept Old Cookies**, type the amount of time in minutes that must pass before the system stops accepting traffic with ASM cookies that use the old key and algorithm.



The default value is 2880 minutes (48 hours).

7. For **Algorithm Selection**, select the overall cookie security level to apply: **Secure** or **Fast**.

---

***Tip:** The **Secure** setting uses more system resources.*

---

Changing this setting changes the Scramble and Mac algorithms used for cookie protection.

8. If you want to review the actual algorithms used for the cookies, you can do this:
  - a) For the **Cookie Protection Configuration** setting, select **Advanced**.  
The screen shows additional settings.
  - b) Review the scramble and Mac algorithms used for the domain cookies and other ASM cookies, and adjust them if needed.  
If you use settings other than the defaults, the **Algorithm Selection** changes to **Custom**.
9. Click **Reconfigure**.  
The system regenerates a new security context but waits to start using it until it surpasses the grace period until signing value.
10. If you need to extend either of the grace periods, click **Extend** and type the number of minutes to add and click **Save**.

## Importing cookie protection configuration

If you want to use the same cookie configuration settings on more than one Application Security Manager™ (ASM) system (especially systems that share traffic), you can export the settings from one system and import them onto another one. This task explains how to import the settings.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Cookie Protection**.  
The Cookie Protection screen opens.
2. Click **Import**.  
The Import Cookie Protection Configuration screen opens.
3. From the **Import Method** list, select **Upload file** and locate the previously exported configuration file.  
The exported file has a name such as  
ASM\_Cookie\_Protection\_Configuration\_2013-08-15\_08-22.txt.
4. To review the details of the cookie protection, click **View Algorithms Configuration**.  
The screen shows the specific algorithms the system uses to protect domain and other ASM cookies.
5. For **Grace Period Until signing with new Security Context**, type the amount of time in minutes that must pass before the system begins signing ASM cookies with the new key and algorithm that you are configuring.  
The default value is 30 minutes. Initially when you start the system, this is the period the system waits to apply the new security context for the new release.
6. For **Grace Period To Accept Old Cookies**, type the amount of time in minutes that must pass before the system stops accepting traffic with ASM cookies that use the old key and algorithm.  
The default value is 2880 minutes (48 hours).
7. Click **Import**.  
The system imports the security context but waits to start using it until the grace period until signing is up.
8. If you need to extend either of the grace periods, click **Extend** and type the number of minutes to add and click **Save**.

### Exporting cookie protection configuration

If you want to use the same cookie configuration settings on more than one Application Security Manager™ system, you can export the settings from one system and import them onto another one. This task explains how to export the settings to a file.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Cookie Protection**.

The Cookie Protection screen opens.

2. Click **Export**.

The system exports the cookie protection configuration to a file with a name such as

`ASM_Cookie_Protection_Configuration_2013-08-15_08-22.txt`.

---

# Chapter

# 34

---

## Adding Allowed Methods to a Security Policy

---

- *Adding allowed methods*
-

## Adding allowed methods

---

All security policies accept standard HTTP methods by default. If your web application uses HTTP methods other than the default allowed methods (GET, HEAD, and POST), you can add them to the security policy.

1. On the Main tab, click **Security > Application Security > Headers > Methods**.  
The Methods screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.
4. For the **Method** setting, select the type of method to allow:
  - To use an existing HTTP method to act as a GET or POST action, select **Predefined** then select the system-supplied method to add to the allowed methods list.
  - To add an option that is not predefined, select **Custom**, and then in the **Custom Method** field, type the name of a method.
5. If using flows in the security policy, from the **Allowed Method Properties** list, select **Advanced**, then from the **Act as Method** list, select an option:
  - If you do not expect requests to contain HTTP data following the HTTP header section, select **GET**.
  - If you expect requests to contain HTTP data following the HTTP header section, select **POST**.
6. Click **Create**.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The method is added to the allowed methods list. The system treats any incoming HTTP request that uses an HTTP method other than an allowed method as an invalid request. The system ignores, learns, logs, or blocks the request depending on the settings configured for the `Illegal Method` violation on the Application Security: Blocking: Settings screen.

---

# Chapter

# 35

---

## Configuring HTTP Headers

---

- *About mandatory headers*
  - *About header normalization*
  - *About default HTTP headers*
  - *Overview: Configuring HTTP headers*
  - *Implementation Result*
-

## About mandatory headers

---

A *mandatory header* is a header that must appear in a request for the request to be considered legal by the system. If a request does not contain the mandatory header and the Mandatory HTTP header is missing violation is set to alarm or block, the system logs or blocks the request. This violation is not set to alarm or block by default, so you have to set the blocking policy if you want to alarm or block requests that do not include a mandatory header.

You can use mandatory headers to make sure, for example, that requests are passing a proxy (which introduces such a header) before they reach the Application Security Manager™.

You configure mandatory headers on the HTTP Headers screen.

## About header normalization

---

*Header normalization* is a process whereby the Application Security Manager™ buffers the contents of request headers to change them into a standard format that can be more easily checked for discrepancies. Normalizing deals with special characters (such as percent encoding), non-ASCII text, URL paths and parameters, Base64 encoded binary content, non-printable characters, HTML codes, and many other formats that may be used in headers that could potentially hide malicious code.

Not all headers need to be normalized. You should normalize referer headers, and custom headers containing binary data, URLs, or other encoded information. But there is a performance trade-off when using normalization, so you should implement it only when needed.

You configure header normalization on the HTTP Headers screen when you select the option to check signatures for the header.

## About default HTTP headers

---

Application Security Manager™ (ASM) includes the default HTTP headers listed in the table.

Header Name	Description
* (wildcard)	This wildcard HTTP header checks signatures against all requests unless they match another HTTP header. No normalization settings are selected by default, but you can edit them. Realize that enabling normalization on the wildcard header may impact performance. The <b>Base64 Decoding</b> and <b>Mandatory</b> check boxes are unavailable for this header.
referer	When requests have referer headers, they include URLs. The system checks signatures against them, performs URL normalization, and validates the URL syntax. Violations are issued if problems are encountered during normalization. The other settings are not typically relevant for this header.
cookie	Cookies have their own process for normalization and attack signature check and so the cookie as a header is always excluded from the normalization and attack signature check. You cannot change the settings, but you can configure the settings of a specific cookie by clicking the <b>Cookie configuration</b> link.

Header Name	Description
authorization	Although the user name may be encoded as Base64, the Base64 decoding is always off for this header; the reason for this is that the user name (and password) are only part of the Authorization header value. ASM™ detects what and when to decode, so the generic Base64 setting should always be off. Therefore, the <b>Base64 Decoding</b> check box is unavailable for this header. Realize that enabling normalization on the authorization header may impact performance.

You cannot delete any of the default HTTP headers.

## Overview: Configuring HTTP headers

This is an advanced task not required in all environments.

Application Security Manager™ (ASM) lets you configure custom headers that deserve special treatment in your security policy. You can add these types of headers:

- Mandatory headers
- Headers that require Base64 decoding
- Headers to exclude from signature checks
- Headers that need to be normalized

The security policy can recognize requests with these headers and handles them with special consideration. For example, if your application uses custom headers that must occur in every request, you can configure mandatory headers in the security policy. Or, if some request headers include binary content encoded in Base64, you can instruct ASM™ to decode the data and examine it for discrepancies.

You can also specify many different options to normalize an HTTP header for which you want to check signatures.

## Configuring HTTP headers

You add HTTP headers to a security policy when you need to define certain headers that require special treatment when found in requests. For example, if you are receiving false positives for a certain type of header, you can create the header and exclude it from signature checks.

1. On the Main tab, click **Security > Application Security > Headers > HTTP Headers**.  
The HTTP Headers screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Header screen opens.
4. From the **Name** list, select a standard HTTP header name type or select **Custom** and type the custom header name that appears in requests.
5. If you want this to be a header that is required in every request, select the **Mandatory** check box.  
If a request does not include this header, the Mandatory HTTP header is missing violation occurs (if set to alarm or block).
6. If you want the security policy to check this header against attack signatures, select the **Check Signatures** check box. Otherwise, this header is excluded from signature checks.  
If the check box is selected, the screen displays additional settings for header normalization.

7. If this is a custom header that may include base64 encoding, select the **Base64 Decoding** check box.

---

***Note:** When this check box is selected, the options **Percent Decoding**, **Url Normalization**, and **Normalization Violations** setting are unavailable because they are not compatible with Base64 decoding.*

---

The system performs decoding on the header and if decoding fails, the Illegal Base64 Value violation occurs (if set to alarm or block).

8. If you want to normalize this header, select the options you need.

Option	Description
<b>Percent Decoding</b>	This option normalizes referer headers or custom headers that may include strings with encoded percent codes (%xx) that replace certain characters, perform unescaping, and require other checks. This is included in URL normalization and thus is not available when checking the URL Normalization option.
<b>Url Normalization</b>	This option normalizes URLs in referer headers or custom headers that may include URLs with multiple slashes, directory traversal, or which require backslash replacement or path parameter removal. Includes percent decoding also.
<b>HTML Normalization</b>	This option removes non-printable characters, comment delimiters, HTML, hex, and decimal codes, and other HTML extras.

9. If you want evasion violations to be issued in case of problems while normalizing the header, select the **Normalization Violations** check box.

10. Click **Create**.

The HTTP Headers screen opens and lists the new header.

When ASM™ receives a request with the type of header you created, the system performs the special considerations indicated in the HTTP header.

## Configuring the maximum HTTP header length

You specify a maximum HTTP header length so that the system knows the acceptable maximum length for the HTTP header in an incoming request. This setting is useful primarily in preventing buffer overflow attacks.

1. On the Main tab, click **Security > Application Security > Security Policies**.

The Active Policies screen opens.

2. Click the name of the security policy you want to work on.

The Properties screen opens.

3. From the **Configuration** list, select **Advanced**.

4. For the **Maximum HTTP Header Length** setting, select one of the options.

Option	Description
<b>Any</b>	Specifies that the system accepts requests with HTTP headers of any length.
<b>Length with a value in bytes</b>	Specifies that the system accepts HTTP headers up to that length. The default maximum length is <b>8192</b> bytes.

5. Click **Save** to save your settings.

6. To put the security policy changes into effect immediately, click **Apply Policy**.



The system calculates and enforces the HTTP header length based on the sum of the length of the HTTP header name and value. Requests with headers that are longer than the maximum length cause an Illegal header length violation.

## Implementation Result

---

When Application Security Manager™ receives requests, the system checks the header to see if it matches any of the HTTP headers other than the wildcard header. If the request header matches one of the headers, the system performs the configured options for that header.

You can review violations that occur on the Manual Traffic Learning screen. HTTP header violations are listed under Evasion Techniques in the section Evasion Techniques Detected in Headers. You can examine the requests to see if they are legitimate or false positives. If they are false positives, you can consider turning off evasion violations or normalization for the header. You can drill down and view the headers causing violations. If a header violation is a false positive, you can also disable normalization from the Evasion Techniques Detected in Headers screen.

If signature violations occur in the header, the system suggests disabling the signature that cause the violation, or disabling the signature check for that header. If a header declared mandatory is missing, the system suggests disabling the violation or making the missing header non-mandatory.

If the Base64 violation occurs in the header, the system suggests disabling the violation or disabling the Base64 decoding for that header.



---

# Chapter

# 36

---

## Configuring How a Security Policy is Automatically Built

---

- *Overview: Configuring automatic policy build settings*

## Overview: Configuring automatic policy build settings

---

Application Security Manager™ completely configures the automated policy build settings according to the selections you make when you created the security policy. You can review the settings, and change them later if needed.

There are two levels of automated policy build settings: basic and advanced. The basic settings are sufficient for most installations, and require less work. The advanced level allows you to view and change all of the configuration settings if you want further control over security policy details. However, in most cases, you do not need to change the default values of these settings. F5 highly recommends that you use the default settings for automatic policy building.

### Task summary

*Configuring automatic policy building settings*

*Modifying security policy elements*

*Modifying security policy rules*

*Adding trusted IP addresses to a security policy*

*Learning from responses*

*Specifying when to add dynamic parameters*

*Collapsing entities in a security policy*

*Learning based on response codes*

*Limiting the maximum number of policy elements*

*Specifying the file types for wildcard URLs*

*Restoring default values for automatic policy building*

*Stopping and starting automatic policy building*

## Configuring automatic policy building settings

If you are an advanced user, you can review or adjust the settings that the system uses for automatic policy building. In most cases, you do not need to change the values of these settings.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings, for **Policy Type**, select the type that defines how you want the security policy built.

Option	Description
<b>Fundamental</b>	Provides security at a level that is appropriate for most organizations, creating a robust security policy, which is highly maintainable and quick to configure. This is the default setting.
<b>Enhanced</b>	Provides extra customization, creating a security policy with more granularity.
<b>Comprehensive</b>	Provides the highest level of customization, creating a security policy with more granularity, but it may take longer to configure.
<b>Vulnerability Assessment</b>	Specifies a security policy that is built using the recommendations from a vulnerability assessment tool. By default, the system does not add explicit

Option	Description
	entities, leaving that to the tool. (Only available if a vulnerability assessment tool is selected on the Vulnerability Assessments Settings screen.)
<b>Custom</b>	Provides the level of security that you specify when you adjust settings such as which security policy elements are included in the security policy. The policy type changes to <b>Custom</b> if you change any of the default settings for a policy type.

The selected security policy elements and other options on the screen change depending on the policy type you choose.

4. Leave the **Explicit Entities Learning** and **Parameter Level** settings at their default values.
5. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
6. For **Rules**, move the slider to change the thresholds of the rules for the security policy:

Option	Description
<b>Fast</b>	Builds a security policy using lower threshold values for the rules so they are likely to meet the thresholds more quickly; for example, this setting is useful for smaller web sites with less traffic. Selecting this value may create a less accurate security policy.
<b>Medium</b>	Builds a security policy based on greater threshold values for the rules. This is the default setting and is recommended for most sites.
<b>Slow</b>	Builds a security policy using even higher thresholds for the rules and takes longer to meet them; for example, this value is useful for large web sites with lots of traffic. Selecting this value may result in fewer false positives and create a more accurate security policy.

Changing this setting also changes the value of the **Chance of adding false entities to the policy** setting.

7. If you want to review or adjust additional advanced configuration settings, next to **Automatic Policy Building Settings**, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
8. Review the settings and modify them as needed.  
Refer to the online help and other tasks for details on each of the settings.
9. Click **Save** to save your settings.
10. To put the security policy changes into effect immediately, click **Apply Policy**.

By adjusting the automatic policy building settings, you change the way that Application Security Manager™ creates the security policy.

## About security policy elements

A *security policy element* specifies a part of the application that Application Security Manager™ (ASM) is protecting, and indicates what to include when building the security policy. Examples of policy elements are HTTP protocol compliance, file type lengths, parameter value lengths and name metacharacters, methods, header and cookie lengths, attack signatures, evasion technique violations, and so on. These elements included form the basis of the security policy that the automatic policy building process is creating.

Different policy types specify different sets of policy elements. The fundamental policy type includes the fewest number of policy elements, and the comprehensive type includes nearly all policy elements. When

traffic accesses the web application that the policy is protecting, ASM™ verifies details about the selected policy elements. For example, if HTTP Protocol Compliance is selected, ASM checks that the traffic is protocol-compliant. If attack signatures is selected, the security policy examines the traffic for patterns in the signatures. The same goes for the other policy elements included in the security policy.

### Modifying security policy elements

When you create a security policy, the policy includes security policy elements such as file types, URLs, parameters, evasion technique violations, and so on. These elements form the basis of the security policy that the automatic policy building process is creating. You can modify which security policy elements are included in the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the **Policy Elements** setting, for **Include the following Security Policy Elements**, select the security policy entities (or violations) that you want the Policy Builder to automatically configure when building the security policy.  
When you change the policy elements that are included in the security policy, the **Policy Type** changes to **Custom**.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The security policy now includes the policy elements that you selected. The system examines legitimate requests and responses from different sessions and different IP addresses, over a period of time. It then populates the security policy with the security policy elements it finds, and puts them in staging.

### About automatic policy building rules

During automatic policy building, the Policy Builder builds security policies in three stages. These stages each have separate sets of settings in the Rules area of the Settings screen. Rules in each stage determine when an element in the security policy moves from one stage to the next.

Some of the rules have different values depending on whether the traffic comes from a trusted or untrusted source. The system generally considers trusted traffic, and the policy elements it contains to be legitimate, and adds them to the policy more quickly than it does those in untrusted traffic.

You can adjust the values for the rules by changing the Policy Builder learning speed. Slow learning speed causes the system to create the policy by looking at more traffic, so the values in the rules are higher. Fast learning speed causes the system to build the policy from fewer requests, and the values you see in the rules are lower.

Advanced users can view and change the conditions under which the Policy Builder modifies the security policy during any of the three stages. Changing the values in any of the rules (to values not matching any of the default values) also changes the learning speed and chances of adding false entities settings to the **Custom** policy type (instead of Slow, Medium, and Fast).

## About automatic policy building stages

Automatic policy building has three stages:

### Accept as Legitimate (Loosen)

During this stage, the Policy Builder identifies legitimate application usage based on repeated behavior from sufficient different user sessions and IP addresses, over a period of time. The system updates the security policy accordingly. Based on wildcard matches, Policy Builder adds the legitimate policy entities (putting most into staging to learn their properties), and disables violations that are probably false positives.

For example, when the Policy Builder sees the same file type, URL, parameter, or cookie from enough different user sessions and IP addresses over time, then it adds the entity to the security policy.

### Stabilize (Tighten)

During this stage, the Policy Builder refines the security policy elements until the number of security policy changes stabilizes. For example, the Policy Builder enforces an entity type after it records a sufficient number of unique requests and sessions, for different IP addresses, over a sufficient length of time since the last time an explicit file type, URL, or parameter was added to the security policy.

Similarly, the Policy Builder enforces the entity's attributes (takes them out of staging) after it records a sufficient number of unique requests and sessions from different IP addresses, over a sufficient length of time for a particular file type, URL, parameter, or cookie.

When the traffic to the application no longer includes new elements, and the Policy Builder has enforced the policy elements, the security policy is considered stable and its progress reaches 100%.

### Track Site Changes

This stage occurs after the security policy is stable. If the **Track Site Changes** setting is enabled and the Policy Builder discovers changes to the web application, it logs the change (Site change detected) and temporarily loosens the security policy to make the necessary adjustments. When the Policy Builder stabilizes the added elements, it re-tightens the security policy.

Although it is not recommended, you can disable the **Track Site Changes** option. If you do, when the security policy progress reaches 100% stability, the system disables automatic policy building. The security policy is not updated unless you manually change it, or restart automatic policy building by re-enabling the **Track Site Changes** option.

## Modifying security policy rules

Automatic policy building rules specify how a security policy is built. When you create the security policy, values for the rules are set according to the policy type you select. Advanced users can view and modify the rules, for trusted and untrusted traffic, if your application has unique requirements. In most cases, you do not need to change the values of the rules.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.

4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

6. For the **Accept as Legitimate (Loosen)** rules, adjust the number of different sessions, different IP addresses, and the time spread after which the Policy Builder accepts and learns a security policy change from traffic.

In this stage of security policy building, the Policy Builder adds entities, configures attributes (such as lengths and meta characters), places entities in staging, and disables violations.

7. For the **Stabilize (Tighten)** rules, adjust the number of requests, the number of different sessions, different IP addresses, and the time spread before the Policy Builder stabilizes the security policy elements.

Stabilizing a security policy element usually means tightening it by deleting wildcard entities, removing entities from staging, and enforcing violations that did not occur.

8. For the **Track Site Changes** rules:

- a) The **Enable Track Site Changes** check box is selected by default. Keep it selected if you want the Policy Builder to quickly loosen the security policy if changes to the web application cause violations.
- b) Select which traffic you want the Policy Builder to use to loosen the security policy:

**From Trusted and Untrusted Traffic:** Specifies that the Policy Builder loosens the security policy based on all traffic. This is the default option.

**Only from Trusted Traffic:** Specifies that the Policy Builder loosens the security policy based only on traffic from trusted sources defined in the Trusted IP Addresses area on this screen.

- c) For untrusted and trusted traffic, adjust the number of different sessions and different IP addresses for which the system detects violations, over a period of time, after which the Policy Builder updates the security policy.

In this stage of security policy building, the Policy Builder adds wildcard entities, places entities in staging, and disables violations.

9. Click **Save** to save your settings.
10. To put the security policy changes into effect immediately, click **Apply Policy**.

The system now automatically builds the security policy with the adjusted security policy rules.

## Adding trusted IP addresses to a security policy

In a security policy, you can include a list of IP addresses that you want the system to consider safe or trusted.



1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the Trusted IP Addresses area, for **IP Addresses**, specify which IP addresses to consider safe:
  - To trust all IP addresses (for internal or test environments), select **All**.
  - To add specific IP addresses or networks, select **Address List**, type the IP address and netmask, then click **Add**. The IP address or network range is added to the list. Add as many trusted IP addresses as needed.
  - To delete IP addresses or networks from the list of trusted IP addresses, select the IP address in the list, then click **Delete**.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

Application Security Manager™ (ASM) processes traffic from trusted clients differently than traffic from untrusted clients. For clients with trusted IP addresses, the rules are configured so that ASM™ requires less traffic (by default, only 1 user session) to update the security policy with entity or other changes. It takes more traffic from untrusted clients to change the security policy (for example, if using the default values).

## Learning from responses

If you are using automatic policy building, you can have the system examine responses as well as requests for entities to include in the security policy. This is called learning from responses, and the system does this by default. You may want to learn from responses because a response might include more information about the web application than is found in the request. You can disable this setting if your application does not need to examine responses for entities to add to the security policy, or if the application does not use dynamic parameters.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. If you do not want the security policy to include elements found in responses when building the security policy, in the Options area, clear the **Learn from responses** check box.  
If the setting is not enabled, the Policy Builder learns from responses that come from valid requests (meaning those that do not generate violations).
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If you disabled the **Learn from responses** check box, the Policy Builder never adds to the security policy elements found in responses. If the check box is enabled, the Policy Builder adds elements found in responses to the security policy.

### Specifying when to add dynamic parameters

*Dynamic parameters* are those whose values can change, and are often linked to a user session. If you are using automatic policy building, you can specify the conditions under which the Policy Builder adds dynamic parameters to the security policy.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the General Policy Building Settings area, for the **Explicit Entities Learning** setting:
  - a) Set **Parameters** to either **Add All Entities** or **Selective**.
  - b) Set **URLs** or **File Types** to either **Add All Entities** or **Selective**.

The system can extract dynamic parameters from parameters, URLs, and file types.

6. In the General Policy Building Settings area, for the **Explicit Entities Learning** setting,
7. In the Options area, ensure that **Learn from responses** has **Enabled** selected.
8. For **Dynamic Parameters**, select one or more of the check boxes to specify the conditions under which the Policy Builder adds dynamic parameters to the security policy.

Option	Description
<b>All HIDDEN Fields</b>	Adds to the security policy all hidden form input parameters, seen in responses, as dynamic content value parameters.
<b>Using statistics - FORM parameters</b>	Adds parameters from forms as dynamic content value parameters.
<b>Using statistics - link parameters</b>	Adds parameters from links as dynamic content value parameters.
<b>Statistics: Configure parameters as dynamic if &lt;num&gt;...</b>	Specifies the number (<num>) of unique value sets that must be seen for a parameter before the system considers it a dynamic content value. The default value is 10.

9. Click **Save** to save your settings.
10. To put the security policy changes into effect immediately, click **Apply Policy**.

When the Application Security Manager™ receives a request that has an entity (for example, a file extension or URL) containing a dynamic parameter, the system collects the parameter value or name from web application's response to the request and adds it to the security policy.

## Collapsing entities in a security policy

When using automatic policy building, the system automatically simplifies your security policy by combining several similarly named explicit entities into wildcard entities. For example, multiple parameters beginning with `paramare` combined into `param*`. You can specify which entities should be collapsed and after how many occurrences.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the Options area, for **Collapse to one entity**, select or clear the check boxes for those entities you want the security policy to collapse.

Option	Description
<b>Collapse Parameters, Cookies and Content Profiles</b>	When selected, collapses many common parameters, cookies, and content profiles (parameter/URL) into one of each type. In the field, type the number of occurrences (2 or greater) the Policy Builder must detect before collapsing them to one entity.
<b>Collapse URLs</b>	When selected, collapses many common explicit URLs into one wildcard URL with a common prefix and suffix. The Policy Builder collapses URLs only in the same directory (with the same prefix path), and if they have the same file extension. For example, the system collapses the URLs <code>/aaa/x.php</code> , <code>/aaa/y.php</code> , and <code>/aaa/z.php</code> into <code>/aaa/*.php</code> . In the field, type the number of occurrences (2 or greater) the Policy Builder must detect before collapsing them to one entity, and type the minimum depth to collapse the URLs.

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The system collapses the entities selected unless the collapse would lead to a loss of security policy information.

## Learning based on response codes

When using automatic policy building, the system automatically learns from legitimate traffic including transactions that return response codes of 1xx, 2xx, and 3xx. These classes of codes are added by default to the policy building settings. You can change which response codes are listed, or add specific response codes, such as those used by the web application you are protecting.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.

3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the Options area, for **Learn from traffic with the following HTTP Response Status Codes**, type the response code you want to add (for example, add specific codes like 304 or a class of codes like 4xx), then click **Add**. Use these formats.

Response code	Description
1xx	All informational responses (the request was received; continuing to process it). Included by default.
2xx	All successful responses (the request was received, understood, accepted, and processed successfully). Included by default.
3xx	All redirection (the client needs to take additional action on the request). Included by default.
4xx	Server failed to fulfill the response as a result of client syntax or input errors.
5xx	All server error responses (the server failed to fulfill a request).
Specific codes such as 100, 306, 400, or 404	Refer to your web application or the Hypertext Transfer Protocol -- HTTP/1.1 specification (RFC-2616).

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

The Policy Builder extracts information for the security policy from traffic based on transactions that return the specified HTTP response status codes.

## Limiting the maximum number of policy elements

When using automatic policy building, the system has reasonable limits to the maximum number of file types, URLs, parameters, and cookies that can be added to the security policy. These limits work fine for most situations. You can adjust the limits if needed.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the Options area, for **Maximum Security Policy Elements**, adjust the maximum number of elements that the Policy Builder can add to the security policy.
  - **File Types** (the default value is 250)
  - **URLs** (the default is value 10000)
  - **Parameters** (the default value is 10000)
  - **Cookies** (the default value is 100)

6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If the Policy Builder reaches the specified limit, it stops adding that type of security policy element. If this happens, you may need to intervene.

- If the web site requires more than the maximum number of elements, you can increase the limits, or reconsider the type of the policy (you may not need to include all the elements explicitly).
- If the site includes a dynamic element that the Policy Builder cannot learn (such as dynamic sessions in URL or dynamically generated parameter names), either configure the security policy to include the element (for example, dynamic sessions in URL), or clear the element type. The Policy Builder should not be configured to learn that element type in such an environment.

## Specifying the file types for wildcard URLs

When using automatic policy building, for security policies that are tracking URLs (policy types other than fundamental), the system adds a wildcard URL instead of explicit URLs for commonly used file types. You can specify which file types are changed to wildcard URLs.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings area, for **Real Traffic Policy Builder**, select **Enabled** (if it is not already selected).  
The screen displays the automatic policy building settings.
4. From the **Automatic Policy Building Settings** list, select **Advanced**.  
The screen displays the advanced configuration details for policy building.
5. In the Options area, for **File Types for which wildcard URLs will be configured**, adjust the file types for which the Policy Builder creates a wildcard URL instead of adding an explicit URL.  
Common file types are included by default. Note that the setting is unavailable in policies that do not include URLs.
  - To add file types, in the **File Type** field, type the file extension and click **Add**.
  - To remove file types, select the file type and click **Delete**.
6. Click **Save** to save your settings.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

For the file types listed, the Policy Builder adds wildcards instead of explicit URLs when encountering them in web application traffic. Also, the wildcards are added to the policy as non-case sensitive; for example, .jpg URLs are added as \*.Jj][Pp][Gg] instead of image1.jpg, IMAGE2.JPG, and image3.jpg.

