# ArcGIS Enterprise
# Web Application Filter Rules

**Restricted Use:** Customer access only, do not distribute or post publicly

Version 2.2.4 – June 2026

Esri Software Security & Privacy Team
**Contact:** SoftwareSecurity@esri.com

# Contents



# Change Log

**v2.2.4 (6.22.2026)**

- Added AWS Specific Rule Exceptions
- Added IP/Network Exclusions

**v2.2.3 (10.8.2025)**

- Corrected enabled/disabled rule information in table.

**v2.2.2 (10.8.2025)**

- Corrected enabled/disabled rule information in table.

**v2.2.1 (10.4.2025)**

- Updated to reflect OWASP CoreRuleset 3.2 rule IDs
- Changed "Inspect Request Body" to "On" which resulted in changing the following 5 rules to disabled: 941340, 942300, 932105, 942310, 931120.

**v2.129 (3.6.2024)**

- Removed Azure v1 WAF scripts.

**v2.128 (3.2.2022)**

- Corrected documentation version numbering error (no technical changes are updates to guidance).

**v2.127 (12.14.21) –**

- Updated Azure WAF Deployment Script to include experimental blocking features that are more aggressive such as "log4shell" attack evasion patterns. These are disabled by default but can be enabled by passing the `-enableExperimentalProtections $true` flag.
- Updated script to provide improved protection against "log4shell" attacks (https://nvd.nist.gov/vuln/detail/CVE-2021-44228).
- Updated guidance to include anti-evasion patterns for "log4shell" attacks.

**v2.126 (12.13.21) –**

- Updated Azure WAF Deployment Script to block “log4shell” attacks (https://nvd.nist.gov/vuln/detail/CVE-2021-44228)

**v2.125 (12.06.21) –**

- Added optional parameter to Azure WAF Deployment Script to support an optional parameter to disable Admin API blocking (`-blockAdminAPI $false`). Default is to block external requests to the Admin API.

## Important Considerations for WAF Deployments

Web Application Firewalls (WAF) are frequently used to filter and monitor traffic to a website from the internet. Unlike traditional network firewalls, WAFs operate at the HTTP layer inspecting URIs, query strings, message body and headers for malicious content. Due to their more complex nature, WAF rules require review and maintenance with each update or change to the application. Most WAF implementations have a "Detect/Learn" and "Protect" mode. In "Detect" mode, the WAF will flag patterns that would otherwise be blocked to alert the WAF administrator to inspect the request and its corresponding rule and determine if the rule needs to be adjusted. This "learning" process is vital to any successful WAF deployment. It is strongly recommended with the rules below, that all deployments start out running in "Detect/Learn" mode while ArcGIS Enterprise is exercised and use cases tested to avoid breaking workflows unexpectedly. Once rules are fully tuned and WAF logs no longer reveal false positives, the WAF can be shifted into "Protect" mode.

To aid with this burn in process, Esri has validated ArcGIS Enterprise against the OWASP Core Rule Set listed within this document. We recommend disabling OWASP Core Rules that are known to conflict with ArcGIS Enterprise's normal operation as specified in the table below.

## OWASP Core Ruleset Guidance

ArcGIS Enterprise has been validated with the with OWASP Core Rule Set v3.2. This update includes testing when "Inspect Request Body" is "Enabled" which helps protect against POST based attacks. Refer to the following table for rule configuration (**Enabled** / **Disabled**) recommendations for ArcGIS Enterprise:

