

# SonicWall® Secure Mobile Access

## 8.6 Web Application Firewall

Feature Guide

SONICWALL®

# Contents

<b>Document Scope</b> .....	<b>4</b>
<b>Licensing Web Application Firewall</b> .....	<b>5</b>
<b>Overview</b> .....	<b>8</b>
What is Web Application Firewall? .....	8
Benefits of Web Application Firewall .....	11
How Does Web Application Firewall Work? .....	11
How are Signatures Used to Prevent Attacks? .....	12
How is Cross-Site Request Forgery Prevented? .....	14
How is Information Disclosure Prevented? .....	14
How are Broken Authentication Attacks Prevented? .....	15
How are Insecure Storage and Communications Prevented? .....	15
How is Access to Restricted URLs Prevented? .....	15
How are Slowloris Attacks Prevented? .....	15
What Type of PCI Compliance Reports Are Available? .....	16
How Does Cookie Tampering Protection Work? .....	16
How Does Application Profiling Work? .....	18
How Does Rate Limiting for Custom Rules Work? .....	19
Supported Platforms .....	20
<b>Configuring Web Application Firewall</b> .....	<b>21</b>
Viewing and Updating Web Application Firewall Status .....	21
Viewing Status and Synchronizing Signatures .....	22
Downloading a PCI Compliance Report .....	22
Configuring Web Application Firewall Settings .....	23
Enabling Web Application Firewall and Configuring General Settings .....	24
Configuring Global Exclusions .....	25
Configuring Intrusion Prevention Error Page Settings .....	26
Configuring Cross-Site Request Forgery Protection Settings .....	27
Configuring Cookie Tampering Protection Settings .....	28
Configuring Web Site Cloaking .....	29
Configuring Information Disclosure Protection .....	30
Configuring Session Management Settings .....	31
Configuring Web Application Firewall Signature Actions .....	32
Enabling Performance Optimization .....	33
Configuring Signature Based Custom Handling and Exclusions .....	33
Reverting a Signature to Global Settings .....	35
Removing a Host from a Per-Signature Exclusion .....	35
Determining the Host Entry for Exclusions .....	35
Viewing the Host Entry in a Bookmark .....	36
Viewing the Host Entry in an Offloaded Application .....	37
Configuring Custom Rules and Application Profiling .....	38
Configuring Application Profiling .....	40

Configuring Rule Chains . . . . .	43
Configuring Rules in a Rule Chain . . . . .	45
Using Web Application Firewall Monitoring . . . . .	55
Monitoring on the Local Screen . . . . .	55
Monitoring on the Global Screen . . . . .	60
Using Web Application Firewall Logs . . . . .	62
Searching the Log . . . . .	63
Controlling the Log Pagination . . . . .	63
Viewing Log Entry Details . . . . .	64
Exporting and Emailing Log Files . . . . .	64
Clearing the Log . . . . .	65
Configuring an Application Offloading Portal . . . . .	65
<b>Verifying and Troubleshooting Web Application Firewall . . . . .</b>	<b>70</b>
<b>SonicWall Support . . . . .</b>	<b>72</b>
About This Document . . . . .	73

# Document Scope

This document describes how to configure and use the Web Application Firewall feature in SonicWall® Secure Mobile Access (SMA) 8.6.

This document contains the following sections:

- [Overview](#) on page 8
- [Licensing Web Application Firewall](#) on page 5
- [Configuring Web Application Firewall](#) on page 21
- [Verifying and Troubleshooting Web Application Firewall](#) on page 70

# Licensing Web Application Firewall

SonicWall SMA/SRA Web Application Firewall must be licensed before you can begin using it. You can access the MySonicWall web site directly from the SonicWall SMA/SRA management interface to obtain a license.

The **Web Application Firewall > Licensing** page in the SonicWall SMA management interface provides a link to the **System > Licenses** page, where you can connect to MySonicWall and purchase the license or start a free trial. You can view all system licenses on the **System > Licenses** page of the management interface.

## To view license details and obtain a license on MySonicWall for Web Application Firewall:

- 1 Log in to your SonicWall SMA/SRA appliance and navigate to **Web Application Firewall > Licensing**.

- 2 If Web Application Firewall is not licensed, click the **System > Licenses** link. The **System > Licenses** page is displayed.

Security Service	Status	Users	Expiration
Nodes/Users	Licensed	25	Never
Secure Virtual Assist	Not Licensed		
ViewPoint	Not Licensed		
Spike License	Not Licensed	0	0
End Point Control	Active		
Web Application Firewall	Not Licensed		
Analyzer	Not Licensed		
Geo IP & Botnet Filter	Not Licensed		

Support Service	Status	Expiration
Dynamic Support	Not Licensed	
Software and Firmware Updates	Not Licensed	
Hardware Warranty	Not Licensed	

- Under Manage Security Services Online, click the **Activate, Upgrade, or Renew services** link. The MySonicWall Login page is displayed.

- Type your MySonicWall credentials into the fields, and then click **Submit**. The **Manage Services Online** table is displayed.

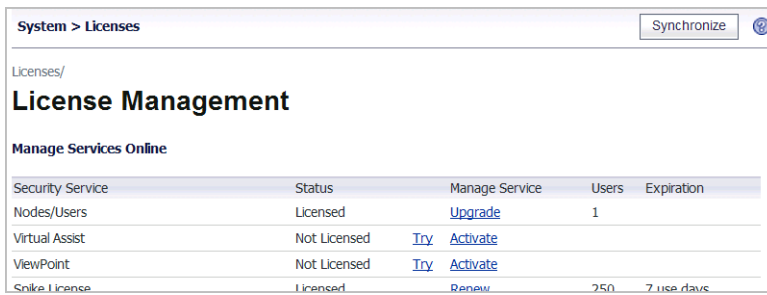
Security Service	Status	Manage Service	Users	Expiration
Nodes/Users	Licensed	<a href="#">Upgrade</a>	1	
Virtual Assist	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>		
ViewPoint	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>		
Spike License	Licensed	<a href="#">Renew</a>	250	7 use days
Web Application Firewall	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>		
Stateful High Availability	Not Licensed	<a href="#">Activate</a>		

Support Service	Status	Manage Service	Expiration
Dynamic Support 8x5	Licensed	<a href="#">Renew</a>	11 Oct 2011
Dynamic Support 24x7	Not Licensed	<a href="#">Activate</a>	
Software and Firmware Updates	Licensed	<a href="#">Renew</a>	11 Oct 2011
Hardware Warranty	Licensed		13 Jul 2012

- Click **Try** to start a 180 day free trial, or click **Activate** to subscribe to the service for 1 year. The screen below is displayed after selecting the free trial.

- 6 Click **Synchronize** to view the license on the **System > Licenses** page.



The screenshot shows the 'System > Licenses' page in a web interface. At the top right, there is a 'Synchronize' button and a refresh icon. Below the breadcrumb 'Licenses/', the main heading is 'License Management'. Underneath, there is a section titled 'Manage Services Online' which contains a table with the following data:

Security Service	Status	Manage Service	Users	Expiration
Nodes/Users	Licensed	<a href="#">Upgrade</a>	1	
Virtual Assist	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>		
ViewPoint	Not Licensed	<a href="#">Try</a> <a href="#">Activate</a>		
Snike License	Licensed	<a href="#">Renew</a>	250	7 use days

Web Application Firewall is now licensed on your SonicWall SMA/SRA appliance. Navigate to **Web Application Firewall > Settings** to enable it, and then restart your appliance to completely activate Web Application Firewall.

# Overview

This section provides an introduction to the Web Application Firewall feature. This section contains the following subsections:

- [What is Web Application Firewall?](#) on page 8
- [Benefits of Web Application Firewall](#) on page 11
- [How Does Web Application Firewall Work?](#) on page 11
- [Supported Platforms](#) on page 20

## What is Web Application Firewall?

Web Application Firewall is subscription-based software that runs on the SonicWall SMA appliance and protects web applications running on servers behind the appliance. Web Application Firewall also provides real-time protection for resources such as HTTP(S) bookmarks, Citrix bookmarks, web applications running on Application Offloading portals, and the SMA management interface and user portal that run on the SonicWall SMA appliance.

The [Definitions of Terms](#) table provides definitions of terminology related to SonicWall SMA Web Application Firewall.

### Definitions of Terms

Term	Definition
Web Application Firewall	Security technology that is placed between a web server and the internet that analyzes layer 7 traffic sessions to protect applications from inbound attacks. A Web Application Firewall determines access permissions based on a pre-defined set of standard and custom rules.
Application Offloading	Application Offloading is the technique of porting part of an application to a nearby server or workstation with more capabilities than the device that will run the application, such as a PDA or mobile phone. Such a server is often public-facing, and may need protection from attacks. Offloaded applications operate in seamless mode in which the URLs in the proxied page are not rewritten by the proxy server.
Reverse Proxy	A proxy server that is deployed between one or more servers (often web servers) and the internet. All connections coming from the internet inbound to one of the web servers are routed through the proxy server, presenting a single interface to external users. The reverse proxy server can fulfill a request itself or pass the request to the main servers.
HTTP(S) Reverse Proxy	This reverse proxy intercepts HTTP(S) requests and responses.

Web Application Firewall provides real-time protection against a whole suite of web attacks such as Cross-site scripting, SQL Injection, OS Command Injection, and many more. The top ten vulnerabilities for web applications are tracked by OWASP, an open source community that focuses its efforts on improving the security of web



applications. SonicWall SMA Web Application Firewall protects against these top ten vulnerabilities, defined in 2007 as follows:

### OWASP Top Ten Vulnerabilities

Name	Description
A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, and possibly introduce worms.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

### Slowloris Protection

In addition to the top ten threats listed above, Web Application Firewall protects against **Slowloris** HTTP Denial of Service attacks. This means that Web Application Firewall also protects all the backend web servers against this attack. Many web servers, including Apache, are vulnerable to Slowloris. Slowloris is especially effective against web servers that use threaded processes and limit the amount of threading allowed.

Slowloris is a stealthy, slow-acting attack that sends partial HTTP requests at regular intervals to hold connections open to the web server. It gradually ties up all the sockets, consuming sockets as they are freed up when other connections are closed. Slowloris can send different host headers, and can send GET, HEAD, and POST requests. The string of partial requests makes Slowloris comparable to a SYN flood, except that it uses HTTP rather than TCP. Only the targeted web server is affected, while other services and ports on the same server are still available. When the attack is terminated, the web server can return to normal within as little as 5 seconds, making Slowloris useful for causing a brief downtime or distraction while other attacks are initiated. Once the attack stops or the session is closed, the web server logs may show several hundred 400 errors.

For more information about how Web Application Firewall protects against the OWASP top ten and Slowloris types of attacks, see the [How Does Web Application Firewall Work?](#) on page 11.

## Offloaded Web Application Protection

Web Application Firewall can also protect an offloaded web application, which is a special purpose portal created to provide seamless access to a web application running on a server behind the SMA/SRA appliance. The portal must be configured as a virtual host. It is possible to disable authentication and access policy enforcement for such an offloaded host. If authentication is enabled, a suitable domain needs to be associated with this portal and all SonicWall advanced authentication features such as One Time Password, Two-factor Authentication, and Single Sign-On apply to the offloaded host.

## Application Profiling

Application Profiling (Phase 1) allows the administrator to generate custom rules in an automated manner based on a trusted set of inputs. This is a highly effective method of providing security to web applications because it develops a profile of what inputs are acceptable by the application. Everything else is denied, providing positive security enforcement. This results in fewer false positives than generic signatures, which adopt a negative security model. When the administrator places the device in learning mode in a staging environment, the SMA/SRA appliance learns valid inputs for each URL accessed by the trusted users. At any point during or after the learning process, the custom rules can be generated based on the “learned” profiles. Multiple applications can be profiled simultaneously.

## Rate Limiting for Custom Rules

It is possible to track the rate at which a custom rule, or rule chain, is being matched. This is extremely useful to block dictionary attacks or brute force attacks. The action for the rule chain is triggered only if the rule chain is matched as many times as configured.

## Cookie Tampering Protection

Cookie Tampering Protection is an important item in the Payment Card Industry Data Security Standard (PCI DSS) section 6.6 requirements and part of the Web Application Firewall evaluation criteria that offers strict security for cookies set by the backend web servers. Various techniques such as encryption and message digest are used to prevent cookie tampering.

## Credit Card and Social Security Number Protection

Credit Card/SSN protection is a Data Loss Prevention technique that ensures that sensitive information, such as credit card numbers and Social Security numbers are not leaked within web pages. Once such leakage is detected, the administrator can choose to mask these numbers partially or wholly, present a configurable error page, or simply log the event.

## PDF Reporting for WAF Monitoring and PCI DSS 6.5 and 6.6 Compliance

SPDF reporting is introduced for Web Application Firewall Monitoring and PCI DSS 6.5 and 6.6 Compliance. You can generate the reports on the **Web Application Firewall > Status** page. The timeline for generating the data published in the reports is configurable on the **Web Application Firewall > Monitoring** page.

## Benefits of Web Application Firewall

Web Application Firewall is secure and can be used in various areas, including financial services, healthcare, application service providers, and e-commerce. The SonicWall SMA appliance uses SSL encryption to encrypt data between the Web Application Firewall and the client. SMA also satisfies OWASP cryptographic storage requirements by encrypting keys and passwords wherever necessary.

Companies using Web Application Firewall can reduce the development cost required to create secure applications and also cut out the huge turnaround time involved in deploying a newly found vulnerability fix in every web application by signing up for Web Application Firewall signature updates.

Resources accessed over Application Offloaded portals and HTTP(S) bookmarks can be vulnerable due to a variety of reasons ranging from badly designed architecture to programming errors. Web Application Firewall provides an effective way to prevent a hacker from exploiting these vulnerabilities by providing real-time protection to web applications deployed behind the SonicWall Secure Mobile Access/SRA appliance.

Deploying Web Application Firewall at the SMA/SRA appliance lets network administrators use application offloading even when it exposes web applications needing security to internal and remote users. Application offloading avoids URL rewriting, which improves the proxy performance and functionality.

There are several benefits of integrating Web Application Firewall with SonicWall SMA appliances. Firstly, identity-based policy controls are core to Web Application Firewall and this is easily achievable using the SonicWall Secure Mobile Access technology. Secondly, there are lower latencies due to the existing hardware-based SSL offloading. Most importantly, SMA/SRA appliances run web applications and must be protected from such attacks.

As small businesses adopt hosted services to facilitate supplier collaboration, inventory management, online sales, and customer account management, they face the same strict compliance requirements as large enterprises. Web Application Firewall on a SonicWall Secure Mobile Access/SRA appliance provides a convenient, cost-effective solution.

Web Application Firewall is easy to configure in the SonicWall SMA management interface. The administrator can configure Web Application Firewall settings globally, by attack priority, and on a per-signature basis. Once custom configuration settings or exclusions are in place, you can disable Web Application Firewall without losing the configuration, allowing you to perform maintenance or testing and then easily re-enable it.

## How Does Web Application Firewall Work?

To use the Web Application Firewall feature, the administrator must first license the software or start a free trial. Web Application Firewall must then be enabled on the **Web Application Firewall > Settings** page of the SonicWall SMA management interface. Web Application Firewall can be configured to log or block detected attacks arriving from the internet.