## Restoring default values for automatic policy building

If you have adjusted the settings for automatic policy building and want to replace those values, you can restore them to the system default values.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the General Policy Building Settings area, for **Policy Type**, select the type of policy for which you want the default values.

---

***Tip:** You can also click the **Restore Defaults** button at the bottom of the Settings screen. If you do, the system refreshes and displays the default values for the Fundamental policy type.*

---

The screen refreshes and displays the default values for the policy type you selected.

4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

## Stopping and starting automatic policy building

You can start the Real Traffic Policy Builder<sup>®</sup>, which automatically builds a security policy. When you use automatic policy building, the Policy Builder can update the security policy as needed, adding elements, for example, if changes occur on the application web site. You can manually stop automatic policy building at any time, such as when the security policy stabilizes, and you think the web application will not change for a while. However, you do not need to stop Policy Builder because the system does this automatically.

For security policies that were created using one of the manual methods or imported from an earlier release, you can start automatic policy building so the system builds the security policy for you. By examining the traffic going to the application, the Policy Builder can add various web site entities to the security policy in order to enhance it.

1. On the Main tab, click **Security > Application Security > Policy Building > Settings**.  
The Settings screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Automatic Policy Building Settings, for **Real Traffic Policy Builder**, clear the **Enabled** check box to stop automatic policy building, and select **Enabled** to start it.
4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

If you stopped automatic policy building, the security policy remains the same unless you manually add to it. If you started automatic policy building, the Policy Builder automatically discovers and populates the security policy with the policy elements (such as file types, URLs, parameters, and cookies). As the Policy Builder runs, you see status messages in the identification and messages area at the top of the screen. You can monitor general policy building progress, and see the number of elements that are included in the policy.

---

# Chapter

# 37

---

## Configuring General ASM System Options

---

- *Adjusting system preferences*
  - *Incorporating external antivirus protection*
  - *Creating user accounts for application security*
  - *Validating regular expressions*
-

## Adjusting system preferences

---

You can change the default user interface and system preferences for the Application Security Manager™ (ASM), and configure fields displayed in the Request List of the Reporting screen.

1. On the Main tab, click **Security > Options > Application Security > Preferences**.
2. In the GUI Preferences area, for **Records Per Screen**, type the number of entries to display (between 1-100). (The default value is 20.)

This setting determines the maximum number of security policies, file types, URLs, parameters, flows, headers, and XML and JSON profiles to display in lists throughout ASM™.

3. For **Titles Tooltip Settings**, select an option for how to display tooltips.

Option	Description
<b>Do not show tooltips</b>	Never display tooltips or icons.
<b>Show tooltip icons</b>	Display an icon if a tooltip is available for a setting, show the tooltip when you move the cursor over the icon.
<b>Show tooltips on title mouseover</b>	Do not display an icon, but show the tooltip when you move the cursor over the setting name. This is the default setting.

4. For **Default Configuration Level**, select **Advanced** to display all possible settings, or **Basic** to display only the essential settings, on screens with that option.

The default is **Basic**.

5. For **Apply Policy Confirmation Message**, you can specify whether to display a popup message asking if you want to perform the **Apply Policy** operation each time you change a security policy.

6. In the Request List GUI Preferences area, for **Records Per Requests Screen**, type the number of requests to display (between 1-1000). (The default value is 500.)

This setting determines the maximum number of requests that appear in any Requests List containing details about any incident, event correlation, or attack.

7. For **Request List Columns**, specify what information you want to display on the Requests screen, and the order in which to display it.

8. For **Request List Size**, specify the number of requests (small, medium, or large) the system displays before adding a scroll bar.

This setting determines how much space the requests list takes up on the Request screen.

9. If you are using the Cenzic service to mitigate web application vulnerabilities, in the **Cenzic ARC Server address field**, type the IP address of a local Cenzic ARC server.

If you use the Cenzic Cloud service, do not provide an address for this setting.

10. If you are using a high-availability configuration, for the **Sync** setting, select the **Recommend Sync when Policy is not applied** check box to display the Sync Recommended message at the top of the screen when you change a security policy, to remind you to perform a ConfigSync with the peer device.

11. For the **Logging** setting, select the **Write all changes to Syslog** check box to record all changes made to security policies in the Syslog (/var/log/asm).

---

**Note:** The system continues to log system data regardless of whether you enable policy change logging.

---

12. Click **Save** to save your settings.

The adjusted settings are used throughout the ASM system.



## Incorporating external antivirus protection

---

Before you can incorporate antivirus protection, you need to have an ICAP server setup in your network.

You can configure the Application Security Manager™ (ASM) to connect with an Internet Content Adaptation Protocol (ICAP) server to check requests for viruses. (ASM was tested with McAfee VirusScan, Trend Micro InterScan, Symantec Protection Engine, and Kaspersky Antivirus products, and may work with others.) You can also set up antivirus checking for HTTP file uploads and SOAP web service requests.

1. On the Main tab, click **Security > Options > Application Security > Integrated Services > Anti-Virus Protection**.

The Anti-Virus Protection screen opens.

2. For the **Server Host Name/IP Address** setting, type the fully qualified domain name of the ICAP server, or its IP address.

---

***Note:** If you specify the host name, you must first configure a DNS server by selecting **System > Configuration > Device > DNS**.*

---

3. For **Server Port Number**, type the port number of the ICAP server.

The default value is 1344.

4. If you want to perform virus checking even if it may slow down the web application, select the **Guarantee Enforcement** check box.

5. Click **Save** to save your settings.

6. On the Main tab, click **Security > Application Security > Blocking**.

The Settings screen opens.

7. For each security policy, configure, as needed, the blocking policy for antivirus protection.

- a) Ensure that the **Current edited policy** is the one for which you want antivirus protection.
- b) In the Negative Security Violations area (near the bottom of the Violations list), for the **Virus Detected** violation, select either or both of the **Alarm** and **Block** check boxes.
- c) Click **Save** to save the settings.

8. For each security policy, configure, as needed, antivirus scanning for file uploads or SOAP attachments.

---

***Note:** Performing antivirus checks on file uploads may slow down file transfers.*

---

- a) On the Main tab, click **Security > Application Security > Integrated Services > Anti-Virus Protection**.

- b) Ensure that the **Current edited policy** is the one that may include HTTP file uploads or SOAP requests.

- c) To have the external ICAP server inspect file uploads for viruses before releasing the content to the web server, select the **Inspect file uploads within HTTP requests** check box.

- d) To perform anti-virus scanning on SOAP attachments, if the security policy includes one or more XML profiles, in the XML Profiles setting, move the profiles from the **Antivirus Protection Disabled** list to the **Antivirus Protection Enabled** list. Alternately, click **Create** to quickly add a new XML profile, with default settings, to the configuration. You can then add the new profile to the **Antivirus Protection Enabled** list.

- e) Click **Save** to save the settings.

9. To put the security policy changes into effect immediately, click **Apply Policy**.

If the `Virus Detected` violation is set to Alarm or Block in the security policy, the system sends requests with file uploads to an external ICAP server for inspection. The ICAP server examines the requests for viruses and, if the ICAP server detects a virus, it notifies ASM, which then issues the `Virus Detected` violation.

If antivirus checking for HTTP file uploads and SOAP web service requests is configured, the system checks the file uploads and SOAP requests before releasing content to the web server.

## Creating user accounts for application security

---

User accounts on the BIG-IP® system are assigned a user role that specifies the authorization level for that account. While an account with the user role of Administrator can access and configure everything on the system, you can further specialize administrative accounts for application security.

1. On the Main tab, click **System > Users**.
2. Click **Create**.  
The New User properties screen opens.
3. From the **Role** list, select a user role for security policy editing.
  - To limit security policy editing to a specific administrative partition, select **Application Security Editor**.
  - To allow security policy editing on all partitions, select **Application Security Administrator**.
4. If you selected **Application Security Editor**, then from the **Partition Access** list, select the partition in which to allow the account to create security policies.  
You can select a single partition name or **All**.
5. From the **Terminal Access** list, select a level of console access.
6. Click **Finished**.

The BIG-IP system now contains a new user account for administering application security.

- Application Security Editors have permission to view and configure most parts of the Application Security Manager™ on specified partitions.
- Application Security Administrators have permission to view and configure all parts of the Application Security Manager, on all partitions. With respect to application security objects, this role is equivalent to the Administrator role.

## Validating regular expressions

---

The RegExp Validator is a system tool designed to help you validate your regular expression syntax. You can type a regular expression in the RegExp Validator, provide a test string pattern, and let the tool analyze the data. The tool is included with Application Security Manager™.

1. Click **Security > Options > Application Security > RegExp Validator**
2. From the **RegExp Type** list, select either **PCRE** or **RE2** (recommended) as the RegExp engine.

---

**Tip:** As of BIG-IP® version 11.2, the system's regular expression library and signatures changed from PCRE to RE2 to increase performance and lower false positives. The system still supports the PCRE library for systems that have user-defined signatures configured in PCRE.

---

3. Specify how you want the validator to work:
  - In the **RegExp** field, type the regular expression you want to validate.
  - Or in the **RegExp** field, type the regular expression to use to verify a test string, and then in the **Test String** field, type the string.
4. Click the **Validate** button.

The screen shows the results of the validation.

The validation result indicates whether the regular expression is valid or not. The first RegExp match displays the result of the verification check (if specified) including if there are matches or not.



---

# Chapter

# 38

---

## Working with Violations

---

- *About violations*
  - *Overview: Creating user-defined violations*
-

## About violations

Application Security Manager™ includes built-in violations. Violations occur when some aspect of a request or response does not comply with the security policy. You can configure the blocking settings for any violation in a security policy. When a violation occurs, the system can learn, alarm, or block a request (blocking is only available when the enforcement mode is set to blocking).

Violation names displayed in the Violation List are the names used as reference in the iRule `ASM::custom_violation` command and the `ASM::violation name` command. The violation name is also used in API, iControl®, and TMAPI code.

You can also create user-defined violations if you need them on your system.

## Types of violations

This table describes the types of violations that can occur. On the **Security > Options > Application Security > Advanced Configuration > Violations List**, you can get details about the violations (and change the severity) by clicking the violation. You also can view descriptions of each violation by clicking the information icon to the left of each violation in the Violations List on the Application Security Blocking Settings screen.

Violation Type	Description
RFC violations	Occur when the format of an HTTP request violates the HTTP RFCs. RFC documents are general specifications that summarize Internet and networking standards. RFCs, as they are commonly known, are published by the International Engineering Task Force (IETF). For more information on RFCs, see <a href="http://www.ietf.org/rfc">http://www.ietf.org/rfc</a> .
Access violations	Occur when an HTTP request tries to gain access to an area of a web application, and the system detects a reference to one or more entities that are not allowed (or are specifically disallowed) in the security policy.
Length violations	Occur when an HTTP request contains an entity that exceeds the length setting that is defined in the security policy.
Input violations	Occur when an HTTP request includes a parameter or header that contains data or information that does not match, or comply with, the security policy. Input violations most often occur when the security policy contains defined user-input parameters.
Cookie violations	Occur when the cookie values in the HTTP request do not comply with the security policy. Cookie violations may indicate malicious attempts to hijack private information.
Negative security violations	Occur when an incoming request contains a string pattern that matches an attack signature in one of the security policy's attack signature sets, or when a response contains exposed user data, for example, a credit card number.
Other violations	Refers to user-defined violations. If your system includes user-defined violations, they occur when instructed by the iRules® that were developed to activate them.

## Viewing descriptions of violations

You can view detailed descriptions of each violation to learn what causes that type of violation, and the type of security risks it could be related to.

1. On the Main tab, click **Security > Application Security > Blocking > .**  
The Blocking Settings screen opens.
2. Click the info icon preceding the violation you are interested in learning about.  
A popup screen shows the violation description, risks, and examples, if available.
3. To view violations that have occurred for the current edited security policy, on the Main tab, click **Security > Application Security > Policy Building > Manual Traffic Learning.**  
The Manual Traffic Learning screen opens and lists any violations that the system found against the security policy. For most violations you can click the violation link to view learning suggestions which you can accept in the security policy, and additional information about the violations.

You can view descriptions for all the violations that can occur and see how the blocking settings are configured for the security policy currently being edited.

## Changing severity levels of violations

You can change the severity levels of security policy violations for all application security events that occur system-wide. If violations occur, the system displays the events and severity level on the Security Alerts screen and logs the message in the Syslog. This is an optional task that you need to do only if you want to change the default severity levels of violations.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Violations List.**
2. Review the list of built-in violations and severities.
3. To change the severity of a violation, click the violation name.  
The Built-In Violation Details popup screen opens where you can view information about the violation and the current severity level.
4. From the **Severity** list, select the severity level you want to use for the violation.  
The available severities are: **Emergency, Alert, CriticalError, Warning, Notice, and Informational.**
5. Click **Update.**

The new severity level is shown in the violations list. If the changed violation occurs, the system uses the new severity level. Changes made to the event severity levels for security policy violations apply globally to all security policies on the Application Security Manager™.

## Overview: Creating user-defined violations

---

You can create user-defined violations so that Application Security Manager™ (ASM) can detect new threats or protect against application-specific vulnerabilities. After creating the violation, you can then configure the system to alert or block requests that cause it. You need to write iRules® to detect the customized attack conditions and issue the violation. In the security policy properties, you then need to activate iRule events.

The iRules are written using application security events and commands. For detailed information on iRules, see the F5 Networks DevCentral web site, <http://devcentral.f5.com>.

## Creating user-defined violations

You can create up to 28 user-defined violations for situations not covered by the built-in violations. User-defined violations are helpful for mitigating zero-day attacks, and to protect your web application

against specific vulnerabilities not yet protected by Application Security Manager™ (ASM). You can write iRules® to detect new attack conditions and issue the violation.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Violations List**.
2. Click **User-Defined Violations**.
3. Click **Create**.  
The Create New User-Defined Violation popup screen opens.
4. In the **Violation Name** field, type a name for the violation using alphanumeric characters and underscores only.  
The recommended format is an uppercase alphanumeric string starting with `VIOLATION`, having words separated by underscores; for example, `VIOLATION_SLOW_POST`.  
The name is used as reference in the `ASM::custom_violation` and `ASM::violation name` iRule commands, and in APIs, iControl®, and TMAPI.
5. In the **Violation Title** field, type descriptive text for the violation. It is typically similar to the name but in a more friendly format.  
This text appears wherever the violation is referred to, including configuration of blocking settings, the proxy log, and reports.
6. From the **Type** list, select the category of the violation, or leave it set to **Unspecified**.
7. From the **Severity** list, select the severity level of the violation.  
The available severities are: **Informational**, **Notice**, **Warning**, **Error**, **Critical**, **Alert**, and **Emergency**.
8. From the **Attack Type** list, select one of the existing attack types.  
If none of the specific attack types is appropriate, select **Other Application Attacks** or **Other Application Activity**.  
The attack type is shown when you click the Info icon next to the violation name on the Blocking Settings screen.
9. In the **Description** field, type a description of the violation.  
The description is shown when you click the Info icon next to the violation name on the Blocking Settings screen.
10. Click **Create**.

The custom violation is added to the list of user-defined violations. It is also listed under other violations on the Blocking Settings screen for each security policy on the system. You can edit all attributes of a user-defined violation except the name.

You should now set up the blocking settings (Alarm and Block only) for the user-defined violation enabling the violation for specific security policies. You also need to write iRules that issue the custom violations based on the conditions available using the `ASM::raise violation_name [violation_details]` command. ASM™ blocks requests according to the violation's blocking settings and operation mode, and logs details in the Requests log. For detailed information on iRules, see the F5 Networks DevCentral web site, <http://devcentral.f5.com>.

## Enabling user-defined violations

Application security iRule events must be activated in the security policy to enable user-defined violations.

You enable user-defined violations by configuring the Alarm and Block flags, or blocking actions, for user-defined violations. The blocking actions (along with the enforcement mode) determine how the system processes requests that trigger the violation.

1. On the Main tab, click **Security > Application Security > Blocking**.



The Settings screen opens.

2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Adjust the **Enforcement Mode** setting if needed.
  - To block traffic that causes violations, select **Blocking**.
  - To not block traffic even if it causes violations (allowing you to make sure that legitimate traffic would not be blocked), select **Transparent**.

You can only configure the Block flag if the enforcement mode is set to **Blocking**.

4. For each user-defined violation (listed in Other Violations), set the Alarm and Block settings.

Option	Description
<b>Alarm</b>	If selected, the system records requests that trigger the violation in the Charts screen, the system log ( <code>/var/log/asm</code> ), and possibly in local or remote logs (depending on the settings of the logging profile).
<b>Block</b>	If selected (and the enforcement mode is set to <b>Blocking</b> ), the system blocks requests that trigger the violation.

5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

Once you have an iRule that determines when to issue the user-defined violation (and the enforcement mode is set to blocking), the specified alarm or block action occurs.

## Sample iRules for user-defined violations

You can write iRules® to activate user-defined violations that you created and enabled in a security policy.

---

**Note:** The examples in this topic may not work depending on your configuration. Some examples include multiple ways of setting them up, or may require additional code. For more information about iRules, refer to [devcentral.f5.com](http://devcentral.f5.com).

---

The following application security iRule issues a user-defined violation called `VIOLATION_NOT_BROWSER` if the request was not sent using Internet Explorer, Mozilla Firefox, Safari, Chrome, or Opera.

```
when ASM_REQUEST_DONE {
    if { {not [HTTP::header "User Agent"]match_regexp
"(IE|Mozilla|Safari|Chrome|Opera)" } and {[length [IP::reputation
[ASM::client_ip]]] > 0} }
        { ASM::raise VIOLATION_NOT_BROWSER
        }
}
```

The following application security iRule issues a user-defined violation when there are too many ASM™ violations.

```
when ASM_REQUEST_DONE {
    if {[ASM::violation count] > 3 and [ASM::severity] eq "Error"} {
        ASM::raise VIOLATION_TOO_MANY_VIOLATIONS
    }
}
```

```
}
```

This iRule uses an ASM event to log in /var/log/ltm all available information about the request that was enforced by ASM.

```
when ASM_REQUEST_DONE {
#Get and log info as it was done before v11.5.
log local0. "====Previous style: Start===="
set x [ASM::violation_data]
for {set i 0} {$i<7} {incr i} {
log local0. [lindex $x $i]
}
log local0. "====Previous style: Done===="
#Using the new command (V11.5 or later) log all available information about

#the enforced request.
log local0. "====New style Start===="
#display ASM policy which enforced request
log local0. "ASM Policy: [ASM::policy];"
#log some part of request using iRule commands Method, URI,
log local0. "Request string: [HTTP::method] [HTTP::uri];"
#log payload from request using ASM::payload command and HTTP::payload or
#log Query string.
log local0. "Payload ASM payload [ASM::payload];"
log local0. "Payload HTTP payload [HTTP::payload];"
log local0. "Query String [HTTP::query];"
# log information about request processed by ASM policy
#support ID
log local0. "SupportID: [ASM::support_id];"
#request status for current moment
log local0. "Request Status: [ASM::status];"
#Severity of attack detected in request
log local0. "Severity: [ASM::severity];"
#client IP
log local0. "ClientIP: [ASM::client_ip];"
# number of violations ASM detected in the request
log local0. "Number Violations: [ASM::violation count]"
# log all ASM violation iControl names detected in the request
log local0. "Violations Names: [ASM::violation names];"
# log all Attack types detected in request
log local0. "Attack Types: [ASM::violation attack types];"
# log all violation details detected in the request.
set details [ASM::violation details]
if { [llength $details]>0 } {
set i 0
foreach pair $details {
if { [lindex $pair 0] contains "viol_name" } {
#Log violation Name
log local0. "Violation Number: $i; $pair"
incr i
} else {
#log other details for violation
set key [lindex $pair 0]
set value [lindex $pair 1]
log local0. "-----$pair-----"
if {$key contains "parameter_data.name" || $key contains
"parameter_data.value"} {
#decode parameter name from base64.
if {[catch {b64decode $value} decoded_value] == 0}{
log local0. "$key ---- $decoded_value"
} else {
log local0. "$key ---- $value"
}
} else {
#log other details

```

```

log local0. "$key ---- $value"
}
}
}
}
#Log all violation details as one string. Could be cut.
log local0. "Violation details: [ASM::violation details];"
log local0. "=====New style Done=====
}

```

When raising user-defined violations within an ASM iRule, you can specify additional violation details to include in the log as shown in the following example. You need to create the violations in ASM.

```

#Raise with lappend

#Using new event

when ASM_REQUEST_DONE {
  # log support id for enforced request
  log local0. "SupportID: [ASM::support_id];"
  #log request status
  log local0. "Request Status: [ASM::status];"
  #log severity of request
  log local0. "Severity: [ASM::severity];"
  #log Client IP
  log local0. "ClientIP: [ASM::client_ip];"
  #log number of different violations detected in request
  log local0. "Number Violations: [ASM::violation count]"
  #log iControl violation names
  log local0. "Violations Names: [ASM::violation names];"

  # Raise 3 user-defined violations without any details
  ASM::raise violation1
  ASM::raise violation2
  ASM::raise violation3
  # Raise a user-defined violation with custom details
  ASM::raise violation4 {{violation.name violation4} {violation.type test1}
{violation.type test2}}

  #log the new number and names of detected violations.
  #ASM logs detected and raised violations.
  #log the number of different violations detected in the request
  log local0. "Number of Violations: [ASM::violation count]"
  #log iControl violation names
  log local0. "Violations Names: [ASM::violation names];"

  #using new command lappend, create violation details and raise
  #another user-defined violation

  set x {}
  lappend $x {key1 value1}
  lappend $x {key1 value2}

  ASM::raise violation5 $x
}

#using old event

when ASM_REQUEST_VIOLATION {

  # log the support ID for the enforced request
  log local0. "SupportID: [ASM::support_id];"
  #log request status
  log local0. "Request Status: [ASM::status];"
  #log the severity of the request

```

```

log local0. "Severity: [ASM::severity];"
#log Client IP
log local0. "ClientIP: [ASM::client_ip];"
#log the number of different violations detected in the request
log local0. "Number of Violations: [ASM::violation count]"
#log iControl violation names
log local0. "Violation Names: [ASM::violation names];"

# Raise 3 user-defined violations without any details
ASM::raise violation1
ASM::raise violation2
ASM::raise violation3
# Raise a user-defined violation with custom details
ASM::raise violation4 {{violation.name violation4} {violation.type test1}
{violation.type test2}}

#log the new number and names of detected and raised violations.
#log the number of different violations detected in the request
log local0. "Number of Violations: [ASM::violation count]"
#log iControl violation names
log local0. "Violations Names: [ASM::violation names];"

#using the new command lappend, create violation details
#and raise another user-defined violation

set x {}
lappend $x {key1 value1}
lappend $x {key1 value2}

ASM::raise violation5 $x
}

```

The following iRule shows how to use request blocking with a blocking response page.

```

#RequestBlockingWithBRP

#Use new ASM iRule commands in old ASM iRule event.

when ASM_REQUEST_BLOCKING {
  log local0. "=====OLD style start=====
  set x [ASM::violation_data]
  for {set i 0} {$i<7} {incr i} {
    log local0. [lindex $x $i]
  }
  log local0. "=====OLD style Done=====

  log local0. "=====New style Start=====
  log local0. "SupportID: [ASM::support_id];"
  log local0. "Request Status: [ASM::status];"
  log local0. "Severity: [ASM::severity];"
  log local0. "ClientIP: [ASM::client_ip];"
  log local0. "Number Violations: [ASM::violation count]"
  log local0. "Violations Names: [ASM::violation names];"
  log local0. "Attack Types: [ASM::violation attack_types];"
  log local0. "Violation details: [ASM::violation details];"

  #check if illegal parameter violation was detected
  #then change Blocking response page.
  if {[ASM::violation names] contains "VIOLATION_PARAM")} {
    log local0. "VIOLATION_PARAM detected, let's customized reject page"
    HTTP::header remove Content-Length
    HTTP::header insert header_1 value_1
    set response "<html><head></body><html>"
    ASM::payload replace 0 [ASM::payload length] ""
    ASM::payload replace 0 0 $response
  }
}

```

```

}

}

```

The following example iRule shows how to use all ASM iRule events and commands.

```

#allRulesforUDV

#Example with all ASM iRule events and commands

when HTTP_REQUEST {
    # get LTM policy matched rule and chosen ASM security policy
    set policy [POLICY::names matched]
    log local0. "Matched policy [POLICY::names matched]"
    log local0. "Matched rule in policy [POLICY::rules matched]"
    log local0. "ASM policy [ASM::policy] enforcing"
}

#New ASM iRule event introduced in 11.5

when ASM_REQUEST_DONE {
    log local0. "====Old iRule Data===="
    log local0. "Compatibility Mode is triggered"
    set x [ASM::violation_data]
    for {set i 0} {$i<7} {incr i} {
        log local0. [lindex $x $i]
    }
    log local0. "====Old iRule Data Done===="

    log local0. "====New iRule Data===="
    log local0. "SupportID: [ASM::support_id];"
    log local0. "Request Status: [ASM::status];"
    log local0. "Severity: [ASM::severity];"
    log local0. "ClientIP: [ASM::client_ip];"
    log local0. "Number Violations: [ASM::violation count]"
    log local0. "Violations Names: [ASM::violation names];"
    log local0. "Attack Types: [ASM::violation attack_types];"
    log local0. "Violation details: [ASM::violation details];"
    log local0. "====New iRule Data Done===="
}

# Old ASM iRule events which were before 11.5.0

when ASM_REQUEST_VIOLATION {
    log local0. "====Old iRule Data===="
    log local0. "Compatibility Mode is triggered"
    set x [ASM::violation_data]
    for {set i 0} {$i<7} {incr i} {
        log local0. [lindex $x $i]
    }
    log local0. "====Old iRule Data Done===="
    log local0. "====New iRule Data===="
    log local0. "SupportID: [ASM::support_id];"
    log local0. "Request Status: [ASM::status];"
    log local0. "Severity: [ASM::severity];"
    log local0. "ClientIP: [ASM::client_ip];"
    log local0. "Number Violations: [ASM::violation count]"
    log local0. "Violations Names: [ASM::violation names];"
    log local0. "Attack Types: [ASM::violation attack_types];"
    log local0. "Violation details: [ASM::violation details];"
    log local0. "====New iRule Data Done===="
}

when ASM_RESPONSE_VIOLATION {
    log local0. "====Old iRule Data===="
    log local0. "Compatibility Mode is triggered"
    set x [ASM::violation_data]

```

```

for {set i 0} {$i<7} {incr i} {
    log local0. [lindex $x $i]
}
log local0. "=====Old iRule Data Done======"
log local0. "=====New iRule Data======"
log local0. "SupportID: [ASM::support_id];"
log local0. "Request Status: [ASM::status];"
log local0. "Severity: [ASM::severity];"
log local0. "ClientIP: [ASM::client_ip];"
log local0. "Number Violations: [ASM::violation count]"
log local0. "Violations Names: [ASM::violation names];"
log local0. "Attack Types: [ASM::violation attack_types];"
log local0. "Violation details: [ASM::violation details];"
log local0. "=====New iRule Data Done======"
}

when ASM_REQUEST_BLOCKING {
    log local0. "=====Old iRule Data======"
    log local0. "Compatibility Mode is triggered"
    set x [ASM::violation_data]
    for {set i 0} {$i<7} {incr i} {
        log local0. [lindex $x $i]
    }
    log local0. "=====Old iRule Data Done======"
    log local0. "=====New iRule Data======"
    log local0. "SupportID: [ASM::support_id];"
    log local0. "Request Status: [ASM::status];"
    log local0. "Severity: [ASM::severity];"
    log local0. "ClientIP: [ASM::client_ip];"
    log local0. "Number Violations: [ASM::violation count]"
    log local0. "Violations Names: [ASM::violation names];"
    log local0. "Attack Types: [ASM::violation attack_types];"
    log local0. "Violation details: [ASM::violation details];"
    log local0. "=====New iRule Data Done======"
}

```

## Deleting user-defined violations

You can delete user-defined violations if you no longer need them.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Violations List**.
2. Click **User-Defined Violations**.
3. Select the user-defined violation that you want to delete.
4. Click **Delete**.