| Rule Id | Description | Status |
|---|---|---|
| 911100 | Method is not allowed by policy | Enabled |
| 913100 | Found User-Agent associated with security scanner | Enabled |
| 913101 | Found User-Agent associated with scripting/generic HTTP client | Disabled |
| 913102 | Found User-Agent associated with web crawler/bot | Enabled |
| 913110 | Found request header associated with security scanner | Enabled |
| 913120 | Found request filename/argument associated with security scanner | Enabled |
| 920100 | Invalid HTTP Request Line | Disabled |
| 920120 | Attempted multipart/form-data bypass | Enabled |
| 920121 | Attempted multipart/form-data bypass | Enabled |
| 920160 | Content-Length HTTP header is not numeric. | Enabled |
| 920170 | GET or HEAD Request with Body Content. | Enabled |
| 920171 | GET or HEAD Request with Transfer-Encoding. | Enabled |
| 920180 | POST request missing Content-Length Header. | Enabled |
| 920190 | Range: Invalid Last Byte Value. | Enabled |
| 920200 | Range: Too many fields (6 or more) | Enabled |
| 920201 | Range: Too many fields for pdf request (35 or more) | Enabled |

| | | |
|---|---|---|
| 920202 | Range: Too many fields for pdf request (6 or more) | Enabled |
| 920210 | Multiple/Conflicting Connection Header Data Found. | Enabled |
| 920220 | URL Encoding Abuse Attack Attempt | Enabled |
| 920230 | Multiple URL Encoding Detected | Disabled |
| 920240 | URL Encoding Abuse Attack Attempt | Enabled |
| 920250 | UTF8 Encoding Abuse Attack Attempt | Enabled |
| 920260 | Unicode Full/Half Width Abuse Attack Attempt | Enabled |
| 920270 | Invalid character in request (null character) | Enabled |
| 920271 | Invalid character in request (non printable characters) | Disabled |
| 920272 | Invalid character in request (outside of printable chars below ascii 127) | Enabled |
| 920273 | Invalid character in request (outside of very strict set) | Enabled |
| 920274 | Invalid character in request headers (outside of very strict set) | Enabled |
| 920280 | Request Missing a Host Header | Enabled |
| 920290 | Empty Host Header | Enabled |
| 920300 | Request Missing an Accept Header | Disabled |
| 920310 | Request Has an Empty Accept Header | Enabled |
| 920311 | Request Has an Empty Accept Header | Enabled |
| 920320 | Missing User Agent Header | Disabled |
| 920330 | Empty User Agent Header | Enabled |
| 920340 | Request Containing Content, but Missing Content-Type header | Disabled |
| 920341 | Request containing content requires Content-Type header | Disabled |
| 920350 | Host header is a numeric IP address | Disabled |
| 920420 | Request content type is not allowed by policy | Disabled |
| 920430 | HTTP protocol version is not allowed by policy | Enabled |
| 920440 | URL file extension is restricted by policy | Disabled |
| 920450 | HTTP header is restricted by policy (%{MATCHED_VAR}) | Enabled |
| 920460 | Abnormal Escape Characters | Enabled |
| 920470 | Illegal Content-Type header | Disabled |
| 920480 | Restrict charset parameter within the content-type header | Disabled |
| 921110 | HTTP Request Smuggling Attack | Enabled |
| 921120 | HTTP Response Splitting Attack | Enabled |
| 921130 | HTTP Response Splitting Attack | Enabled |
| 921140 | HTTP Header Injection Attack via headers | Enabled |
| 921150 | HTTP Header Injection Attack via payload (CR/LF detected) | Disabled |
| 921151 | HTTP Header Injection Attack via payload (CR/LF detected) | Disabled |
| 921160 | HTTP Header Injection Attack via payload (CR/LF and header-name detected) | Enabled |
| 921170 | HTTP Parameter Pollution | Enabled |
| 921180 | HTTP Parameter Pollution (%{TX.1}) | Enabled |
| 930100 | Path Traversal Attack (/../) | Disabled |
| 930110 | Path Traversal Attack (/../) | Disabled |
| 930120 | OS File Access Attempt | Enabled |