The following sections describe how Web Application Firewall and SonicWall SMA prevent attacks such as Slowloris or those listed in the OWASP top ten, and how Web Application Firewall protects against information disclosure, and other capabilities:

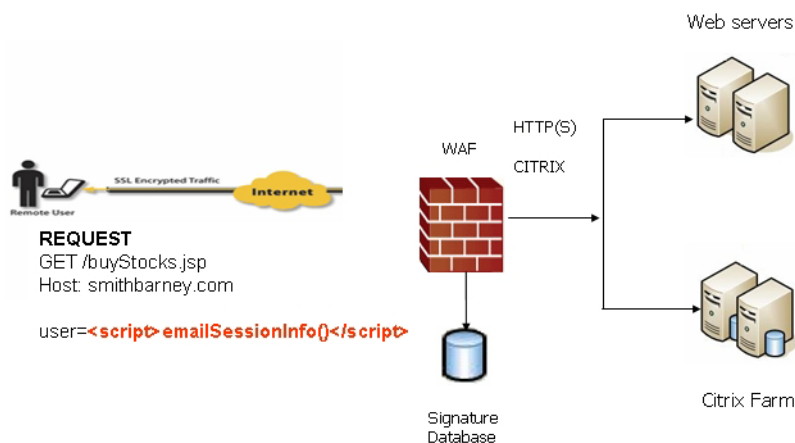
- [How are Signatures Used to Prevent Attacks?](#) on page 12
- [How is Cross-Site Request Forgery Prevented?](#) on page 14

- [How is Information Disclosure Prevented?](#) on page 14
- [How are Broken Authentication Attacks Prevented?](#) on page 15
- [How are Insecure Storage and Communications Prevented?](#) on page 15
- [How is Access to Restricted URLs Prevented?](#) on page 15
- [How are Slowloris Attacks Prevented?](#) on page 15
- [What Type of PCI Compliance Reports Are Available?](#) on page 16
- [How Does Cookie Tampering Protection Work?](#) on page 16
- [How Does Application Profiling Work?](#) on page 18
- [How Does Rate Limiting for Custom Rules Work?](#) on page 19

## How are Signatures Used to Prevent Attacks?

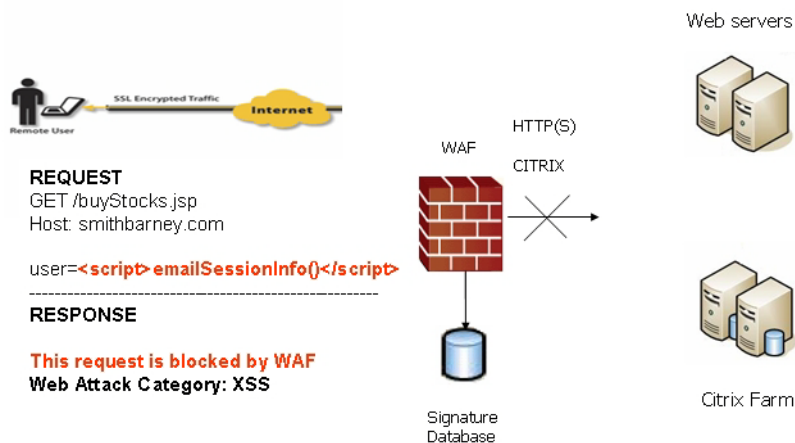
For Cross Site Scripting, Injection Flaws, Malicious File Execution, and Insecure Direct Object Reference vulnerabilities, the Web Application Firewall feature uses a black list of signatures that are known to make web applications vulnerable. New updates to these signatures are periodically downloaded from a SonicWall signature database server, providing protection from recently introduced attacks.

### How signatures prevent attacks



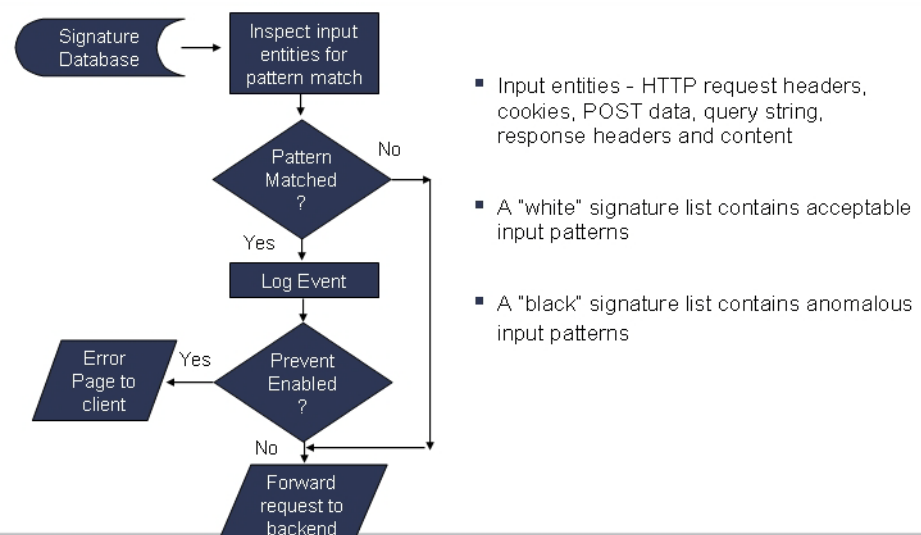
When input arrives from the internet, Web Application Firewall inspects HTTP/HTTPS request headers, cookies, POST data, query strings, response headers, and content. It compares the input to both a black list and a white list of signatures. If pattern matching succeeds for any signature, the event is logged and/or the input is blocked if so configured. If blocked, an error page is returned to the client and access to the resource is prevented. The threat details are not exposed in the URL of the error page. If configured for detection only, the attack is logged but the client can still access the resource. If no signature is matched, the request is forwarded to the web server for handling.

## What happens when no signature is matched



The Web Application Firewall process is outlined in the following flowchart.

## Web Application Firewall process



In the case of a blocked request, the following error page is returned to the client:



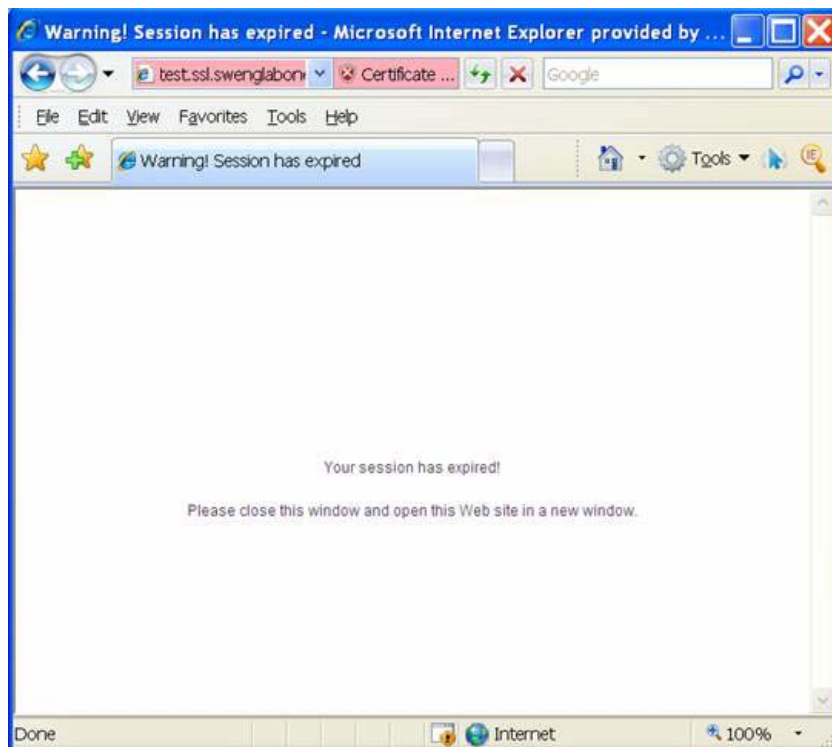
This page is customizable under **Web Application Firewall > Settings** in the SMA management interface. Some administrators might want to customize the HTML contents of this page. Others might not want to present a user friendly page for security reasons. Instead, they might prefer the option to present an HTTP error code such as 404 (Not found) or 403 (Access Denied).

## How is Cross-Site Request Forgery Prevented?

CSRF attacks are not detected with signature matching. Using this vulnerability, a hacker disguised as the victim can gain unauthorized access to application even without stealing the session cookie of a user. While a victim user is authenticated to a web site under attack, the user may unwittingly load a malicious web page from a different site within the same browser process context, for instance, by launching it in a new tab part of the same browser window. If this malicious page makes a hidden request to the victim web server, the session cookies in the browser memory are made part of this request making this an authenticated request. The web server serves the requested web page as it assumes that the request was a result of a user action on its site. To maximize the benefits, hackers typically target actionable requests such as data updates to carry out this attack.

To prevent CSRF attacks, every HTTP request within a browser session needs to carry a token based on the user session. To ensure that every request carries this token, Web Application Firewall rewrites all URLs contained in a web page similarly to how they are rewritten by the Reverse Proxy for HTTP(S) Bookmarks feature. If CSRF protection is enabled, this is also performed for Application Offloading.

CSRF protection is provided for anonymous mode as well. If CSRF protection is enabled, then an idle timeout set to the global idle timeout is enforced for anonymous access. If the session times out, an error message is displayed, forcing the user to revisit the site in a new window. If authentication is enforced for the portal, then the user is redirected to the login page for the portal.



## How is Information Disclosure Prevented?

Web Application Firewall prevents Information Disclosure and Improper Error Handling by providing a way for the administrator to configure text containing confidential and sensitive information so that no web site accessed through the Web Application Firewall reveals this text. These text strings are entered on the **Web Application Firewall > Settings** page.

Beside the ability to pattern match custom text, signatures pertaining to information disclosure are also used to prevent these types of attacks.

Web Application Firewall protects against inadvertent disclosure of credit card and Social Security numbers (SSN) in HTML web pages.

**i** | **NOTE:** Only text or HTML pages, and only the first 512K bytes are inspected for credit card or SSN disclosure.

Web Application Firewall can identify credit card and SSN numbers in various formats. For example, a SSN can be specified as XXX XX XXXX or XXX-XX-XXXX. Web Application Firewall attempts to eliminate false-positives by filtering out formats that do not conform to the credit card or SSN specification. For example, credit cards follow the Luhn's algorithm to determine if an n-digit number could be a credit card number or not.

The administrator can set an appropriate action, such as detect (log), prevent, or just mask the digits that can reveal the user identity. Masking can be done fully or partially, and you can select any of the following characters for masking: #, \*, -, x, X, ., !, \$, and ?. The resulting masked number is similar to the appearance of credit card numbers printed on an invoice.

## How are Broken Authentication Attacks Prevented?

The requirement for Broken Authentication and Session Management requires Web Application Firewall to support strong session management to enhance the authorization requirements for web sites. SonicWall SMA already has strong authentication capabilities with the ability to support One Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication.

For Session Management, Web Application Firewall pops up a session logout dialog box when the user portal is launched or when a user logs into an application offloaded portal. This feature is enabled by default when Web Application Firewall is licensed and can be disabled from the **Web Application Firewall > Settings** page.

The **Web Application Firewall > Settings** page also allows the administrator to configure the global idle session timeout. It is highly recommended that this timeout value is kept as low as possible.

## How are Insecure Storage and Communications Prevented?

Insecure Cryptographic Storage and Insecure Communications are prevented by encrypting keys and passwords wherever necessary, and by using SSL encryption to encrypt data between the Web Application Firewall and the client. SonicWall SMA also supports HTTPS with the backend web server.

## How is Access to Restricted URLs Prevented?

SonicWall SMA supports access policies based on host, subnet, protocol, URL path, and port to allow or deny access to web sites. These policies can be configured globally or for users and groups.

## How are Slowloris Attacks Prevented?

Slowloris attacks can be prevented if there is an upstream device, such as a SonicWall SMA appliance, that limits, buffers, or proxies HTTP requests. Web Application Firewall uses a rate-limiter to thwart Slowloris HTTP Denial of Service attacks.

# What Type of PCI Compliance Reports Are Available?

Payment Card Industry Data Security Standard (PCI DSS) 6.5 (Version 2.0) and PCI DSS 6.6 (Version 1.2) are covered in PCI reporting. The administrator can configure Web Application Firewall to satisfy these PCI requirements.

You can generate and download the PCI report file on the **Web Application Firewall > Status** page.

**NOTE:** This is not an official PCI Compliance report. It is for your self-assessment only.



Two tables are dynamically generated in the PCI compliance report to display the status of each PCI requirement. The format of the table is shown in the example below:

PCI DSS 6.5 Compliance Report		
PCI DSS 6.5 Requirements	Status	Comments
1. Injection flaws, particularly SQLInjection. Also consider OS CommandInjection, LDAP and XPath injectionflaws as well as other injection flaws.	Partially Satisfied	Please update your WAF signatures.

The first column describes the PCI requirement.

The second column displays the status of the PCI requirement under current Web Application Firewall settings. There are four possible values for the status, distinguished by color.

- Satisfied (Green)
- Partially Satisfied (Orange)
- Unsatisfied (Red)
- Unable to determine (Black)

The third column provides comments and details explaining the status rating. If the status is Satisfied, no comments are provided.

## How Does Cookie Tampering Protection Work?

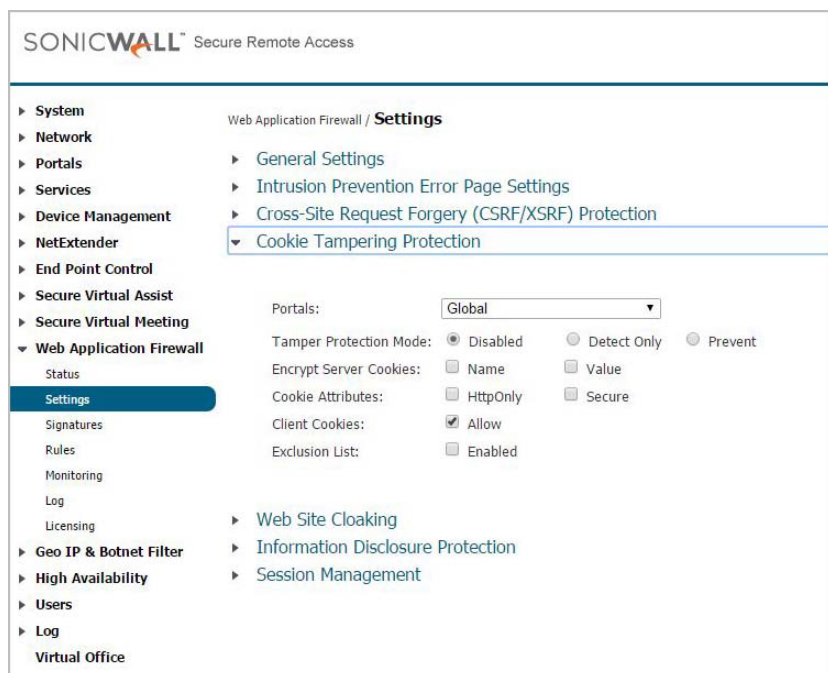
The SonicWall Secure Mobile Access/SRA appliance protects important server-side cookies from tampering. There are two kinds of cookies:

**Server-Side Cookies** – These cookies are generated by backend web servers. They are important and have to be protected. They have optional attributes like *Path*, *Domain*, *Secure*, and *HttpOnly*.

**Client-Side Cookies** – These cookies are created by client side scripts in user browsers. They are not safe, and can be easily tampered with.



This feature is found on the **Web Application Firewall > Settings** page.



This page contains the following options:

**Portals** – A list of all application offloading portals. Each portal will have its own setting. The item **Global** is the default setting for all portals.

**Tamper Protection Mode** – Three modes are available:

- **Disabled** – Cookie tamper protection is disabled.
- **Detect only** – Log the tampered cookies only.
- **Prevent** – Strip all the tampered cookies and log them.
- **Inherit Global** – Use the global setting for this portal. This option is not available when **Global** is selected in the **Portals** drop-down list.

**Encrypt Server Cookies** – Choose to encrypt name and value separately. This affects client-side script behavior because it makes cookie names or values unreadable. Only server-side cookies are encrypted by these options.

**Cookie Attributes** – The attributes *HttpOnly* and *Secure* are appended to server-side cookies if they are enabled.

The attribute *HttpOnly* prevents the client-side scripts from accessing the cookies, which is important in mitigating attacks such as Cross Site Scripting and session hijacking. The attribute *Secure* ensures that the cookies are transported only in HTTPS connections. Both together add a strong layer of security for the server-side cookies.

**NOTE:** By default, the attribute *Secure* is always appended to an HTTP connection even if Cookie Tampering Protection is disabled. This behavior is a configurable option, and can be turned off.

**Client Cookies** – The Client Cookies **Allow** option is enabled by default. In Strict mode, the **Allow** option is disabled. When disabled, client-side cookies are not allowed to be sent to the backend systems. This option does not affect server-side cookies.

**Exclusion List** – If the Exclusion List is enabled and contains a cookie, the cookie is passed as usual and is not protected. You can exclude server-side cookies and client-side cookies.

Exclusion list items are case sensitive, and in the format 'CookieName@CookiePath'. Cookies with the same name and different paths are treated as different cookies. 'CookiePath' can be left empty to represent any path.

**Import Global** – Application Offloading portals can import the Global exclusion list.

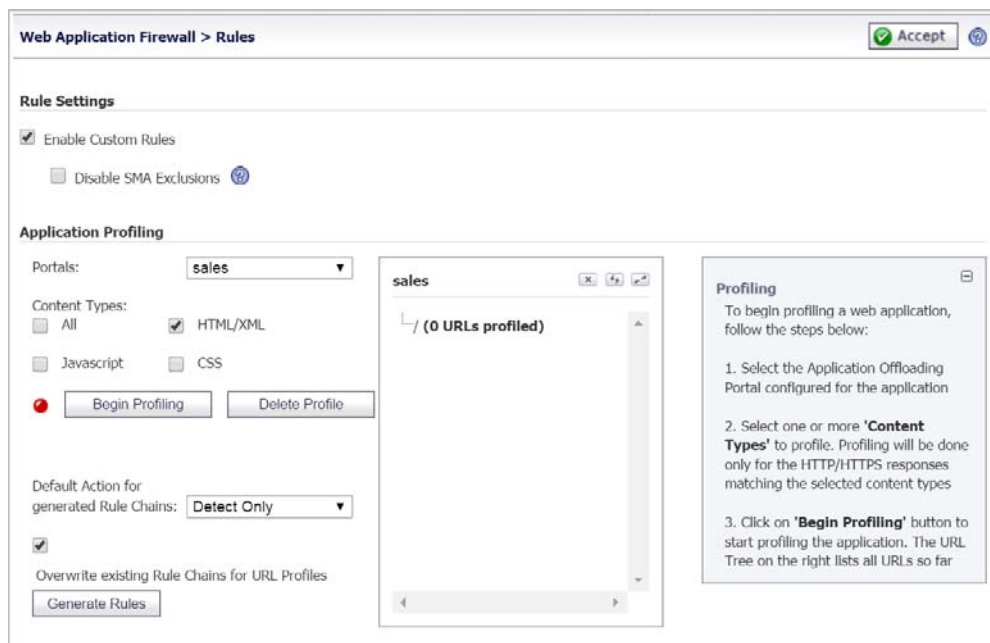
## How Does Application Profiling Work?