The deleted violation is moved to the list of Historical Violations.

The deleted user-defined violation and details about it remain on the system in the Historical Violations list. From there, you can restore previously removed user-defined violations if you need to.

## Exporting and importing user-defined violations

You can export user-defined violations to back them up, or for importing onto another Application Security Manager™ system.

1. On the Main tab, click **Security > Options > Application Security > Advanced Configuration > Violations List**.

2. Click **User-Defined Violations**.
3. Select the user-defined violations to export.
4. Click **Export**.  
The violations are saved in an XML file with the name, date, and time stamp:  
`user_defined_violations_YYYY-mm-dd_hh-mm.xml`.
5. To import the user-defined violations onto another system, navigate to the User-Defined Violations List on the other system, click **Import**, and specify the exported file.





---

# Chapter

# 39

---

## Working with Attack Signatures

---

- *About attack signatures*
  - *Overview: Creating and assigning attack signature sets*
  - *Overview: Managing the attack signature pool*
  - *Overview: Creating user-defined attack signatures*
-

## About attack signatures

*Attack signatures* are rules or patterns that identify attacks or classes of attacks on a web application and its components. A security policy compares patterns in the attack signatures against the contents of requests and responses looking for potential attacks. Some of the signatures are designed to protect specific operating systems, web servers, databases, frameworks or applications. Additionally, you can assign some signatures to protect certain alpha-numeric user-input parameters.

All of the attack signatures on the Application Security Manager™ are stored in the attack signature pool.

You can develop customized (user-defined) attack signatures, however, this is an advanced feature only needed for specific cases. User-defined signatures are stored in the attack signatures pool along with the system-supplied signatures. You can import and export user-defined attack signatures.

## About attack signature staging

When you first activate a security policy, the system puts the attack signatures into staging (if staging is enabled for the security policy). *Staging* means that the system applies the attack signatures to the web application traffic, but does not apply the blocking policy action to requests that trigger those attack signatures. The default staging period is seven days.

Whenever you add or change signatures in assigned sets, those are also put into staging. You also have the option of putting updated signatures in staging.

Placing new and updated attack signatures in staging helps to reduce the number of violations triggered by false-positive matches. When signatures match attack patterns during the staging period, the system generates learning suggestions. From Manual Traffic Learning, if you see that an attack signature violation has occurred, you can view these attack signatures from the Attack Signature Detected screen.

Upon evaluation, if the signature is a false-positive, you can disable the signature, and the system no longer applies that signature to traffic for the corresponding web application. Alternately, if the detected signature match is legitimate, you can enable the corresponding attack signature. Note that enabling the signature removes it from staging, and puts the blocking policy into effect.

## Types of attacks that attack signatures detect

Attack signatures in a security policy are compared with requests or responses to attempt to identify classes of attacks, for example, SQL injection, command injection, cross-site scripting, and directory traversal. The following table describes the types of attacks that attack signatures can detect. You can filter lists of attack signatures by these attack types.

Attack Type	Description
Abuse of Functionality	Uses a web site's own features and functionality to consume, defraud, or circumvent the application's access control mechanisms.
Authentication/Authorization Attacks	Targets a web site's method of validating the identity of a user, service or application. Authorization attacks target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action.
Buffer Overflow	Alters the flow on an application by overwriting parts of memory. An attacker could trigger a buffer overflow by sending a large amount of unexpected data to a vulnerable component of the web server.

Attack Type	Description
Command Execution	Occurs when an attacker manipulates the data in a user-input field, by submitting commands that could alter the web page content or web application by running a shell command on a remote server to reveal sensitive data—for example, a list of users on a server.
Cross-site Scripting (XSS)	Forces a web site to echo attacker-supplied executable code, which loads in a user's browser.
Denial of Service	Overwhelms system resources to prevent a web site from serving normal user activity.
Detection Evasion	Attempts to disguise or hide an attack to avoid detection by an attack signature.
Directory Indexing	Involves a web server function that lists all of the files within a requested directory if the normal base file is not present.
HTTP Response Splitting	Pertains to an attempt to deliver a malicious response payload to an application user.
Information Leakage	Occurs when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system.
LDAP Injection	Concerns an attempt to exploit web sites that construct LDAP statements from user-supplied input.
Non-browser Client	Relates to an attempt by automated client access to obtain sensitive information. HTML comments, error messages, source code, or accessible files may contain sensitive information.
Other Application Attacks	Represents attacks that do not fit into the more explicit attack classifications, including email injection, HTTP header injection, attempts to access local files, potential worm attacks, CDATA injection, and session fixation.
Path Traversal	Forces access to files, directories, and commands that potentially reside outside the web document root directory.
Predictable Resource Location	Attempts to uncover hidden web site content and functionality.
Remote File Include	Occurs as a result of unclassified application attacks such as when applications use parameters to pass URLs between pages.
Server Side Code Injection	Attempts to exploit the server and allow an attacker to send code to a web application, which the web server runs locally.
SQL-Injection	Attempts to exploit web sites that construct SQL statements from user-supplied input.
Trojan/Backdoor/Spyware	Tries to circumvent a web server's or web application's built-in security by masking the attack within a legitimate communication. For example, an attacker may include an attack in an email or Microsoft® Word document, and when a user opens the email or document, the attack starts.
Vulnerability Scan	Uses an automated security program to probe a web application for software vulnerabilities.
XPath Injection	Occurs when an attempt is made to inject XPath queries into the vulnerable web application.

## Attack signature properties

The following table describes the attack signature properties, listed on the Attack Signature Properties screen, that you can view for more information about the signatures in the pool.

Property	Description
<b>Name</b>	Displays the signature name.
<b>ID</b>	Specifies the signature number automatically provided by the system.
<b>Signature Type</b>	Specifies whether the signatures are for all traffic, for requests only, or for responses only.
<b>Apply To</b>	Indicates whether the rule inspects the client's request (Request) or the server's response (Response).
<b>Attack Type</b>	Forces a web site to echo attacker-supplied executable code, which loads in a user's browser.
<b>Systems</b>	Displays which systems (for example, web applications, web server databases, or application frameworks) the signature or set protects.
<b>Accuracy</b>	Indicates the ability of the attack signature to identify the attack including susceptibility to false-positive alarms: <ul style="list-style-type: none"> <li>• <b>Low</b>: Indicates a high likelihood of false positives.</li> <li>• <b>Medium</b>: Indicates some likelihood of false positives.</li> <li>• <b>High</b>: Indicates a low likelihood of false positives.</li> </ul>
<b>Risk</b>	Indicates the level of potential damage this attack might cause if it is successful: <ul style="list-style-type: none"> <li>• <b>Low</b>: Indicates the attack does not cause direct damage or reveal highly sensitive data.</li> <li>• <b>Medium</b>: Indicates the attack may reveal sensitive data or cause moderate damage.</li> <li>• <b>High</b>: Indicates the attack may cause a full system compromise.</li> </ul>
<b>User-defined</b>	Indicates whether this signature is a system supplied rule ( <b>No</b> ) or was defined by a user ( <b>Yes</b> ).
<b>Revision</b>	Indicates the version of the attack signature.
<b>Last Updated</b>	Indicates the date when the attack signature was most recently updated.
<b>Documentation</b>	Indicates whether the system provides documentation explaining this attack signature ( <b>View</b> ) or not ( <b>N/A</b> ). Click the <b>View</b> link to display the available documentation.
<b>References</b>	Displays a clickable link to an external web site explaining this attack signature, or displays ( <b>N/A</b> ) if no link is available.

## Overview: Creating and assigning attack signature sets

You can create attack signature sets in two ways: by using a filter or by manually selecting the signatures to include.

Filter-based signature sets are based solely on criteria you define in the signatures filter. The advantage to filter-based signature sets is that you can focus on the criteria that define the attack signatures you are

interested in, rather than trying to manage a specific list of attack signatures. Another advantage to filter-based sets is that when you update the attack signatures database, the system also updates any signature sets affected by the update.

When manually creating a signature set, you must select each of the signatures to include from the signature pool. To simplify using this method, you can still filter the signatures first, then select the individual signatures from the filtered list.

Once you create the attack signature sets that you need, you can assign them to security policies.

## About attack signature sets

An *attack signature set* is a group of attack signatures. Rather than applying individual attack signatures to a security policy, you can apply one or more attack signature sets. The Application Security Manager™ ships with several system-supplied signature sets.

Each security policy has its own attack signature set assignments. By default, a generic signature set is assigned to new security policies. You can assign additional signature sets to the security policy. Certain sets are more applicable to certain types of applications or types of attack. The sets are named logically so you can tell which ones to choose. Additionally, you can create your own attack signature sets.

## List of attack signature sets

The following table lists the attack signature sets included with Application Security Manager™.

Signature Set	Contains These Signatures
All Response Signatures	All signatures in the attack signature pool that can review responses.
All Signatures	All attack signatures in the attack signature pool.
Generic Detection Signatures	Signatures that target well-known or common web and application attacks.
High Accuracy Signatures	Signatures with a high level of accuracy that produce few false positives when identifying attacks.
Low Accuracy Signatures	Signatures that may result in more false positives when identifying attacks.
Medium Accuracy Signatures	Signatures with a medium level of accuracy when identifying attacks.
OWA Signatures	Signatures that target attacks against the Microsoft Outlook Web Access (OWA) application.
WebSphere Signatures	Signatures that target attacks on many computing platforms that are integrated using WebSphere including general database, Microsoft Windows, IIS, Microsoft SQL Server, Apache, Oracle, Unix/Linux, IBM DB2, PostgreSQL, and XML.
Command Execution Signatures	Signatures involving attacks perpetrated by executing commands.
Cross Site Scripting Signatures	Signatures that target attacks caused by cross-site scripting techniques which force a user to execute unwanted actions in a web application where the user is currently authenticated.
HTTP Response Splitting Signatures	Signatures targeting attacks that take advantage of responses for which input values have not been sanitized
OS Command Injection Signatures	Signatures targeting attacks that attempt to run system level commands through a vulnerable application.

Signature Set	Contains These Signatures
Path Traversal Signatures	Signatures targeting attacks that attempt to access files and directories that are stored outside the web root folder.
SQL Injection Signatures	Signatures targeting attacks that attempt to insert (inject) a SQL query using the input data from a client to an application.
Server Side Code Injection Signatures	Signatures that target code injection attacks on the server side.
XPath Injection Signatures	Signatures targeting attacks that attempt to gain access to data structures or bypass permissions or access when a web site uses user-supplied information to construct XPath queries for XML data.

## Creating a set of attack signatures

When you create an attack signature set, you can include the attack signatures that are relevant to your specific systems and applications.

- On the Main tab, click **Security > Options > Application Security > Attack Signatures > Attack Signatures Sets**.  
The Attack Signature Sets screen opens and displays the attack signature sets on the system.
- Click **Create**.  
The Create New Signature Set screen opens.
- In the **Name** field, type a unique name for the signature set.  
Do not use system-supplied attack signature names when you create a user-defined attack signature. Although the system does not prohibit duplicate attack signature names, future attack-signature updates may fail because of name conflicts.
- For the **Type** setting, select the appropriate option:

Option	Use
<b>Filter-based</b>	To create a signature set by using a filter only.
<b>Manual</b>	To create a signature set by selecting signatures from the signature pool, and optionally a filter as well.
- For the **Default Blocking Actions** setting, select the blocking actions you want the system to enforce for the signature set when you associate it with a new security policy.

---

***Note:** The **Learn**, **Alarm**, and **Block** actions take effect only when you assign this signature set to a new security policy. If this signature set is already assigned to an existing security policy, these settings have no affect.*

---

- If you want the system to automatically include this signature set in any new security policies you create, enable the **Assign To Policy By Default** setting.
- In the Signatures Filter area, select the filter options to narrow the scope of the signatures to include in the new signature set.

Filter Option	What It Does
<b>Signature ID</b>	Manual only. Leave blank unless you want to include a signature with a specific ID number in the signature set.
<b>Signature Type</b>	Select to include signatures that apply to all traffic, requests only, or responses only.

Filter Option	What It Does
<b>Apply To</b>	Manual only. Select whether to include in the set all signatures or only signatures that apply to alpha-numeric user-input parameters defined in the security policy, XML documents, or JSON data.
<b>Attack Type</b>	Select the threat classifications for which to include signatures in the set.
<b>Systems</b>	Select the systems (for example web applications, web server databases, and application frameworks) that you want protected by the set.
<b>Accuracy</b>	Select the level of accuracy you want for the signatures in the set. Higher accuracy results in fewer false positives.
<b>Risk</b>	Select the level of potential damage for attacks protected by the signatures in the set.
<b>User-defined</b>	Specify whether to include signatures based on who created them (the user, system, or both).
<b>Update Date</b>	Specify whether to include signatures in the set based on the date the signature was changed.

8. In the **Signatures** setting,

- If creating the set using the filter only, review the signatures list that the filter settings generate to make sure it is correct.
- If creating the set manually, move the signatures to include in the set from the **Available Signatures** list into the **Assigned Signatures** list.

9. Click **Create** to create the new signature set.

The new signature set is added to the bottom of the list of attack signature sets that are available on the system. You can assign attack signature sets to security policies. The signature set is also available to be applied when creating new security policies.

If, in the future, you no longer need a user-defined signature set, you can delete it. When you delete a signature set, you are not deleting the attack signatures that make up the set, just the set.

## Assigning signature sets to a security policy

Each security policy enforces one or more attack signature sets. When creating a security policy, you select the attack signature sets to include. You can assign additional attack signature sets to the security policy. For each attack signature set, you can also specify the blocking policy, which is what you want to happen if an attack signature in the set discovers a potential attack.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures Configuration**.  
The Attack Signatures Configuration screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. If you want signatures to be put into staging before being enforced, select the **Signature Staging** check box.

Staging means that the system applies the attack signatures to the web application traffic, but does not apply the blocking policy action to requests that trigger those attack signatures. The default staging period is seven days.

4. For the **Attack Signature Sets Assignment** setting, in the **Available Signature Sets** list, select the attack signature sets that you want to assign to the security policy and move them into the **Assigned Signature Sets** list.
5. In the **Attack Signature Sets Assignment** setting, for each signature set in the **Available Signature Sets** list, configure the blocking policy: select or clear the **Learn**, **Alarm**, and **Block** check boxes.

---

***Note:** You can enable or disable the **Block** action only when the enforcement mode of the security policy is set to blocking.*

---

6. To specify the file types for which to enforce response attack signatures:
  - a) For **Check Response Settings**, select the **Apply Response Signatures** check box.  
You need at least one file type in the security policy to use this setting.
  - b) Click **Create** if you need to create file types.
  - c) Use the Move buttons to adjust the file types for which to apply or not apply response signatures.
7. Click **Save** to save your settings.
8. To configure headers that you do not want attack signatures to examine, in the **Excluded Headers** setting, click the **Configure HTTP Headers** link.  
By specifying excluded headers, you can keep header-based attack signatures enabled in the security policy but prevent false positives produced if those signatures match legitimate header names and values found in requests to the protected web application.  
The HTTP Headers screen opens where you can create the custom, cookie, or referrer headers to exclude.
9. To put the security policy changes into effect immediately, click **Apply Policy**.

The signature sets are assigned to the security policy, and the blocking policy applies to all of the signatures in the signature set.

What happens depends on the blocking policy options you selected. If you selected **Learn**, the security policy learns all requests that match enabled signatures included in the signature set, and displays the request data on the Traffic Learning Attack Signature Detected screen. If **Alarm** is selected, the security policy logs the request data if a request matches a signature in the signature set. If you selected **Block**, and the enforcement mode is **Blocking**, the security policy blocks all requests that match a signature included in the signature set, and sends the client a support ID number.

## Viewing the signature sets in a security policy

You can review the attack signature sets that are associated with a security policy.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures Configuration**.  
The Attack Signatures Configuration screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the **Attack Signature Sets Assignment** setting, you can review the signature sets that are associated with the security policy, as well as the blocking policy actions for them.
4. Click a signature set name to review its properties and the attack signatures in that set.



## Viewing the attack signatures in a security policy

You can review all of the attack signatures in a security policy, including their current blocking policy and their state.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures List**.  
The Attack Signatures List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Policy Attack Signatures area, you can review the signatures that are associated with the security policy, the signature ID, the blocking policy actions, and whether or not they are enabled.
4. Click a signature name to view its properties on the Policy Attack Signature Properties screen, and get more information about the signature.  
Here you can also enable or disable the signature for the active security policy. Clicking on the signature name again displays additional properties.
5. Click **Cancel** (if you made no changes) or **Update** (if you changed the **Enable** setting) to return to the Attack Signatures List screen.

## Enabling or disabling a specific attack signature

You can enable or disable specific attack signatures in a security policy, one at a time. For example, if one of the attack signatures in a selected set causes false positives in your environment, you can disable it.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures List**.  
The Attack Signatures List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. In the Policy Attack Signatures area, you can review the signatures that are associated with the security policy, the signature ID, the blocking policy actions, and whether or not they are enabled.
4. Click the name of the signature you want to enable or disable.  
The Policy Attack Signature Properties screen opens.
5. Select or clear the **Enable** check box to enable or disable the signature for the active policy.
6. Click **Update** (if you changed the **Enable** setting) to return to the Attack Signatures List screen.
7. To put the security policy changes into effect immediately, click **Apply Policy**.

If disabled, the signature does not cause a violation even if patterns match the traffic. If enabled, if traffic matches the pattern in the signature, an *Attack Signature Detected* violation occurs, and traffic is handled in accordance with the signature blocking policy. Note that enabling a signature that is in staging removes it from staging, and puts the blocking policy into effect.

## Enabling or disabling staging for attack signatures

For each security policy, you can enable or disable staging in general for attack signatures. By default, attack signature staging is enabled.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures Configuration**.  
The Attack Signatures Configuration screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. For the **Signature Staging** setting, specify your staging preference:
  - To enforce staging on new or changed signatures, select the **Enabled** check box.
  - To disable signature staging, clear the **Enabled** check box.
4. Click **Save** to save your settings.
5. To put the security policy changes into effect immediately, click **Apply Policy**.

When signature staging is enabled, the system places all new or updated signatures in staging for the number of days specified in the enforcement readiness period. The system does not enforce signatures that are in staging, even if it detects a violation. Instead, the system records the request information.

If staging is disabled, attack signatures are not put into staging before they are enforced, regardless of the staging configuration for each individual signature. The system enforces the **Learn**, **Alarm**, and **Block** settings for each signature immediately. (If traffic causes an attack signature violation, it is blocked only if the security policy's enforcement mode is Blocking.)

## Overriding attack signatures based on content

Before you can perform this task, you must have previously created a JSON, XML, or Google Web Toolkit (GWT) content profile.

You can have the system perform attack signature checks based on the content of a request as defined in content profiles (XML, JSON, or GWT). In addition, you can override the security policy settings so that the system avoids checking specific attack signatures in particular content.

1. On the Main tab, point to **Security > Application Security > Content Profiles** and click a content profile type (**XML**, **JSON**, or **GWT**).
2. In the profiles list, click the name of the content profile for which you want to specify attack signature checks.  
The profile properties screen opens.
3. Click the Attack Signatures tab.
4. Make sure that the **Check attack signatures** check box is selected if you want the system to perform attack signature checking against the content profile.
5. In the **Global Security Policy Settings** list, review the attack signatures that are assigned to the security policy, and which are enabled and enforced in the content profile.
6. From the **Global Security Policy Settings** list, move any attack signatures that you want to override for this content profile into the **Overridden Security Policy Settings** list.

---

**Tip:** In the **Overridden Security Policy Settings** list, click an attack signature link to display details about the attack signature.

---

7. Click **Update** to update the content profile.
8. To put the security policy changes into effect immediately, click **Apply Policy**.

Attack signatures in the overridden settings list are set to **Disabled**. The system does not issue a violation even when part of a request matches an overridden attack signature.

## Overview: Managing the attack signature pool

---

The system includes an *attack signatures pool* from which you can select signatures to include in any security policy. The pool includes the system-supplied attack signatures, which are the attack signatures that are shipped with the Application Security Manager™, and any user-defined attack signatures.

F5 develops new attack signatures to handle the latest attacks, and you can schedule periodic updates to the attack signatures pool, or update it manually. You can have the system send you an email when an update to the attack signature pool is available.

## Updating the attack signature pool

Before you can update the attack signature pool, you must have a valid service agreement with F5 Networks, and a service check date within 18 months of the update request. The Application Security Manager™ must also have external network access for the update process to work.

You can schedule automatic updates to the attack signature pool, or update the pool manually.

1. On the Main tab, click **Security > Options > Application Security > Attack Signatures**. The Attack Signatures Update screen opens.
2. For the **Update Mode** setting, specify the type of update:
  - To schedule automatic updates, select **Scheduled**, and then from **Update Interval**, select how often to perform an update.
  - For manual updates or systems without Internet access, select **Manual**, and then select the **Delivery Mode**: select **Automatic** to get the update directly from F5, or **Manual** to specify a file from F5 containing the updates (specify the file in the **Upload File** setting).
3. To put into staging signatures that are changed by the update, enable the **Place updated signatures in staging** setting.

---

***Note:** The system places any new signatures added by the update into staging regardless of this setting.*

---

After the update, the system puts changed signatures into staging for the **Enforcement Readiness Period** (specified in Policy properties).

4. If you want the system to automatically apply the updated signatures to the security policy after installing attack signature updates, make sure the **Auto Apply New Signatures Configuration After Update** setting is enabled.
5. Click the **Save Settings** button to preserve any changes you may have made to the configuration.
6. If performing manual updates, click the **Update Signatures** button when you want to start the update process.

If you scheduled automatic updates, the system connects to the F5 server periodically to see if there are any updates, and if there are, it downloads and applies available updates. When updated either manually or automatically, the attack signature pool includes any new signatures and updates to any existing attack signatures that were revised. The new signatures are placed in staging.

The Application Security Manager records details about the most recent update activity, and displays this information on the Attack Signatures Update screen. There you can review the last update time as well as the readme file that pertains to the update.

### Getting email about signature updates

To receive the attack signature update notifications, you must have a valid service contract, and an AskF5™ account.

If you want to receive notification from F5 Networks about attack signature updates available for download, you can sign up for the Security email distribution list.

1. To subscribe to the Security email distribution list, send a blank email to `security-subscribe@lists.f5.com` from the email address you want to subscribe with.
2. Unsubscribe by sending a blank email to `security-unsubscribe@lists.f5.com`.

F5 adds your email address to the Security email distribution list. You will be sent an email message whenever attack signature updates are available.

### Viewing the attack signature pool and signature details

The attack signatures pool contains all of the attack signatures that are on the system. You can view the attack signature pool contents, and see details about each signature.

1. On the Main tab, click **Security > Application Security > Attack Signatures > Attack Signatures List**.  
The Attack Signatures List screen opens.
2. If you are looking for specific signatures, use the filter to display the ones you are interested in.  
You can use one of the predefined filters, or click **Show Filter Details** to develop a custom filter.
3. In the Signature Name column, click the signature for which you want to view information.  
The Policy Attack Signature Properties screen opens and shows details about that signature.
4. For the **Signature Name** setting, click the signature name link.  
The Attack Signature Properties screen opens and shows additional details about that signature.
5. In the **Documentation** setting (if available), click **View** to see additional information that applies to the selected attack signature.  
The Documentation for Attack Signature screen opens in a new browser window, and displays the additional related documentation.
6. On the Attack Signature Properties screen, click the **References** setting link to an external web site that describes the attack signature.  
If no additional documentation is available, you see **N/A**.
7. When you finish reviewing the details, close the additional documentation screens and click **Cancel** to close the Attack Signature Properties screens.

### Overview: Creating user-defined attack signatures

---

*User-defined attack signatures* are those that your organization creates and adds to the attack signature pool. User-defined attack signatures must adhere to a specific rule syntax. They are never updated by F5 Networks. All user-defined signatures are carried forward as-is when the system is updated to a new software version.

You can develop user-defined attack signatures if needed for specific purposes in your environment. You can also export and import user-defined signatures to and from other Application Security Manager™ systems.

## Creating a user-defined attack signature

You can create a user-defined attack signature using the F5 attack signature syntax.

1. On the Main tab, click **Security > Options > Application Security > Attack Signatures > Attack Signature List**.

The Attack Signature List screen opens.

2. Click **Create**.

The Create New Attack Signature screen opens.

3. In the **Name** field, type a unique name for the attack signature.

---

***Note:** If you create a user-defined attack signature with the same name as a system-supplied attack signature, subsequent signature updates may fail.*

---

4. In the **Description** field, type an optional description of the signature.
5. To include this signature in all active security policies, make sure that **Auto Apply New Signatures Configuration After Edit** is enabled.
6. For the **Signature Type** setting, select **Request** or **Response** to determine whether the new signature applies to client requests or server responses.
7. For the **Systems** setting, select from the **Available Systems list** any systems to which the new signature applies, and move them to the **Assigned Systems list**.
8. For the **Attack Type** setting, select the type of threat that the new signature protects against.
9. For the **Rule** setting, type a rule according to the syntax guidelines to specify the content of the signature.
10. For the **Accuracy** setting, select an accuracy level.  
The accuracy level indicates the ability of the attack signature to identify the attack, including susceptibility to false-positive alarms.
11. For the **Risk** setting, select a risk level.  
The risk level indicates the level of potential damage this attack may cause, if it were successful.
12. Click **Create** to create the new attack signature.

The new attack signature is added to the attack signature pool. If you left the **Auto Apply New Signatures Configuration After Edit** check box selected, the system applies this signature to all active security policies.

## Importing user-defined attack signatures

Before you can import user-defined signatures, you must first export them in XML file format.

You can import user-defined attack signatures from other Application Security Manager™ systems. Both systems must be running the same software version.

1. On the Main tab, click **Security > Options > Application Security > Attack Signatures > Attack Signature List**.  
The Attack Signature List screen opens.
2. Click **Import**.  
The Import Attack Signatures screen opens.
3. In the **Choose File** field, specify the path to the XML file that contains the exported user-defined attack signature.
4. To place in staging any signatures that are updated as a result of the import, select the **Place updated signatures in staging** check box.

---

***Note:** The system places all new signatures added by the update into staging regardless of this setting.*

---

After the import, the system puts updated signatures into staging for the Enforcement Readiness Period (specified in Policy properties).

5. To include this signature in all active security policies, make sure that **Auto Apply New Signatures Configuration After Import** is enabled.
6. Click **Import**.

The system imports the user-defined signature, and issues either a success message or a failed message. If the import was not successful, make any required changes to the XML file, and then try to import the file again.

## Exporting user-defined attack signatures

You can export all user-defined attack signatures from one Application Security Manager™ system for use on another system. Both systems must be running the same software version.

1. On the Main tab, click **Security > Options > Application Security > Attack Signatures > Attack Signature List**.  
The Attack Signature List screen opens.
2. Click **Export**.  
The web browser opens a file download screen.
3. Save the file in a convenient location.  
Application Security Manager uses a file name with this format:

sigfile\_<date>\_<time>.xml

The system exports all user-defined attack signatures to the XML file.