| | | |
|---|---|---|
| 930130 | Restricted File Access Attempt | Enabled |
| 931100 | Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address | Disabled |
| 931110 | Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL Payload | Enabled |
| 931120 | Possible Remote File Inclusion (RFI) Attack: URL Payload Used w/Trailing Question Mark Character (?) | Disabled |
| 931130 | Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link | Disabled |
| 932100 | Remote Command Execution: Unix Command Injection | Enabled |
| 932105 | Remote Command Execution: Unix Command Injection | Disabled |
| 932106 | Remote Command Execution: Unix Command Injection | Enabled |
| 932110 | Remote Command Execution: Windows Command Injection | Disabled |
| 932115 | Remote Command Execution: Windows Command Injection | Disabled |
| 932120 | Remote Command Execution: Windows PowerShell Command Found | Disabled |
| 932130 | Remote Command Execution: Unix Shell Expression Found | Enabled |
| 932140 | Remote Command Execution: Windows FOR/IF Command Found | Enabled |
| 932150 | Remote Command Execution: Direct Unix Command Execution | Disabled |
| 932160 | Remote Command Execution: Unix Shell Code Found | Disabled |
| 932170 | Remote Command Execution: Shellshock (CVE-2014-6271) | Enabled |
| 932171 | Remote Command Execution: Shellshock (CVE-2014-6271) | Enabled |
| 932180 | Restricted File Upload Attempt | Enabled |
| 932190 | Remote Command Execution: Wildcard bypass technique attempt | Enabled |
| 933100 | PHP Injection Attack: Opening/Closing Tag Found | Enabled |
| 933110 | PHP Injection Attack: PHP Script File Upload Found | Enabled |
| 933111 | PHP Injection Attack: PHP Script File Upload Found | Enabled |
| 933120 | PHP Injection Attack: Configuration Directive Found | Enabled |
| 933130 | PHP Injection Attack: Variables Found | Enabled |
| 933131 | PHP Injection Attack: Variables Found | Enabled |
| 933140 | PHP Injection Attack: I/O Stream Found | Enabled |
| 933150 | PHP Injection Attack: High-Risk PHP Function Name Found | Enabled |
| 933151 | PHP Injection Attack: Medium-Risk PHP Function Name Found | Enabled |
| 933160 | PHP Injection Attack: High-Risk PHP Function Call Found | Enabled |
| 933161 | PHP Injection Attack: Low-Value PHP Function Call Found | Enabled |
| 933170 | PHP Injection Attack: Serialized Object Injection | Enabled |
| 933180 | PHP Injection Attack: Variable Function Call Found | Disabled |
| 933190 | PHP Injection Attack: PHP Closing Tag Found | Enabled |
| 933200 | PHP Injection Attack: Wrapper scheme detected | Enabled |
| 933210 | PHP Injection Attack: Variable Function Call Found | Enabled |
| 941100 | XSS Attack Detected via libinjection | Disabled |
| 941101 | XSS Attack Detected via libinjection. | Enabled |
| 941110 | XSS Filter - Category 1: Script Tag Vector | Disabled |
| 941120 | XSS Filter - Category 2: Event Handler Vector | Enabled |