The administrator can configure application profiling on the **Web Application Firewall > Rules** page. Application profiling is performed independently for each portal.

After selecting the portal, you can select the type of application content that you want to profile. You can choose **HTML/XML**, **Javascript**, **CSS**, or **All**, which includes all content types such as images, HTML, and CSS. HTML/XML content is the most important from a security standpoint, because it typically covers the more sensitive web transactions. This content type is selected by default.

**NOTE:** Content types can be saved for applications currently being profiled.

Then the SonicWall SMA appliance is placed in learning mode by clicking on the **Begin Profiling** button (the button then changes to **End Profiling**). The profiling should be done while trusted users are using applications in an appropriate way. The SMA records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the **Web Application Firewall > Rules** page in the Application Profiling section.



Only the URLs presented as hyperlinks are accessible URLs on the backend server. You can click on the hyperlink to edit the learned values for that URL if the values are not accurate. You can then generate rules to use the modified URL profile.

The SMA learns the following HTTP Parameters:

- Response Status Code
- Post Data Length – The Post Data Length is estimated by learning the value in the Content-Length header. The maximum size is set to the power of two that is closest to and higher than this value. This accommodates the amount of memory that may have been allocated by the backend application. For example, for a Content Length of 65, the next power of two greater than 65 is 128. This is the limit configured in the URL profile. If the administrator determines that this is not accurate, the value can be modified appropriately.
- Request Parameters – This is the list of parameters that a particular URL can accept.

When an adequate amount of input has been learned, you can click the **End Profiling** button and are ready to generate the rules from the learned input. You can set one of the following as a default action for the generated rule chains:

- Disabled – The generated rules will be disabled rather than active.
- Detect Only – Content triggering the generated rule will be detected and logged.
- Prevent – Content triggering the generated rule will be blocked and logged.

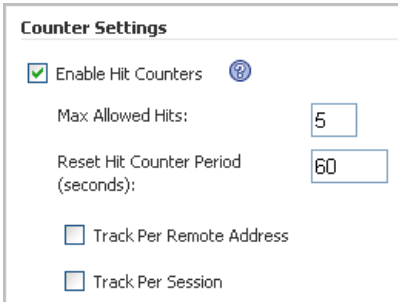
If a rule chain has already been generated from a URL profile in the past, then the rule chain will be overwritten only if **Overwrite existing Rule Chains for URL Profiles** is selected. When you click the **Generate Rules** button, the rules are generated from the URL profiles. If a URL profile has been modified, those changes are incorporated.


## How Does Rate Limiting for Custom Rules Work?

The administrator can configure rate limiting when adding or editing a rule chain from the **Web Application Firewall > Rules** page. When rate limiting is enabled for a rule chain, the action for the rule chain is triggered only when the number of matches within a configured time period is above the configured threshold.

This type of protection is useful in preventing Brute Force and Dictionary attacks. An example rule chain with a Rule Chain ID of 15002 is available in the management interface for administrators to use as reference.

The associated fields are exposed when **Enable Hit Counters** is selected at the bottom of the **New Rule Chain** or **Edit Rule Chain** screen.



Counter Settings	
<input checked="" type="checkbox"/> Enable Hit Counters	
Max Allowed Hits:	<input type="text" value="5"/>
Reset Hit Counter Period (seconds):	<input type="text" value="60"/>
<input type="checkbox"/> Track Per Remote Address	
<input type="checkbox"/> Track Per Session	

Once a rule chain is matched, Web Application Firewall keeps an internal counter to track how many times the rule chain is matched. The **Max Allowed Hits** field contains the number of matches that must occur before the rule chain action is triggered. If the rule chain is not matched for the number of seconds configured in the **Reset Hit Counter Period** field, then the counter is reset to zero.

Rate limiting can be enforced per remote IP address or per user session or both. **Track Per Remote Address** enables rate limiting based on the attacker's remote IP address.

**Track Per Session** enables rate limiting based on the attacker's browser session. This method sets a cookie for each browser session. Tracking by user session is not as effective as tracking by remote IP if the attacker initiates a new user session for each attack.

The **Track Per Remote Address** option uses the remote address as seen by the SMA/SRA appliance. In the case where the attack uses multiple clients from behind a firewall that is configured with NAT, the different clients effectively send packets with the same source IP address and will be counted together.

# Supported Platforms

Web Application Firewall is available on the following SMA/SRA appliances:

- SMA 200
- SMA 400
- SRA 1600
- SRA 4600
- SMA 500v Virtual Appliance

 **NOTE:** Application profiling is supported only on the SMA 400, SRA 4600, and SMA 500v Virtual Appliance.

# Configuring Web Application Firewall

**NOTE:** Web Application Firewall requires the purchase of an additional license.

To configure the Web Application Firewall feature, see the following sections:

- [Viewing and Updating Web Application Firewall Status](#) on page 21
- [Configuring Web Application Firewall Settings](#) on page 23
- [Configuring Web Application Firewall Signature Actions](#) on page 32
- [Determining the Host Entry for Exclusions](#) on page 36
- [Configuring Custom Rules and Application Profiling](#) on page 38
- [Using Web Application Firewall Monitoring](#) on page 55
- [Using Web Application Firewall Logs](#) on page 62

Web Application Firewall is often used to protect an Application Offloading portal. [Configuring an Application Offloading Portal](#) on page 65 summarizes how to configure an Application Offloading portal. See the *SonicWall SMA Application Offloading and HTTP(S) Bookmarks Feature Guide* or the *SMA 8.6 Administration Guide* for more detailed information.

## Viewing and Updating Web Application Firewall Status

The **Web Application Firewall > Status** page provides status information about the Web Application Firewall signature database and displays the license status and expiration date. The **Synchronize** button allows you to download the latest signatures from the SonicWall online database. You can use the **Download** button to generate and download a PCI compliance report file.

Web Application Firewall / **Status** ?

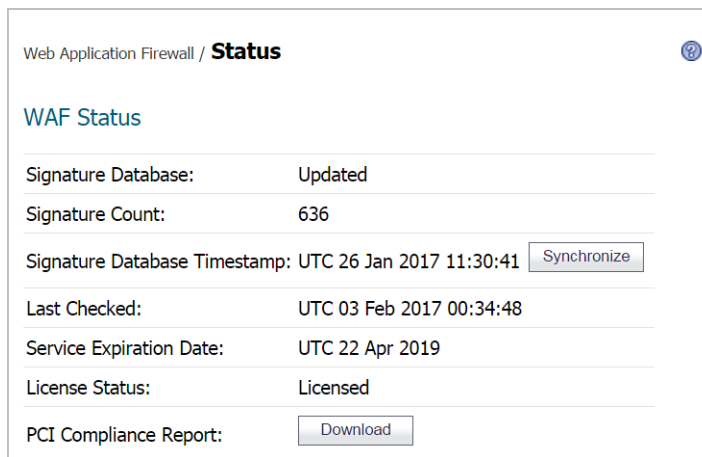
**WAF Status**

Signature Database:	Update available	<input type="button" value="Apply"/>
Signature Count:	632	
Signature Database Timestamp:	UTC 26 Jan 2017 11:30:41	<input type="button" value="Synchronize"/>
Last Checked:	UTC 02 Feb 2017 23:54:22	
Service Expiration Date:	UTC 22 Apr 2019	
License Status:	Licensed	
PCI Compliance Report:		<input type="button" value="Download"/>

# Viewing Status and Synchronizing Signatures

To view the status of the signature database and Web Application Firewall service license, and synchronize the signature database, perform the following steps in the appliance management interface:

- 1 Navigate to **Web Application Firewall > Status**. The WAF Status section displays the following information:
  - Status of updates to the signature database
  - Timestamp of the signature database
  - Time that the system last checked for available updates to the signature database
  - Expiration date of the Web Application Firewall subscription service
  - Status of the Web Application Firewall license



- 2 If updates are available for the signature database, the **Apply** button is displayed. Click **Apply** to download the updates.  
  
You can select an option to update and apply new signatures automatically on the **Web Application Firewall > Settings** page. If this automatic update option is enabled, the **Apply** button disappears from the **Web Application Firewall > Status** page as soon as the new signatures are automatically applied.
- 3 To synchronize the signature database with the SonicWall online database server, click **Synchronize**. The timestamp is updated.

## Downloading a PCI Compliance Report

*To download a PCI DSS 6.5/6.6 compliance report:*

- 1 Navigate to **Web Application Firewall > Status**.
- 2 Click the **Download** button.

- In the File Download dialog box, click **Open** to create the PCI report as a temporary file and view it with Adobe Acrobat, or click **Save** to save the report as a PDF file.



## Configuring Web Application Firewall Settings

The **Web Application Firewall > Settings** page allows you to enable and disable Web Application Firewall on your SonicWall SMA/SRA appliance globally and by attack priority. You can individually specify detection or prevention for three attack classes: high, medium, and low priority attacks.

Web Application Firewall / **Settings** Accept ?

▶ **General Settings**

WAF Global Settings

Enable Web Application Firewall

Apply Signature Updates Automatically ?

Request Payload Limit (KB):  ?

Signature Groups	Prevent All	Detect All
High Priority Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Medium Priority Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Low Priority Attacks	<input type="checkbox"/>	<input checked="" type="checkbox"/>

▶ [Intrusion Prevention Error Page Settings](#)

▶ [Cross-Site Request Forgery \(CSRF/XSRF\) Protection](#)

▶ [Cookie Tampering Protection](#)

▶ [Web Site Cloaking](#)

▶ [Information Disclosure Protection](#)

▶ [Session Management](#)

This page also provides configuration options for other Web Application Firewall settings. The following sections describe the procedures for enabling and configuring Web Application Firewall settings:

- [Enabling Web Application Firewall and Configuring General Settings](#) on page 24
- [Configuring Global Exclusions](#) on page 25
- [Configuring Intrusion Prevention Error Page Settings](#) on page 26
- [Configuring Cross-Site Request Forgery Protection Settings](#) on page 27
- [Configuring Cookie Tampering Protection Settings](#) on page 28
- [Configuring Web Site Cloaking](#) on page 30
- [Configuring Information Disclosure Protection](#) on page 30
- [Configuring Session Management Settings](#) on page 32

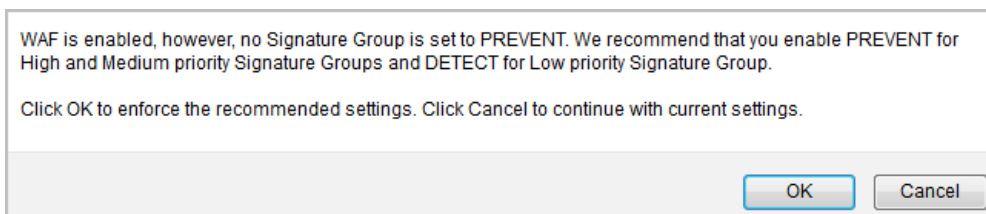
## Enabling Web Application Firewall and Configuring General Settings

To enable and activate Web Application Firewall, you must select the checkbox to globally enable it and select at least one of the checkboxes in the Signature Groups table. The settings in the General Settings section on this page allow you to globally manage your network protection against attacks by selecting the level of protection for high, medium, or low priority attacks. You can also clear the global **Enable Web Application Firewall** checkbox to temporarily disable Web Application Firewall without losing any of your custom configuration settings.

You can enable automatic signature updates in the **General Settings** section, so that new signatures are automatically downloaded and applied when available. A log entry is generated for each automatic signature update. If a signature is deleted during automatic updating, its associated Exclusion List is also removed. A log entry is generated to record the removal. You can view the log entries on the **Web Application Firewall > Logs** page.

### *To configure global settings for Web Application Firewall:*

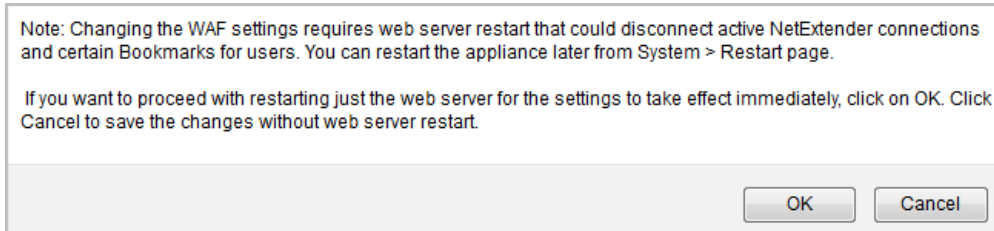
- 1 On the **Web Application Firewall > Settings** page, expand the **General Settings** section.
- 2 Select **Enable Web Application Firewall**.
- 3 A warning dialog box is displayed if none of the signature groups have **Prevent All** already selected. Click **OK** in the dialog box to set all signature groups to **Prevent All**, or click **Cancel** to leave the settings as they are or to manually continue the configuration.



- 4 Select **Apply Signature Updates Automatically** to enable new signatures to be automatically downloaded and applied when available. You do not have to click the **Apply** button on the **Web Application Firewall > Status** page to apply the new signatures.
- 5 Select the desired level of protection for **High Priority Attacks** in the Signature Groups table. Select one of the following options:
  - Select **Prevent All** to block access to a resource when an attack is detected. Selecting **Prevent All** automatically selects **Detect All**, turning on logging.
  - Clear **Prevent All** and select **Detect All** to log attacks while allowing access to the resource.



- To globally disable all logging and prevention for this attack priority level, clear both checkboxes.
- 6 Select the desired level of protection for **Medium Priority Attacks** in the Signature Groups table.
  - 7 Select the desired level of protection for **Low Priority Attacks** in the Signature Groups table.
  - 8 When finished, click **Accept**.
  - 9 Click **OK** in the confirmation dialog if it is displayed.



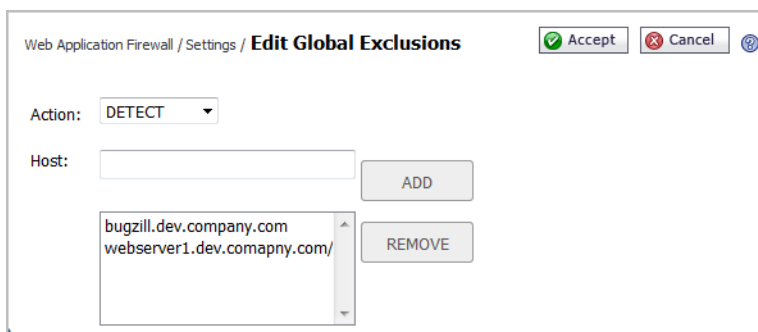
## Configuring Global Exclusions

There are three ways that you can exclude certain hosts from currently configured global Web Application Firewall settings. You can completely disable Web Application Firewall for certain hosts, you can lower the action level from Prevent to Detect for certain hosts, or you can set Web Application Firewall to take no action.

The affected hosts must match the host names used in your HTTP(S) bookmarks and Citrix bookmarks, and the Virtual Host Domain Name configured for an offloaded web application.

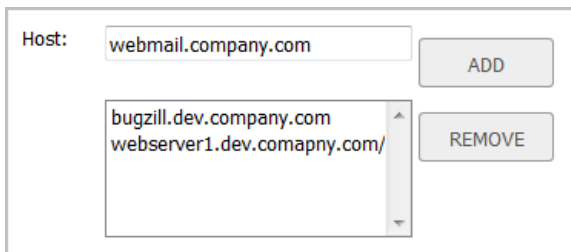
### To configure global exclusions:

- 1 On the **Web Application Firewall > Settings** page, expand the **General Settings** section.
- 2 Click **Global Exclusions**.
- 3 In the Edit Global Exclusions page, the action you set overrides the signature group settings for the resources configured on these host pages. Select one of the following from the **Action** drop-down list:
  - **Disable** – Disables Web Application Firewall inspection for the host.
  - **Detect** – Lowers the action level from prevention to only detection and logging for the host.
  - **No Action** – Web Application Firewall inspects host traffic, but takes no action.



- 4 In the **Host** field, type the host entry as it appears in the bookmark or offloaded application. This can be a host name or IP address. Up to 32 characters are allowed. To determine the correct host entry for this

exclusion, see [Determining the Host Entry for Exclusions](#) on page 36.