## About attack signatures in XML format

The XML file format is the only accepted import format for attack signatures. Following is an example of the XML format used when saving user-defined attack signatures for import onto another system.

```
<?xml version="1.0" encoding="utf-8"?>
<signatures export_version="11.X.X">
  <sig id="300000000">
    <rev num="1">
      <sig_name>Unique signature name</sig_name>
      <rule>msg:"Signature Name"; content:"foo";</rule>
      <last_update>2011-04-15 13:37:17</last_update>
      <apply_to>Request</apply_to>
      <risk>3</risk>
      <accuracy>2</accuracy>
      <doc>Any additional descriptive text</doc>
      <attack_type>Cross Site Scripting (XSS)</attack_type>
      <systems>
        <system_name>IIS</system_name>
        <system_name>Microsoft Windows</system_name>
      </systems>
    </rev>
  </sig>
</signatures>
```

---

**Warning:** The `sig_name` attribute uniquely identifies a user-defined attack signature. Therefore, when you import an attack signature XML file, if there are any signatures in the XML file whose `sig_name` attribute matches that of any existing user-defined signatures, the system overwrites the existing definition with the imported definition.

---





---

# Chapter

# 40

---

## Maintaining Security Policies

---

- *Overview: Activating and deactivating security policies*
- *Overview: Importing and exporting security policies*
- *Overview: Comparing security policies*
- *Overview: Merging security policies*

### Overview: Activating and deactivating security policies

---

When you use the Deployment wizard to create a security policy, it is created as an *active security policy*. You can have up to 249 active security policies on a BIG-IP® system. You can view the list of active security policies in Application Security Manager™ (ASM). The policy that you are currently working on is selected in the list, and on many of the ASM™ screens, it is specified as the current edited policy.

To be actively securing traffic, a security policy should be associated with a virtual server and a local traffic policy. When you create a security policy that uses an existing or new virtual server, the policy is automatically associated with a virtual server and a default local traffic policy. You can edit the local traffic policy, but then it becomes a custom local traffic policy. You can also create a security policy that is not associated with a virtual server, and it is listed in the active security policies.

If you are no longer using a security policy or if you want to delete it, you must deactivate the policy first. You deactivate a security policy from the list of active policies. However, you cannot deactivate a security policy that is associated with a virtual server and a custom (not default) local traffic policy. You need to remove all mention of the security policy from the local traffic policy and virtual server before you can deactivate the security policy.

Once the security policy is deactivated and moved to the list of inactive security policies, you can select it and delete it.

### Deactivating security policies

If you no longer want to use a security policy, you can deactivate it, and if you want to delete a security policy, you must first deactivate it. Deactivating a security policy makes it inactive.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Select the security policy you want to deactivate.
3. Click **Deactivate**, and then click **OK** when prompted to confirm your action.

If a custom local traffic policy refers to the security policy, the security policy is not deactivated. You need to first remove mention of the security policy in the associated local traffic policy rules.

If a default local traffic policy is associated with the security policy, the system disassociates the local traffic policy first, then deactivates the security policy. The system moves the security policy to the Inactive Security Policies list, and permanently deletes all of the request log entries generated by the deactivated security policy.

### Activating security policies

If you want to resume using an inactive security policy, you can activate it and re-associate it with a virtual server and local traffic policy.

1. On the Main tab, click **Security > Application Security > Security Policies > Inactive Policies**.  
The Inactive Policies screen opens showing security policies that were deactivated or imported from another system (as an inactive policy).
2. Select the security policy you want to activate.
3. Click **Activate**.  
The Activate Policy screen opens.

4. For **Activation Type**, specify whether to associate a virtual server with the security policy.
  - To activate the security policy using the virtual server from another active security policy, click **Replace policy associated with virtual server**. For **Replaced Policy**, select the name of the security policy you want to replace.
  - To wait until later to associate a virtual server with the security policy, click **Do not associate with virtual server**.
5. Click **Activate**.

The system moves the security policy to the Active Security Policies list. If you associated the security policy with a virtual server, application security is enabled on the virtual server and the system creates a default local traffic policy. The security policy you activated becomes the current active security policy, and the old security policy moves to the Inactive Security Policies list.

If you did not associate a virtual server with the security policy, the security policy is unusable because no traffic can go through it. As a result, it is meaningless to run the Policy Builder on this type of security policy. You will need to manually associate it with a virtual server (in which case, the system automatically creates a default local traffic policy) in order for the security policy to handle traffic. You can also manually associate a custom local traffic policy with a security policy.

## Deleting security policies

Before you can delete a security policy, you must deactivate it first.

If you no longer want to use a security policy, you can delete it.

1. On the Main tab, click **Security > Application Security > Security Policies > Inactive Policies**. The Inactive Policies screen opens.
2. Select the security policy you want to delete.
3. Click **Delete**, and then click **OK** when prompted to confirm your action. The system permanently removes the security policy from the system.

## Overview: Importing and exporting security policies

---

You can export or import security policies from one Application Security Manager™ (ASM) system to another.

You can export a security policy as a binary archive file or as a readable XML file. For example, you might want to export a security policy protecting one web application to use it as a baseline policy for another similar web application. You might want to export a security policy to archive it on a remote system before upgrading the system software, to create a backup copy, to replace an existing policy, or to merge with another security policy.

You can import a security policy that was previously exported from another ASM™ system. When you import a security policy, you can import it as an inactive security policy or so that it replaces an existing security policy. If you replace an existing policy, the replaced policy is automatically archived with the inactive security policies.

### About security policy export formats

Application Security Manager™ can export security policies in binary or XML format. The XML or archive file includes the partition name, the name of the security policy, and the date and time it was exported. For example, a policy called `finance` in the `Common` partition is exported to a file called `Common_finance__2014-04-28_12-10-00__source.device` with either a `.plc` (binary) or `.xml` extension. The time used in the file name is the policy version timestamp (which includes the source hostname where the policy was last modified, the time modified, and the policy name).

An exported security policy includes any user-defined attack signature sets that are in use by the policy, but not the actual signatures. Therefore, it is a good idea to make sure that the attack signatures and user-defined signatures are the same on the two systems.

If you save the policy as an XML file, you can open it to view the configured settings of the security policy in a human readable format.

In addition when exporting to XML, you can save the security policy in a compact format, which results in a smaller XML file. The compact XML format does not include information about the staging state of attack signatures. Also, information about the following items is only included if it was changed from the default values:

- Meta-character sets
- Learn, Alarm, and Block settings for violations
- Response pages
- IP address intelligence Alarm and Block settings

### Exporting security policies

You can export a security policy and save it in a file. The exported security policy can be used as backup, or you can import it onto another system.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. In the Active Security Policies list, select the security policy that you want to export, then click **Export**.

---

***Note:** You can also export security policies from the Inactive Policies list using the same method.*

---

The Select Export Method popup screen opens.

3. Select an export method.
  - To save the security policy as an XML file, select **Export security policy in XML format**. To reduce the size of the XML file, select the **Compact format** check box.
  - To save the security policy as a policy archive file (`.plc` file), select **Binary export of the security policy**.
  - If the security policy integrates with a vulnerability assessment tool, select the **Include Vulnerability Assessment configuration and data** check box.
4. Click **Export**.  
The system exports the security policy in the format you specified.

The exported security policy includes any user-defined signature sets that are in the policy, but not the user-defined signatures themselves. Optionally, you can export user-defined signatures from the Attack Signature List (to see the list, go to **Security > Options > Application Security > Attack Signatures > Attack Signatures List**).

## Importing security policies

Before you import a security policy from another system, make sure that the attack signatures and user-defined signatures are the same on both systems. You also need access to the exported policy file.

You can import a security policy that was previously exported from another Application Security Manager™ system.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click **Import**.  
The Import Security Policy screen opens.
3. Use the **Choose File** setting to navigate to the previously exported security policy.  
The exported security policy can be in XML (regular or compact) or binary (.plc) format.  
The system shows the name of the policy you plan to import and the policy encoding.
4. For the **Import Target** setting, select how to import the security policy.
  - To place the uploaded policy into the list of inactive policies for later use, select **Inactive Security Policies List**.
  - To replace the currently active policy with the security policy you are importing, select **Replaced Policy**.
5. Click **Import**.  
The system imports the security policy and displays a success status message when the operation is complete.

If you replaced an existing policy, the imported security policy completely overwrites the existing security policy. Also, the imported policy is then associated with the virtual server and local traffic policy that was previously associated with the policy you replaced. The replaced policy is automatically archived with the inactive security policies.

If you imported a security policy to the list of inactive policies, it does not protect any application. You have to activate the inactive policy and associate it with a virtual server before it can protect an application.

## Overview: Comparing security policies

---

Application Security Manager™ has a Policy Diff feature that lets you compare two security policies, view the differences between them, and copy the settings from one policy to the other. You can use the comparison for auditing purposes, to make two policies act similarly, or to simply view the differences between two security policies. The Policy Diff feature is particularly useful for comparing a security policy in staging and a production version. You can compare active security policies (with or without Policy Builder running), inactive security policies, and exported security policies. When you import security policies that were exported from another system, they are placed in the inactive policies list.

You need to have a user role on the BIG-IP® system of Administrator or Web Application Security Editor to use Policy Diff to compare security policies.

## Comparing security policies

Before you can compare security policies, the two policies must be on the same BIG-IP system, or accessible from the system you are using (such as imported policies). They must also have the same language encoding, the same protocol independence (**Differentiate between HTTP and HTTPS URLs**) configuration, and the same case sensitivity configuration. You can compare policies even if they are running Policy Builder, but because they are constantly changing, the comparison is done on copies of the policies to avoid corrupting them.

---

***Note:** Only users with a role of Administrator, Application Security Administrator, or Application Security Editor can use Policy Diff to compare security policies.*

---

You can compare two security policies to review the differences between them. While the two security policies are being compared, the system prevents other users from saving changes to them.

1. On the Main tab, click **Security > Application Security > Security Policies > Policy Diff**.
2. From the **First Policy** and **Second Policy** lists, select the security policies you want to compare or merge, or click **Browse** to search your computer for an exported security policy.  
The two security policies you are comparing can be active, inactive, policies imported in binary or XML format, or a combination of both.
3. If you plan to merge security policy attributes, it is a good idea to safeguard the original security policy. In the **Working Mode** field, select how you want to work.

Option	Description
<b>Work on Original</b>	Incorporate changes to one (or both) of the original security policies depending on the merge options you select without making a copy of it.
<b>Make a Copy</b>	Make a copy of the security policy into which you are incorporating changes.
<b>Work on Copy</b>	Work on a copy of the original security policy. First, a copy is made, then incorporate possible changes on the original policies. If comparing one or more policies with Policy Builder enabled, this option is automatically selected (and the other options become unavailable).

4. Click the **Calculate Differences** button to compare the two security policies.

---

***Note:** The system does not compare navigation parameters. They are ignored and do not appear in the results.*

---

The Policy Differences Summary lists the number of differences for each entity type.

5. Click any row in the Policy Differences Summary to view the differing entities with details about the conflicting attributes.  
The system displays a list of the differing entities and shows details about each entity's conflicting attributes.
6. Review the differences between the two policies and determine whether or not you want to merge attributes from one policy to the other.

## Overview: Merging security policies

---

Application Security Manager™ has a policy merge option to combine two security policies. In the merge process, the system compares, and then merges, specific features from one security policy to another.

The merge mechanism is lenient when merging security policies. The system resolves any conflicts that occur by using the more open settings in the target security policy. When the merge is complete, the system shows the results of the merge process.

You can perform the merge in two ways:

- Automatically merge missing entities changing one policy or both policies.
- Manually merge specific differing entities from one security policy to another.

## Merging security policies

Only users with a role of Administrator, Application Security Administrator, or Application Security Editor can use Policy Diff to merge security policies.

If you have two security policies with entities and attributes that you want to combine into one policy, you can merge the two policies. For example, you can merge a security policy that you built offline into a security policy that is on a production system. You can merge two security policies automatically, or by reviewing the specific differences between them. You can perform the merge in two ways:

- Automatically merge missing entities changing one policy or both policies.
- Manually merge specific differing entities from one security policy to another.

1. On the Main tab, click **Security > Application Security**.

The Active Policies screen opens.

2. In the Security Policies area, click the **Merge** button.

The Policy Diff screen opens.

3. From the **First Policy** and **Second Policy** lists, select the security policies you want to compare or merge, or click **Browse** to search your computer for an exported security policy.

The two security policies you are comparing can be active, inactive, policies imported in binary or XML format, or a combination of both.

4. If you plan to merge security policy attributes, it is a good idea to safeguard the original security policy. In the **Working Mode** field, select how you want to work.

Option	Description
<b>Work on Original</b>	Incorporate changes to one (or both) of the original security policies depending on the merge options you select without making a copy of it.
<b>Make a Copy</b>	Make a copy of the security policy into which you are incorporating changes.
<b>Work on Copy</b>	Work on a copy of the original security policy. First, a copy is made, then incorporate possible changes on the original policies. If comparing one or more policies with Policy Builder enabled, this option is automatically selected (and the other options become unavailable).

5. Click the **Calculate Differences** button to compare the two security policies.

---

**Note:** The system does not compare navigation parameters. They are ignored and do not appear in the results.

---

The Policy Differences Summary lists the number of differences for each entity type.

6. Decide whether you want to examine each difference in detail, or have the system resolve the differences.
  - To merge the security policies automatically, skip to step 9.
  - To examine the differences before merging, proceed to step 7.

7. Click any row in the Policy Differences Summary to view the differing entities with details about the conflicting attributes.

The system displays a list of the differing entities and shows details about each entity's conflicting attributes.

8. To merge the two security policies manually, address each difference.
  - a) For each differing entity and attribute, move the ones you want into the merged security policy, or click **Ignore** to leave them different.

---

***Tip:** Click the **Details** link to see very specific information about the entity in each security policy.*

---

- b) Click **Save** to save the changes you make.

When you click Save, the changed section is removed from the screen because it was resolved. Other differing entities that still need to be resolved are still shown.

9. To automatically merge the differences between the two security policies, click **Auto Merge**.

An Auto Merge popup screen opens.

10. In the **Handle missing entities** setting, specify how you want the system to treat entities that exist in one security policy but not the other.

By default, both check boxes are selected; the auto-merge process adds unique entities from each policy into the policy from which they are missing.

- To move missing entities from the second policy to the first, select **Add all unique entities from <second policy> to <first policy>**.
- To move missing entities from the first policy to the second, select **Add all unique entities from <first policy> to <second policy>**.
- If you do not want to merge missing entities, leave both check boxes blank.

11. In the **Handle common entities for <first policy> and <second policy>**, specify how you want the system to treat entities that have conflicting attributes.

- To make no changes to either policy when entities are different, select **Leave unchanged**.
- To use the differing entities from the first policy and move them to the second, select **Accept all from <first policy> to <second policy>**.
- To use the differing entities from the second policy and move them to the first, select **Accept all from <second policy> to <first policy>**.

12. Click **Merge**.

The system merges the two security policies.

13. On the right of **First** or **Second Policy** (for active policies only), click the **Apply Policy** button to put into effect the changes made to the merged security policy.

The system logs all changes made either manually or automatically in the policy log, for auditing purposes.



---

## Chapter

# 41

---

## Configuring ASM with Local Traffic Policies

---

- *About application security and local traffic policies*
- *About application security and manually adding local traffic policies*
- *Overview: Configuring ASM with local traffic policies*
- *Implementation results*

### About application security and local traffic policies

---

When you use Application Security Manager™ (ASM) to create a security policy attached to a virtual server, the BIG-IP® system automatically creates a local traffic policy. The local traffic policy forms a logical link between the local traffic components and the application security policy.

By default, the system automatically creates a simple local traffic policy directs all HTTP traffic coming to the virtual server to the ASM security policy that you created. ASM examines the traffic to ensure that it meets the requirements of the security policy. If that is all you need to do, your task is done. If, however, you want more flexibility, such as applying different security policies depending on the type of traffic or disabling ASM for certain types of traffic, you can use the local traffic policy to do that.

Local traffic policies can include multiple rules. Each rule consists of a condition and one or more actions to be performed if the condition holds. So you can create a local traffic policy that works with ASM and includes multiple rules that do different things depending on the conditions you set up. In this type of traffic policy, each rule must include one of these ASM actions:

- Enable ASM enforcing a specific security policy
- Disable ASM

For example, you may want a local traffic traffic policy directed to a specific URL to enforce a security policy. As a default rule, all other traffic could disable ASM. You can also direct people using different aspects of an application (or different applications) to various security policies. Many other options are available for directing ASM traffic using local traffic policies.

### About application security and manually adding local traffic policies

---

If you use the Deployment wizard to create a security policy not attached to a virtual server, the system creates the security policy but does not create a local traffic policy. However, you will need to have a virtual server and local traffic policy to select the traffic for the security policy to enforce.

In that case, you can develop the security policy adding the features that you want to use. Without a virtual server, the system cannot build the security policy automatically until you have traffic going through. But you can manually develop the security policy.

When you are ready to enforce the security policy and start sending traffic through the system, create a virtual server with an http profile, and enable the security policy you created in the virtual server resources. When you save the virtual server, the system automatically creates a default local traffic policy that enforces the security policy on all traffic. You can edit the local traffic policy rules if you want more flexibility concerning how the security policies are implemented.

### Overview: Configuring ASM with local traffic policies

---

Application Security Manager™ applies security policy rules to traffic that is controlled and defined using a local traffic policy. To provide more flexibility in selecting the traffic, you can edit the local traffic policy and add rules to it.

This implementation shows how to create a security policy and edit at the local traffic policy that is created. The example provided describes how to add rules to the local traffic policy so that the security policy applies only to administrative traffic beginning with `/admin`. No security policy applies to the other traffic.

Many other options are available for configuring local traffic policies with ASM. By following through the steps in this example, you can see the other options that are available on the screens, and can adjust the example for your needs.

### Task Summary

*Creating a security policy automatically*

*Creating local traffic policy rules for ASM*

## Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the **Create** button.  
The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
  - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
  - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
  - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
  - If creating a new virtual server, specify the protocol, name, IP address and port, pool IP address, and port.
  - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy.
  - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

The name of the new or existing virtual server becomes the name of the security policy.

The Select Deployment Scenario screen opens.

5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.  
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

---

**Important:** You cannot change this setting after you have created the security policy.

---

7. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

---

**Important:** *You cannot change this setting after you have created the security policy.*

---

8. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.

9. Click **Next**.

The Configure Attack Signatures screen opens.

10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.

The system adds the attack signatures needed to protect the selected systems.

11. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

---

**Note:** *Because the Real Traffic Policy Builder<sup>®</sup> begins building the security policy in Blocking mode, you can keep signature staging enabled to make sure that false positives do not occur.*

---

New and updated attack signatures remain in staging for 7 days, and are not enforced (according to the learn, alarm, and block flags) during that time.

12. Click **Next**.

The Configure Automatic Policy Building screen opens.

13. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
<b>Fundamental</b>	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
<b>Enhanced</b>	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, Explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles.
<b>Comprehensive</b>	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

14. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

15. For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
<b>All</b>	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted, the policy is created faster when you select this option.
<b>Address List</b>	Specifies networks to consider safe. Fill in the <b>IP Address</b> and <b>Netmask</b> fields, then click <b>Add</b> . This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

16. If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.

17. If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.

18. Click **Next**.

The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.

19. Click **Finish** to create the security policy.

The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM™ creates the virtual server with an HTTP profile, and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

---

**Tip:** This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.

---

## Creating local traffic policy rules for ASM

You can add rules to define conditions and perform specific actions for different types of application traffic. This example creates two rules to implement different security protection for different traffic.

1. On the Main tab, click **Local Traffic > Policies**.
2. Click the name of the local traffic policy that was created automatically. The name is `asm_auto_l7policy__name` where *name* is the name of the security policy.
3. In the Rules area, click **Add** to create a rule that defines when traffic is handled by the security policy.
4. In the **Rule** field, type the name `admin`.

5. In the Manage Conditions area, define the application traffic to which this rule applies. Specify the following values and use the default values for the rest.
  - a) From the **Operand** list, select **http-uri**.
  - b) From the **Selector** list, select **path**.
  - c) From the **Condition** list, select **starts\_with**; then, in the field below, type `/admin` and click **Add**.
  - d) Click **Add Condition**.
6. In the Manage Actions area, define the action to apply to the traffic. Specify the following values and use the default values for the rest.
  - a) From the **Target** list, select **asm**.  
**Event** is set to **request**, **Action** is set to **enable**, and a security policy is selected.
  - b) In the **Action** setting, for **policy**, select the security policy you created, then click **Add**.
  - c) Click **Add Action**.
7. Click **Finished** to add the rule to the local traffic policy.
8. Click **Properties** to return to the local traffic policy.
9. In the Rules area, click the rule called **default**.  
The **default** rule was added to the local traffic policy when the system created it.  
The screen displays the General Properties of the rule.
10. To change the default action for all other traffic, in the Manage Actions area, edit the action that is shown there.
  - a) In the **Actions** setting, select the action that you see in the list and click **Edit Action**.
  - b) From the **Action** list, select **disable**.
  - c) Click **Add Action**.

The default rule now disables ASM protection for other traffic.

You have edited the local traffic policy so that administrative traffic must meet the security policy you assigned to it. But other traffic will not be subject to that security policy.

## Implementation results

---

When you have completed the steps in this implementation, you have configured the Application Security Manager™ (ASM) to enforce security policy rules only on traffic with a URI beginning with `/admin`. All other traffic bypasses ASM™.

This is simply one way to illustrate how you can use a local traffic policy to determine different conditions and specify multiple actions instead of having all traffic treated the same way. We encourage you to explore the local traffic policy options and documentation to learn how to use this flexible feature to best suit your needs.

---

# Chapter

# 42

---

## Automatically Synchronizing Application Security Configurations

---

- *Overview: Automatically synchronizing ASM systems*
  - *Implementation result*
-

## Overview: Automatically synchronizing ASM systems

This implementation describes how to set up multiple BIG-IP® systems running Application Security Manager™ (ASM) so that they automatically synchronize their security policies and ASM™ configurations. In addition, the ASM devices can fail over to one another if any of the devices goes offline. For synchronizing local traffic configuration data, you can manually synchronize that data as needed.



**Figure 10: Automatically synchronizing ASM configuration data**

In this case, multiple BIG-IP systems are all processing similar traffic for one or more web applications behind a router (or load balancer). All systems are running BIG-IP ASM™ and are in the local trust domain. You organize the systems into two device groups: one Sync-Failover device group for all systems (not ASM-enabled) and one Sync-Only device group with ASM-enabled for all of the systems. The ASM configurations and web applications are automatically duplicated on all of the systems. You can manually synchronize the BIG-IP configuration of the systems in the Sync-Failover device group.

### Task summary

*Performing basic network configuration for synchronization*

*Specifying an IP address for config sync*

*Establishing device trust*

*Creating a Sync-Failover device group*

*Syncing the BIG-IP configuration to the device group*

*Specifying IP addresses for failover communication*

*Creating a Sync-Only device group*

*Enabling ASM synchronization on a device group*

*Synchronizing an ASM-enabled device group*

## About device management and synchronizing application security configurations

You can use device management to set up several BIG-IP® systems running Application Security Manager™ (ASM) so that the systems synchronize their security policies and configurations, and fail over to one another if a system goes offline for any reason. By using application security synchronization, you can set up application security and create security policies on one system, and can propagate them to other systems in an application security device group. In BIG-IP ASM™, a *device group* is two or more BIG-IP devices using the same configuration and providing consistent security policy enforcement.

You can set up application security synchronization, for example, behind an Application Delivery Controller where multiple BIG-IP systems running Application Security Manager are deployed as members of a pool. The options and security policies on all of the systems stay in sync regardless of where you update them.



When you set up ASM™ synchronization, in addition to security policies, other settings such as custom attack signatures, logging profiles, SMTP configuration, anti-virus protection, system variables, and policy templates, are synchronized with all devices in the ASM-enabled device group.

## Considerations for application security synchronization

When using device management with Application Security Manager™ (ASM™), you need to be aware of the following considerations that apply specifically to application security synchronization.

- A BIG-IP® system with Application Security Manager can be a member of only one ASM-enabled device group.
- All BIG-IP systems in a device group must be running the same version (including hot fix updates) of Application Security Manager (version 11.0 or later).
- The BIG-IP systems in the ASM-enabled device group synchronize application security configuration data and security policies, providing consistent enforcement on all the devices.
- Real Traffic Policy Builder® can run on only one system per security policy. For example, you can set up automatic security policy building on one system that is a member of an ASM-enabled device group, the policy is built on that system and then automatically updated on all of the systems in the device group.
- If using a VIPRION® platform (with multiple blades), it is considered one device, and you need to add only the master blade to the device trust and group.

## Performing basic network configuration for synchronization

You need to perform basic networking configuration for each of the BIG-IP® systems whose Application Security Manager™ (ASM) configurations you want to synchronize.

1. Install the same BIG-IP system version (including any hot fixes) on each device.
2. Provision LTM® and ASM™ on each device (**System > Resource Provisioning**).
3. On each device, create one or more VLANs, depending on your networking configuration (**Network > VLANs**).
4. On each device, create a self IP (**Network > Self IPs**).  
When creating the self IP, set **Traffic Group** to **traffic-group-local-only (non-floating)**.
5. On each device, create a default gateway, if needed (**Network > Routes**).
6. On each device, configure DNS (**System > Configuration > Device > DNS**) and NTP (**System > Configuration > Device > NTP**) so they are set to the same time.
7. Verify connectivity between the devices (self IP address to self IP address). For example, use this command to ensure communications: `ping -I vlan_interface device_self_IP`
8. On each device, specify the IP address to use when synchronizing configuration objects to the local device:
  - a) Click **Device Management > Devices**.
  - b) Click the name of the local device.
  - c) From the Device Connectivity menu, choose ConfigSync.
  - d) For the **Local Address** setting, select the self IP address.
  - e) Click **Update**.
9. If your company requires special device certificates, install them on each device (**System > Device Certificates** and click **Import**).

The basic networking setup is complete for the BIG-IP ASM systems for which you want to share security policies and configurations.

### Specifying an IP address for config sync

Before configuring the config sync address, verify that all devices in the device group are running the same version of BIG-IP® system software.

You perform this task to specify the IP address on the local device that other devices in the device group will use to synchronize their configuration objects to the local device.

---

**Note:** You must perform this task locally on each device in the device group.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose ConfigSync.
5. For the **Local Address** setting, retain the displayed IP address or select another address from the list.  
F5 Networks recommends that you use the default value, which is the self IP address for VLAN `internal`. This address must be a non-floating self IP address and not a management IP address.

---

**Important:** If the BIG-IP device you are configuring is accessed using Amazon Web Services, then the internal self IP address that you specify must be the internal private IP addresses that you configured for this EC2 instance as the **Local Address**.

---

6. Click **Update**.

After performing this task, the other devices in the device group can sync their configurations to the local device.

### Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices A, B, and C each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device A and add devices B and C to the local trust domain. Note that there is no need to repeat this process on devices B and C.

1. On the Main tab, click **Device Management > Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.

3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
  - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
  - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
  - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
  - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Creating a Sync-Failover device group

This task establishes failover capability between two or more BIG-IP® devices. If an active device in a Sync-Failover device group becomes unavailable, the configuration objects fail over to another member of the device group and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

Repeat this task for each Sync-Failover device group that you want to create for your network configuration.

1. On the Main tab, click **Device Management > Device Groups**.
2. On the Device Groups list screen, click **Create**.  
The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Failover**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. In the Configuration area of the screen, select a host name from the **Available** list for each BIG-IP device that you want to include in the device group, including the local device. Use the Move button to move the host name to the **Includes** list.  
The **Available** list shows any devices that are members of the device's local trust domain but not currently members of a Sync-Failover device group. A device can be a member of one Sync-Failover group only.
6. For the **Network Failover** setting, select or clear the check box:
  - Select the check box if you want device group members to handle failover communications by way of network connectivity. This choice is required for active-active configurations.
  - Clear the check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

For active-active configurations, you must select network failover, as opposed to serial-cable (hard-wired) connectivity.

7. For the **Automatic Sync** setting, select or clear the check box:

- Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
- Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.