| | | |
|---|---|---|
| 941130 | XSS Filter - Category 3: Attribute Vector | Disabled |
| 941140 | XSS Filter - Category 4: Javascript URI Vector | Disabled |
| 941150 | XSS Filter - Category 5: Disallowed HTML Attributes | Disabled |
| 941160 | NoScript XSS InjectionChecker: HTML Injection | Disabled |
| 941170 | NoScript XSS InjectionChecker: Attribute Injection | Enabled |
| 941180 | Node-Validator Blacklist Keywords | Enabled |
| 941190 | XSS Using style sheets | Enabled |
| 941200 | XSS using VML frames | Disabled |
| 941210 | XSS using obfuscated JavaScript | Enabled |
| 941220 | XSS using obfuscated VB Script | Enabled |
| 941230 | XSS using 'embed' tag | Enabled |
| 941240 | XSS using 'import' or 'implementation' attribute | Enabled |
| 941250 | IE XSS Filters - Attack Detected. | Enabled |
| 941260 | XSS using 'meta' tag | Enabled |
| 941270 | XSS using 'link' href | Enabled |
| 941280 | XSS using 'base' tag | Enabled |
| 941290 | XSS using 'applet' tag | Enabled |
| 941300 | XSS using 'object' tag | Enabled |
| 941310 | US-ASCII Malformed Encoding XSS Filter - Attack Detected. | Disabled |
| 941320 | Possible XSS Attack Detected - HTML Tag Handler | Disabled |
| 941330 | IE XSS Filters - Attack Detected. | Disabled |
| 941340 | IE XSS Filters - Attack Detected. | Disabled |
| 941350 | UTF-7 Encoding IE XSS - Attack Detected. | Disabled |
| 941360 | JavaScript obfuscation detected. | Enabled |
| 942100 | SQL Injection Attack Detected via libinjection | Disabled |
| 942110 | SQL Injection Attack: Common Injection Testing Detected | Disabled |
| 942120 | SQL Injection Attack: SQL Operator Detected | Disabled |
| 942130 | SQL Injection Attack: SQL Tautology Detected. | Disabled |
| 942140 | SQL Injection Attack: Common DB Names Detected | Enabled |
| 942150 | SQL Injection Attack | Disabled |
| 942160 | Detects blind sqli tests using sleep() or benchmark(). | Enabled |
| 942170 | Detects SQL benchmark and sleep injection attempts including conditional queries | Enabled |
| 942180 | Detects basic SQL authentication bypass attempts 1/3 | Disabled |
| 942190 | Detects MSSQL code execution and information gathering attempts | Disabled |
| 942200 | Detects MySQL comment-/space-obfuscated injections and backtick termination | Disabled |
| 942210 | Detects chained SQL injection attempts 1/2 | Disabled |
| 942220 | Looking for intiger overflow attacks, these are taken from skipfish, except 3.0.00738585072007e-308 is the \"magic number\" crash | Enabled |
| 942230 | Detects conditional SQL injection attempts | Disabled |

| | | |
|---|---|---|
| 942240 | Detects MySQL charset switch and MSSQL DoS attempts | Enabled |
| 942250 | Detects MATCH AGAINST, MERGE and EXECUTE IMMEDIATE injections | Enabled |
| 942251 | Detects HAVING injections | Enabled |
| 942260 | Detects basic SQL authentication bypass attempts 2/3 | Disabled |
| 942270 | Looking for basic sql injection. Common attack string for mysql, oracle and others. | Enabled |
| 942280 | Detects Postgres pg_sleep injection, waitfor delay attacks and database shutdown attempts | Enabled |
| 942290 | Finds basic MongoDB SQL injection attempts | Enabled |
| 942300 | Detects MySQL comments, conditions and ch(a)r injections | Disabled |
| 942310 | Detects chained SQL injection attempts 2/2 | Disabled |
| 942320 | Detects MySQL and PostgreSQL stored procedure/function injections | Enabled |
| 942330 | Detects classic SQL injection probings 1/2 | Disabled |
| 942340 | Detects basic SQL authentication bypass attempts 3/3 | Disabled |
| 942350 | Detects MySQL UDF injection and other data/structure manipulation attempts | Enabled |
| 942360 | Detects concatenated basic SQL injection and SQLLFI attempts | Enabled |
| 942361 | Detects basic SQL injection based on keyword alter or union | Enabled |
| 942370 | Detects classic SQL injection probings 2/2 | Disabled |
| 942380 | SQL Injection Attack | Disabled |
| 942390 | SQL Injection Attack | Disabled |
| 942400 | SQL Injection Attack | Enabled |
| 942410 | SQL Injection Attack | Disabled |
| 942420 | Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (8) | Enabled |
| 942421 | Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (3) | Enabled |
| 942430 | Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12) | Disabled |
| 942431 | Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (6) | Enabled |
| 942432 | Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (2) | Enabled |
| 942440 | SQL Comment Sequence Detected. | Disabled |
| 942450 | SQL Hex Encoding Identified | Disabled |
| 942460 | Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters | Disabled |
| 942470 | SQL Injection Attack | Enabled |
| 942480 | SQL Injection Attack | Enabled |
| 942490 | Detects classic SQL injection probings 3/3 | Enabled |
| 942500 | MySQL in-line comment detected. | Enabled |
| 943100 | Possible Session Fixation Attack: Setting Cookie Values in HTML | Enabled |
| 943110 | Possible Session Fixation Attack: SessionID Parameter Name with Off-Domain Referer | Enabled |