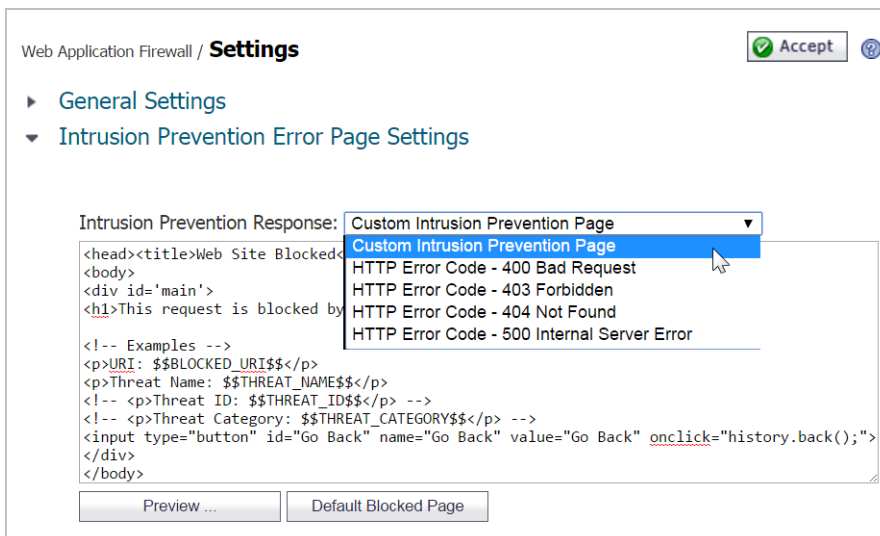
You can configure a path to a particular folder or file along with the host. The protocol, port, and the request parameters are simply ignored in the URL. If a path is configured, then the exclusion is recursively applied to all subfolders and files. For instance, if **Host** is set to **webmail.company.com/exchange**, then all files and folders under **exchange** are also excluded.

- 5 Click **ADD** to move the host name into the list box.
- 6 Repeat [Step 4](#) and [Step 5](#) to add more hosts to this exclusion.
- 7 When finished, click **Accept**.

## Configuring Intrusion Prevention Error Page Settings

*To configure the error page to use when intrusions are detected:*

- 1 Expand the **Intrusion Prevention Error Page Settings** section.
- 2 In the **Intrusion Prevention Response** drop-down list, select the type of error page to be displayed when blocking an intrusion attempt.



- 3 To create a custom page, select **Custom Intrusion Prevention Page** and modify the sample HTML in the text box.
- 4 To view the resulting page, click the **Preview** button.
- 5 To reset the current customized error page to the default error page, click the **Default Blocked Page** button and then click **OK** in the confirmation dialog box.
- 6 If you do not want to use a customized error page, select one of the following for the error page:
  - HTTP Error Code 400 Bad Request

- HTTP Error Code 403 Forbidden
- HTTP Error Code 404 Not Found
- HTTP Error Code 500 Internal Server Error

7 When finished, click **Accept**.

## Configuring Cross-Site Request Forgery Protection Settings

Cross-Site Request Forgery protection is configured independently for each Application Offloading portal. New with this release is the Form based Protection Method, which provides a seamless solution and results in less false positives. Optionally when upgrading from a previous release, you can keep the original Protection Method, URL Rewrite-based Protection Method.

When a CSRF attack is detected, log entries are created in both the **Web Application Firewall > Logs** and **Logs > View** pages. For more information about CSRF/XSRF attacks, see [How is Cross-Site Request Forgery Prevented?](#) on page 14.

### To configure the settings for CSRF protection with the Form-based Protection Method:

- 1 Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.
- 2 In the **Portals** drop down list, select the Portal to which these CSRF protection settings will apply. To make these CSRF settings the default for all portals, select **Global**.
- 3 Select **Form-based Protection** from the **Protection Method** drop down list.
- 4 For **Content Types**, select the types of content you want to be profiled by CSRF. You can select **All**, **HTML/XML**, **Javascript**, or **CSS**.
- 5 Click the **Begin Profiling** button to start the CSRF Form-based Protection. If you wish to stop profiling, click **End Profiling**.
- 6 When finished, click **Accept**.

Web Application Firewall / **Settings** Accept

- ▶ General Settings
- ▶ Intrusion Prevention Error Page Settings
- ▼ Cross-Site Request Forgery (CSRF/XSRF) Protection
  - Portals:
  - Protection Method:
  - Protection Mode:  Disabled  Detect Only  Prevent  Inherit Global
- ▶ Cookie Tampering Protection
- ▶ Web Site Cloaking
- ▶ Information Disclosure Protection
- ▶ Session Management

**NOTE:** If you are upgrading from a previous firmware version and switch the Protection Method to **Form-based Protection**, the controls may appear grayed and disabled. Simply click the **Accept** button to activate the controls.

**To configure the settings for CSRF protection with URL Rewrite-based Protection Method:**

- 1 Expand the **Cross-Site Request Forgery (CSRF/XSRF) Protection** section.
- 2 In the **Portals** drop-down list, select the Application Offloading portal to which these CSRF protection settings will apply. To make these CSRF settings the default for all portals, select **Global**.
- 3 Select **URL Rewrite-based Protection** from the **Protection Method** drop down list.
- 4 For **Protection Mode**, select the desired level of protection against CSRF attacks. You can select **Detect Only** to log these attacks, or **Prevent** to log and block them. Select **Disabled** to disable CSRF protection on the portal.
- 5 When finished, click **Accept**.

## Configuring Cookie Tampering Protection Settings

Cookie tampering protection is configured independently for each Application Offloading portal.

**To configure the settings for cookie tampering protection:**

- 1 Expand the **Cookie Tampering Protection** section.

Web Application Firewall / **Settings** Accept ?

- ▶ General Settings
- ▶ Intrusion Prevention Error Page Settings
- ▶ Cross-Site Request Forgery (CSRF/XSRF) Protection
- ▼ **Cookie Tampering Protection**

Portals:

Tamper Protection Mode:  Disabled  Detect Only  Prevent

Encrypt Server Cookies:  Name  Value

Cookie Attributes:  HttpOnly  Secure

Client Cookies:  Allow

Exclusion List:  Enabled

- ▶ Web Site Cloaking
- ▶ Information Disclosure Protection
- ▶ Session Management

- 2 In the **Portals** drop-down list, select the Application Offloading portal to which these cookie tampering protection settings will apply. To make these cookie tampering settings the default for all portals, select **Global**.
- 3 For **Tamper Protection Mode**, select the desired level of protection against cookie tampering. You can select **Detect Only** to log these attacks, or **Prevent** to log and block them. Select **Disabled** to disable cookie tampering protection on the portal.
- 4 For **Encrypt Server Cookies**, select **Name** to encrypt cookie names, and/or select **Value** to encrypt cookie values. This affects client-side script behavior because it makes cookie names or values unreadable. Only server-side cookies are encrypted by these options.
- 5 For **Cookie Attributes**, select **HttpOnly** to append the *HttpOnly* attribute to server-side cookies, and/or select **Secure** to append the *Secure* attribute to server-side cookies. The attribute *HttpOnly* prevents the

client-side scripts from accessing the cookies, which is important in mitigating attacks such as Cross Site Scripting and session hijacking. The attribute *Secure* ensures that the cookies are transported only in HTTPS connections. Both together add a strong layer of security for the server-side cookies.

- 6 For **Client Cookies**, select **Allow** if an application on the portal needs all of the client cookies. When disabled, client-side cookies are not allowed to be sent to the backend systems. This option does not affect server-side cookies.
- 7 For the **Exclusion List**, select **Enabled** to display additional fields for configuration.

- 8 To enter a custom cookie name and path to the **Exclusion List**, click in the **Cookie Name** field to type in the name of the cookie, and click in the **Cookie Path** field to type in the path. Then click the **Add >** button.
- 9 To add one or more already-detected cookies to the **Exclusion List**, select the desired cookies in the **Detected Cookies** list, holding the **Ctrl** key while clicking multiple cookies, and then click the **< Add** button to add them to the **Exclusion List**.
- 10 To remove cookies from the **Exclusion List**, select the cookies to be removed and then click the **Remove** button.
- 11 To clear the **Detected Cookies** list, click the **Clear** button.
- 12 When finished, click **Accept**.

## Configuring Web Site Cloaking

Under **Web Site Cloaking**, you can filter out headers in response messages that could provide information to clients about the backend web server, which could possibly be used to find a vulnerability.

### To configure web site cloaking:

- 1 Expand the **Web Site Cloaking** section.
- 2 In the **Block Response Header** fields, type the server host name into the first field and type the header name into the second field, then click **Add**.

For example, if you set the host name to “webmail.xyz.com” and the header name to “X-OWA-version”, headers with the name “X-OWA-version” from host “webmail.xyz.com” will be blocked. In general, listed

headers will not be sent to the client if an HTTP/HTTPS bookmark or offloaded application is used to access a listed web server.

To block a certain header from all hosts, set the host name to an asterisk (\*). You can add up to 64 host/header pairs. In the HTTP protocol, response headers are not case sensitive.

**NOTE:** Blocking will not occur for headers such as Content-Type that are critical to the HTTP protocol.

- 3 To remove a host/header pair from the list to be blocked, select the pair in the text box and then click the **Remove** button.
- 4 When finished, click **Accept**.

## Configuring Information Disclosure Protection

Under **Information Disclosure Protection**, you can protect against inadvertent disclosure of credit card and Social Security numbers (SSN) in HTML web pages. You can also enter confidential text strings that should not be revealed on any web site protected by Web Application Firewall.

### To configure information disclosure protection:

- 1 Expand the **Information Disclosure Protection** section. The table contains a row for each possible pattern or representation of a social security number or credit card number that Web Application Firewall can detect in the HTML response.

**Information Disclosure Protection**

Credit Card/SSN Protection

Enable Credit Card/SSN Protection

Mask Character:

ID	Type	Disabled	Detect	Mask Partially	Mask Fully	Block
20000	Social Security Number (SSN) Disclosure - United States	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20001	Social Security Number (SSN) Disclosure - United States (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20002	Visa Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20003	Visa Credit Card Number Disclosure (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
20004	MasterCard Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20005	MasterCard Credit Card Number Disclosure (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
20006	American Express Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20007	American Express Credit Card Number Disclosure (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
20008	Discover Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20009	Discover Credit Card Number Disclosure (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
20010	Diners Club Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20011	Diners Club Credit Card Number Disclosure(with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20012	JCB Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20013	JCB Credit Card Number Disclosure (with spaces or dashes)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20014	enRoute Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20015	Solo Credit Card Number Disclosure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
20016	Taiwan Identification Number	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Information Disclosure Protection

Block sensitive information within HTML pages

- 2 Select **Enable Credit Card/SSN Protection**.
- 3 In the **Mask Character** drop-down list, select the character to be substituted when masking the SSN or credit card number.
- 4 In the table, select the level of protection desired for each representation of a SSN or credit card number. You can select one of the following in each row:

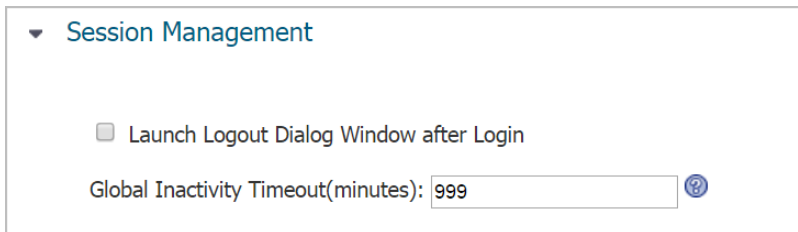
- **Disabled** – Do not match numbers in this format. No logging or masking is performed.
  - **Detect** – Detect numbers in this format and create a log entry when detected.
  - **Mask Partially** – Substitute the masking character for the all digits in the number, except the last few digits such that the confidentiality of the number is still preserved.
  - **Mask Fully** – Substitute the masking character for all digits in the number.
  - **Block** – Do not transmit or display the number at all, even in masked format.
- 5 Below the table, in the **Block sensitive information within HTML pages** text box, type confidential text strings that should not be revealed on any web site protected by Web Application Firewall. This text is case insensitive, can include any number of spaces between the words, but cannot include wildcard characters. Add new phrases on separate lines. Each line is pattern matched within any HTML response.
  - 6 When finished, click **Accept**.

## Configuring Session Management Settings

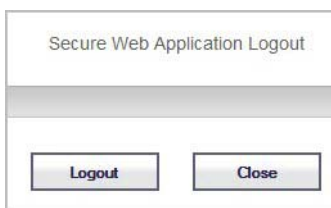
Under **Session Management**, you can control whether the logout dialog window is displayed when a user logs into the user portal or into an application offloaded portal. You can also set the inactivity timeout for users in this section.

*To configure session management settings:*

- 1 Expand the **Session Management** section.



- 2 Select **Launch Logout Dialog Window after Login** to display the session logout popup dialog box when the user portal is launched or when a user logs into an application offloaded portal.



- 3 In the **Global Inactivity Timeout** field, type the number of inactive minutes allowed before the user is logged out. This setting can be overridden by Group or User settings.

**i** **NOTE:** To mitigate CSRF attacks, it is important to keep a low idle timeout value for user sessions, such as 10 minutes.

- 4 When finished, click **Accept**.

# Configuring Web Application Firewall Signature Actions

The **Web Application Firewall > Signatures** page allows you to configure custom handling or exclusion of certain hosts on a per-signature basis. You can use signature-based exclusions to apply exclusions for all hosts for each signature.

You can also revert back to using the global settings for the signature group to which this signature belongs without losing the configuration details of existing exclusions.

Web Application Firewall / **Signatures** Accept

WAF Signature Settings

Enable Performance Optimization

Search  in All Fields Search Exclude Reset

Items per page  Items  to 100 (of 636)

ID	Signature	Threat Classification	Severity	Configure
1000	Blind SQL Injection Attack Variant 4	Command Execution--SQL Injection	HIGH	
1001	Blind SQL Injection Attack Variant 5	Command Execution--SQL Injection	MEDIUM	
1002	Blind SQL Injection Attack Variant 6	Command Execution--SQL Injection	MEDIUM	
1003	Blind SQL Injection Attack Variant 7	Command Execution--SQL Injection	MEDIUM	
1004	Blind SQL Injection Attack Variant 8	Command Execution--SQL Injection	MEDIUM	
1005	Blind SQL Injection Attack Variant 9	Command Execution--SQL Injection	MEDIUM	
1008	AnyInventory environment.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1009	WebED viewitem.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1010	absolute_path Remote File Inclusion	Command Execution--SSI Injection	LOW	
1011	iziContents search.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1012	php wcms XT config_PHPLM.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1013	Trionic Cite CMS custom.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1014	WebDesktop apps.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	
1015	Pindorama client.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	

Signatures listed on this page can be divided into pages (default is 50 signatures per page) and filtered by searching for a key word. To display only signatures containing a key word in all fields or a specific field, type the key word in the Search field, select All Fields or a specific field to search, and click **Search**. All matches are highlighted. Or, click **Exclude** to display only signatures that do not contain the key word. Click **Reset** to display all signatures. In addition, the list can be sorted by the contents of any column in ascending or descending order by clicking the column heading.

On the Settings page, global settings must be set to either Prevent All or Detect All for the Signature Group to which the specific signature belongs. If neither is set, that Signature Group is globally disabled and cannot be modified on a per-signature basis. See [Enabling Web Application Firewall and Configuring General Settings](#) on page 24.

Signature Groups	Prevent All	Detect All
High Priority Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Medium Priority Attacks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Low Priority Attacks	<input type="checkbox"/>	<input checked="" type="checkbox"/>

See the following sections:

- [Enabling Performance Optimization](#) on page 33
- [Configuring Signature Based Custom Handling and Exclusions](#) on page 34
- [Reverting a Signature to Global Settings](#) on page 35



- [Removing a Host from a Per-Signature Exclusion](#) on page 36

## Enabling Performance Optimization

The Performance Optimization option allows you to disable some relatively less severe signatures that significantly affect the performance of certain web applications. These signatures are identified by the SonicWall signature team and the list is pushed out to SonicWall SMA/SRA appliances. When you select **Enable Performance Optimization**, these signatures are disabled for Web Application Firewall.

The **Web Application Firewall > Signatures** page indicates the disabled signatures by displaying them in gray, as shown in [Enabling Performance Optimization](#).