**8.** For the **Full Sync** setting, select or clear the check box:

- Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
- Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

**9.** In the **Maximum Incremental Sync Size (KB)** field, retain the default value of 1024, or type a different value.

This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

**10.** Click **Finished**.

You now have a Sync-Failover type of device group containing BIG-IP devices as members.

## Syncing the BIG-IP configuration to the device group

Before you sync the configuration, verify that the devices targeted for config sync are members of a device group and that device trust is established.

This task synchronizes the BIG-IP<sup>®</sup> configuration data from the local device to the devices in the device group. This synchronization ensures that devices in the device group operate properly. When synchronizing self IP addresses, the BIG-IP system synchronizes floating self IP addresses only.

---

**Important:** *You perform this task on either of the two devices, but not both.*

---

1. On the Main tab, click **Device Management > Overview**.
2. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of `Changes Pending`.
4. In the Sync Options area of the screen, select **Sync Device to Group**.
5. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.

Except for non-floating self IP addresses, the entire set of BIG-IP configuration data is replicated on each device in the device group.

## Specifying IP addresses for failover communication

You typically perform this task during initial Device Service Clustering (DSC®) configuration, to specify the local IP addresses that you want other devices in the device group to use for continuous health-assessment communication with the local device. You must perform this task locally on each device in the device group.

---

**Note:** The IP addresses that you specify must belong to route domain 0.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose Failover.
5. For the Failover Unicast Configuration settings, click **Add** for each IP address on this device that other devices in the device group can use to exchange failover messages with this device. The unicast IP addresses you specify depend on the type of device:

<b>Platform</b>	<b>Action</b>
-----------------	---------------

<b>Non-VIPRION</b>	Type a self IP address associated with an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP address for the device.
--------------------	--

<b>VIPRION without vCMP</b>	Type the self IP address for an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP addresses for all slots in the VIPRION cluster. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
-----------------------------	--

<b>VIPRION with vCMP</b>	Type a self IP address that is defined on the guest and associated with an internal VLAN on the host (preferably VLAN <sub>HA</sub> ). You must also specify the management IP addresses for all of the slots configured for the guest. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
--------------------------	---

6. To enable the use of a failover multicast address on a VIPRION® platform (recommended), then for the **Use Failover Multicast Address** setting, select the **Enabled** check box.
7. If you enabled **Use Failover Multicast Address**, either accept the default **Address** and **Port** values, or specify values appropriate for the device.  
If you revise the default **Address** and **Port** values, but then decide to revert to the default values, click **Reset Defaults**.
8. Click **Update**.

After you perform this task, other devices in the device group can send failover messages to the local device using the specified IP addresses.

## Creating a Sync-Only device group

You perform this task to create a Sync-Only type of device group. When you create a Sync-Only device group, the BIG-IP® system can then automatically synchronize certain types of data such as security policies and acceleration applications and policies to the other devices in the group, even when some of those devices reside in another network. You can perform this task on any BIG-IP device within the local trust domain.

1. On the Main tab, click **Device Management > Device Groups**.

2. On the Device Groups list screen, click **Create**.  
The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Only**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. For the **Members** setting, select an IP address and host name from the **Available** list for each BIG-IP device that you want to include in the device group. Use the Move button to move the host name to the **Includes** list.  
The list shows any devices that are members of the device's local trust domain.
6. For the **Automatic Sync** setting, select or clear the check box:
  - Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
  - Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.
7. For the **Full Sync** setting, select or clear the check box:
  - Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
  - Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.
8. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of 1024, or type a different value.  
This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.
9. Click **Finished**.

You now have a Sync-Only type of device group containing BIG-IP devices as members.

## Enabling ASM synchronization on a device group

You need to have already set up the BIG-IP<sup>®</sup> systems you want to synchronize in a device trust and a device group. Application Security Manager<sup>™</sup> (ASM) must be provisioned on all the systems in the device group.

You can enable ASM<sup>™</sup> synchronization on a device group to synchronize security policies and configurations on all devices in the device group. You do this task on one system; for example, the active system in an active-standby pair.

1. On the Main tab, click **Security > Application Security > Synchronization**.  
The system displays a list of device groups of which this device is a member.
2. For **Device Group**, select the device group whose members you want to synchronize.
3. Click **Save**.

The BIG-IP ASM systems that you want to share security policies and configurations are part of a device group with ASM synchronization.

## Synchronizing an ASM-enabled device group

You need to have set up the BIG-IP® Application Security Manager™ (ASM) systems you want to synchronize in a Sync-Failover device group that is ASM™-enabled.

You can manually synchronize security policies and configuration of systems in an ASM-enabled device group.

1. On one system in the ASM-enabled failover device group, create an application security policy. Because the two systems are not in sync, you see a **Changes Pending** status message on the screen.
2. Click the **Changes Pending** message.

---

***Tip:** You can also click **Device Management > Overview**.*

---

The Overview screen opens.

3. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
4. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of **Changes Pending**.
5. In the Sync Options area of the screen, select **Sync Device to Group**.
6. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.
7. Verify that the devices are synchronized.  
For example, log in to another device in the device group and verify that the security policy you created also resides on that system. Click **Security > Application Security > Security Policies** and see if the policy is listed.

Except for static self IP addresses, the entire set of BIG-IP configuration data including ASM™ security policies and configuration is replicated on one or more devices in the ASM-enabled device group. If the active device is not available, the standby device becomes active and handles traffic.

You can create new security policies or update existing ones on any of the devices in the group, or update the ASM configuration options. You can manually synchronize changes you make on one device with the other devices in the ASM-enabled device group.

## Implementation result

---

You have set up multiple BIG-IP® systems running Application Security Manager™ (ASM) so that they automatically synchronize their ASM security policies and ASM configuration data. In addition, with this implementation, you can manually synchronize the local traffic configuration, as needed.

You can create new security policies or update existing ones on any of the devices in the group, or update the ASM™ configuration options. Any ASM changes you make on one device are automatically synchronized with the other devices in the ASM-enabled Sync-Only device group.

If Attack Signatures **Update Mode** is scheduled for automatic update, the attack signature update settings are synchronized. Each device in the device group updates itself independently according to the configured schedule. If you manually upload attack signatures or click **Update Signatures** to update from the server, the update is propagated to all of the devices in the device group.



---

# Chapter

# 43

---

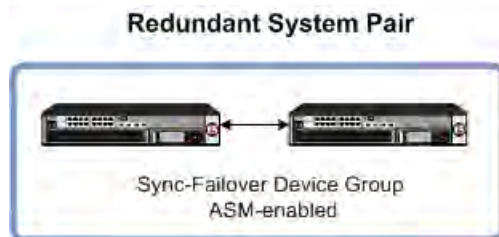
## Manually Synchronizing Application Security Configurations

---

- *Overview: Manually synchronizing ASM systems*
  - *Implementation result*
-

## Overview: Manually synchronizing ASM systems

This implementation describes how to set up two BIG-IP® systems running Application Security Manager™ (ASM) so that you can synchronize their security policies and configurations. With this implementation, the BIG-IP systems can fail over to one another, and you can manually sync all of the BIG-IP configuration data, including ASM policy data.



**Figure 11: Manually synchronizing ASM configuration data**

The two BIG-IP systems are set up for redundancy: one active and the other standby. Both systems are in the local trust domain and in the same Sync-Failover device group. If one system is unavailable, the other system begins to process application traffic. You can manually synchronize the systems. The ASM™ configurations and security policies are duplicated on both systems.

You can use this implementation as the basis for more complex configurations. For example, if you have multiple redundant pairs each supporting a different web application, you can use this implementation to set up each pair. You could create a Sync-Failover device group for each pair and then synchronize the data within each pair only. In this configuration, you all devices reside in the local trust domain.

### Task summary

*Performing basic network configuration for synchronization*

*Specifying an IP address for config sync*

*Establishing device trust*

*Creating a Sync-Failover device group*

*Syncing the BIG-IP configuration to the device group*

*Specifying IP addresses for failover communication*

*Enabling ASM synchronization on a device group*

*Synchronizing an ASM-enabled device group*

## About device management and synchronizing application security configurations

You can use device management to set up several BIG-IP® systems running Application Security Manager™ (ASM) so that the systems synchronize their security policies and configurations, and fail over to one another if a system goes offline for any reason. By using application security synchronization, you can set up application security and create security policies on one system, and can propagate them to other systems in an application security device group. In BIG-IP ASM™, a *device group* is two or more BIG-IP devices using the same configuration and providing consistent security policy enforcement.

You can set up application security synchronization, for example, behind an Application Delivery Controller where multiple BIG-IP systems running Application Security Manager are deployed as members of a pool. The options and security policies on all of the systems stay in sync regardless of where you update them.

When you set up ASM™ synchronization, in addition to security policies, other settings such as custom attack signatures, logging profiles, SMTP configuration, anti-virus protection, system variables, and policy templates, are synchronized with all devices in the ASM-enabled device group.

## Considerations for application security synchronization

When using device management with Application Security Manager™ (ASM™), you need to be aware of the following considerations that apply specifically to application security synchronization.

- A BIG-IP® system with Application Security Manager can be a member of only one ASM-enabled device group.
- All BIG-IP systems in a device group must be running the same version (including hot fix updates) of Application Security Manager (version 11.0 or later).
- The BIG-IP systems in the ASM-enabled device group synchronize application security configuration data and security policies, providing consistent enforcement on all the devices.
- Real Traffic Policy Builder® can run on only one system per security policy. For example, you can set up automatic security policy building on one system that is a member of an ASM-enabled device group, the policy is built on that system and then automatically updated on all of the systems in the device group.
- If using a VIPRION® platform (with multiple blades), it is considered one device, and you need to add only the master blade to the device trust and group.

## Performing basic network configuration for synchronization

You need to perform basic networking configuration for each of the BIG-IP® systems whose Application Security Manager™ (ASM) configurations you want to synchronize.

1. Install the same BIG-IP system version (including any hot fixes) on each device.
2. Provision LTM® and ASM™ on each device (**System > Resource Provisioning**).
3. On each device, create one or more VLANs, depending on your networking configuration (**Network > VLANs**).
4. On each device, create a self IP (**Network > Self IPs**).  
When creating the self IP, set **Traffic Group** to **traffic-group-local-only (non-floating)**.
5. On each device, create a default gateway, if needed (**Network > Routes**).
6. On each device, configure DNS (**System > Configuration > Device > DNS**) and NTP (**System > Configuration > Device > NTP**) so they are set to the same time.
7. Verify connectivity between the devices (self IP address to self IP address). For example, use this command to ensure communications: `ping -I vlan_interface device_self_IP`
8. On each device, specify the IP address to use when synchronizing configuration objects to the local device:
  - a) Click **Device Management > Devices**.
  - b) Click the name of the local device.
  - c) From the Device Connectivity menu, choose ConfigSync.
  - d) For the **Local Address** setting, select the self IP address.
  - e) Click **Update**.
9. If your company requires special device certificates, install them on each device (**System > Device Certificates** and click **Import**).

The basic networking setup is complete for the BIG-IP ASM systems for which you want to share security policies and configurations.

### Specifying an IP address for config sync

Before configuring the config sync address, verify that all devices in the device group are running the same version of BIG-IP® system software.

You perform this task to specify the IP address on the local device that other devices in the device group will use to synchronize their configuration objects to the local device.

---

**Note:** You must perform this task locally on each device in the device group.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose ConfigSync.
5. For the **Local Address** setting, retain the displayed IP address or select another address from the list.  
F5 Networks recommends that you use the default value, which is the self IP address for VLAN `internal`. This address must be a non-floating self IP address and not a management IP address.

---

**Important:** If the BIG-IP device you are configuring is accessed using Amazon Web Services, then the internal self IP address that you specify must be the internal private IP addresses that you configured for this EC2 instance as the **Local Address**.

---

6. Click **Update**.

After performing this task, the other devices in the device group can sync their configurations to the local device.

### Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices A, B, and C each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device A and add devices B and C to the local trust domain. Note that there is no need to repeat this process on devices B and C.

1. On the Main tab, click **Device Management > Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.

3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
  - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
  - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
  - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
  - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Creating a Sync-Failover device group

This task establishes failover capability between two or more BIG-IP® devices. If an active device in a Sync-Failover device group becomes unavailable, the configuration objects fail over to another member of the device group and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

Repeat this task for each Sync-Failover device group that you want to create for your network configuration.

1. On the Main tab, click **Device Management > Device Groups**.
2. On the Device Groups list screen, click **Create**.  
The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Failover**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. In the Configuration area of the screen, select a host name from the **Available** list for each BIG-IP device that you want to include in the device group, including the local device. Use the Move button to move the host name to the **Includes** list.  
The **Available** list shows any devices that are members of the device's local trust domain but not currently members of a Sync-Failover device group. A device can be a member of one Sync-Failover group only.
6. For the **Network Failover** setting, select or clear the check box:
  - Select the check box if you want device group members to handle failover communications by way of network connectivity. This choice is required for active-active configurations.
  - Clear the check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

For active-active configurations, you must select network failover, as opposed to serial-cable (hard-wired) connectivity.

7. For the **Automatic Sync** setting, select or clear the check box:

- Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
- Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.

8. For the **Full Sync** setting, select or clear the check box:

- Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
- Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

9. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of 1024, or type a different value.

This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

10. Click **Finished**.

You now have a Sync-Failover type of device group containing BIG-IP devices as members.

## Syncing the BIG-IP configuration to the device group

Before you sync the configuration, verify that the devices targeted for config sync are members of a device group and that device trust is established.

This task synchronizes the BIG-IP® configuration data from the local device to the devices in the device group. This synchronization ensures that devices in the device group operate properly. When synchronizing self IP addresses, the BIG-IP system synchronizes floating self IP addresses only.

---

**Important:** You perform this task on either of the two devices, but not both.

---

1. On the Main tab, click **Device Management > Overview**.
2. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of `Changes Pending`.
4. In the Sync Options area of the screen, select **Sync Device to Group**.
5. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.

Except for non-floating self IP addresses, the entire set of BIG-IP configuration data is replicated on each device in the device group.

## Specifying IP addresses for failover communication

You typically perform this task during initial Device Service Clustering (DSC®) configuration, to specify the local IP addresses that you want other devices in the device group to use for continuous health-assessment communication with the local device. You must perform this task locally on each device in the device group.

---

**Note:** The IP addresses that you specify must belong to route domain 0.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose Failover.
5. For the Failover Unicast Configuration settings, click **Add** for each IP address on this device that other devices in the device group can use to exchange failover messages with this device. The unicast IP addresses you specify depend on the type of device:

<b>Platform</b>	<b>Action</b>
-----------------	---------------

<b>Non-VIPRION</b>	Type a self IP address associated with an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP address for the device.
--------------------	--

<b>VIPRION without vCMP</b>	Type the self IP address for an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP addresses for all slots in the VIPRION cluster. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
-----------------------------	--

<b>VIPRION with vCMP</b>	Type a self IP address that is defined on the guest and associated with an internal VLAN on the host (preferably VLAN <sub>HA</sub> ). You must also specify the management IP addresses for all of the slots configured for the guest. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
--------------------------	---

6. To enable the use of a failover multicast address on a VIPRION® platform (recommended), then for the **Use Failover Multicast Address** setting, select the **Enabled** check box.
7. If you enabled **Use Failover Multicast Address**, either accept the default **Address** and **Port** values, or specify values appropriate for the device.  
If you revise the default **Address** and **Port** values, but then decide to revert to the default values, click **Reset Defaults**.
8. Click **Update**.

After you perform this task, other devices in the device group can send failover messages to the local device using the specified IP addresses.

## Enabling ASM synchronization on a device group

You need to have already set up the BIG-IP® systems you want to synchronize in a device trust and a device group. Application Security Manager™ (ASM) must be provisioned on all the systems in the device group.

You can enable ASM™ synchronization on a device group to synchronize security policies and configurations on all devices in the device group. You do this task on one system; for example, the active system in an active-standby pair.

1. On the Main tab, click **Security > Application Security > Synchronization**.  
The system displays a list of device groups of which this device is a member.
2. For **Device Group**, select the device group whose members you want to synchronize.
3. Click **Save**.

The BIG-IP ASM systems that you want to share security policies and configurations are part of a device group with ASM synchronization.

### Synchronizing an ASM-enabled device group

You need to have set up the BIG-IP® Application Security Manager™ (ASM) systems you want to synchronize in a Sync-Failover device group that is ASM™-enabled.

You can manually synchronize security policies and configuration of systems in an ASM-enabled device group.

1. On one system in the ASM-enabled failover device group, create an application security policy.  
Because the two systems are not in sync, you see a **Changes Pending** status message on the screen.
2. Click the **Changes Pending** message.

---

***Tip:** You can also click **Device Management > Overview**.*

---

The Overview screen opens.

3. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
4. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of **Changes Pending**.
5. In the Sync Options area of the screen, select **Sync Device to Group**.
6. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.
7. Verify that the devices are synchronized.  
For example, log in to another device in the device group and verify that the security policy you created also resides on that system. Click **Security > Application Security > Security Policies** and see if the policy is listed.

Except for static self IP addresses, the entire set of BIG-IP configuration data including ASM™ security policies and configuration is replicated on one or more devices in the ASM-enabled device group. If the active device is not available, the standby device becomes active and handles traffic.

You can create new security policies or update existing ones on any of the devices in the group, or update the ASM configuration options. You can manually synchronize changes you make on one device with the other devices in the ASM-enabled device group.



## Implementation result

---

You have now set up two BIG-IP® systems running Application Security Manager™ (ASM) so that you can synchronize their security policies and configurations. With this implementation, you manually synchronize the ASM and BIG-IP configurations.

The two BIG-IP systems are in the same Sync-Failover device group. If one system becomes unavailable, the other system begins processing application traffic.



---

# Chapter

# 44

---

## Synchronizing Application Security Configurations Across LANs

---

- *Overview: Synchronizing ASM systems across LANs*
  - *Implementation result*
-

## Overview: Synchronizing ASM systems across LANs

This implementation describes how to set up multiple BIG-IP® systems running Application Security Manager™ (ASM) so that you can synchronize their security policies and configurations for disaster recovery. You can use this implementation to synchronize BIG-IP ASM™ security policies and configurations on systems that reside in different network segments or LANs, such as those in separate offices or data centers. Note that traffic must be routable between the network segments. If a disaster occurs at one of the offices and both devices are disabled, the latest security policies are still available on the systems in the other location.

This implementation also configures failover between systems in a redundant pair on a particular network segment. If one of the devices in a pair goes offline for any reason, the other device in the pair begins processing the application traffic.



**Figure 12: Automatically synchronizing ASM configuration data across LANs**

In the figure, two sets of BIG-IP systems are set up for redundancy: one active and the other standby. Each pair is in a different network segment (LAN), and there can be additional pairs, as needed. Each LAN has one pair of devices, where both have the same default routing, but routing is not the same for the devices in the other LAN.

All of the systems are running ASM and are in the trust domain. Three device groups are set up: one Sync-Failover device group for each pair (not ASM-enabled), and one Sync-Only device group with ASM enabled using automatic synchronization for all of the systems. The systems automatically duplicate the ASM configurations and security policies on all of the systems. You can manually synchronize the BIG-IP configurations of each pair of systems when needed.

### Task summary

- Performing basic network configuration for synchronization*
- Specifying an IP address for config sync*
- Establishing device trust*
- Creating a Sync-Failover device group*
- Syncing the BIG-IP configuration to the device group*
- Specifying IP addresses for failover communication*
- Creating a Sync-Only device group*
- Enabling ASM synchronization on a Sync-Only device group*
- Synchronizing an ASM-enabled device group*

## About device management and synchronizing application security configurations

You can use device management to set up several BIG-IP® systems running Application Security Manager™ (ASM) so that the systems synchronize their security policies and configurations, and fail over to one another if a system goes offline for any reason. By using application security synchronization, you can set up application security and create security policies on one system, and can propagate them to other systems in an application security device group. In BIG-IP ASM™, a *device group* is two or more BIG-IP devices using the same configuration and providing consistent security policy enforcement.

You can set up application security synchronization, for example, behind an Application Delivery Controller where multiple BIG-IP systems running Application Security Manager are deployed as members of a pool. The options and security policies on all of the systems stay in sync regardless of where you update them.

When you set up ASM™ synchronization, in addition to security policies, other settings such as custom attack signatures, logging profiles, SMTP configuration, anti-virus protection, system variables, and policy templates, are synchronized with all devices in the ASM-enabled device group.

## Considerations for application security synchronization

When using device management with Application Security Manager™ (ASM™), you need to be aware of the following considerations that apply specifically to application security synchronization.

- A BIG-IP® system with Application Security Manager can be a member of only one ASM-enabled device group.
- All BIG-IP systems in a device group must be running the same version (including hot fix updates) of Application Security Manager (version 11.0 or later).
- The BIG-IP systems in the ASM-enabled device group synchronize application security configuration data and security policies, providing consistent enforcement on all the devices.
- Real Traffic Policy Builder® can run on only one system per security policy. For example, you can set up automatic security policy building on one system that is a member of an ASM-enabled device group, the policy is built on that system and then automatically updated on all of the systems in the device group.
- If using a VIPRION® platform (with multiple blades), it is considered one device, and you need to add only the master blade to the device trust and group.

## Performing basic network configuration for synchronization

You need to perform basic networking configuration for each of the BIG-IP® systems whose Application Security Manager™ (ASM) configurations you want to synchronize.

1. Install the same BIG-IP system version (including any hot fixes) on each device.
2. Provision LTM® and ASM™ on each device (**System > Resource Provisioning**).
3. On each device, create one or more VLANs, depending on your networking configuration (**Network > VLANs**).
4. On each device, create a self IP (**Network > Self IPs**).  
When creating the self IP, set **Traffic Group** to **traffic-group-local-only (non-floating)**.
5. On each device, create a default gateway, if needed (**Network > Routes**).
6. On each device, configure DNS (**System > Configuration > Device > DNS**) and NTP (**System > Configuration > Device > NTP**) so they are set to the same time.

7. Verify connectivity between the devices (self IP address to self IP address). For example, use this command to ensure communications: `ping -I vlan_interface device_self_IP`
8. On each device, specify the IP address to use when synchronizing configuration objects to the local device:
  - a) Click **Device Management > Devices**.
  - b) Click the name of the local device.
  - c) From the Device Connectivity menu, choose ConfigSync.
  - d) For the **Local Address** setting, select the self IP address.
  - e) Click **Update**.
9. If your company requires special device certificates, install them on each device (**System > Device Certificates** and click **Import**).

The basic networking setup is complete for the BIG-IP ASM systems for which you want to share security policies and configurations.

### Specifying an IP address for config sync

Before configuring the config sync address, verify that all devices in the device group are running the same version of BIG-IP® system software.

You perform this task to specify the IP address on the local device that other devices in the device group will use to synchronize their configuration objects to the local device.

---

**Note:** You must perform this task locally on each device in the device group.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose ConfigSync.
5. For the **Local Address** setting, retain the displayed IP address or select another address from the list.  
F5 Networks recommends that you use the default value, which is the self IP address for VLAN `internal`. This address must be a non-floating self IP address and not a management IP address.

---

**Important:** If the BIG-IP device you are configuring is accessed using Amazon Web Services, then the internal self IP address that you specify must be the internal private IP addresses that you configured for this EC2 instance as the **Local Address**.

---

6. Click **Update**.

After performing this task, the other devices in the device group can sync their configurations to the local device.

### Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You perform this task to establish trust among devices on one or more network segments. Devices that trust each other constitute the *local trust domain*. A device must be a member of the local trust domain prior to joining a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices A, B, and C each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can simply log into device A and add devices B and C to the local trust domain. Note that there is no need to repeat this process on devices B and C.

1. On the Main tab, click **Device Management > Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.
3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
  - If the BIG-IP device is a non-VIPRION device, type the management IP address for the device.
  - If the BIG-IP device is a VIPRION device that is not licensed and provisioned for vCMP, type the primary cluster management IP address for the cluster.
  - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
  - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the name of the remote device is correct.
7. Verify that the management IP address and name of the remote device are correct.
8. Click **Finished**.

The device you added is now a member of the local trust domain.

Repeat this task for each device that you want to add to the local trust domain.

## Creating a Sync-Failover device group

This task establishes failover capability between two or more BIG-IP® devices. If an active device in a Sync-Failover device group becomes unavailable, the configuration objects fail over to another member of the device group and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

Repeat this task for each Sync-Failover device group that you want to create for your network configuration.

1. On the Main tab, click **Device Management > Device Groups**.
2. On the Device Groups list screen, click **Create**.  
The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Failover**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. In the Configuration area of the screen, select a host name from the **Available** list for each BIG-IP device that you want to include in the device group, including the local device. Use the Move button to move the host name to the **Includes** list.

The **Available** list shows any devices that are members of the device's local trust domain but not currently members of a Sync-Failover device group. A device can be a member of one Sync-Failover group only.

6. For the **Network Failover** setting, select or clear the check box:

- Select the check box if you want device group members to handle failover communications by way of network connectivity. This choice is required for active-active configurations.
- Clear the check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

For active-active configurations, you must select network failover, as opposed to serial-cable (hard-wired) connectivity.

7. For the **Automatic Sync** setting, select or clear the check box:

- Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
- Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.

8. For the **Full Sync** setting, select or clear the check box:

- Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
- Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

9. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of 1024, or type a different value.

This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

10. Click **Finished**.

You now have a Sync-Failover type of device group containing BIG-IP devices as members.

## Syncing the BIG-IP configuration to the device group

Before you sync the configuration, verify that the devices targeted for config sync are members of a device group and that device trust is established.

This task synchronizes the BIG-IP® configuration data from the local device to the devices in the device group. This synchronization ensures that devices in the device group operate properly. When synchronizing self IP addresses, the BIG-IP system synchronizes floating self IP addresses only.

---

**Important:** You perform this task on either of the two devices, but not both.

---

1. On the Main tab, click **Device Management > Overview**.



2. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of *Changes Pending*.
4. In the Sync Options area of the screen, select **Sync Device to Group**.
5. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.

Except for non-floating self IP addresses, the entire set of BIG-IP configuration data is replicated on each device in the device group.

## Specifying IP addresses for failover communication

You typically perform this task during initial Device Service Clustering (DSC®) configuration, to specify the local IP addresses that you want other devices in the device group to use for continuous health-assessment communication with the local device. You must perform this task locally on each device in the device group.

---

**Note:** The IP addresses that you specify must belong to route domain 0.

---

1. Confirm that you are logged in to the actual device you want to configure.
2. On the Main tab, click **Device Management > Devices**.  
This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose Failover.
5. For the Failover Unicast Configuration settings, click **Add** for each IP address on this device that other devices in the device group can use to exchange failover messages with this device. The unicast IP addresses you specify depend on the type of device:

<b>Platform</b>	<b>Action</b>
-----------------	---------------

<b>Non-VIPRION</b>	Type a self IP address associated with an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP address for the device.
--------------------	--

<b>VIPRION without vCMP</b>	Type the self IP address for an internal VLAN (preferably VLAN <sub>HA</sub> ) and the management IP addresses for all slots in the VIPRION cluster. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
-----------------------------	--

<b>VIPRION with vCMP</b>	Type a self IP address that is defined on the guest and associated with an internal VLAN on the host (preferably VLAN <sub>HA</sub> ). You must also specify the management IP addresses for all of the slots configured for the guest. Note that if you also configure a multicast address (using the <b>Use Failover Multicast Address</b> setting), then these management IP addresses are not required.
--------------------------	---

6. To enable the use of a failover multicast address on a VIPRION® platform (recommended), then for the **Use Failover Multicast Address** setting, select the **Enabled** check box.
7. If you enabled **Use Failover Multicast Address**, either accept the default **Address** and **Port** values, or specify values appropriate for the device.  
If you revise the default **Address** and **Port** values, but then decide to revert to the default values, click **Reset Defaults**.

### 8. Click **Update**.

After you perform this task, other devices in the device group can send failover messages to the local device using the specified IP addresses.