| | | |
|---|---|---|
| 943120 | Possible Session Fixation Attack: SessionID Parameter Name with No Referer | Enabled |
| 944100 | Remote Command Execution: Apache Struts, Oracle WebLogic | Disabled |
| 944110 | Detects potential payload execution | Disabled |
| 944120 | Possible payload execution and remote command execution | Enabled |
| 944130 | Suspicious Java classes | Disabled |
| 944200 | Exploitation of Java deserialization Apache Commons | Enabled |
| 944210 | Possible use of Java serialization | Enabled |
| 944240 | Remote Command Execution: Java serialization | Enabled |
| 944250 | Remote Command Execution: Suspicious Java method detected | Disabled |
| 800100 | Rule to help detect and mitigate log4j vulnerability - CVE-2021-44228, CVE-2021-45046 | Enabled |
| 800110 | Spring4Shell Interaction Attempt | Enabled |
| 800111 | Attempted Spring Cloud routing-expression injection - CVE-2022-22963 | Enabled |
| 800112 | Attempted Spring Framework unsafe class object exploitation - CVE-2022-22965 | Enabled |
| 800113 | Attempted Spring Cloud Gateway Actuator injection - CVE-2022-22947 | Enabled |
| 800114 | Attempted Apache Struts file upload exploitation - CVE-2023-50164 | Enabled |

## AWS Core rule set (CRS) managed rule group Guidance

ArcGIS Enterprise has been validated with the AWS (Amazon Web Services) WAF CoreRuleSet. Refer to the following table for rule configuration (**Enabled** / **Disabled**) recommendations for ArcGIS Enterprise:

| Rule Group ID | Rule ID | Status |
|---|---|---|
| AWSManagedRulesCommonRuleSet | NoUserAgent_HEADER | Enabled |
| AWSManagedRulesCommonRuleSet | UserAgent_BadBots_HEADER | Enabled |
| AWSManagedRulesCommonRuleSet | SizeRestrictions_QUERYSTRING | Enabled |
| AWSManagedRulesCommonRuleSet | SizeRestrictions_Cookie_HEADER | Enabled |
| AWSManagedRulesCommonRuleSet | SizeRestrictions_BODY | Disabled |
| AWSManagedRulesCommonRuleSet | SizeRestrictions_URIPATH | Enabled |
| AWSManagedRulesCommonRuleSet | EC2MetaDataSSRF_BODY | Enabled |
| AWSManagedRulesCommonRuleSet | EC2MetaDataSSRF_COOKIE | Enabled |
| AWSManagedRulesCommonRuleSet | EC2MetaDataSSRF_URIPATH | Enabled |
| AWSManagedRulesCommonRuleSet | EC2MetaDataSSRF_QUERYARGUMENTS | Enabled |
| AWSManagedRulesCommonRuleSet | GenericLFI_QUERYARGUMENTS | Enabled |
| AWSManagedRulesCommonRuleSet | GenericLFI_URIPATH | Enabled |
| AWSManagedRulesCommonRuleSet | GenericLFI_BODY | Enabled |
| AWSManagedRulesCommonRuleSet | RestrictedExtensions_URIPATH | Enabled |
| AWSManagedRulesCommonRuleSet | RestrictedExtensions_QUERYARGUMENTS | Enabled |
| AWSManagedRulesCommonRuleSet | GenericRFI_QUERYARGUMENTS | Enabled |
| AWSManagedRulesCommonRuleSet | GenericRFI_BODY | Disabled |
| AWSManagedRulesCommonRuleSet | GenericRFI_URIPATH | Enabled |
| AWSManagedRulesCommonRuleSet | CrossSiteScripting_COOKIE | Enabled |
| AWSManagedRulesCommonRuleSet | CrossSiteScripting_QUERYARGUMENTS | Enabled |
| AWSManagedRulesCommonRuleSet | CrossSiteScripting_BODY | Disabled |
| AWSManagedRulesCommonRuleSet | CrossSiteScripting_URIPATH | Enabled |

## WAF Policy Settings

The following settings should be applied to the WAF Policy/Protection Rules that protects ArcGIS Enterprise for all deployments to ensure ArcGIS Enterprise traffic is correctly inspected while minimizing instances of false blocks/detections.