### Enabling Performance Optimization

The screenshot shows the 'Web Application Firewall / Signatures' page. At the top right, there is an 'Accept' button with a green checkmark. Below the title, there are 'WAF Signature Settings' including a checkbox for 'Enable Performance Optimization' which is checked. There is a search bar with a dropdown set to 'All Fields', a 'SEARCH' button, and 'EXCLUDE' and 'RESET' buttons. Below the search bar, it shows 'Items per page 100' and 'Items 1 to 100 (of 642)'. A table lists three signatures that are disabled (shown in gray):


ID	Signature	Threat Classification	Severity	Configure
1000	Blind SQL Injection Attack Variant 4	Command Execution--SQL Injection	HIGH	
1001	Blind SQL Injection Attack Variant 5	Command Execution--SQL Injection	MEDIUM	
1002	Blind SQL Injection Attack Variant 6	Command Execution--SQL Injection	MEDIUM	

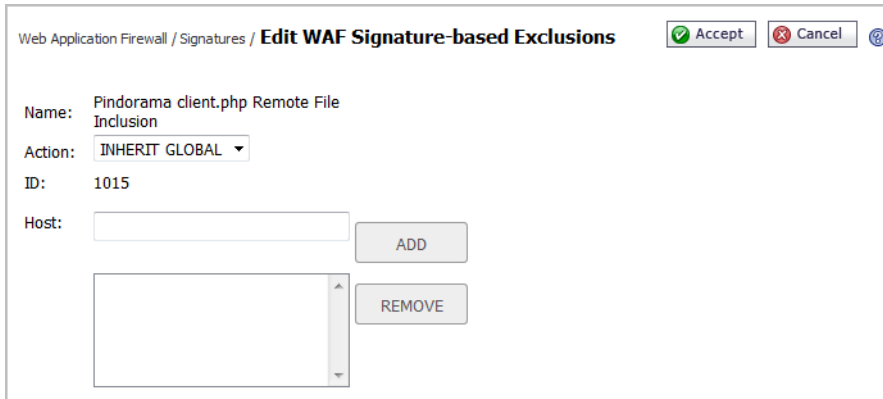
## Configuring Signature Based Custom Handling and Exclusions

You can disable inspection for a signature in traffic to an individual host, or for all hosts. You can also change the handling of detected threats for an individual host or for all hosts. If the signature group to which the signature belongs is set globally to Detect All, you can raise the level of protection to Prevent for the configured hosts. If no hosts are configured, the action is applied to the signature itself and acts as a global setting for all hosts. This change will block access to a host when the attack signature is detected. Similarly, you can lower the level of protection to Detect if the associated signature group is globally set to Prevent All.

**NOTE:** For signature based customization to take effect, the signature group of the modified signature must be globally enabled for either prevention or detection on the **Web Application Firewall > Settings** page.

To configure one or more hosts with an exclusion from inspection for a signature, or to configure custom handling when Web Application Firewall detects a specific signature for one or more hosts,:

- 1 On the **Web Application Firewall > Signatures** page, click the **Configure** button  for the signature that you wish to change. The **Edit WAF Signature-based Exclusions** screen displays.



- 2 In the Edit WAF Signature-based Exclusions screen, select one of the following actions from the **Action** drop-down list:
  - **DISABLE** – Disable Web Application Firewall inspections for this signature in traffic from hosts listed in this exclusion
  - **DETECT** – Detect and log threats matching this signature from hosts listed in this exclusion, but do not block access to the host
  - **PREVENT** – Log and block host access for threats matching this signature from hosts listed in this exclusion
  - **INHERIT GLOBAL** - Use the global signature exclusion list configured on the **Web Application Firewall > Settings** page.

- 3 To apply this action globally to all hosts, leave the **Host** field blank. To apply this action to an individual host, type the host entry as it appears in the bookmark or offloaded application into the **Host** field. This can be a host name or an IP address. To determine the correct host entry for this exclusion, see [Determining the Host Entry for Exclusions](#) on page 36.


You can configure a path to a particular folder or file along with the host. The protocol, port, and the request parameters are simply ignored in the URL. If a path is configured, then the exclusion is recursively applied to all subfolders and files. For instance, if **Host** is set to **webmail.sonicwall.com/exchange**, then all files and folders under **exchange** are also excluded.

- 4 If you specified a host, click **Add** to move the host name into the list box.
- 5 If you want to apply this action to additional individual hosts, repeat [Step 3](#) and [Step 4](#) to add more hosts to this exclusion.
- 6 Click **Accept**. If the Host list contains host entries. The SonicWall SMA/SRA appliance verifies that each host entry is valid. If no hosts were specified, a dialog box confirms that this is a global action to be applied to the signature itself.
- 7 Click **OK** in the confirmation dialog box.
- 8 Click **Accept** on the **Web Application Firewall > Signatures** page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests continue to use the old settings until they are terminated.

## Reverting a Signature to Global Settings


You can revert to using global signature group settings for a signature that was previously configured with an exclusion, without losing the configuration. This allows you to leave the host names in place in case you need to re-enable the exclusion.

### *To revert to using global signature group settings for a signature:*

- 1 On the **Web Application Firewall > Signatures** page, click the **Configure** button  for the signature that you wish to change.
- 2 In the Edit WAF Signature-based Exclusions screen, select **INHERIT GLOBAL** from the **Action** drop-down list.
- 3 The **Host** field may be blank if global settings were previously applied to this signature. To revert to global signature settings for all hosts, leave the **Host** field blank. To apply this action to one or more individual hosts, leave these host entries in the **Host** field and remove any host entries that are not to be reverted.
- 4 Click **Accept**. The SonicWall SMA/SRA appliance verifies that each host entry is valid.
- 5 Click **OK** in the confirmation dialog box.
- 6 Click **Accept** on the **Web Application Firewall > Signatures** page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests will continue to use the old settings until they are terminated.

## Removing a Host from a Per-Signature Exclusion

### *To remove a host from a configured exclusion for a signature:*

- 1 On the **Web Application Firewall > Signatures** page, click **Configure**  for the signature that you wish to change.
- 2 Select the host entry in the list box under the **Host** field, and then click **Remove**.
- 3 Repeat [Step 2](#) to remove other listed hosts, if desired.
- 4 Click **Accept**. The SonicWall SMA/SRA appliance verifies that each host entry is valid.
- 5 Click **OK** in the confirmation dialog box.
- 6 Click **Accept** on the **Web Application Firewall > Signatures** page to apply the updated settings. New settings are applied to any new HTTP connections and requests. The existing HTTP connections and requests will continue to use the old settings until they are terminated.

## Determining the Host Entry for Exclusions

When configuring an exclusion, either globally or per-signature, you must provide the host name or IP address. The affected hosts must match the host names used in your HTTP(S) bookmarks and Citrix bookmarks, and the virtual host domain name configured for an offloaded web application.

For a description of how to determine the correct host name, see the following sections:

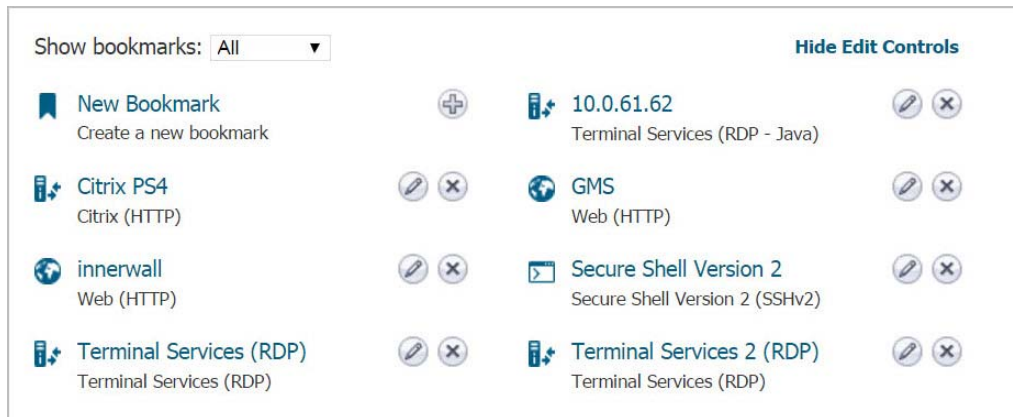
- [Viewing the Host Entry in a Bookmark](#) on page 36
- [Viewing the Host Entry in an Offloaded Application](#) on page 37

# Viewing the Host Entry in a Bookmark

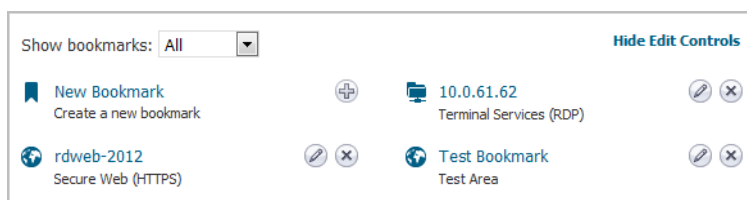
You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the bookmark.

## To view the host entry in a bookmark:

- 1 Navigate to the Virtual Office page, and click **Show Edit Controls** above the list of bookmarks.



- 2 Click the Edit button  for the bookmark.



- 3 In the Edit Bookmark screen, view the host entry in the **Name or IP Address** field.

### Edit Bookmark

Bookmark Name: \*

Name or IP Address: \*  ?

Description:  ?

Tabs:  ?

Allow user to edit/delete:  ▼

Service:  ▼ ?

Resource Window Size:  ▼ ?

Access Type Selection: Smart  Manual

Disable client detection by Citrix server ?

HTTPS Mode ?

Always use specified Citrix ICA Server ?

Automatically log in

Display Bookmark to Mobile Connect clients ?

**Note:** Citrix Portal Bookmarks have been tested and verified to support the following Citrix Application Virtualization platforms through Citrix StoreFront:

- Servers: Citrix XenApp 7.6, XenApp 6.5, XenApp 6.0, and XenApp 5.0
- Clients: Citrix Receiver for Windows 4.4, 4.2, 4.1, 4.0


Citrix Native Bookmark supports Advanced features and can be launched on Windows and OS X platforms after installing SMA Connect Agent and the Citrix Receiver.

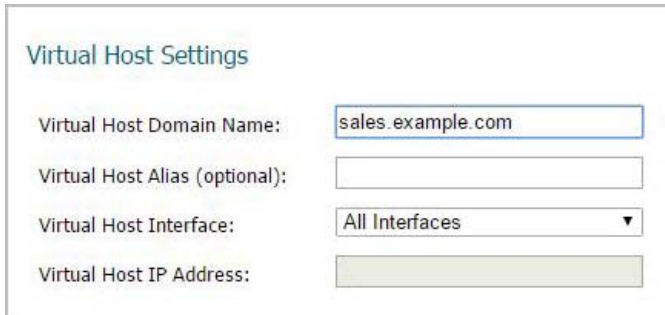
- 4 Click **Cancel**.

## Viewing the Host Entry in an Offloaded Application

You can determine exactly what host name to enter in your exclusion by viewing the configuration details of the offloaded application. In an offloaded application, you will use the virtual host domain name.

**To view the virtual host domain name in an offloaded application:**

- 1 Navigate to the **Portals > Portals** page and click Configure  next to the offloaded application.
- 2 In the Edit Portal screen, click the **Virtual Host** tab.



Virtual Host Settings

Virtual Host Domain Name:

Virtual Host Alias (optional):

Virtual Host Interface:


Virtual Host IP Address:

- 3 View the host entry for your exclusion in the **Virtual Host Domain Name** field.
- 4 Click **Cancel**.

## Configuring Custom Rules and Application Profiling

The **Web Application Firewall > Rules** page allows you to configure custom rules and application profiling.

Application profiling allows you to generate custom rules in an automated manner based on a trusted set of inputs used to develop a profile of what inputs are acceptable by an application. Other inputs are denied, providing positive security enforcement. When you place the SonicWall SMA/SRA appliance in learning mode in a staging environment, it learns valid inputs for each URL accessed by the trusted users. At any point during or after the learning process, custom rules can be generated based on the “learned” profiles. For more information about application profiling, see the [How Does Application Profiling Work?](#) on page 18.

 **NOTE:** Application profiling is supported only on the SonicWall SMA 400, SRA 4600, and the SonicWall SMA 500v Virtual Appliance.

Custom rules created on this page have all the same properties as the signatures that SonicWall pushes out to Web Application Firewall-enabled appliances.

## Web Application Firewall > Rules Page

To add a rule manually, you create a rule chain and then add rules within it. A rule chain is a collection of rules and includes additional attributes such as the severity rating, name, description, hit counters for rate limiting, and the action to take when the rule chain matches some traffic.

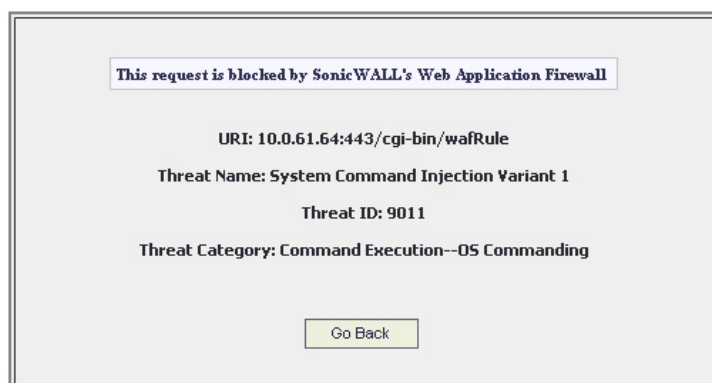
Rules listed on the Rules page can be divided into pages (default is 50 rules per page) and filtered by searching for a key word. To display only rules containing a key word in all fields or a specific field, type the key word in the Search field, select **All Fields** or a specific field to search, and click **Search**. All matches are highlighted. Or, click **Exclude** to display only rules that do not contain the key word. Click **Reset** to display all rules.

Rule chains generated by application profiles can be filtered by application. Select the **Filter by Application** check box to filter rule chains.

To add a rule manually, you create a **rule chain** and then add rules within it. A rule chain contains a collection of rules, and includes additional attributes such as the severity rating, name, description, hit counters for rate limiting, and the action to take when the rule chain matches some traffic.

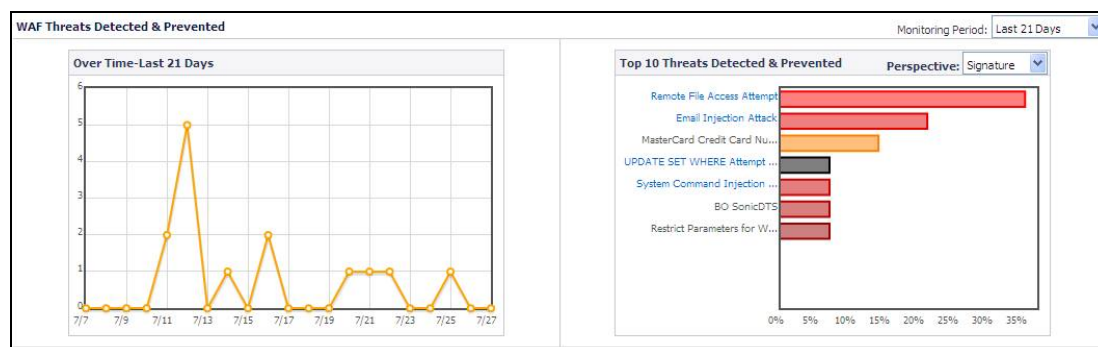
For example, custom rules and rule chains can be used to distinguish between legitimate and illegitimate traffic as defined by a web application that is using a certain URI or running on a certain portal. One rule in the chain is configured to match the URI or portal host name, while another rule is created that matches an undesirable value for another element of the HTTP(S) traffic. When the rule chain (both rules) matches some traffic, the configured action is performed to block or log the bad traffic from that URI or portal. When the request is blocked, the user sees a custom block page such as that in [Block Page](#).

## Block Page



The **Web Application Firewall > Monitoring** page also shows the activity in the graphs. [Monitoring Page After Blocking](#) shows detected and prevented threats during a 30 day period. For more information about the Monitoring page, see [Using Web Application Firewall Monitoring](#) on page 55.

## Monitoring Page After Blocking



Rules are matched against both inbound and outbound HTTP(S) traffic. When all rules in a rule chain find a match, the action defined in the rule chain is performed. You can also enable rate limiting in rule chains to trigger an action only after the number of matching attacks exceeds a threshold within a certain time period. You can configure the action to block the traffic and log the match, or to simply log it. You can also set the action to **Disabled** to remove the rule chain from active status and stop comparing traffic against those rules.

The Custom Rules feature can be enabled or disabled using the **Enable Custom Rules** global setting.

**NOTE:** Rule chains are enforced in the order that the rule chains were added. This order can be changed by deleting and re-creating rule chains.

Similarly, rules within rule chains are enforced in the order that the rules were added. This order can be changed by deleting and re-creating rules.

## Configuring Application Profiling

You can create URL profiles by putting the SonicWall SMA/SRA appliance into learning mode while applications are in use by trusted users, and then use those URL profiles to generate rule chains that prevent malicious misuse of the applications.

**NOTE:** Application profiling is supported on the SMA 400, SRA 4600, and SMA 500v Virtual Appliance only.

### To configure application profiling and automatically generate rules:

- 1 Navigate to the **Web Application Firewall > Rules** page.



- Under Application Profiling, select one or more portals with the application(s) to be profiled from the **Portals** drop-down list. Use Shift+click or CTRL+click to select multiple portals.