## Creating a Sync-Only device group

You perform this task to create a Sync-Only type of device group. When you create a Sync-Only device group, the BIG-IP® system can then automatically synchronize certain types of data such as security policies and acceleration applications and policies to the other devices in the group, even when some of those devices reside in another network. You can perform this task on any BIG-IP device within the local trust domain.

1. On the Main tab, click **Device Management > Device Groups**.
2. On the Device Groups list screen, click **Create**.  
The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Only**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. For the **Members** setting, select an IP address and host name from the **Available** list for each BIG-IP device that you want to include in the device group. Use the Move button to move the host name to the **Includes** list.

The list shows any devices that are members of the device's local trust domain.

6. For the **Automatic Sync** setting, select or clear the check box:
  - Select the check box when you want the BIG-IP system to automatically sync the BIG-IP configuration data whenever a config sync operation is required. In this case, the BIG-IP system syncs the configuration data whenever the data changes on any device in the device group.
  - Clear the check box when you want to manually initiate each config sync operation. In this case, F5 networks recommends that you perform a config sync operation whenever configuration data changes on one of the devices in the device group.
7. For the **Full Sync** setting, select or clear the check box:
  - Select the check box when you want all sync operations to be full syncs. In this case, the BIG-IP system syncs the entire set of BIG-IP configuration data whenever a config sync operation is required.
  - Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.

8. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of 1024, or type a different value.

This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.

9. Click **Finished**.

You now have a Sync-Only type of device group containing BIG-IP devices as members.

## Enabling ASM synchronization on a Sync-Only device group

You need to have set up the BIG-IP® systems you want to synchronize in a device trust and a device group. Application Security Manager™ (ASM) must be provisioned on all the systems in the device group.

You can enable ASM™ synchronization on a device group to synchronize security policies and configurations on all devices in the device group. You do this task on one system, for example, the active system in an active-standby pair.

1. On the Main tab, click **Security > Application Security > Synchronization**.  
The system displays a list of device groups of which this device is a member.
2. For **Device Group**, select the Sync-Only device group you created.
3. Click **Save**.

The BIG-IP ASM™ systems that you want to share security policies and configurations are part of a Sync-Only device group with ASM synchronization.

## Synchronizing an ASM-enabled device group

You need to have set up the BIG-IP® Application Security Manager™ (ASM) systems you want to synchronize in a Sync-Failover device group that is ASM™-enabled.

You can manually synchronize security policies and configuration of systems in an ASM-enabled device group.

1. On one system in the ASM-enabled failover device group, create an application security policy.  
Because the two systems are not in sync, you see a **Changes Pending** status message on the screen.
2. Click the **Changes Pending** message.

---

**Tip:** You can also click **Device Management > Overview**.

---

The Overview screen opens.

3. In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.  
The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
4. In the Devices area of the screen, in the Sync Status column, select the device that shows a sync status of **Changes Pending**.
5. In the Sync Options area of the screen, select **Sync Device to Group**.
6. Click **Sync**.  
The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.
7. Verify that the devices are synchronized.  
For example, log in to another device in the device group and verify that the security policy you created also resides on that system. Click **Security > Application Security > Security Policies** and see if the policy is listed.

Except for static self IP addresses, the entire set of BIG-IP configuration data including ASM™ security policies and configuration is replicated on one or more devices in the ASM-enabled device group. If the active device is not available, the standby device becomes active and handles traffic.

You can create new security policies or update existing ones on any of the devices in the group, or update the ASM configuration options. You can manually synchronize changes you make on one device with the other devices in the ASM-enabled device group.

### Implementation result

---

You have set up disaster recovery for multiple BIG-IP® systems running Application Security Manager™ (ASM). Each office or data center has an active system and a standby that takes over if the active system should fail. You must manually synchronize the BIG-IP configuration from one system to the other if you change the configuration.

You can create new security policies or update existing ones on any of the devices in the group, or update the ASM™ configuration options (**Application Security>Options**). Any changes you make on one device are automatically synchronized with the other devices in the ASM-enabled Sync-Only device group.

If Attack Signatures **Update Mode** is scheduled for automatic update, the attack signature update settings are synchronized. Each device in the device group updates itself independently according to the configured schedule. If you manually upload attack signatures or click **Upload Signatures** to update from the server, the update is propagated to all of the devices in the device group.

---

# Chapter

# 45

---

## Integrating ASM with Database Security Products

---

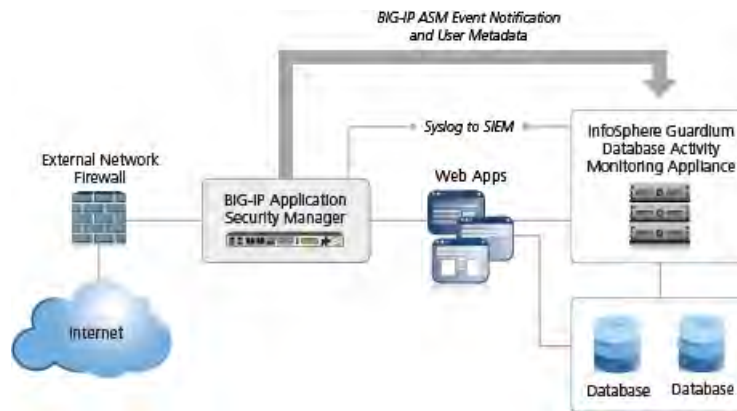
- *Overview: Integrating ASM with database security products*
  - *Implementation result*
-

## Overview: Integrating ASM with database security products

You can deploy Application Security Manager™ (ASM) with database security products, such as IBM® InfoSphere® Guardium® to increase security visibility, receive alerts about suspicious activity, and prevent attacks. When integrated with database security, ASM™ provides information about each HTTP request and database query to the database security product's logging and reporting system. This allows the database security system to correlate the web transaction with the database query to make a security assessment of the transaction.

Before you can integrate ASM with a database security product, the database security server itself must have been configured, and be accessible from ASM. On the BIG-IP® system, you specify the host name or IP address of the database security server. Then, you enable database security integration for one or more security policies that are set up to protect web application resources.

When using database security, Application Security Manager monitors web application traffic and sends information about the users, the requests, and the reporting events to the database security server. The following figure shows an example of how ASM can integrate with the IBM InfoSphere Guardium Database Activity Monitoring Appliance.



**Figure 13: Integrating ASM with external database security example**

The security policy can get user names from requests using login pages configured from within ASM, or the policy can retrieve the user names from Access Policy Manager® (APM). This implementation describes how to integrate with an external database security server using login pages.

When using login pages for the application, you define the URLs, parameters, and validation criteria required for users to log in to the application. User and session information is included in the system logs so you can track a particular session or user. The system can log activity, or block a user or session if either generates too many violations.

### Task Summary

*Creating a security policy automatically*

*Creating login pages*

*Enforcing login pages*

*Configuring a database security server*

*Enabling database security integration in a security policy*

## Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the **Create** button.  
The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
  - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
  - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
  - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
  - If creating a new virtual server, specify the protocol, name, IP address and port, pool IP address, and port.
  - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy.
  - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

The name of the new or existing virtual server becomes the name of the security policy.

The Select Deployment Scenario screen opens.

5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.  
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

---

**Important:** You cannot change this setting after you have created the security policy.

---

7. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.

---

**Important:** You cannot change this setting after you have created the security policy.

---

8. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
9. Click **Next**.

The Configure Attack Signatures screen opens.

10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.

The system adds the attack signatures needed to protect the selected systems.

11. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.

---

***Note:** Because the Real Traffic Policy Builder<sup>®</sup> begins building the security policy in Blocking mode, you can keep signature staging enabled to make sure that false positives do not occur.*

---

New and updated attack signatures remain in staging for 7 days, and are not enforced (according to the learn, alarm, and block flags) during that time.

12. Click **Next**.

The Configure Automatic Policy Building screen opens.

13. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
<b>Fundamental</b>	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
<b>Enhanced</b>	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, Explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles.
<b>Comprehensive</b>	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

14. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

15. For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
<b>All</b>	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted, the policy is created faster when you select this option.



Option	Description
<b>Address List</b>	Specifies networks to consider safe. Fill in the <b>IP Address</b> and <b>Netmask</b> fields, then click <b>Add</b> . This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

16. If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.

17. If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.

18. Click **Next**.

The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.

19. Click **Finish** to create the security policy.

The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM™ creates the virtual server with an HTTP profile, and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

---

***Tip:** This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.*

---

## Creating login pages

In your security policy, you can create a login page to specify a login URL that presents a site that users must pass through to gain access to the web application. The login URL commonly leads to the login page of the web application.

1. On the Main tab, click **Security > Application Security > Sessions and Logins**.  
The Login Pages List screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Click **Create**.  
The New Login Page screen opens.
4. For the **Login URL** setting, specify a URL that users must pass through to get to the application.
  - a) From the list, select the type of URL: **Explicit** or **Wildcard**.
  - b) Select either **HTTP** or **HTTPS** based on the type of traffic the web application accepts.
  - c) Type an explicit URL or wildcard expression in the field.

When you click in the field, the system lists URLs that it has seen, and you can select a URL from the list. Or, you can type explicit URLs in the format `/login`, and wildcard URLs without the slash, such as `*.php`.

- From the **Authentication Type** list, select the method the web server uses to authenticate the login URL's credentials with a web user.

Option	Description
<b>None</b>	The web server does not authenticate users trying to access the web application through the login URL. This is the default setting.
<b>HTML Form</b>	The web application uses a form to collect and authenticate user credentials. If using this option, you also need to type the user name and password parameters written in the code of the HTML form.
<b>HTTP Basic Authentication</b>	The user name and password are transmitted in Base64 and stored on the server in plain text.
<b>HTTP Digest Authentication</b>	The web server performs the authentication; user names and passwords are not transmitted over the network, nor are they stored in plain text.
<b>NTLM</b>	Microsoft LAN Manager authentication (also called Integrated Windows Authentication) does not transmit credentials in plain text, but requires a continuous TCP connection between the server and client.

- In the Access Validation area, define at least one validation criteria for the login page response.  
If you define more than one validation criteria, the response must meet all the criteria before the system allows the user to access the application login URL.

---

***Note:** The system checks the access validation criteria on the response of the login URL only if the response has one of the following content-types: `text/html`, `text/xml`, `application/sgml`, `application/xml`, `application/html`, `application/xhtml`, `application/x-asp`, and `application/x-aspix`.*

---

- Click **Create** to add the login page to the security policy.  
The new login page is added to the login pages list.
- Add as many login pages as needed for your web application.
- In the editing context area, click **Apply Policy** to put the changes into effect.

The security policy now has one or more login pages associated with it.

You can now configure how the login pages are enforced, including the authentication URLs, logout URLs, and whether or not the login pages have time limits.

## Enforcing login pages

Login enforcement settings prevent forceful browsing attacks where attackers gain access to restricted parts of the web application by supplying a URL directly. You can use login enforcement to force users to pass through one URL (known as the *login URL*) before being allowed to display a different URL (known as the *target URL*) where they can access restricted pages and resources. Login enforcement settings specify how the security policy enforces login pages including the expiration time, authenticated URLs, and logout URLs. You can also use authenticated URLs to enforce idle time-outs on applications that are missing this functionality.

- On the Main tab, click **Security > Application Security > Sessions and Logins > Login Enforcement**.  
The Login Enforcement screen opens.

2. If you want the login URL to be valid for a limited time, set **Expiration Time** to **Enabled**, and type a value, in seconds.
3. For the **Authenticated URLs** setting, specify the target URLs that users can access only by way of the login URL:
  - a) In the **Authenticated URLs** field, type the target URL name in the format `/private.php` (wildcards are allowed).
  - b) Click **Add** to add the URL to the list of authenticated URLs.
  - c) Repeat to add as many authenticated URLs as needed.
4. Optionally, use the **Logout URLs** setting to specify the URLs used to log out of the web application:
  - a) In the **Logout URLs** field, type the URL in the format `/logout.html` (explicit URLs only).
  - b) Click **Add**.
  - c) Repeat to add as many logout URLs as needed.
5. Click **Save** to save your settings.
6. To put the security policy changes into effect immediately, click **Apply Policy**.

If you specify authenticated URLs and a user tries to bypass them, the system issues the `Login URL bypassed` violation. If a user session is idle and exceeds the expiration time, the system now issues the `Login URL expired` violation, and the user can no longer reach the authenticated URLs. For both login violations, if the enforcement mode is blocking, the system now sends the Login Page Response to the client (see **Application Security > Blocking > Response Pages**).

## Configuring a database security server

To integrate Application Security Manager™ (ASM) with a third-party database security product, you need to configure the database security server on ASM™. You can configure one database security server per system.

1. On the Main tab, click **Security > Options > Application Security > Integrated Services > Database Security**.  
The Database Security screen opens.
2. Specify the database security server by typing either its **Server Host Name** or its **Server IP Address**.  
Only one of the two fields is required.

---

***Note:** If using SSL to establish a secured session between the BIG-IP® system and the database security server, type the IP address of a virtual server configured for the secure connection. The virtual server uses any open IP address for the destination, the IBM Guardium port (16016, by default) for the service port, `serverssl` or a customized profile for the **SSL Profile (Server)** setting, and specifies a default pool (containing one member, the database security server, using its IP address and service port, typically, 16016).*

---

3. For **Server Port Number**, type the port number of the database server.  
The default value is 16016, the port used by IBM® InfoSphere® Guardium.®
4. If you want the system to wait for an ACK response from the database security server before sending the request to the application server, from the **Request Hold Timeout** list, select **Enabled** and type the number of milliseconds to wait for the response.  
The default value is 5 milliseconds.

When this setting is enabled, the system forwards the request to the application server as soon as the database security server sends an ACK, or when the timeout has passed. If you leave this setting disabled, the system forwards the request to the application server immediately.

**5. Click **Save**.**

The system saves the configuration settings.

The Application Security Manager is now configured to connect to the database security server.

For ASM to forward request data to the database security server, you next need to enable database security integration in one or more security policies.

## Enabling database security integration in a security policy

Before you can enable database security integration, you need to have created a security policy to protect your web application. For the policy to retrieve the user names of those making requests, you need to create login pages in Application Security Manager™ (ASM).

You enable database security integration in a security policy so that Application Security Manager (ASM™) forwards request information to a third-party database server.

1. On the Main tab, click **Security > Application Security > Integrated Services > Database Security**. The Database Security screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select the **Database Security Integration** check box.
4. For **User Source**, select **Use Login Pages** to have the system use an ASM login page to determine the user source.

If there is no login page configured in the security policy, click the login pages link to open a popup screen where you can add one.

**5. Click **Save**.**

The system saves the configuration settings.

The Application Security Manager connects to the database security server and can forward request data about traffic to it.

## Implementation result

---

You have set up a BIG-IP® system to use Application Security Manager™ (ASM) to secure application traffic and use login pages to check user credentials.

Client traffic is routed to the virtual server for the web application. ASM™ analyzes the request and checks for security violations. ASM also verifies user credentials on the login page and sends the database security server a request notification. When ASM receives an acknowledgment from the database security server or the request hold timeout is over, ASM forwards traffic that meets the security policy requirements to the application.

The database security server includes the application and user information provided by ASM, so it can be viewed in logs and reports on that system. The database security server can perform a more in-depth security assessment of the web request.

If you want to review reports and event logs that associate the user name with the session information on the BIG-IP system, you can set up session tracking (by enabling session awareness). When session awareness is enabled, you can see the user names on the Event Logs: Application: Requests screen in the General Details section of specific requests. In addition, the Reporting: Application: Charts screen displays the users who sent the illegal requests.



---

# Chapter

# 46

---

## Integrating ASM and APM with Database Security Products

---

- *Overview: Integrating ASM and APM with database security products*
- *Prerequisites for integrating ASM and APM with database security*
- *Implementation result*

## Overview: Integrating ASM and APM with database security products

You can deploy Application Security Manager™ (ASM) and Access Policy Manager® (APM®) with database security products, such as IBM® InfoSphere® Guardium® to increase security visibility, receive alerts about suspicious activity, and prevent attacks. When integrated with database security, ASM™ can provide information about each HTTP request and database query. This allows the database security system to correlate the web transaction with the database query to make a security assessment of the transaction. ASM also provides application level details to improve the database security system's logging and reporting.

For you to integrate ASM with a database security product, the database security server itself must have been configured and accessible on the network. On the BIG-IP® system, you specify the host name or IP address of the database security server. Then, you enable database security integration for one or more security policies that are set up to protect web application resources.

When using database security, Application Security Manager monitors web application traffic and sends information about the users, the requests, and reporting events to the database security server. The following figure shows an example of how ASM can integrate with the IBM InfoSphere Guardium Database Activity Monitoring Appliance.

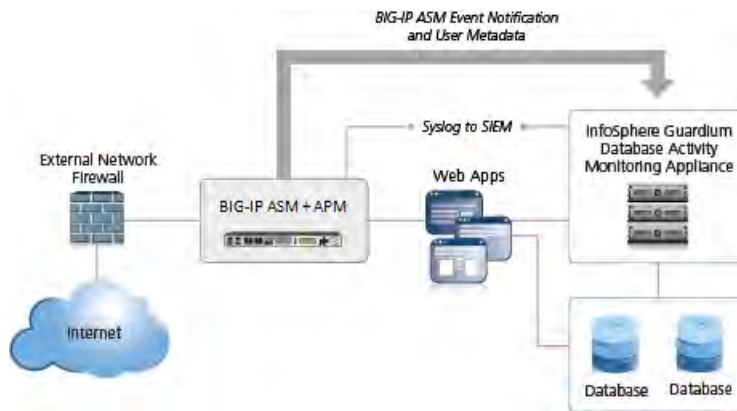


Figure 14: Integrating ASM and APM with external database security example

The security policy can get user names from requests using login pages configured from within ASM, or the policy can retrieve the user names from Access Policy Manager® (APM). This implementation describes how to integrate ASM and APM™ with an external database security server. APM handles user authentication in this case and provides the information that is sent to the database security server.

## Prerequisites for integrating ASM and APM with database security

In order to integrate a database security server from within Application Security Manager™ (ASM™) so that the security policy retrieves the user names from Access Policy Manager® (APM®), you need to perform basic these system configuration tasks according to the needs of your networking configuration:

- Run the setup utility and create a management IP address.
- License and provision ASM, APM, and Local Traffic Manager™ (LTM®).
- Configure a DNS address (**System > Configuration > Device > DNS**).
- Configure an NTP server (**System > Configuration > Device > NTP**).
- Restart ASM (at the command line, type `tmsh restart /sys service asm`).



**Task Summary***Creating a VLAN**Creating a self IP address for a VLAN**Creating a local traffic pool for application security**Creating a virtual server to manage HTTPS traffic**Creating a security policy automatically**Creating an access profile**Configuring an access policy**Adding the access profile to the virtual server**Configuring a database security server**Enabling database security integration with ASM and APM***Creating a VLAN**

VLANs represent a collection of hosts that can share network resources, regardless of their physical location on the network. You create a VLAN to associate physical interfaces with that VLAN.

1. On the Main tab, click **Network > VLANs**.  
The VLAN List screen opens.
2. Click **Create**.  
The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting, click an interface number from the **Available** list, and use the Move button to add the selected interface to the **Untagged** list. Repeat this step as necessary.
5. Click **Finished**.  
The screen refreshes, and displays the new VLAN from the list.

**Creating a self IP address for a VLAN**

Ensure that you have at least one VLAN configured before you create a self IP address.

Self IP addresses enable the BIG-IP® system, and other devices on the network, to route application traffic through the associated VLAN.

1. On the Main tab, click **Network > Self IPs**.  
The Self IPs screen opens.
2. Click **Create**.  
The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type an IPv4 or IPv6 address.  
This IP address should represent the address space of the VLAN that you specify with the **VLAN/Tunnel** setting.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address.
  - On the internal network, select the VLAN that is associated with an internal interface or trunk.
  - On the external network, select the VLAN that is associated with an external interface or trunk.
7. Use the default values for all remaining settings.

8. Click **Finished**.

The screen refreshes, and displays the new self IP address.

The BIG-IP system can now send and receive TCP/IP traffic through the specified VLAN.

### Creating a local traffic pool for application security

You can use a local traffic pool with Application Security Manager™ system to forward traffic to the appropriate resources.

---

***Note:** You can optionally create a pool as part of creating a security policy using the Deployment wizard.*

---

1. On the Main tab, click **Local Traffic > Pools**.  
The Pool List screen opens.
2. Click **Create**.  
The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, for the **New Members** setting, add to the pool the application servers that host the web application:
  - a) Type an IP address in the **Address** field.
  - b) In the **Service Port** field, type a port number (for example, type 80 for the HTTP service), or select a service name from the list.
  - c) Click **Add**.
5. Click **Finished**.

The BIG-IP® system configuration now includes a local traffic pool containing the resources that you want to protect using Application Security Manager™.

### Creating a virtual server to manage HTTPS traffic

You can create a virtual server to manage HTTPS traffic.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the **Create** button.  
The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type 443 or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select **clientssl**, and using the Move button, move the name to the **Selected** list.
9. (Optional) From the **SSL Profile (Server)** list, select **serverssl**.

---

***Note:** This setting ensures that there is an SSL connection between the HTTP virtual server and the external HTTPS server.*

---

10. From the **Source Address Translation** list, select **Auto Map**.
11. From the **Default Pool** list, select the pool that is configured for application security.
12. Click **Finished**.

The HTTPS virtual server appears in the Virtual Server List screen.

## Creating a security policy automatically

Before you can create a security policy, you must perform the minimal system configuration tasks including defining a VLAN, a self IP address, and other tasks required according to the needs of your networking environment.

Application Security Manager™ can automatically create a security policy that is tailored to secure your web application.

1. On the Main tab, click **Security > Application Security > Security Policies**.  
The Active Policies screen opens.
2. Click the **Create** button.  
The Deployment wizard opens to the Select Local Traffic Deployment Scenario screen.
3. For the **Local Traffic Deployment Scenario** setting, specify a virtual server to use for the security policy.
  - To secure an existing virtual server that has no security policy associated with it, select **Existing Virtual Server** and click **Next**.
  - To create a new virtual server and pool with basic configuration settings, select **New Virtual Server** and click **Next**.
  - To create an active but unused security policy, select **Do not associate with Virtual Server** and click **Next**. No traffic will go through this security policy until you associate it with a virtual server. The Policy Builder cannot begin automatically creating a policy until traffic is going to ASM through the virtual server.

The virtual server represents the web application you want to protect.

The Configure Local Traffic Settings screen opens.

4. Configure the new or existing virtual server, and click **Next**.
  - If creating a new virtual server, specify the protocol, name, IP address and port, pool IP address, and port.
  - If using an existing virtual server, it must have an HTTP profile and cannot be associated with a local traffic policy.
  - If you selected **Do not associate with Virtual Server**, you will have to manually associate the security policy with a virtual server at a later time. On the policy properties screen, you need to specify a name for the security policy.

The name of the new or existing virtual server becomes the name of the security policy.

The Select Deployment Scenario screen opens.

5. For **Deployment Scenario**, select **Create a policy automatically** and click **Next**.  
The Configure Security Policy Properties screen opens.
6. From the **Application Language** list, select the language encoding of the application, or select **Auto detect** and let the system detect the language.

---

**Important:** You cannot change this setting after you have created the security policy.

---

7. If the application is not case-sensitive, clear the **Security Policy is case sensitive** check box. Otherwise, leave it selected.
- 

**Important:** You cannot change this setting after you have created the security policy.

---

8. If you do not want the security policy to distinguish between HTTP and HTTPS URLs, clear the **Differentiate between HTTP and HTTPS URLs** check box. Otherwise, leave it selected.
9. Click **Next**.  
The Configure Attack Signatures screen opens.
10. To configure attack signatures, move the systems used by your web application from the **Available Systems** list into the **Assigned Systems** list.  
The system adds the attack signatures needed to protect the selected systems.
11. For the **Signature Staging** setting, verify that the default option **Enabled** is selected.
- 

**Note:** Because the Real Traffic Policy Builder<sup>®</sup> begins building the security policy in Blocking mode, you can keep signature staging enabled to make sure that false positives do not occur.

---

New and updated attack signatures remain in staging for 7 days, and are not enforced (according to the learn, alarm, and block flags) during that time.

12. Click **Next**.  
The Configure Automatic Policy Building screen opens.
13. For **Policy Type**, select an option to determine the security features to include in the policy.

Option	Description
<b>Fundamental</b>	Creates a security policy enforcing HTTP protocol compliance, evasion techniques, explicit file types (including length checks), explicit parameters in selective mode at the global level, attack signatures, the violation Request Length Exceeds Defined Buffer Size, host names, header lengths, cookie lengths, the violation Failed to Convert Character, and learn explicit redirection domains.
<b>Enhanced</b>	Creates a security policy with all the elements of the Fundamental policy type; also checks for explicit URLs in selective mode plus meta characters, Explicit parameter length checks in selective mode at the global level, methods, explicit cookies, and content profiles.
<b>Comprehensive</b>	Creates a security policy with all the elements of the Enhanced policy type; also checks for explicit URLs and meta characters, explicit parameters and lengths at the URL level, parameter meta characters, and dynamic parameters.

A bulleted list on the screen describes which security features are included in each type.

14. For **Rules**, move the slider to set the Policy Builder learning speed.

Option	Description
<b>Fast</b>	Use if your application supports a small number of requests from a small number of sessions; for example, useful for web sites with less traffic. However, choosing this option may present a greater chance of adding false entities to the security policy.
<b>Medium</b>	Use if your application supports a medium number of requests, or if you are not sure about the amount of traffic on the application web site. This is the default setting.
<b>Slow</b>	Use if your application supports a large number of requests from many sessions; for example, useful for web sites with lots of traffic. This option creates the most accurate security policy, but takes Policy Builder longer to collect the statistics.

Based on the option you select, the system sets greater or lesser values for the number of different user sessions, different IP addresses, and length of time before it adds to the security policy and enforces the elements.

15. For **Trusted IP Addresses**, select which IP addresses to consider safe:

Option	Description
<b>All</b>	Specifies that the policy trusts all IP addresses. For example, if the traffic is in a corporate lab or preproduction environment where all of the traffic is trusted, the policy is created faster when you select this option.
<b>Address List</b>	Specifies networks to consider safe. Fill in the <b>IP Address</b> and <b>Netmask</b> fields, then click <b>Add</b> . This option is typically used in a production environment where traffic could come from untrusted sources. The IP Address can be either an IPv4 or an IPv6 address.

If you leave the trusted IP address list empty, the system treats all traffic as untrusted. In general, it takes more untrusted traffic, from different IP addresses, over a longer period of time to build a security policy.

16. If you want the security policy to automatically detect JSON and XML protocols, select the **JSON/XML payload detection** check box.

If requests contain legitimate XML or JSON data, the Policy Builder creates content profiles in the security policy according to the data it detects.

17. If you want to display a response page when an AJAX request does not adhere to the security policy, select the **AJAX blocking response behavior** check box.

18. Click **Next**.

The Security Policy Configuration Summary opens where you can review the settings to be sure they are correct.

19. Click **Finish** to create the security policy.

The Automatic Policy Building Status screen opens where you can view the current state of the security policy.

ASM™ creates the virtual server with an HTTP profile, and on the Security tab, **Application Security Policy** is enabled and associated with the security policy you created. A local traffic policy is also created and by default sends all traffic for the virtual server to ASM. The Policy Builder automatically begins examining the traffic to the web application and building the security policy (unless you did not associate a virtual server). The system sets the enforcement mode of the security policy to Blocking, but it does not block requests until the Policy Builder processes sufficient traffic, adds elements to the security policy, and enforces the elements.

---

**Tip:** This is a good point at which to test that you can access the application being protected by the security policy and check that traffic is being processed by the BIG-IP® system.