### WAF Exclusions by IP/Network:

The following table outlines suggested WAF Policy exclusions which must be implemented along with the above Core Ruleset rules to allow ArcGIS Enterprise to function when deployed behind a WAF:

| Description | Example IP / Network(s) | WAF Protection |
|---|---|---|
| ArcGIS Enterprise Network Segment | 10.x.x.x/24<br>172.16.x.x/24 | Disabled |
| ArcGIS Enterprise Outbound Public IPs | 54.x.x.x/32 | Disabled |
| Administration Network Segment | 10.x.x.x/24<br>172.16.x.x/24 | Disabled |
| General Private IPs | 10.0.0.0/8<br>172.16.0.0/12<br>192.168.0.0/16<br>fc00::/7 | Enabled |
| Public IPs | 0.0.0.0/0<br>::/0 | Enabled |

### Cookie/Querystring parameters:

The following is a list of cookies and querystring parameters that should be excepted from WAF processing as they contain authentication tokens that will lead to false positives:

```
Querystring:     "token"
Cookie:          "esri_auth"
Cookie:          "esri_aopc"
```

### Enable Body Inspection:

Due to disabling the following 5 rules 941340, 942300, 932105, 942310, 931120, we now recommend enabling body inspection to ensure WAF rules protect from GET and POST request attacks:

```
Inspect request body:       "On"
```

***The above setting is a major improvement in WAF coverage of your ArcGIS Enterprise deployment and is strongly recommended.***

## Extended Endpoint Filtering (Block Admin API)

**IMPORTANT:** Implementing the following guidance is an advanced option that will disallow access to administrative APIs through the front-end web interface of ArcGIS Enterprise. This hardening step creates additional administrative burden as these rules will block global administrative changes to ArcGIS Enterprise including: federation, read-only mode, system & security configuration. Organizations implementing this restriction will need to implement at least **one** of the following additional steps to administer ArcGIS Enterprise:

1) Implement an IP-whitelisted administrative Load Balancer that proxies requests directly to ArcGIS Enterprise's Portal host over port 7443; thereby allowing "administrators" unrestricted access to ArcGIS Enterprise if their requests originate from the whitelisted IP range.
2) Temporarily switch Web Application Firewall (WAF) configuration to "Detect Mode". Upon completing administrative changes, switch WAF configuration back to "Protect Mode".
3) Access ArcGIS Enterprise's Admin API on the Portal host itself or over a secured network connection on port 7443. (eg. https://localhost:7443/arcgis/admin)

**GUIDANCE:** The following application specific endpoints may be safely filtered from external access, however these restrictions **will block administrative access** (see above.) These regular expression rules may be applied at the WAF deny external access to sensitive URIs within your ArcGIS Enterprise site.

```
.*\/portaladmin\/federation\/.*federate.*
.*\/portaladmin\/mode.*
.*\/portaladmin\/security\/config.*update.*
.*\/portaladmin\/security\/sslCertificates.*
.*\/portaladmin\/system\/database.*
.*\/portaladmin\/system\/directories.*
.*\/portaladmin\/system\/emailSettings.*
.*\/portaladmin\/system\/properties.*update.*
.*\/portaladmin\/system\/webadaptors.*
.*\/admin\/.*federate.*
.*\/admin\/clusters.*
.*\/admin\/deleteSite.*
.*\/admin\/exportSite.*
.*\/admin\/importSite.*
.*\/admin\/machines.*
.*\/admin\/security.*
.*\/admin\/system.*
.*\/admin\/uploads.*
.*\/manager\/.*
.*\/portal\/sharing\/rest\/config\/.*
```