**Application Profiling**

Portals:

Content Types:

All  HTML/XML

Javascript  CSS

Default Action for generated Rule Chains:

Overwrite existing Rule Chains for URL Profiles

- For **Content Types**, select the type of content to be profiled:
  - All** – Includes all content types such as images, HTML, and CSS.
  - HTML/XML** – Selected by default, this is the most important from a security standpoint, because it typically covers the more sensitive web transactions.
  - Javascript** – Appropriate for an application written in Javascript.
  - CSS** – Select CSS to profile the cascading style sheet content used to control the formatting of web pages written in HTML, XHTML, or XML variants.
- Click **Begin Profiling** to start the “learning” process. Trusted users should be using the relevant applications on the selected portal during the active profiling period. The **Begin Profiling** button changes to **End Profiling**. Profiling continues until you click **End Profiling**.

**Web Application Firewall > Rules** Accept

**Rule Settings**

Enable Custom Rules

Disable SMA Exclusions

**Application Profiling**

Portals:

Content Types:

All  HTML/XML

Javascript  CSS

Default Action for generated Rule Chains:

Overwrite existing Rule Chains for URL Profiles

**sales**

.../ (0 URLs profiled)

**Profiling**

To begin profiling a web application, follow the steps below:

1. Select the Application Offloading Portal configured for the application
2. Select one or more '**Content Types**' to profile. Profiling will be done only for the HTTP/HTTPS responses matching the selected content types
3. Click on '**Begin Profiling**' button to start profiling the application. The URL Tree on the right lists all URLs so far

During profiling, the SonicWall SMA records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the **Web Application Firewall > Rules** page in the Application Profiling section.

- 5 After a period of time adequate to record inputs from normal application use, click **End Profiling** to stop the profiling process.
- 6 Optionally click any of the links in the URL profile tree display to edit the learned values. The editing page for the clicked URL is displayed. Click **Expand** to expand all URLs at that level in the tree.

The screenshot shows the configuration page for a URL profile. At the top, there is a breadcrumb trail: "Web Application Firewall > URL Profile > /owa/". To the right of the breadcrumb are three buttons: "Accept" (with a green checkmark icon), "Cancel" (with a red X icon), and a help icon. Below the breadcrumb is the title "URL Profile".

The configuration is organized into four sections:

- HTTP Methods:** A list box containing "get" and "post". To the right of the list are a plus sign (+) button and a minus sign (-) button.
- Request Parameters:** A list box containing "ae", "t", "a", "id", and "mrd". To the right of the list are a plus sign (+) button and a minus sign (-) button. There are also up and down arrow icons next to the list box.
- POST Payload Size:** A text input field containing the value "4194304".
- Response Status Codes:** A list box containing "200", "302", and "440". To the right of the list are a plus sign (+) button and a minus sign (-) button.

- 7 To add a value, type the value into the field next to the parameter and then click the plus button. To remove a value, select it in the list and then click the minus button.
- 8 Click **Accept** when finished editing. Repeat for other URLs as needed.
- 9 Before generating the rules from the URL profiles, select one of the following actions from the **Default Action for generated Rule Chains** drop-down list:
  - **Disabled** – The generated rules will be disabled rather than active.
  - **Detect Only** – Content triggering the generated rule will be detected and logged.
  - **Prevent** – Content triggering the generated rule will be blocked and logged.
- 10 Select **Overwrite existing Rule Chains for URL Profiles** to overwrite rule chains that have already been generated from a URL profile.
- 11 Click the **Generate Rules** button to generate rules from the URL profiles. If a URL profile has been modified, those changes are incorporated.

If rule chains are successfully generated, the status bar indicates how many rule chains were generated, including any that were overwritten.
- 12 If you do not want to accept the generated rule chains, click the **Delete Selected Rule Chains** button, which is available below the rule chain list. All of the automatically added rule chains are pre-selected right after generation for easy deletion of the group.
- 13 Click **Accept** to apply the generated rule chains to the SonicWall SMA configuration.

# Configuring Rule Chains

You can add, edit, delete and clone rule chains. Example rule chains (with Rule Chain ID greater than 15000) are available in the management interface for administrators to use as reference. These cannot be edited or deleted. You can view the rules associated with the rule chain by clicking its Edit Rule Chain icon under Configure.

For ease of configuration, you can clone example rule chains or regular rule chains. Cloning a rule chain clones all rules associated with the chain. After cloning the rule chain, you can edit it by clicking its Edit Rule Chain icon under Configure.

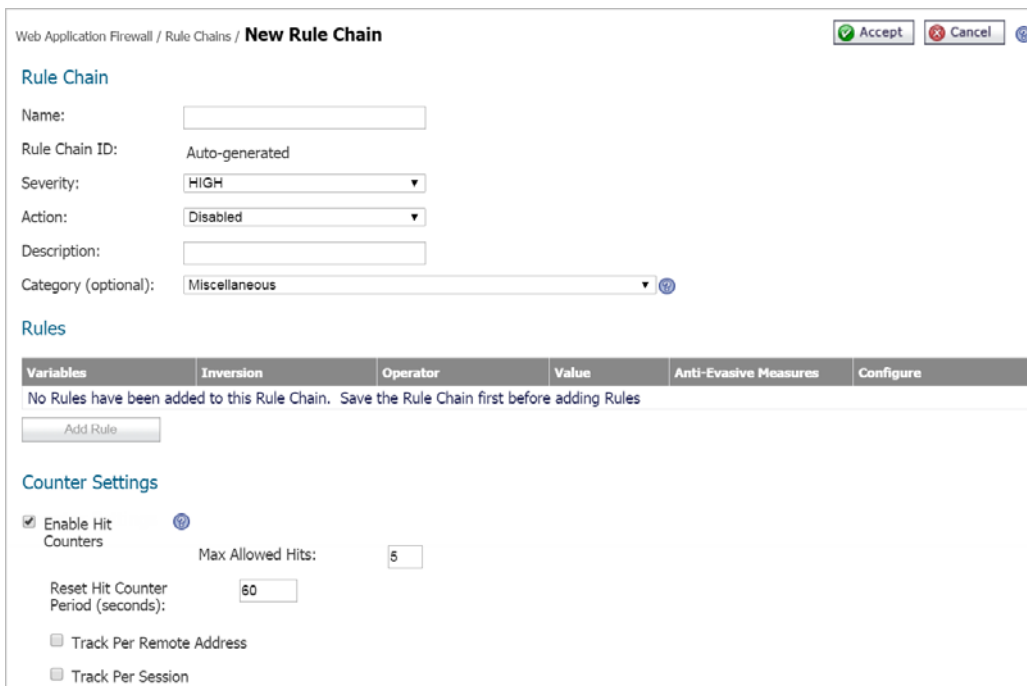
## Adding or Editing a Rule Chain

### To add or edit a rule chain:

- 1 On the **Web Application Firewall > Rules** page, click the **Add Rule Chain** button to add a new rule chain.

To edit an existing rule chain, click its Edit Rule Chain icon  under **Configure**.

The New Rule Chain screen or the screen for the existing rule chain displays. Both screens have the same configurable fields in the **Rule Chain** section.



- 2 On the New Rule Chain page, type a descriptive name for the rule chain in the **Name** field.
- 3 Select a threat level from the **Severity** drop-down list. You can select **HIGH**, **MEDIUM**, or **LOW**.
- 4 Select **Prevent**, **Detect Only**, or **Disabled** from the **Action** drop-down list.
  - **Prevent** – Block traffic that matches the rule.
  - **Detect** – Allow the traffic, but log it.
  - **Disabled** – The rule chain should not take effect.


The **Disabled** option allows you to temporarily deactivate a rule chain without deleting its configuration.

- 5 In the **Description** field, type a short description of what the rule chain will match or other information.

- 6 Select a category for this threat type from the **Category** drop-down list. This field is for informational purposes, and does not change the way the rule chain is applied.
- 7 Under **Counter Settings**, to enable tracking the rate at which the rule chain is being matched and to configure rate limiting, select **Enable Hit Counters**. Additional fields are displayed.
- 8 In the **Max Allowed Hits** field, enter the number of matches for this rule chain that must occur before the selected action is triggered.
- 9 In the **Reset Hit Counter Period** field, enter the number of seconds allowed to reach the Max Allowed Hits number. If Max Allowed Hits is not reached within this time period, the selected action is not triggered and the hits counter is reset to zero.
- 10 Select **Track Per Remote Address** to enforce rate limiting against rule chain matches coming from the same IP address. Tracking per remote address uses the remote address as seen by the SonicWall SMA/SRA appliance. This covers the case where different clients sit behind a firewall with NAT enabled, causing them to effectively send packets with the same source IP.
- 11 Select **Track Per Session** to enable rate limiting based on an attacker's browser session. This method sets a cookie for each browser session. Tracking by user session is not as effective as tracking by remote IP if the attacker initiates a new user session for each attack.
- 12 Click **Accept** to save the rule chain. A **Rule Chain ID** is automatically generated.
- 13 Next, add one or more rules to the rule chain. See [Configuring Rules in a Rule Chain](#) on page 45 for detailed information.


## Cloning a Rule Chain

### *To clone a rule chain:*


- 1 On the **Web Application Firewall > Rules** page, click its Clone Rule Chain icon  under **Configure**.
- 2 Click **OK** in the confirmation dialog box.

You can now edit the rule chain to customize it. See [Adding or Editing a Rule Chain](#) on page 43.

## Deleting a Rule Chain


 **NOTE:** Deleting a rule chain also deletes all the associated rules.

### *To delete a rule chain:*

- 1 On the **Web Application Firewall > Rules** page, click the Delete Rule Chain icon  under **Configure** for the rule chain you want to delete.
- 2 Click **OK** in the confirmation dialog box.
- 3 Click **Accept**.

## Correcting Misconfigured Rule Chains

Misconfigured rule chains are not automatically detected at the time of configuration. When a misconfiguration occurs, the administrator must log in and fix or delete the bad rules.

 **NOTE:** If any rules or rule chains are misconfigured, the appliance will not enforce any custom rules or rule chains.

It is difficult to detect a false positive from a misconfigured rule chain unless a user runs into it and reports it to the administrator. If the rule chain has been set to PREVENT, then the user will see the Web Application Firewall block page (as configured on the **Web Application Firewall > Settings** page). If not, there will be a log message indicating that the “threat” has been detected.

Consider a scenario in which the administrator inadvertently creates a custom rule chain that blocks access to all portals of the SonicWall SMA/SRA appliance. For example, the admin may have wanted to enforce a rule for an Application Offloading portal. However, he or she forgot to add another rule to narrow the criteria for the match to requests for that portal, host or URL. If the first rule was too broad, then this will mean a denial of service for the appliance. Specifically, the administrator creates a rule chain to deny using the GET HTTP method for a specific URL, which expects a POST request.

***For this, the administrator needs to create two rules:***

- 1 The first rule is to match GET requests.
- 2 The second rule is to match a specific URL.

If the administrator forgets to create the second rule, then access to the SonicWall SMA/SRA appliance will be denied, because the web management interface depends on the GET method.

***To fix a misconfigured rule chain:***

- 1 Point your browser to <https://<SonicWall SMA IP>/cgi-bin/welcome>.  
If you try to reach the welcome page by simply using the URL <https://<SonicWall SMA IP>/>, the usual redirect to <https://<SonicWall SMA IP>/cgi-bin/welcome> may not work. To repair misconfigured rules, you need to explicitly go to <https://<SonicWall SMA IP>/cgi-bin/welcome>, where <SonicWall SMA IP> is the host name or IP address of your SonicWall SMA/SRA appliance.
- 2 Log in as admin.
- 3 Navigate to the **Web Application Firewall > Rules** page.
- 4 Edit or delete the bad rules.
- 5 Click **Accept**.

## Configuring Rules in a Rule Chain

You can add, edit, delete and clone rules. A rule is a condition that is checked against inbound or outbound HTTP(S) traffic. Each rule chain can have one or more rules configured, and must have at least one rule before it can be used. [Add Rule Page](#) shows the Add Rule page.

## Add Rule Page

Web Application Firewall / Rule Chains / TestRC / Add Rule

Rule Chain ID: 10000

Variables: Host

Operator:  Not Contains

Value:

Anti-Evasive Measures: Remove Spaces

**Tips/Help**

**When do I use Remove Spaces?**  
Hackers attempt to get around the Rules by adding spaces within Strings, which escape the Rules but are interpreted by the backend Web application. Select this operator to overcome this type of evasion.

**When do I use Trim?**  
Hackers attempt to get around the Rules by padding spaces before and after the input data. Use this operator to get rid of the padding before comparison.

**What are Anti-Evasive Measures?**  
These are operations done on input before the input identified by the Variables is matched against the specified 'Value'. For instance, the String Length operator is used to compute the length of the matched input and use it for comparison. Some of these operations are used to thwart attempts by hackers to encode inputs to bypass Rules. Please click on an Anti-Evasive Measure to read more information on it on the Tips/Help sidebar.

Rules allow the administrator to employ both a positive security model and a negative security model. In a positive security model, policies are written only to allow known traffic and block everything else.

A rule has several components:

- **Variables** – These are HTTP protocol entities that are scanned by Web Application Firewall to help identify legitimate or illegitimate traffic. Multiple variables can be matched against the configured value in the **Value** field. The '+' and '-' buttons allow you to add variables from the **Variables** drop-down list or delete them from the list of selected variables. You can combine multiple variables as required to match the specified value. If multiple variables are configured, then the rule is matched if any one of the configured variables matches the target value. See [About Variables](#) on page 47 for more information about variables.
- **Operators** – These are arithmetic and logical operators. **Not** is an inversion operator used to match any value except the configured condition. See [About Operators](#) on page 49 for more information about the operators.
- **Value** – This entity can be a number, literal string, or a regular expression. It is compared with the value of the configured variable(s) according to the specified operator. To compare the variable(s) to more than one value, you can enter multiple values separated by spaces into the **Value** field, and select the **Matches Keyword** operator. Delimiting by spaces only works if the **Matches Keyword** operator is selected.
- **Anti-Evasive Measures** – This field allows you to apply operations beyond those supported by the **Operators** field, especially to enforce Anti-Evasive protection. See [About Anti-Evasive Measures](#) on page 50 for more information about these operations.

The following sections provide detailed information about rules:

- [About the Tips/Help Sidebar](#) on page 47
- [About Variables](#) on page 47
- [About Operators](#) on page 49

- [About Anti-Evasive Measures](#) on page 50
- [Example Use Cases for Rules](#) on page 51
- [Deleting a Rule](#) on page 54
- [Cloning a Rule](#) on page 54
- [Adding or Editing a Rule](#) on page 54

## About the Tips/Help Sidebar

You can select a variable in the **Variables** drop-down list to display more information about that variable in the **Tips/Help** sidebar. The sidebar explains when each variable would be used and where it is found in the HTTP protocol. An example use case is provided for each variable.

You can also select an entry in the **Anti-Evasive Measures** drop-down list to display more information about it in the **Tips/Help** sidebar.

The sidebar also provides context-sensitive search. When you click on a variable and then search for a particular keyword, the search results are only related to variables.

## About Variables

Variables are HTTP protocol entities that are scanned by Web Application Firewall to help identify legitimate or illegitimate traffic. Multiple variables can be matched against the configured value in the **Value** field. The '+' and '-' buttons allow you to add variables from the **Variables** drop-down list or delete them from the list of selected variables.

You can combine multiple variables as required to match the specified value. If multiple variables are configured, then the rule is matched if any one of the configured variables matches the target value.

A variable can represent a single value or a collection. If a variable represents a collection, such as **Parameter Values**, then a specific variable within the collection can be configured by entering its name in the selection text box to the right of the colon (:). For example, the value for the **URI** or **Host** variable is unique in each HTTP(S) request. For such variables, the selection text box is not displayed. Other variables, such as **Request Header Values** and **Response Header Names**, represent a collection.

If you need to test the collection itself against an input, then you would leave the selection text box empty. However, if you need to retrieve the value of a specific item in the collection, you would specify that item in the selection text box. For example, if you need to test if the parameter **password** exists in the HTTP(S) request, then you would configure the variable **Parameter Names** and leave the selection text box empty. You would set the **Operator** to **String equals** and the **Value** to **password**. But, if you want to check whether the value of the password parameter matches a particular string, such as "foo", then you would select the **Parameter Values** variable and specify **password** in the selection text box. In the **Value** field, you would enter **foo**.

The [Variables for use in rules](#) table describes the available variables.

### Variables for use in rules

Variable Name	Collection	Description
Host	No	Refers to the host name or the IP address in the Host header of an HTTP request. This typically refers to the host part of the URL in the address bar of your browser.
URI	No	Refers to the combination of path and the query arguments in a URL.
HTTP Method	No	Refers to the method, such as GET and POST, used by the browser to request a resource on the web server.