---

## Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy > Access Profiles**.  
The Access Profiles List screen opens.
2. Click **Create**.  
The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.
4. From the **Profile Type** list, select one:

- **APM-LTM** - Select for a web access management configuration.
- **SSO** - Select only when you do not need to configure an access policy.
- **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
- **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
- **SSL-VPN** - Select for other types of access, such as network access, portal access, application access. (Most access policy items are available for this type.)
- **ALL** - Select for any type of access.

Additional settings display.

5. To configure timeout and session settings, select the **Custom** check box.
6. In the **Inactivity Timeout** field, type the number of seconds that should pass before the access policy times out. Type 0 to set no timeout.  
If there is no activity (defined by the **Session Update Threshold** and **Session Update Window** settings in the Network Access configuration) between the client and server within the specified threshold time, the system closes the current session.
7. In the **Access Policy Timeout** field, type the number of seconds that should pass before the access profile times out because of inactivity.  
Type 0 to set no timeout.
8. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.  
Type 0 to set no timeout.
9. In the **Max Concurrent Users** field, type the maximum number of users that can use this access profile at the same time.  
Type 0 to set no maximum.
10. In the **Max Sessions Per User** field, type the maximum number of concurrent sessions that one user can start.  
Type 0 to set no maximum.
11. In the **Max In Progress Sessions Per Client IP** field, type the maximum number of concurrent sessions that one client IP address can support.  
Type 0 to set no maximum.
12. Select the **Restrict to Single Client IP** check box to restrict the current session to a single IP address.  
This setting associates the session ID with the IP address.  
Upon a request to the session, if the IP address has changed the request is redirected to a logout page, the session ID is deleted, and a log entry is written to indicate that a session hijacking attempt was detected. If such a redirect is not possible, the request is denied and the same events occur.
13. To configure logout URIs, in the Configurations area, type each logout URI in the **URI** field, and then click **Add**.
14. In the **Logout URI Timeout** field, type the delay in seconds before logout occurs for the customized logout URIs defined in the **Logout URI Include** list.
15. To configure SSO:
  - For users to log in to multiple domains using one SSO configuration, skip the settings in the SSO Across Authentication Domains (Single Domain mode) area. You can configure SSO for multiple domains only after you finish the initial access profile configuration.
  - For users to log in to a single domain using an SSO configuration, configure settings in the SSO Across Authentication Domains (Single Domain mode) area, or you can configure SSO settings after you finish the initial access profile configuration.
16. In the **Domain Cookie** field, specify a domain cookie, if the application access control connection uses a cookie.

17. In the **Cookie Options** setting, specify whether to use a secure cookie.
  - If the policy requires a secure cookie, select the **Secure** check box to add the **secure** keyword to the session cookie.
  - If you are configuring an LTM access scenario that uses an HTTPS virtual server to authenticate the user and then sends the user to an existing HTTP virtual server to use applications, clear this check box.
18. If the access policy requires a persistent cookie, in the **Cookie Options** setting, select the **Persistent** check box.
 

This sets cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent; but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value will be used to set the persistent cookie expiration.
19. From the **SSO Configurations** list, select an SSO configuration.
20. In the Language Settings area, add and remove accepted languages, and set the default language.
 

A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
21. Click **Finished**.

The access profile appears in the Access Profiles List.

To add an SSO configuration for multiple domains, click **SSO / Auth Domains** on the menu bar. To provide functionality with an access profile, you must configure the access policy. The default access policy for a profile denies all traffic and contains no actions. Click **Edit** in the **Access Policy** column to edit the access policy.

## Configuring an access policy

You configure an access policy to provide authentication, endpoint checks, and resources for an access profile. This procedure configures a simple access policy that adds a logon page, gets user credentials, submits them to an authentication type of your choice, then allows authenticated users, and denies others.

1. On the Main tab, click **Access Policy > Access Profiles**.  
The Access Profiles List screen opens.
2. Click the name of the access profile you want to edit.
3. On the menu bar, click **Access Policy**.
4. For the **Visual Policy Editor** setting, click the **Edit access policy for Profile *policy\_name*** link.  
The visual policy editor opens the access policy in a separate window or tab.
5. Click the (+) icon anywhere in the access policy to add a new action item.  
A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. On the Logon tab, select **Logon Page** and click the **Add Item** button.  
The Logon Page Agent properties screen opens.
7. Click **Save**.  
The Access Policy screen reopens.
8. On the rule branch, click the plus sign (+) between **Logon Page** and **Deny**.
9. Set up the appropriate authentication and client-side checks required for application access at your company, and click **Add Item**.

10. Change the Successful rule branch from **Deny** to **Allow** and click the **Save** button.
11. If needed, configure further actions on the successful and fallback rule branches of this access policy item, and save the changes.
12. At the top of the screen, click the **Apply Access Policy** link to apply and activate your changes to this access policy.
13. Click the **Close** button to close the visual policy editor.

### Adding the access profile to the virtual server

Before you can perform this task, you need to create an access profile using Access Policy Manager™.

You associate the access profile with the virtual server created for the web application that Application Security Manager™ is protecting.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server that manages the network resources for the web application you are securing.
3. In the Access Policy area, from the **Access Profile** list, select the access profile.
4. Click **Update**.

Your access policy is now associated with the virtual server.

### Configuring a database security server

To integrate Application Security Manager™ (ASM) with a third-party database security product, you need to configure the database security server on ASM™. You can configure one database security server per system.

1. On the Main tab, click **Security > Options > Application Security > Integrated Services > Database Security**.  
The Database Security screen opens.
2. Specify the database security server by typing either its **Server Host Name** or its **Server IP Address**.  
Only one of the two fields is required.

---

***Note:** If using SSL to establish a secured session between the BIG-IP® system and the database security server, type the IP address of a virtual server configured for the secure connection. The virtual server uses any open IP address for the destination, the IBM Guardium port (16016, by default) for the service port, `serverssl` or a customized profile for the **SSL Profile (Server)** setting, and specifies a default pool (containing one member, the database security server, using its IP address and service port, typically, 16016).*

---

3. For **Server Port Number**, type the port number of the database server.  
The default value is 16016, the port used by IBM® InfoSphere® Guardium.®
4. If you want the system to wait for an ACK response from the database security server before sending the request to the application server, from the **Request Hold Timeout** list, select **Enabled** and type the number of milliseconds to wait for the response.  
The default value is 5 milliseconds.



When this setting is enabled, the system forwards the request to the application server as soon as the database security server sends an ACK, or when the timeout has passed. If you leave this setting disabled, the system forwards the request to the application server immediately.

**5. Click **Save**.**

The system saves the configuration settings.

The Application Security Manager is now configured to connect to the database security server.

For ASM to forward request data to the database security server, you next need to enable database security integration in one or more security policies.

## Enabling database security integration with ASM and APM

Before you can enable database security integration, you need to have created a security policy to protect your web application. For the policy to retrieve the user names of those making requests, you need to have set up Access Policy Manager® (APM®) on the BIG-IP® system.

You enable database security integration in a security policy so that Application Security Manager™ (ASM) forwards request information to a third-party database server.

1. On the Main tab, click **Security > Application Security > Integrated Services > Database Security**. The Database Security screen opens.
2. In the **Current edited policy** list near the top of the screen, verify that the edited security policy is the one you want to work on.
3. Select the **Database Security Integration** check box.
4. For **User Source**, select **Use APM Usernames and Session ID**.  
The system uses Access Policy Manager (APM) user names and session ID to determine the user source. You can choose this option only if you have APM licensed and provisioned.
5. Click **Save**.  
The system saves the configuration settings.

The Application Security Manager connects to the database security server and can forward request data to it.

## Implementation result

---

You have set up a BIG-IP® system to use Application Security Manager™ (ASM) to secure application traffic, and Access Policy Manager™ (APM) to check user credentials.

Client traffic is routed to the virtual server for the web application. At first, traffic is handled by the APM module. APM® verifies user credentials and allows those with valid credentials to use web application. APM also sends user names and session IDs of valid users to ASM™. After that, ASM checks for security violations and forwards traffic that meets the security policy requirements to the backend server.

The database security server includes the application and user information provided by ASM and APM, so it can be viewed in logs and reports on that system. The database security server can perform a more in depth security assessment of the web request.

If you want to review reports and event logs that associate the user name with the session information on the BIG-IP system, you can set up session tracking (by enabling session awareness). When session awareness is enabled, you can see the user names on the Event Logs: Application: Requests screen in the General

Details section of specific requests. IN addition, the Reporting: Application: Charts screen displays the users who sent the illegal requests.

---

# Chapter 47

---

## Securing FTP Traffic Using the Default Configuration

---

- *Overview: Securing FTP traffic using default values*

### Overview: Securing FTP traffic using default values

---

This implementation describes how to secure FTP traffic the easy way--by using default values. When you use an FTP security profile, the BIG-IP® system inspects FTP traffic for network vulnerabilities. A default FTP security profile is included in the system that you can use. To activate security checks for FTP traffic, you enable protocol security in an FTP service profile, and associate the service profile with a virtual server.

You can use the default configuration to protect against the following FTP security risks:

- Port scanning exploits
- Anonymous FTP requests
- Command line length exceeds the defined length
- Potentially dangerous FTP commands
- Traffic that fails FTP protocol compliance checks
- Brute force attacks (due to excessive FTP login attempts)
- File stealing exploits

#### Task summary

*Creating an FTP service profile with security enabled*

*Enabling protocol security for an FTP virtual server*

*Reviewing violation statistics for security profiles*

### Creating an FTP service profile with security enabled

The easiest method for initiating FTP protocol security for your FTP virtual server traffic is to use the system default settings. You do this by enabling protocol security for the system-supplied FTP service profile, and then associating that service profile with a virtual server.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **FTP**.  
The FTP profile list screen opens.
2. In the **Name** column, click **ftp**.  
The Properties screen for the system-supplied FTP profile opens.
3. In the Settings area, clear the **Translate Extended** check box, if you want to disable IPv6 translation.
4. Leave the **Data Port** setting at the default value, **20**.
5. Select the **Protocol Security** check box to enable FTP security checks.
6. Click **Update**.

You now have a security-enabled service profile that you can associate with a virtual server so that FTP protocol checks are performed on the traffic that the FTP virtual server receives.

### Enabling protocol security for an FTP virtual server

When you enable protocol security for an FTP virtual server, the system scans any incoming FTP traffic for vulnerabilities before the traffic reaches the FTP servers.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the **Create** button.

The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.

The IP address you type must be available and not in the loopback network.

5. In the **Service Port** field, type 21 or select **FTP** from the list.
6. In the Configuration area, for the **FTP Profile** setting, select the default profile, `ftp`.
7. From the **Source Address Translation** list, select **Auto Map**.
8. For the **Default Pool** setting, either select an existing pool from the list, or click the Create (+) button and create a new pool.
9. Click **Finished**.

The custom FTP virtual server appears in the Virtual Servers list.

## Reviewing violation statistics for security profiles

You can view statistics and transaction information for each security profile that triggers security violations.

1. On the Main tab, click **Security > Event Logs > Protocol** and click **HTTP**, **FTP**, **SMTP**, or **DNS**. The appropriate statistics screen opens listing all violations for that protocol, with the number of occurrences.
2. Type a Support ID, if you have one, to filter the violations and view one in particular.
3. Click a violation's hyperlink to see details about the requests causing the violation.

On the Statistics screen, in the left column, you can review information regarding the traffic volume for each security profile configured.



---

# Chapter 48

---

## Securing FTP Traffic Using a Custom Configuration

---

- *Overview: Securing FTP traffic using a custom configuration*
-

## Overview: Securing FTP traffic using a custom configuration

---

This implementation describes how to secure FTP traffic using a custom configuration. When you use an FTP security profile, the BIG-IP® system inspects FTP traffic for network vulnerabilities. A default FTP security profile is included in the system that you can modify, or you can create a new one as described in the tasks included here. To activate security checks for FTP traffic, you enable protocol security in an FTP service profile, and associate the service profile with a virtual server.

You can customize an FTP security profile to generate alarms or block requests for the following FTP security risks:

- Port scanning exploits
- Anonymous FTP requests
- Command line length exceeds the defined length
- Specific FTP commands
- Traffic that fails FTP protocol compliance checks
- Brute force attacks (excessive FTP login attempts)
- File stealing exploits

### Task summary

*Creating a custom FTP profile for protocol security*

*Creating a security profile for FTP traffic*

*Modifying associations between service profiles and security profiles*

*Configuring an FTP virtual server with a server pool*

*Reviewing violation statistics for security profiles*

## Creating a custom FTP profile for protocol security

You create a custom FTP profile when you want to fine-tune the way that the BIG-IP® system manages FTP traffic. This procedure creates an FTP service profile that optimizes FTP traffic in the LAN, and enables Protocol Security in the profile so it can scan for vulnerabilities specific to the protocol.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **FTP**.  
The FTP profile list screen opens.
2. Click **Create**.  
The New FTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select the default **ftp** profile.
5. Select the **Custom** check box.
6. In the Settings area, clear the **Translate Extended** check box, if you want to disable IPv6 translation.
7. For the **Inherit Parent Profile** setting, select the check box.  
This optimizes data channel traffic.
8. Leave the **Data Port** setting at the default value, **20**.
9. Select the **Protocol Security** check box to enable FTP security checks.
10. Click **Finished**.

The custom FTP profile now appears in the FTP profile list screen.



## Creating a security profile for FTP traffic

An *FTP security profile* provides security checks that are applicable to the FTP protocol. You can create an FTP profile that specifies whether the system allows, logs, or blocks commands and requests from servers that use the FTP protocol.

1. On the Main tab, click **Security > Protocol Security > Security Profiles > FTP**.  
The Security Profiles: FTP screen opens.
2. Click the **Create** button.  
The New FTP Security Profile screen opens.
3. In the **Profile Name** field, type a unique name for the profile.
4. In the Defense Configuration area, modify the blocking policy settings for each violation.  
If you do not enable either **Alarm** or **Block** for a violation, the system does not perform the corresponding security check.

Option	Description
<b>Alarm</b>	The system logs any requests that trigger the violation.
<b>Block</b>	The system blocks any requests that trigger the violation.
<b>Alarm and Block</b>	The system both logs and blocks any requests that trigger the violation.

5. Click **Create**.  
The screen refreshes, and you see the new security profile in the list.

The BIG-IP® system automatically assigns this service profile to FTP traffic that a designated virtual server receives.

## Modifying associations between service profiles and security profiles

Before you can modify associations between service profiles and security profiles, you must have created at least one security profile.

When you enable the **Protocol Security** setting on an FTP, HTTP, or SMTP service profile, the system automatically assigns the first-listed security profile to the service profile you configured for that profile. You can review and modify the current associations between the service profiles and the security profiles for each protocol.

1. On the Main tab, click **Security > Protocol Security > Profiles Assignment**.  
The Profiles Assignment: HTTP screen opens.
2. From the Profiles Assignment menu, select the service profile type, if different from HTTP.
3. For each traffic profile, select the protocol security profile to use from the list in the Assigned Security Profile column.
4. Click **Save**.

## Configuring an FTP virtual server with a server pool

You can configure a local traffic virtual server and a default pool for your network's FTP servers.

1. On the Main tab, click **Local Traffic > Virtual Servers**.

The Virtual Server List screen opens.

2. Click the **Create** button.  
The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select the type, and type an address, or an address and mask, as appropriate for your network.
5. In the **Service Port** field, type 21 or select **FTP** from the list.
6. From the **FTP Profile** list, select either **ftp** or a custom profile.
7. From the **Source Address Translation** list, select **Auto Map**.
8. In the Resources area of the screen, for the **Default Pool** setting, click the **Create (+)** button.  
The New Pool screen opens.
9. In the **Name** field, type a unique name for the pool.
10. In the Resources area, for the **New Members** setting, select the type of new member you are adding, then type the appropriate information in the **Node Name**, **Address**, and **Service Port** fields, and click **Add** to add as many pool members as you need.
11. Click **Finished** to create the pool.  
The screen refreshes, and reopens the New Virtual Server screen. The new pool name appears in the **Default Pool** list.
12. Click **Finished** to create the virtual server.  
The screen refreshes, and you see the new virtual server in the list.

The custom FTP virtual server appears in the Virtual Servers list.

## Reviewing violation statistics for security profiles

You can view statistics and transaction information for each security profile that triggers security violations.

1. On the Main tab, click **Security > Event Logs > Protocol** and click **HTTP**, **FTP**, **SMTP**, or **DNS**.  
The appropriate statistics screen opens listing all violations for that protocol, with the number of occurrences.
2. Type a Support ID, if you have one, to filter the violations and view one in particular.
3. Click a violation's hyperlink to see details about the requests causing the violation.  
On the Statistics screen, in the left column, you can review information regarding the traffic volume for each security profile configured.

---

# Chapter

# 49

---

## Securing SMTP Traffic Using the Default Configuration

---

- *Overview: Securing SMTP traffic using system defaults*
-

## Overview: Securing SMTP traffic using system defaults

---

This implementation describes how to secure SMTP traffic using system defaults. When you create an SMTP security profile, the BIG-IP® Advanced Firewall Manager™ (AFM) provides several security checks for requests sent to a protected SMTP server. When you enable a security check, the system either generates an alarm for, or blocks, any requests that trigger the security check.

You can configure the SMTP security profile to include the following checks:

- Verify SMTP protocol compliance, as defined in RFC 2821.
- Validate incoming mail using several criteria.
- Inspect email and attachments for viruses.
- Apply rate limits to the number of messages.
- Validate DNS SPF records.
- Prevent directory harvesting attacks.
- Disallow or allow some of the SMTP methods, such as VRFY, EXPN, and ETRN, that spam senders typically use to attack mail servers.
- Reject the first message from a sender, because legitimate senders retry sending the message, and spam senders typically do not. This process is known as *greylisting*. The system does not reject subsequent messages from the same sender to the same recipient.

### Task Summary

*Creating an SMTP service profile with security enabled*

*Creating an SMTP virtual server with protocol security*

*Reviewing violation statistics for security profiles*

## Creating an SMTP service profile with security enabled

The easiest method for initiating SMTP protocol security for your SMTP virtual server traffic is to use the system default settings. You do this by enabling protocol security for the system-supplied SMTP service profile, and then associating that service profile with a virtual server.

1. On the Main tab, click **Local Traffic > Profiles > Services > SMTP**.  
The SMTP profile list screen opens.
2. In the **Name** column, click **smtp**.  
The Properties screen for the system-supplied SMTP profile opens.
3. Select the **Protocol Security** check box to enable SMTP security checks.
4. Click **Update**.

You now have a security-enabled service profile that you can associate with a virtual server so that SMTP protocol checks are performed on the traffic that the SMTP virtual server receives.

## Creating an SMTP virtual server with protocol security

When you enable protocol security for an SMTP virtual server, the system scans any incoming SMTP traffic for vulnerabilities before the traffic reaches the SMTP servers.

1. On the Main tab, click **Local Traffic > Virtual Servers**.

The Virtual Server List screen opens.

2. Click the **Create** button.

The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.

4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.

The IP address you type must be available and not in the loopback network.

5. In the **Service Port** field, type 25 or select **SMTP** from the list.

6. In the Configuration area, for the **SMTP Profile** setting, select the default profile, `smtp`.

7. From the **Source Address Translation** list, select **Auto Map**.

8. For the **Default Pool** setting, either select an existing pool from the list, or click the Create (+) button and create a new pool.

9. Click **Finished**.

The custom SMTP virtual server appears in the Virtual Servers list.

## Reviewing violation statistics for security profiles

You can view statistics and transaction information for each security profile that triggers security violations.

1. On the Main tab, click **Security > Event Logs > Protocol** and click **HTTP**, **FTP**, **SMTP**, or **DNS**.

The appropriate statistics screen opens listing all violations for that protocol, with the number of occurrences.

2. Type a Support ID, if you have one, to filter the violations and view one in particular.

3. Click a violation's hyperlink to see details about the requests causing the violation.

On the Statistics screen, in the left column, you can review information regarding the traffic volume for each security profile configured.



---

# Chapter

# 50

---

## Securing SMTP Traffic Using a Custom Configuration

---

- *Overview: Creating a custom SMTP security profile*
-

## Overview: Creating a custom SMTP security profile

---

This implementation describes how to secure SMTP traffic. When you create an SMTP security profile, the system provides several security checks for requests sent to a protected SMTP server. When you enable a security check, the system either generates an alarm for, or blocks, any requests that trigger the security check.

You can configure the SMTP security profile to include the following checks:

- Verify SMTP protocol compliance as defined in RFC 2821.
- Validate incoming mail using several criteria.
- Inspect email and attachments for viruses.
- Apply rate limits to the number of messages.
- Validate DNS SPF records.
- Prevent directory harvesting attacks.
- Disallow or allow some of the SMTP methods, such as VRFY, EXPN, and ETRN, that spam senders typically use to attack mail servers.
- Reject the first message from a sender, because legitimate senders retry sending the message, and spam senders typically do not. This process is known as *greylisting*. The system does not reject subsequent messages from the same sender to the same recipient.

### Task summary

*Creating a custom SMTP service profile*

*Creating a security profile for SMTP traffic*

*Enabling anti-virus protection for email*

*Modifying associations between service profiles and security profiles*

*Creating and securing an SMTP virtual server and pool*

*Reviewing violation statistics for security profiles*

## Creating a custom SMTP service profile

You create an SMTP service profile optimized for security when you want to fine-tune the way that the BIG-IP® system scans SMTP traffic for vulnerabilities.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **SMTP**.  
The SMTP profile list screen opens.
2. Click **Create**.  
The New SMTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select the existing SMTP protocol from which you want the new profile to inherit settings. The default is **smtp**.
5. Select the **Custom** check box.
6. Select the **Protocol Security** check box to enable SMTP security checks.
7. Click **Finished**.

The custom SMTP service profile now appears in the SMTP list screen.



## Creating a security profile for SMTP traffic

The SMTP security profile provides security checks that are applicable to the SMTP protocol.

1. On the Main tab, click **Security > Protocol Security > Security Profiles > SMTP**.  
The Security Profiles: SMTP screen opens.
2. Click the **Create** button.  
The New SMTP Security Profile screen opens.
3. In the **Profile Name** field, type a unique name for the profile.
4. In the Defense Configuration area, modify the blocking policy settings for each violation.  
If you do not enable either **Alarm** or **Block** for a violation, the system does not perform the corresponding security check.

Option	Description
<b>Alarm</b>	The system logs any requests that trigger the violation.
<b>Block</b>	The system blocks any requests that trigger the violation.
<b>Alarm and Block</b>	The system both logs and blocks any requests that trigger the violation.

5. Click **Create**.  
The screen refreshes, and you see the new security profile in the list.

The BIG-IP® system automatically assigns this service profile to SMTP traffic that a designated virtual server receives.

## Enabling anti-virus protection for email

You can warn or block against email attachments containing a suspected virus. To do this, you configure the Application Security Manager™ to act as an ICAP client, and make sure that the SMTP profile has anti-virus options selected. This prompts an external ICAP server to inspect email and email attachments for viruses before releasing the content to the SMTP server.

1. On the Main tab, click **Security > Options > Application Security > Integrated Services > Anti-Virus Protection**.  
The Anti-Virus Protection screen opens.
2. For the **Server Host Name/IP Address** setting, type the fully qualified domain name of the ICAP server, or its IP address.

---

***Note:** If you specify the host name, you must first configure a DNS server by selecting **System > Configuration > Device > DNS**.*

---

3. For **Server Port Number**, type the port number of the ICAP server.  
The default value is 1344.
4. If you want to perform virus checking even if it may slow down the web application, select the **Guarantee Enforcement** check box.
5. Click **Save**.
6. On the Main tab, click **Security > Options > Protocol Security > Advanced Configuration**.  
The Advanced Configuration screen opens.
7. In the System Variables area, ensure that the values for the **icap\_uri** (URI for the ICAP service), and **virus\_header\_name** (header name used) internal parameters correspond to your ICAP server's settings.

By default, the system supports an ICAP server with McAfee anti-virus protection. If your organization uses a different ICAP server, update the parameters and save your changes.

ICAP Server	icap_uri Value
McAfee VirusScan	/REQMOD
Trend Micro InterScan Web Security	/reqmod
Kaspersky	/av/reqmod
Symantec	/symscanreq-av-url

ICAP Server	virus_header_name Value
McAfee VirusScan	X-Infection-Found,X-Virus-Name
Trend Micro InterScan Web Security	X-Virus-ID
Kaspersky	X-Virus-ID
Symantec	X-Violations-Found

- On the Main tab, click **Security > Protocol Security > Security Profiles > SMTP**.  
The Security Profiles: SMTP screen opens.
- Click an existing SMTP security profile name or create a new one.  
The (New) SMTP Profile Properties screen opens.
- For the **Virus Detection** setting, select the **Alarm** or **Block** options as required.

Option	Description
<b>Alarm</b>	The system logs any requests that trigger the virus detected violation, and displays them on the Protocol Security statistics screen.
<b>Block</b>	The system blocks any email requests that trigger the virus detected violation.
<b>Alarm and Block</b>	The system both logs and blocks any requests that trigger the virus detected violation.

- Click **Create** to create a new profile, or **Update** to update an existing one.

All incoming email attachments will be inspected for viruses.

## Modifying associations between service profiles and security profiles

Before you can modify associations between service profiles and security profiles, you must have created at least one security profile.

When you enable the **Protocol Security** setting on an FTP, HTTP, or SMTP service profile, the system automatically assigns the first-listed security profile to the service profile you configured for that profile. You can review and modify the current associations between the service profiles and the security profiles for each protocol.

- On the Main tab, click **Security > Protocol Security > Profiles Assignment**.  
The Profiles Assignment: HTTP screen opens.
- From the Profiles Assignment menu, select the service profile type, if different from HTTP.
- For each traffic profile, select the protocol security profile to use from the list in the Assigned Security Profile column.
- Click **Save**.

## Creating and securing an SMTP virtual server and pool

Configure a virtual server and a default pool for your network's SMTP servers, and assign the custom SMTP service profile. When the virtual server receives SMTP traffic, the SMTP security profile created in Application Security Manager™ scans for security vulnerabilities, and then the virtual server can be configured to perform other actions (such as load balancing) on traffic that passes the scan.

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the **Create** button.  
The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select the type, and type an address, or an address and mask, as appropriate for your network.
5. In the **Service Port** field, type 25 or select **SMTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **SMTP Profile** list, select the custom SMTP profile that you created.
8. From the **Source Address Translation** list, select **Auto Map**.
9. In the Resources area of the screen, for the **Default Pool** setting, click the **Create (+)** button.  
The New Pool screen opens.
10. In the **Name** field, type a unique name for the pool.
11. In the Resources area, for the **New Members** setting, select the type of new member you are adding, then type the appropriate information in the **Node Name**, **Address**, and **Service Port** fields, and click **Add** to add as many pool members as you need.
12. Click **Finished** to create the pool.  
The screen refreshes, and reopens the New Virtual Server screen. The new pool name appears in the **Default Pool** list.
13. Click **Finished**.

The custom SMTP virtual server appears in the Virtual Servers list.

## Reviewing violation statistics for security profiles

You can view statistics and transaction information for each security profile that triggers security violations.

1. On the Main tab, click **Security > Event Logs > Protocol** and click **HTTP**, **FTP**, **SMTP**, or **DNS**.  
The appropriate statistics screen opens listing all violations for that protocol, with the number of occurrences.
2. Type a Support ID, if you have one, to filter the violations and view one in particular.
3. Click a violation's hyperlink to see details about the requests causing the violation.  
On the Statistics screen, in the left column, you can review information regarding the traffic volume for each security profile configured.



---

## Chapter

# 51

---

## Configuring Remote High-Speed Logging of Protocol Security Events

---

- *Overview: Configuring Remote Protocol Security Event Logging*
  - *Implementation result*
-

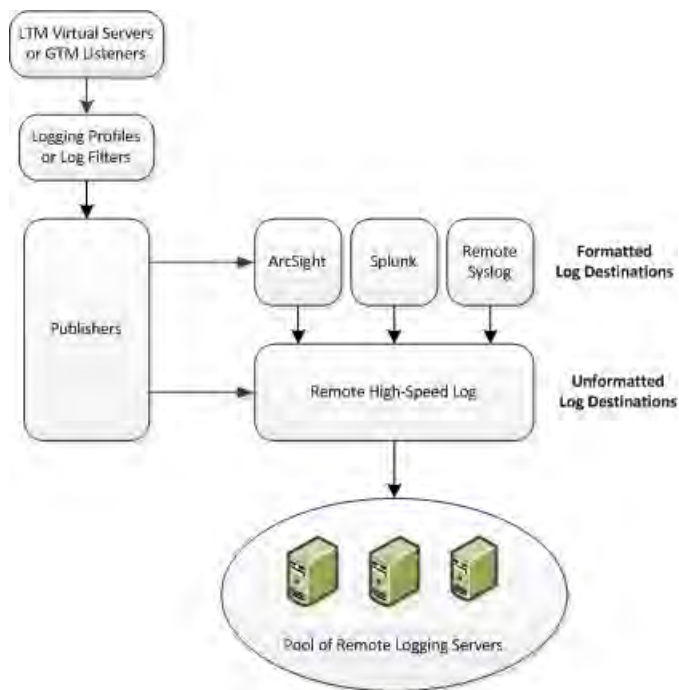
## Overview: Configuring Remote Protocol Security Event Logging

You can configure the BIG-IP® system to log information about BIG-IP system Protocol Security events and send the log messages to remote high-speed log servers.

**Important:** *The Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Protocol Security event logging.*

When configuring remote high-speed logging of Protocol Security events, it is helpful to understand the objects you need to create and why, as described here:

Object to create in implementation	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.



**Figure 15: Association of remote high-speed logging configuration objects**

### Task summary

Perform these tasks to configure Protocol Security event logging on the BIG-IP® system.

---

**Note:** Enabling remote high-speed logging impacts BIG-IP system performance.

---

*Creating a pool of remote logging servers*

*Creating a remote high-speed log destination*

*Creating a formatted remote high-speed log destination*

*Creating a publisher*

*Creating a custom Protocol Security Logging profile*

*Configuring a virtual server for Protocol Security event logging*

*Disabling logging*

## Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click **DNS > Delivery > Load Balancing > Pools** or **Local Traffic > Pools**.  
The Pool List screen opens.
2. Click **Create**.  
The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:

- a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
- b) Type a service number in the **Service Port** field, or select a service name from the list.

---

**Note:** Typical remote logging servers require port 514.

---

- c) Click **Add**.

5. Click **Finished**.

### Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**.  
The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

---

**Important:** If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the **Remote High-Speed Log** type. With this configuration, the BIG-IP system can send data to the servers in the required format.

---

The BIG-IP system is configured to send an unformatted string of text to the log servers.

5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

### Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**.  
The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.



---

**Important:** *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager (ASM™), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway.*

---

The BIG-IP system is configured to send a formatted string of text to the log servers.

5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.
6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

## Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System > Logs > Configuration > Log Publishers**.  
The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click << to move the destination to the **Selected** list.

---

**Note:** *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

---

5. Click **Finished**.

## Creating a custom Protocol Security Logging profile

Create a logging profile to log Protocol Security events for the traffic handled by the virtual server to which the profile is assigned.

---

**Note:** *You can configure logging profiles for HTTP and DNS security events on Advanced Firewall Manager™, and FTP and SMTP security events on Application Security Manager™.*

---

1. On the Main tab, click **Security > Event Logs > Logging Profiles**.  
The Logging Profiles list screen opens.
2. Click **Create**.  
The New Logging Profile screen opens.
3. Select the **Protocol Security** check box, to enable the BIG-IP system to log HTTP, FTP, DNS, and SMTP protocol request events.
4. In the HTTP, FTP, and SMTP Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log HTTP, FTP, and SMTP Security events.

5. In the DNS Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS Security events.
6. Select the **Log Dropped DNS Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
7. Select the **Log Filtered Dropped DNS Requests** check box, to enable the BIG-IP system to log DNS requests dropped due to DNS query/header-opcode filtering.

---

***Note:** The system does not log DNS requests that are dropped due to errors in the way the system processes DNS packets.*

---

8. Select the **Log Malformed DNS Requests** check box, to enable the BIG-IP system to log malformed DNS requests.
9. Select the **Log Rejected DNS Requests** check box, to enable the BIG-IP system to log rejected DNS requests.
10. Select the **Log Malicious DNS Requests** check box, to enable the BIG-IP system to log malicious DNS requests.
11. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
<b>None</b>	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: <pre>"management_ip_address", "bigip_hostname", "context_type", "context_name", "src_ip", "dest_ip", "src_port", "dest_port", "vlan", "protocol", "route_domain", "acl_rule_name", "action", "drop_reason"</pre>
<b>Field-List</b>	This option allows you to: <ul style="list-style-type: none"> <li>• Select from a list, the fields to be included in the log.</li> <li>• Specify the order the fields display in the log.</li> <li>• Specify the delimiter that separates the content in the log. The default delimiter is the comma character.</li> </ul>
<b>User-Defined</b>	This option allows you to: <ul style="list-style-type: none"> <li>• Select from a list, the fields to be included in the log.</li> <li>• Cut and paste, in a string of text, the order the fields display in the log.</li> </ul>

12. Click **Finished**.

Assign this custom Protocol Security Logging profile to a virtual server.

## Configuring a virtual server for Protocol Security event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom Protocol Security Logging profile to a virtual server when you want the BIG-IP system to log Protocol Security events on the traffic the virtual server processes.

---

***Note:** This task applies only to systems provisioned at a minimum level (or higher) for **Local Traffic (LTM)**. You can check the provisioning level on the **System > Resource Provisioning** screen.*

---

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security > Policies**.  
The screen displays Policy settings and Inline Rules settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

## Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

---

***Note:** You can disable and re-enable logging for a specific resource based on your network administration needs.*

---

1. On the Main tab, click **Local Traffic > Virtual Servers**.  
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security > Policies**.  
The screen displays Policy settings and Inline Rules settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

## Implementation result

---

You now have an implementation in which the BIG-IP® system logs specific Protocol Security events and sends the logs to a specific location.



# Index

## A

Accept as Legitimate (Loosen)  
 about 255

access policy  
 configuring 117, 359

access profile  
 adding to virtual server 117, 360  
 creating 115, 357

access validation criteria 83

active security policy  
 overview 298

AJAX applications  
 and login response page 156  
 configuring blocking policy 156  
 configuring blocking response 156  
 configuring login response 156  
 overview 150  
 securing JSON data 150  
 using JSON 146

allowed cookies  
 adding 234  
 deleting 237  
 editing 236

allowed methods  
 adding 244

allowed URL properties 220

allowed URLs  
 adding 218  
 adding cross-domain enforcement 128

alpha-numeric parameters, See user-input parameters

anonymous proxy, disallowing 78

antivirus protection  
 configuring external 265

anti-virus protection  
 creating for email and attachments 377

APM and ASM setup  
 result 361

Application Security Administrator  
 creating user accounts 266

Application Security Editor  
 creating user accounts 266

application security overview 92

ArcSight log message format  
 about 99

ASM\_REQUEST\_BLOCKING  
 description 193

ASM\_REQUEST\_DONE  
 description 193  
 examples 273

ASM\_REQUEST\_VIOLATION  
 description 193

ASM\_RESPONSE\_VIOLATION  
 description 193

attack signature pool  
 defined 291  
 getting update emails 292  
 updating 291

attack signature pool (*continued*)  
 viewing details 292

attack signatures  
 about user-defined 292  
 and staging 282  
 and XML format 294  
 assigning sets to policies 287  
 creating a set of 286  
 creating user-defined 293  
 enabling or disabling in a policy 289  
 enabling or disabling staging 289  
 exporting user-defined 294  
 importing user-defined 293  
 list of attack types 282  
 list of properties 284  
 list of signature sets 285  
 overriding in content profiles 290  
 overview 282  
 overview of creating sets 284  
 specifying blocking policy 287  
 viewing all in a policy 289  
 viewing sets in a policy 288

attack signature sets  
 defined 285  
 listed 285

authenticated URL 84, 103, 346

authenticated URLs 82

automatic policy building  
 collapsing entities 259  
 learning from response codes 259  
 learning from responses 257  
 limiting maximum policy elements 260  
 restoring default values 261  
 specifying file types for wildcard URLs 261  
 specifying when to add dynamic parameters 258  
 stopping/starting Policy Builder 262

automatic policy building stages  
 about 255

automatic synchronization  
 enabling and disabling 317, 338

awareness, user and session 102, 110

## B

base64 decoding  
 for file upload parameters 214  
 for user-input parameters 214

blocking  
 defined 172, 190

blocking actions  
 about 174  
 configuring 173  
 configuring for user-defined violations 272  
 configuring for web services 136, 175  
 configuring login response 179  
 configuring response pages 178  
 customizing XML response 180

- blocking methods
  - overview [172](#)
- blocking policy
  - configuring for AJAX [156](#)
- blocking response page
  - configuring for AJAX [156](#)
- blocking responses
  - overview [178](#)
- bot detection
  - enabling [55](#)
- brute force attacks
  - about [48](#)
  - configuring protection [50](#)
  - viewing event logs [52](#)
  - viewing reports [52](#)
- brute force mitigation
  - overview [48](#)
- buffer overflow attacks
  - preventing [248](#)

## C

- case-sensitive security policy [191](#)
- certificates
  - about [132](#)
  - adding [132](#)
- characters
  - specifying legal in URLs [225](#)
- character sets
  - changing for parameter names [209](#)
  - changing for parameter values [208](#)
- client certificates [132](#)
- comprehensive security policy type [185](#)
- config sync addresses
  - specifying [314](#), [324](#), [334](#)
- configuration synchronization
  - configuring for ASM [312](#), [322](#), [333](#)
  - performing basic networking [313](#), [323](#), [333](#)
  - result for synchronizing multiple ASM systems [319](#)
  - result for two ASM systems [329](#)
  - result of synchronizing ASM devices [340](#)
  - synchronizing ASM devices [322](#), [332](#)
  - syncing to group [316](#), [326](#), [336](#)
- content
  - defining with queries [135](#)
- content profiles
  - overriding attack signatures [290](#)
  - overriding meta characters [143](#)
- cookie header
  - setting maximum length [238](#)
- cookie protection
  - exporting [242](#)
  - importing [241](#)
  - overview [240](#)
  - reconfiguring [240](#)
- cookies
  - about [232](#)
  - about adding [233](#)
  - about pure wildcard [232–233](#)
  - adding [234](#)
  - adding enforced [235](#)
  - changing wildcard order [236](#)

- cookies (*continued*)
  - deleting [237](#)
  - editing [236](#)
  - learning explicit entities [237](#)
- CORS headers
  - defined [129](#)
- credit card masking
  - configuring [90](#)
  - overview [90](#)
- cross-domain request enforcement
  - defined [128](#)
  - how it works [129](#)
  - setting up [128](#)
- cross-domain requests
  - authorization [129](#)
- Cross-Origin Resource Sharing (CORS)
  - about [128](#)
- Cross-site request forgery (CSRF)
  - enabling protection [195](#)
- CSRF
  - enabling protection [195](#)
- custom profiles
  - and Protocol Security logging [385](#)

## D

- database security integration
  - configuring the server [347](#), [360](#)
  - enabling [348](#), [361](#)
  - overview [342](#), [352](#)
  - prerequisites [352](#)
  - result [348](#)
- Data Guard
  - and response headers inspected [86](#)
  - protecting sensitive data [86](#)
- data masking
  - defined [86](#)
- decryption
  - enabling [133](#)
- default DoS profile
  - modifying [43](#)
- defense configuration
  - fine-tuning [140](#)
  - setting definitions [140](#)
- denial-of-service protection
  - adding to a virtual server [33](#), [45](#)
- destinations
  - for logging [384](#)
  - for remote high-speed logging [384](#)
- detection interval [48](#)
- device discovery
  - for device trust [314](#), [324](#), [334](#)
- device groups
  - creating [315](#), [317](#), [325](#), [335](#), [338](#)
  - enabling ASM [318](#), [327](#), [339](#)
  - synchronizing ASM-enabled [319](#), [328](#), [339](#)
- device management
  - considerations [313](#), [323](#), [333](#)
  - setting up application security synchronization [312](#), [322](#), [332–333](#)
- device trust
  - establishing [314](#), [324](#), [334](#)

- disallowed file types
  - adding 200
- disallowed URLs
  - adding 223
- disaster recovery
  - result of synchronizing ASM devices 340
  - synchronizing ASM devices 332
- displaying 92
- DoS
  - sample event log 34
  - sample Statistics report 35
- DoS attacks
  - about 22
  - about heavy URL protection 23
  - about site-wide mitigation 24
  - configuring heavy URL protection 32
  - configuring latency-based protection 28
  - configuring protection 25
  - configuring TPS protection 25
  - recognizing 22
  - recording traffic 33
  - viewing DoS Statistics 34
  - viewing event logs 34
  - viewing URL Latencies report 36
- DoS policy switching
  - creating LTM policy 44
  - creating LTM policy rules 44
  - overview 42
  - result 46
- DoS profile
  - creating for Layer 7 traffic 43
  - modifying default 43
- DoS profiles
  - associating with virtual servers 33, 45
  - recording traffic 33
- DoS protection
  - about latency-based 23
  - about TPS-based 22
- DoS protection setup
  - overview 24
  - result 38
- dynamic content value parameters
  - creating 206
  - defined 206
- dynamic flows
  - configuring for URLs 228
- dynamic parameter name
  - creating 208
- dynamic parameters
  - specifying when to add 258

## E

- elements
  - about security policy 253
  - modifying security policy 254
- email and attachments
  - inspecting 377
- encryption
  - enabling 133
- enforced cookies
  - adding 235

- enforced cookies (*continued*)
  - deleting 237
  - editing 236
- enforcement, login 84, 103–104, 346
- enforcement mode
  - changing 172, 190
  - defined 172, 190
- enforcement readiness
  - about 169
- enforcement readiness period
  - adjusting 191
  - defined 191
- enhanced security policy type 185
- entities
  - enforcing 169
- event logs
  - viewing application security 100
- explicit entities
  - adding cookies 237
- explicit entities learning
  - configuring 166, 186
- explicit entities learning settings 185
- export formats
  - about 300

## F

- failover IP addresses
  - specifying 317, 327, 337
- file types
  - about adding 198
  - adding 198
  - disallowing 200
  - specifying for URLs 261
- file upload parameters, *See* user-input parameters
- fingerprinting
  - enabling 60
- flow parameters
  - creating 204, 226
- flows to URLs
  - configuring 225
  - configuring dynamic 228
- FTP profiles
  - creating custom security enabled 368
  - creating manually for FTP security 368
  - creating security enabled 364
- FTP traffic
  - creating security profile 369
  - securing 364, 368
- fundamental security policy type 185

## G

- geolocation
  - enforcing 78
  - enforcing from Requests list 79
  - overview 78
- global parameters
  - creating 202
  - defined 202
- Google Web Toolkit
  - GWT 160

Google Web Toolkit (*continued*)  
 see GWT 160  
 GWT  
   adding to support security policies 160  
 GWT profile  
   and implementation result 162  
   associating with URL 161  
   creating 160

## H

header-based content profiles  
   adding 224  
 header content  
   enforcing requests for URLs 224  
 header normalization  
   about 246  
 headers  
   configuring trusted XFF 194  
 heavy URL protection  
   about 23  
   configuring 32  
 heavy URLs  
   viewing URL Latencies report 36  
 high-speed logging  
   and server pools 383  
 history interval 48  
 host names  
   about adding multiple 195  
   adding 194  
 HTTP and HTTPS  
   differentiating between 192  
 HTTP header length  
   setting maximum 248  
 HTTP headers  
   about mandatory 246  
 HTTP header security  
   configuring 247  
   overview 246–247  
   results 249  
 HTTP protocol compliance  
   configuring dynamic session IDs 174  
 HTTPS traffic  
   creating virtual servers for 112, 354

## I

IBM InfoSphere Guardium integration  
   configuring the server 347, 360  
   enabling 348, 361  
   overview 342, 352  
 ICAP server  
   configuring 265  
 ignored entities  
   viewing 169  
 IP addresses  
   tracking specific 106  
 IP address exceptions  
   creating 74  
   deleting 75  
   overview 74  
   updating 75

IP address intelligence  
   categories 72  
   downloading the database 68  
   enabling 68  
   logging information 70  
   rejecting bad requests 71  
 IP address intelligence blocking  
   overview 68  
   reviewing statistics 70  
   setting up 69  
 IP intelligence database 72  
 iprep.autoupdate command 68  
 IP reputation blocking  
   overview 68  
 iRule  
   violation examples 273  
 iRule events  
   activating 193  
   table for ASM 193

## J

JSON data  
   masking 146  
 JSON profile  
   creating 146

## L

latency-based DoS detection 23  
 latency-based DoS protection  
   configuring 28  
 learning  
   configuring explicit entities 166, 186  
   overview 164  
   screens 164  
 learning suggestions  
   about 165  
   accepting 168  
   clearing 168  
   viewing requests 167  
 local traffic policies  
   and ASM 306, 310  
   and manual ASM policies 306  
 local traffic policy  
   associating with virtual servers 46  
   creating ASM rules 309  
   creating for DoS 44  
   creating rules 44  
 local traffic pools  
   creating 111, 354  
 local trust domain  
   and device groups 315, 317, 325, 335, 338  
   defined 314, 324, 334  
 logging  
   and destinations 384  
   and pools 383  
   and Protocol Security 382  
   and Protocol Security profiles 385  
   and publishers 385  
   of IP address intelligence information 70



- Logging profile
  - and Protocol Security events 386
- logging profiles
  - associating with security policy 98
  - creating 96
  - creating for remote logging 97
  - overview of application security 96
  - using the storage filter 99
- Logging profiles, disabling 387
- logging responses
  - about 99
- login enforcement 84, 103, 346
- login pages
  - about 82
  - access validation criteria 83
  - creating 48, 82, 102, 345
  - enforcing 84, 103, 346
- login response
  - configuring 179
- login response page
  - configuring for AJAX 156
- logout URL 82, 84, 103, 346
- logs
  - viewing application security 100

## M

- malicious IP address 69
- mandatory headers
  - about 246
- Manual Traffic Learning screen 165
- merge feature
  - overview 303
- meta characters
  - overriding in content profiles 143
- methods
  - adding allowed 244
- monitoring application security 92

## N

- navigation parameters
  - creating 206
  - defined 206
- network failover
  - configuring 315, 325, 335
- Network Firewall Logging
  - disabling 387
- normalization for headers
  - about 246

## O

- open redirects
  - overview 122
  - protecting against 122–123
  - summary 124

## P

- parameter level
  - adjusting 187, 209
- parameters
  - about adding 202
  - associating with JSON profiles 148
  - changing character sets 208–209
  - creating dynamic content value 206
  - creating dynamic names 208
  - creating flow 204, 226
  - creating global 202
  - creating navigation 206
  - creating sensitive 205
  - creating URL 203
  - list of value types 210
  - overview of how processed 211
  - securing base64-encoded 214
  - specifying when to add dynamic 258
- parameters path
  - enforcing security 212
  - overview 211
- parameter value types 210
- path parameters
  - enforcing security 212
  - overview 211
- policy, *See* security policy.
- Policy Builder
  - stopping and starting 262
- policy building rules
  - about 254
- policy building settings
  - configuring automatic 252
- policy differences
  - 302
  - merging 303
- Policy Diff feature
  - overview 301
- policy type
  - changing 184
- policy types, elements 185
- pools
  - creating local traffic 111, 354
  - for high-speed logging 383
- preferences
  - adjusting system 264
- preflight request
  - defined 129
- profiles
  - and disabling Network Firewall Logging 387
  - associating parameters with JSON 148
  - associating URLs with GWT 161
  - associating URLs with JSON 147
  - creating for FTP security 364, 368
  - creating for Protocol Security logging 385
  - creating for SMTP security 372, 376
  - creating GWT 160
  - creating JSON 146
- Protocol Security logging
  - customizing profiles 385
  - overview 382

Protocol Security Logging profile, assigning to virtual server 386  
 publishers  
   creating for logging 385  
 pure wildcard cookies 232–233

## R

redirection domains  
   enforcing 124  
 redirection protection  
   checking status 123  
   configuring 122  
   overview 122  
   summary 124  
 redirect URL  
   overview 178  
 referrer URLs  
   about referrer 218  
 RegExp Validator tool 266  
 regular expressions  
   validating 266  
 remote logging servers  
   configuring 97  
 remote servers  
   and destinations for log messages 384  
   for high-speed logging 383  
 reporting  
   for IP address intelligence blocking 70  
 reporting tools 92  
 requests  
   exporting 94  
 response codes  
   learning from 259  
   specifying allowed 192  
 response pages  
   configuring 178  
 responses  
   learning from 257  
 response scrubbing  
   defined 86  
 responses to blocking  
   overview 178  
 routing  
   based on XML content 135  
 rules  
   local traffic policy 309  
   modifying security policy 255

## S

search engine, customize  
   considerations 55  
 search engines  
   allowing for web scraping 55  
 security  
   configuring for FTP traffic 364, 368  
   configuring for SMTP traffic 372  
 security for web services  
   about 132  
 security policies  
   and local traffic policies 306, 310

security policies (*continued*)  
   and manually adding local traffic policies 306  
 security policy  
   about configuring automatic build settings 252  
   about export formats 300  
   about general building settings 184  
   about learning suggestions 165  
   about policy building rules 254  
   activating 298  
   adding trusted IP addresses 256  
   adjusting the parameter level 187, 209  
   and elements for each policy type 185  
   changing policy type 184  
   comparing 301–302  
   configuring automatic settings 252  
   configuring explicit entities learning 166, 186  
   creating automatically 112, 150, 307, 343, 355  
   deactivating 298  
   deleting 299  
   differentiating between HTTP and HTTPS 192  
   editing manually 190  
   exporting 300  
   fine-tuning 165  
   import/export overview 299  
   importing 301  
   learning overview 164  
   learning screens 164  
   limiting maximum elements 260  
   merging 303  
   overview merging 303  
   reviewing status 153  
   setting cookie header length 238  
   setting enforcement mode 172, 190  
   setting enforcement readiness period 191  
   setting HTTP header length 248  
   specifying allowed response codes 192  
   specifying file types for URLs 261  
   synchronizing ASM 319, 328, 339  
   viewing requests 93, 167  
   viewing whether case-sensitive 191  
 security policy activation  
   overview 298  
 security policy deactivation  
   overview 298  
 security policy elements  
   about 253  
   modifying 254  
 security policy rules  
   modifying 255  
 security policy synchronization  
   configuring 312, 322, 332–333  
 security policy types 185  
 security profiles  
   creating for FTP 369  
   creating for SMTP 377  
   viewing statistics 365, 370, 373, 379  
 security profiles, protocol  
   and service profiles 369, 378  
   modifying assignments 369, 378  
 selective learning setting 185  
 self IP addresses  
   and VLANs 111, 353

- self IP addresses (*continued*)
  - creating 111, 353
- sensitive data
  - masking 142
  - masking credit card numbers 90
  - masking JSON 146
  - protecting 86
  - protecting, overview 86
- sensitive parameters
  - creating 205
- server certificates 132
- servers
  - and destinations for log messages 384
  - and publishers for log messages 385
  - for high-speed logging 383
- service profiles
  - creating for SMTP security 376
- service profiles, protocol
  - and security profiles 369, 378
  - modifying assignments 369, 378
- session awareness
  - enabling 104
  - enabling with APM 118
- session ID numbers
  - tracking specific 106
- session IDs
  - configuring dynamic 174, 228
- session opening detection
  - enabling 57
- sessions, monitoring 106, 119
- session tracking
  - enabling 104
  - enabling with APM 118
  - overview 102, 110
  - prerequisites 110
- session transaction anomalies
  - enabling detection 59
- SMTP profiles
  - creating custom security enabled 376
  - creating manually for SMTP security 376
  - creating security enabled 372
  - creating with custom security enabled 376
  - manually creating for SMTP security 376
- SMTP traffic
  - creating security profile 377
  - securing 372
- SOAP messages
  - encrypting 133
  - verifying 133
- SOAP methods
  - enabling 144
- Stabilize (Tighten)
  - about 255
- staging
  - enabling or disabling for attack signatures 289
- statistics
  - viewing for security profiles 365, 370, 373, 379
- storage filter
  - configuring 99
- Sync-Failover device groups
  - creating 315, 325, 335

- synchronization
  - configuring for ASM 322, 332
  - result for configuring multiple ASM systems 319
  - result for configuring two ASM systems 329
- Sync-Only device groups
  - creating 317, 338
- syslog server
  - configuring 97
- system preferences
  - adjusting 264

## T

- TCP dump
  - diagnosing DoS attacks 33
- TPS DoS protection
  - configuring 25
- Track Site Changes
  - about 255
- transaction rate
  - about detection 22
- transparent
  - defined 172, 190
- trust domains
  - and local trust domain 314, 324, 334
- trusted IP addresses
  - adding 256

## U

- URL Latencies report
  - sample report 37
  - viewing 36
- URL parameters
  - creating 203
  - defined 203
- URLs
  - about adding 218
  - about referrer 218
  - adding 218
  - adding authenticated 84, 103, 346
  - adding header-based content profiles 224
  - adding logout 84, 103, 346
  - associating with GWT profiles 161
  - associating with JSON profiles 147
  - configuring dynamic flows 228
  - configuring dynamic session IDs 228
  - configuring flows 225
  - disallowing 223
  - enforcing requests for 224
  - modifying legal character set 225
- user awareness
  - overview 102, 110
- user-defined attack signatures
  - about 292
  - creating 293
  - exporting 294
  - importing 293
- user-defined violations
  - about 271
  - creating 271
  - deleting 278

- user-defined violations (*continued*)
  - example of iRules 273
  - exporting and importing 278
- user information
  - monitoring 106, 119
  - tracking specific 106
- user-input parameters
  - and base64 decoding 214
- user interface
  - adjusting preferences 264
- user roles
  - for application security 266

## V

- violations
  - about 270
  - about user-defined 271
  - changing severity levels 271
  - configuring blocking actions 173
  - configuring blocking for web services 136, 175
  - creating user-defined 271
  - deleting user-defined 278
  - disabling learning on 170
  - enabling user-defined 272
  - exporting user-defined 278
  - importing user-defined 278
  - table of types 270
  - viewing descriptions of 270
  - viewing illegal requests 93
- violations statistics
  - viewing 365, 370, 373, 379
- virtual server
  - assigning Protocol Security Logging profile 386
- virtual servers
  - associating DoS profiles 33, 45
  - associating local traffic policy 46
  - creating for FTP traffic 364, 369
  - creating for HTTPS traffic 112, 354
  - creating for SMTP traffic 372, 379
  - for FTP, with pool 369
- VLANs
  - and self IP addresses 111, 353
  - creating 110, 353

## W

- web scraping
  - overview 54
  - prerequisites 54
- web scraping attack
  - result 65
- web scraping attacks
  - detecting with fingerprinting 60
  - enabling bot detection 55
  - enabling session opening detection 57
  - enabling session transaction anomalies 59
  - example of statistics chart 64
  - examples of viewing statistics event log 61
  - viewing event logs 61
  - viewing statistics 64
- web scraping attack types 63
- web services
  - configuring blocking 136, 175
- web services security
  - about 132
- wildcards
  - and cookies 232–233
  - changing cookie order 236
- wildcard syntax 199, 220, 233

## X

- x509 certificates
  - for device trust 314, 324, 334
- XFF headers
  - configuring trusted 194
- XML blocking response
  - customizing 180
- XML profile
  - defense configuration settings 140
  - editing defense configuration 140
  - enabling SOAP methods 144
  - masking sensitive data 142
- XPath expressions
  - samples of syntax 136
- XPath queries
  - rules for writing 135
- XPath query
  - examples 136