## Variables for use in rules (Continued)

Variable Name	Collection	Description
HTTP Status Code	No	Refers to the response status from the web server. You can use this to configure actions for various error codes from the web server.
Parameter Values	Yes	<p>Refers to the collection of all request parameter values, including the values of all query arguments and form parameters that are part of the current request.</p> <p>To match against some aspect of the entire list of parameter values, such as the number of parameter values, leave the selection field empty.</p> <p>To match against the value of a particular parameter, specify the name of the parameter in the selection field to the right of the colon.</p>
Parameter Names	Yes	<p>Refers to the collection of all request parameter names, including the names of all query arguments and form parameters that are part of the current request.</p> <p>To match against some aspect of the entire list of parameter names, leave the selection field empty.</p> <p>To match against the name of a particular parameter, specify the parameter name in the selection field to the right of the colon.</p>
Remote Address	No	Refers to the client's IP address. This variable allows you to allow or block access from certain IP addresses.
Request Header Values	Yes	<p>Refers to the collection of all HTTP(S) request header values for the current request.</p> <p>To match against some aspect of the entire list of request header values, leave the selection field empty.</p> <p>To match against a particular header value, specify the name of the header in the selection field to the right of the colon.</p> <p>For example, to block Ajax requests, select <b>Request Header Values</b> as the Variable, specify <b>X-Request-With</b> in the selection text box, and specify <b>ajax</b> in the <b>Value</b> field.</p>
Request Header Names	Yes	<p>Refers to the collection of all HTTP(S) request header names for the current request.</p> <p>To match against some aspect of the entire list of request header names, leave the selection field empty.</p> <p>To match against a particular header name, specify the name of the header in the selection field to the right of the colon.</p> <p>For example, to block requests that are not referred by a trusted host, select <b>Request Header Names</b> as the <b>Variable</b>, specify <b>Referrer</b> in the selection text box, enter the host names or IP addresses of the trusted hosts in the <b>Value</b> field, select <b>Not</b> and select the <b>Matches Keyword</b> operator.</p>
Response Header Values	Yes	<p>Refers to the collection of all HTTP(S) response header values for the current request.</p> <p>To match against some aspect of the entire list of response header values, leave the selection field empty.</p> <p>To match against a particular header value, specify the name of the header in the selection field to the right of the colon.</p>



### Variables for use in rules (Continued)

Variable Name	Collection	Description
Response Header Names	Yes	Refers to the collection of all HTTP(S) response header names for the current request.  To match against some aspect of the entire list of response header names, leave the selection field empty.  To match against a particular header name, specify the name of the header in the selection field to the right of the colon.
Response Content Length	No	Refers to the size of the response payload.
Response Payload	No	Refers to the web page content that is displayed to the user.
Portal Hostname	No	Refers to the virtual host name of the SonicWall SMA portal which accepts the request from the client.  To create a rule chain that applies to a particular virtual host, one rule would match the host and another would specify other criteria for the match.
Portal Address	No	Refers to the IP address or virtual IP address of the SonicWall SMA portal which accepts the request from the client.
Request Path	No	Refers to the relative path used to access a particular resource in a web site.

## About Operators

There are a number of arithmetic and logical operators. **Not** is an inversion operator, which results in a match for any value except the configured condition.

These operators can be used in conjunction with **Anti-Evasive Measures**. For example, you might use the **Equals String** operator with **Convert to Lowercase** or **Normalize URI Path** in **Anti-Evasive Measures**.

The **Rule operators** table describes the available operators for use with rules.

### Rule operators

Operator	Type	Description
Contains	String	One or more of the scanned variables contains the content of the <b>Value</b> field.
Equals String	String	The scanned variable(s) match the alphanumeric string in the <b>Value</b> field exactly.
=	Arithmetic	The scanned variable is equal to the content of the <b>Value</b> field.
>	Arithmetic	The scanned variable is greater than the content of the <b>Value</b> field.
>=	Arithmetic	The scanned variable is greater than or equal to the content of the <b>Value</b> field.
<	Arithmetic	The scanned variable is less than the content of the <b>Value</b> field.
<=	Arithmetic	The scanned variable is less than or equal to the content of the <b>Value</b> field.

## Rule operators (Continued)

Operator	Type	Description
Matches Keyword	String	One or more of the scanned variables matches one of the keywords in the <b>Value</b> field. If multiple keywords are specified, they should be separated by spaces.
Matches Regex	String	One or more of the scanned variables matches the in the <b>Value</b> field. An example of a regular expression that matches any four decimal numbers is <code>\d{4}</code> .

## About Anti-Evasive Measures

Anti-evasive measures are applied to input identified by the selected variables before the input is matched against the specified value. For instance, the **String Length** operation is used to compute the length of the matched input and use it for comparison. Some of the anti-evasive measures are used to thwart attempts by hackers to encode inputs to bypass Web Application Firewall rules. You can click on an anti-evasive measure in the list to read more information on it in the **Tips/Help** sidebar.

The anti-evasive measures can be used in conjunction with regular operators. There are ten operations to choose from in the **Anti-Evasive Measures** field, including the **None** operation which leaves the input alone.

Multiple anti-evasive measures can be selected together and individually enforced. You can select multiple measures by holding the **Ctrl** key while clicking an additional measure. When the **None** measure is selected along with other measures in your rule, the input is compared as is and also compared after decoding it or converting it with another measure.

The [Anti-Evasive Measures for Rules](#) table describes the anti-evasive measures available for use with rules.

### Anti-Evasive Measures for Rules

Operation	Description
None	Use the <b>None</b> measure when you want to compare the scanned input to the configured variable(s) and value(s) without changing the input.
String Length	Use the <b>String Length</b> operation when the selected variable is a string and you want to compute the length of the string before applying the selected operator.
Convert to Lowercase	Use the <b>Convert to Lowercase</b> measure when you want to make case-insensitive comparisons by converting the input to all lowercase before the comparison. When you use this measure, make sure that strings entered in the <b>Value</b> field are all in lowercase.  This is an anti-evasive measure to prevent hackers from changing case to bypass the rule.
Normalise URI Path	Use the <b>Normalise URI Path</b> measure to remove invalid references, such as back-references (except at the beginning of the URI), consecutive slashes, and self-references in the URI. For example, the URI <code>www.eshop.com/././././login.aspx</code> is converted to <code>www.eshop.com/login.aspx</code> .  This is an anti-evasive measure to prevent hackers from adding invalid references in the URI to bypass the rule.
Remove Spaces	Use the <b>Remove Spaces</b> measure to remove spaces within strings in the input before the comparison. Extra spaces can cause a rule to not match the input, but are interpreted by the backend web application.  This is an anti-evasive measure to prevent hackers from adding spaces within strings to bypass the rule.

## Anti-Evasive Measures for Rules (Continued)

Operation	Description
Base64 Decode	<p>Use the <b>Base64 Decode</b> measure to decode base64 encoded data before the comparison is made according to the rule.</p> <p>Some applications encode binary data in a manner convenient for inclusion in URLs and in form fields. Base64 encoding is done to this type of data to keep the data compact. The backend application decodes the data.</p> <p>This is an anti-evasive measure to prevent hackers from using base64 encoding of their input to bypass the rule.</p>
Hexadecimal Decode	<p>Use the <b>Hexadecimal Decode</b> measure to decode hexadecimal encoded data before the comparison is made according to the rule.</p> <p>This is an anti-evasive measure to prevent hackers from using hexadecimal encoding of their input to bypass the rule.</p>
URL Decode URL Decode (Unicode)	<p>Use the <b>URL Decode</b> measure to decode URL encoded strings in the input. Use the <b>URL Decode (Unicode)</b> measure to handle %uXXXX encoding. URL encoding is used to safely transmit data over the internet when URLs contain characters outside the ASCII character set.</p> <p><b>NOTE:</b> Do not use these measures against an input that has been decoded already.</p> <p>This is an anti-evasive measure to prevent hackers from using URL encoding to bypass rules, knowing that the backend web server can interpret their malicious input after decoding it.</p> <p>For example, the URI <a href="http://www.eshop.com/hack+URL%3B">www.eshop.com/hack+URL%3B</a> is converted to <a href="http://www.eshop.com/hack">www.eshop.com/hack</a> URL by this operator before the comparison is made.</p>
Trim	<p>Use the <b>Trim</b> measure to remove spaces before and after the input data before the comparison. Extra spaces can cause a rule to not match the input, but are interpreted by the backend web application.</p> <p>This is an anti-evasive measure to prevent hackers from adding spaces before and after the input data to bypass the rule.</p>

## Example Use Cases for Rules

This section provides examples of positive and negative security models, as well as several examples showing the use of anti-evasive measures to provide a deeper understanding of these anti-evasive techniques.

### Example – Positive Security Model: Blocking Bad Logins

To prevent login to an Application Offloaded web site if the length of the password is less than 8 characters, you would create a rule chain containing the following two rules:

- 1 Select **Host** as the **Variable** and click + to add it, set the **Operator** to **Equals String**, and set **Value** to the Virtual Host name of the portal. This checks that the Host header of the login request matches the site you are trying to protect. In this case, the rule chain is only being applied to one site.
- 2 Select **Parameter Value** as the **Variable** and type **password** into the selection field, then click + to add the variable and selected item to the rule, set the **Operator** to < (less than), and set **Value** to **8**. Select **String Length** in the **Anti-Evasive Measures** list to compute the length of the password form parameter.

The action for the rule chain would be set to **Prevent**. [Example Rule Chain – Blocking Bad Logins](#) shows the rule chain for this example.

### Example Rule Chain – Blocking Bad Logins

The screenshot shows the configuration for a rule chain named "Block Invalid OWA Login". The interface includes fields for Name, Rule Chain ID, Severity, Action, Description, and Category. Below these fields is a table of rules.

**Rule Chain Configuration:**

- Name: Block Invalid OWA Login
- Rule Chain ID: 10000
- Severity: HIGH
- Action: Prevent
- Description: Block Bad logins
- Category (optional): Authentication--Weak Password Recovery Validation

**Rules Table:**

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
Host	False	Equals String	192.168.200.7	Convert to Lowercase	[Edit] [Delete] [Copy]
Parameter Values:password	False	<	8	String Length	[Edit] [Delete] [Copy]

**Note:** All the individual Rules have to match for the Rule Chain to match

### Example – Positive Security Model: Blocking a Form Submission with Unwanted Parameters

This rule chain blocks a form submission if the form has a request parameter other than **formId** or if the value of **formId** contains more than four digits. To accomplish this, you would need two rule chains:

- The first rule chain contains two rules:
  - The first rule identifies the URL where the form is submitted.
  - The second rule checks if **Parameter Names** does not match the name of the valid parameter, **formId**. It uses the **Equals String** operator with the **Not** inversion checkbox selected.

The screenshot shows the Rules table for the first rule chain.

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Member Of (CSV)	/owa/auth/login.aspx	Convert to Lowercase AND URL Decode	[Edit] [Delete] [Copy]
Parameter Names	True	Equals String	formID	Convert to Lowercase AND URL Decode	[Edit] [Delete] [Copy]

- The second rule chain contains two rules:
  - The first rule identifies the URL where the form is submitted.
  - The second rule checks if the value contained by the **Parameter Value: formId** variable matches the **^\d{1,4}\$** which matches anything that does not consist of 1 to 4 digits. The **Not** inversion

check box is selected to change the rule to match anything that does not consist of one to four digits.

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Member Of (CSV)	/owa/auth/login.aspx	Convert to Lowercase AND URL Decode	  
Parameter Values:formID	True	Matches Regex	^\d{1,4}\$	Convert to Lowercase AND URL Decode	  

## Example – Negative Security Model: Blocking Malicious Input to a Form

To block malicious input to a form, you would create a rule chain containing the following two rules:

- 1 The first rule identifies the URL for the form.
- 2 The second rule identifies the form parameter, **shell\_cmd** and the bad input, **tracert**.

Variables	Inversion	Operator	Value	Advanced Ops	Configure
URI	False	Matches Regex	/exec.cgi	Convert to Lowercase AND URL Decode	  
Parameter Values:shell_cmd	False	Equals String	tracert	Convert to Lowercase AND URL Decode	  

## Example – Using URL Decode and None

If a hacker perceives that a Request URI is being scanned for CR and LF characters (carriage return and line feed), the hacker may attempt to sneak those characters into the request by performing URL encoding on the characters before adding them to the request. The URI will then contain **%0D** and **%0A** characters, which could be used to launch an HTTP response splitting attack. The **URL Decode** and/or **URL Decode (Unicode)** operations can be used to thwart this type of attack by decoding the scanned input before comparing it against the configured value(s) to check for a match.

Specifically, if a request is made to the URI <http://www.host.com/foo%20bar/> and the **URL Decode** operation is selected, the scanned URI becomes <http://www.host.com/foo bar/> after decoding, which can now be safely matched. To thwart a hacker who sends a non-encoded request in addition to the encoded one, the administrator can select the **None** and the **URL Decode** options in the rule.

## Example – Using Convert to Lowercase and URL Decode with Parameter Values

An administrator wants to check whether the content of the variable **Parameter Values** matches the value **foo bar** in order to block such a request. Because the backend application accepts case-insensitive inputs (foo bar and FOO BAR), the hacker can pass **foo BAR** in the request and evade the rule. To prevent this evasion, the administrator specifies **Convert to Lowercase** as an anti-evasive operation and configures the value as **foo bar** in all lower case. This causes all request parameter values to be converted to lower case and compared against the value for a case-insensitive check.

Similarly, the hacker could pass **foo%20BAR**, which is the URL encoded version typically used by browsers. To prevent this evasion, the administrator specifies **URL Decode** as the anti-evasive operation to apply to the request entity. The input **foo%20BAR** is URL decoded to **foo BAR**. If the input is already **foo BAR**, then URL decoding is not applied.



## Example – Using String Length and URL Decode with Parameter Values:ID

Comparing against a decoded input allows the administrator to use the **String Length** measure to check the length of the input against the matching variable. For example, if a web application ID parameter should not be more than four characters, the administrator could select **Parameter Values** in the **Variable** field, enter **ID** in

the selection field, click **+** to add the variable and selected item to the rule, enter **4** in the **Value** field, select **>** in the **Operator** list, and select both **URL Decode** and **String Length** in the **Anti-Evasive Measures** list.



## Deleting a Rule

*To delete a rule from a rule chain:*

- 1 On the **Web Application Firewall > Rules** page, click the Edit Rule Chain icon  under **Configure** for the rule chain from which you want to delete a rule. The page for that rule chain opens.
- 2 Click the Delete icon  under **Configure** for the rule you want to delete.
- 3 Click **OK** in the confirmation dialog box.
- 4 Click **Accept**.

## Cloning a Rule



*To clone a rule:*


- 1 On the **Web Application Firewall > Rules** page, click the Edit Rule Chain icon  under **Configure** for the rule chain which contains the rule you want to clone. The page for that rule chain opens.
- 2 Click the Clone icon  under **Configure** for the rule you want to clone.
- 3 Click **OK** in the confirmation dialog box.

You can now edit the rule to customize it. See [Adding or Editing a Rule Chain](#) on page 43.

## Adding or Editing a Rule

*To add or edit a rule in a rule chain:*

- 1 Click the Edit Rule Chain icon  under **Configure** for the rule chain on which you want to add or edit a rule. The page for that rule chain opens.
- 2 Click the **Add Rule** button to add a new rule, or click the Edit icon under **Configure** for the rule you want to edit.
- 3 In the Add Rule page or the page for the edited rule, select a variable from the **Variables** drop-down list. See [About Variables](#) on page 47 for information about the available variables.
- 4 If the chosen variable is a collection of variables, a selection field is displayed to the right of the **Variables** field, after the colon. If you wish to make a comparison against a particular member of the collection, type the name of that item into the selection field.  
  
To test the collection itself against an input, leave the selection field blank. For example, to test whether a certain parameter exists in the request, you could select the **Parameter Names** variable and then type the specific parameter name into the **Value** field (but not into the variable selection field).
- 5 Click the Plus button  to add the variable to the rule. Repeat [Step 2](#) through [Step 5](#) to add more variables.

To delete a variable, select it in the large text box and click the Minus button .

- 6 Select a string or arithmetic operator from the **Operators** drop-down list. To perform the inverse operation, select **Not**.
- 7 In the **Value** field, type in the value to be compared with the selected variable(s) in the scanned HTTP(S) input. To compare the input against multiple values, type in each value separated by a space. Each value will be compared individually.
- 8 Select one or more measures from the **Anti-Evasive Measures** list. Hold the **Ctrl** key on your keyboard while clicking to select multiple measures.
- 9 Click **Accept** when finished.

## Using Web Application Firewall Monitoring

The **Web Application Firewall > Monitoring** page provides two screens: **Local** and **Global**. Both screens display statistics and graphs for detected/prevented threats over time and top 10 threats. The Local screen also displays web server status statistics and graphs of the number of requests and the amount of traffic during the selected monitoring period.

The monitoring functions of each screen are explained in the following sections:

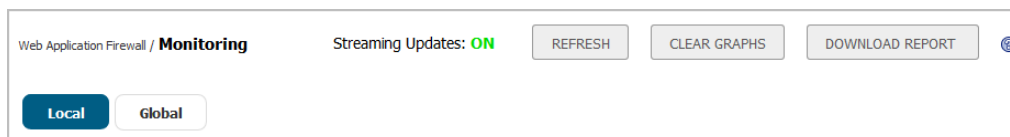
- [Monitoring on the Local Screen](#) on page 55
- [Monitoring on the Global Screen](#) on page 60

## Monitoring on the Local Screen

The **Local** screen displays statistics and graphs for the local appliance. Graphs are displayed for Web Server Status and WAF Threats Detected & Prevented. For the latter, you can use the Perspective options to change the view between Signature, Severity, and Server, and you can display the statistics in list format rather than as graphs.

## Using the Control Buttons

The control buttons are displayed at the top of the screen. They control the statistics that are displayed on this screen. On the Local screen, you can use the control buttons to turn streaming updates on or off, refresh the data on the screen, clear the graphs, and download a report. If streaming is turned on, Web Application Firewall statistics information is fetched periodically, and displayed in the graphs and threat list. If streaming is turned off, no new information can be displayed.



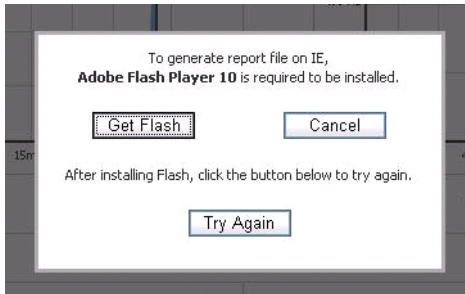
### *To use the control buttons:*

- 1 Select the **Local** screen. The active screen name is displayed in blue, while the inactive screen name is white. The control buttons act on the screen that is currently displayed.
- 2 To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.
- 3 To refresh the display, click **Refresh**.
- 4 To clear all Web Application Firewall statistics from the graphs and list, click **Clear Graphs**.

5 To generate a PDF report with Web Application Firewall statistics, click **Download Report**.

**i** | **NOTE:** Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.

6 If prompted to install Adobe Flash Player, click **Get Flash** and then after the installation click **Try Again** to generate the PDF report from Internet Explorer.



## Monitoring Web Server Status

On the **Local** screen, below the control buttons, this screen displays graphs for web server status. One graph shows the number of web requests detected over time, and another graph shows the amount of traffic in kilobytes (KB).

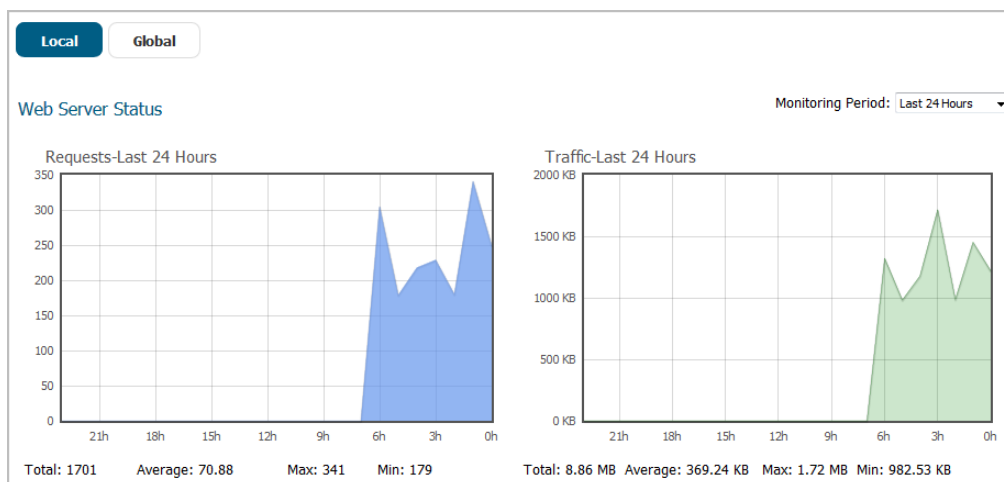
The web servers tracked are those servers within the local network of the SonicWall SMA/SRA appliance that provide HTTP/HTTPS bookmarks, offloaded applications, and other web services. The Traffic graph indicates the amount of HTTP/HTTPS payload data that is sent to client browsers.

You can view web server activity on the **Local** screen over different time periods by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 60 Seconds
- Last 60 Minutes
- Last 24 Hours
- Last 30 Days

**Web Server Status For Last 24 Hours** shows a 24 hour period of web server activity.

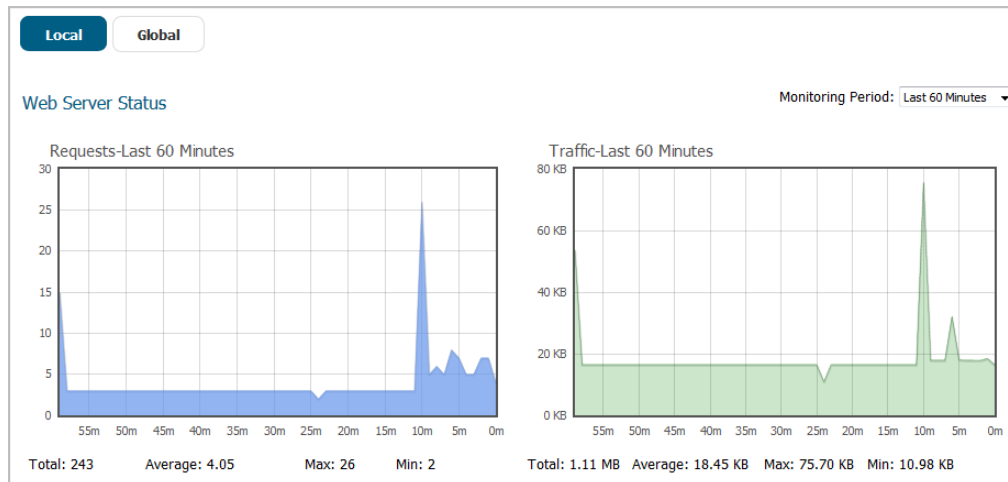
### Web Server Status For Last 24 Hours





**Web Server Status For Last 60 Minutes** shows a 60 minute period of web server activity.

### Web Server Status For Last 60 Minutes



## Monitoring Detected and Prevented Threats

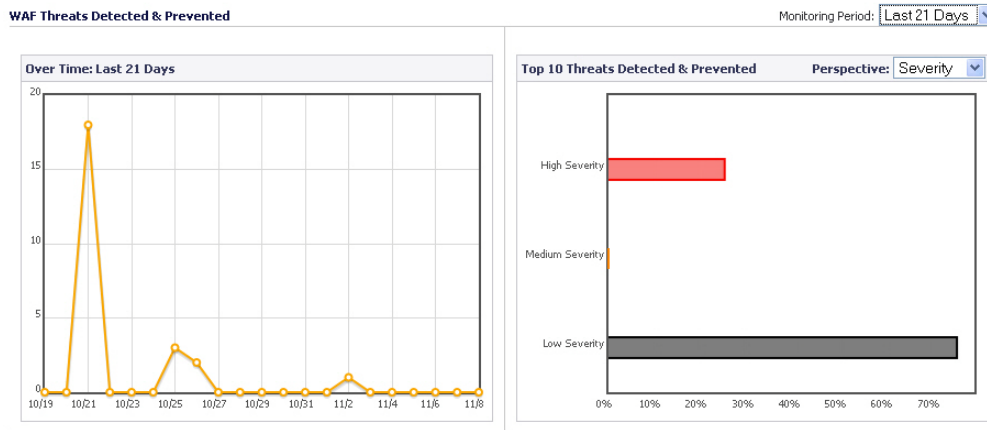
On the **Local** screen below the web server status graphs, the **Web Application Firewall > Monitoring** page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that time frame.

You can change the time frame displayed in both graphs or change the view to display all threats in list format by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 12 Hours
- Last 14 Days
- Last 21 Days
- Last 6 Months
- All in Lists

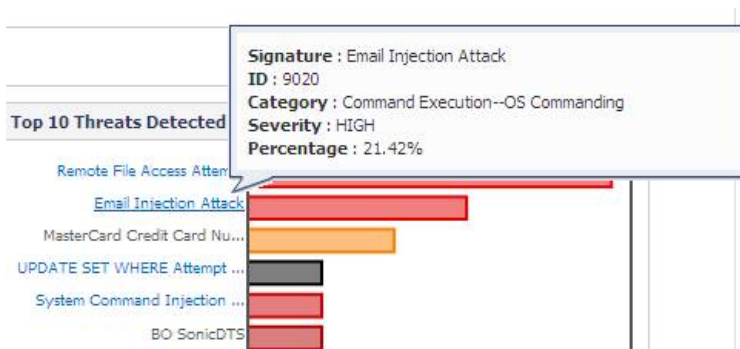
**Threats Over Last 21 Days** shows the number and severities of threats detected and prevented over the last 21 days.

## Threats Over Last 21 Days



When displaying the top 10 threats graph with **Perspective** set to **Signature**, hovering your mouse pointer over the signature ID causes a tooltip to appear with details about the threat.

### Threat Details Tooltip



## Viewing Threats in List Format

To see the threats in list format rather than as a graph, select **All in Lists** from the **Monitoring Period** drop-down list. **Threats in List Format** shows the list format.

The Severity column of the threat list is color coded for quick reference, as follows:

- High severity threats – **Red**
- Medium severity threats – **Orange**
- Low severity threats – **Black**

The initial, default sorting order lists the high severity threats with highest frequency values first. You can change the order of listed threats by clicking on the column headings to sort them by ID, signature name, classification, severity, or frequency. Click again to toggle between ascending and descending order. The active sorting column is marked by an arrowhead pointing upwards for ascending order, and downwards for descending order.

## Threats in List Format

WAF Threats Detected & Prevented				Monitoring Period:	All in Lists
ID	Signature	Threat Classification	Severity	Frequency	
10179	Restrict Parameters for Webmail:/owa/auth/logon.aspx	Authorization--Insufficient Authorization	HIGH	2	
9001	Session Fixation	Authorization--Session Fixation	HIGH	2	
1366	Cross-site Scripting (XSS) Attack 2	Client-side Attacks--Cross-site Scripting	HIGH	40	
9008	Cross-site Scripting (XSS) Attack	Client-side Attacks--Cross-site Scripting	HIGH	1014	
10000	BO SonicDTS	Command Execution--Buffer Overflow	HIGH	1	
1186	HTTP Location Response Header Overflow Attempt	Command Execution--Buffer Overflow	MEDIUM	4	
1196	HTTP Via Response Header Overflow Attempt	Command Execution--Buffer Overflow	MEDIUM	6	
9020	Email Injection Attack	Command Execution--OS Commanding	HIGH	5	

### To view and hide threat details:

- 1 On the **Web Application Firewall > Monitoring** page, select **All in Lists** from the **Monitoring Period** drop-down list. The list of detected or prevented threats is displayed in the **WAF Threats Detected & Prevented** table.
- 2 To display details about a threat, click on the threat. The details include the following:
  - **URL** – The URL to the SonicWall knowledge base for this threat
  - **Category** – The category of the threat
  - **Severity** – The severity of the threat, either high, medium, or low
  - **Summary** – A short description of how the threat behaves

ID	Signature	Threat Classification	Severity	Frequency
9008	Cross-site Scripting (XSS) Attack	Client-side Attacks--Cross-site Scripting	HIGH	8

#### Cross-site Scripting (XSS) Attack

**URL:** <http://software.sonicwall.com/applications/waf/index.asp?ev=sig&sigid=9008>

**Category:** Client-side Attacks--Cross-site Scripting

**Severity:** HIGH

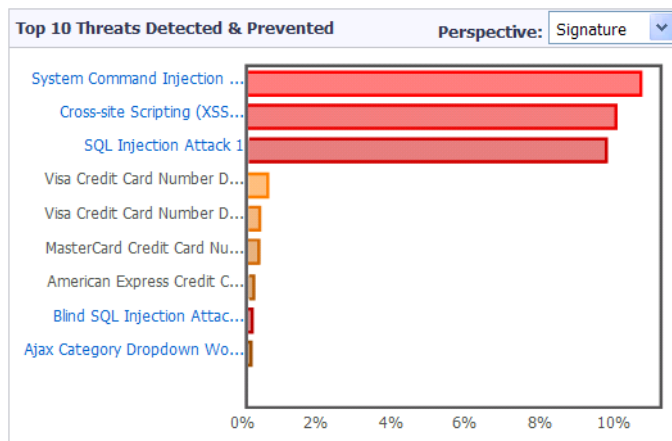
**Summary:** XSS is a technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser

- 3 To collapse the threat details, click the threat link again.

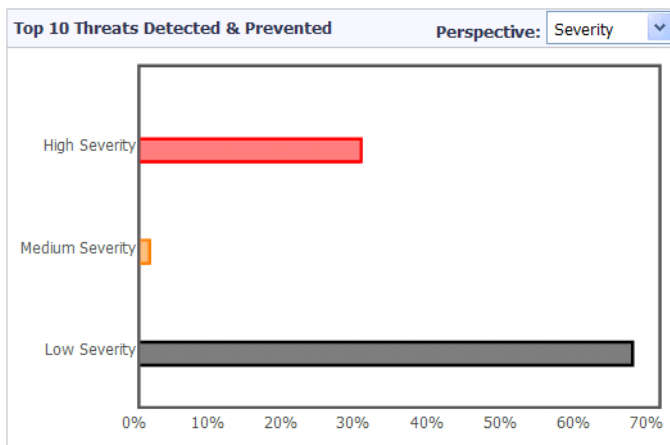
## Changing Perspective

For the Top 10 Threats graph, you can select the following display options from the **Perspective** drop-down list:

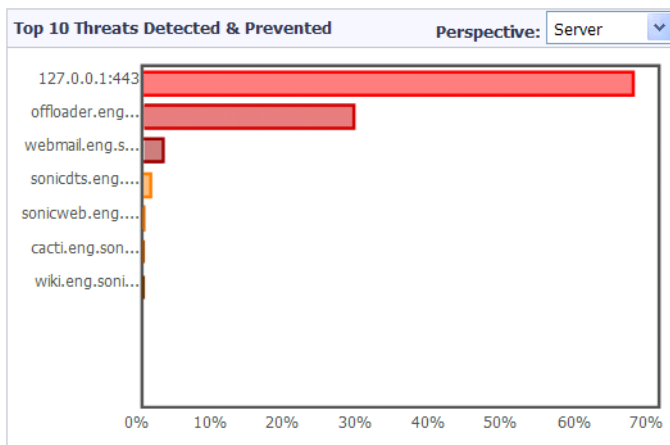
- **Signature** – The name of each threat shown is listed at the left side of the graph.



- Severity – High, medium, and low severity threats are displayed using color coding.



- Server – The server names are listed at the left side of the graph.

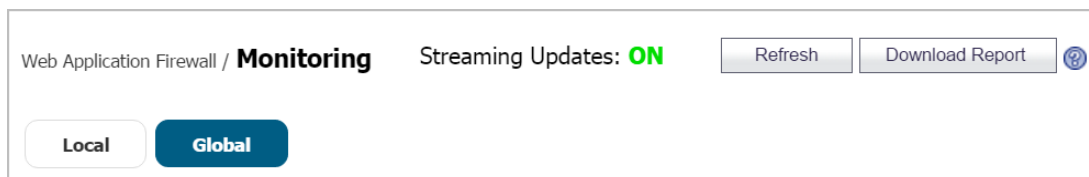


## Monitoring on the Global Screen

The **Global** screen displays statistics and graphs for threats reported by all SonicWall SMA/SRA appliances with Web Application Firewall enabled. Graphs are displayed for WAF Threats Detected & Prevented.

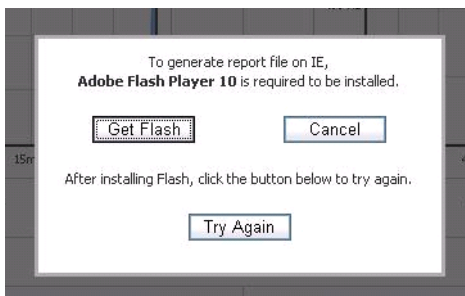
### Using the Control Buttons

The control buttons are displayed at the top of the page. They control the statistics that are displayed on this page. On the Global screen, you can use the control buttons to turn streaming updates on or off, refresh the data on the screen, and download a report. If streaming is turned on, Web Application Firewall statistics information is fetched periodically, and displayed in the graphs and threat list. If streaming is turned off, no new information can be displayed.



### To use the control buttons:

- 1 Select the **Global** screen. The active screen name is displayed in blue, while the inactive tab name is white. The control buttons act on the screen that is currently displayed.
- 2 To turn streaming on or off, click the **ON** or **OFF** indicator next to **Streaming Updates**.
- 3 To refresh the display, click the **Refresh** button.
- 4 To generate a PDF report containing Web Application Firewall statistics, click the **Download Report** button.  
**i** **NOTE:** Internet Explorer requires Adobe Flash Player version 10 or higher to generate the report.
- 5 If prompted to install Adobe Flash Player, click **Get Flash** and then after the installation click **Try Again** to generate the PDF report from Internet Explorer.



## Monitoring Detected and Prevented Threats

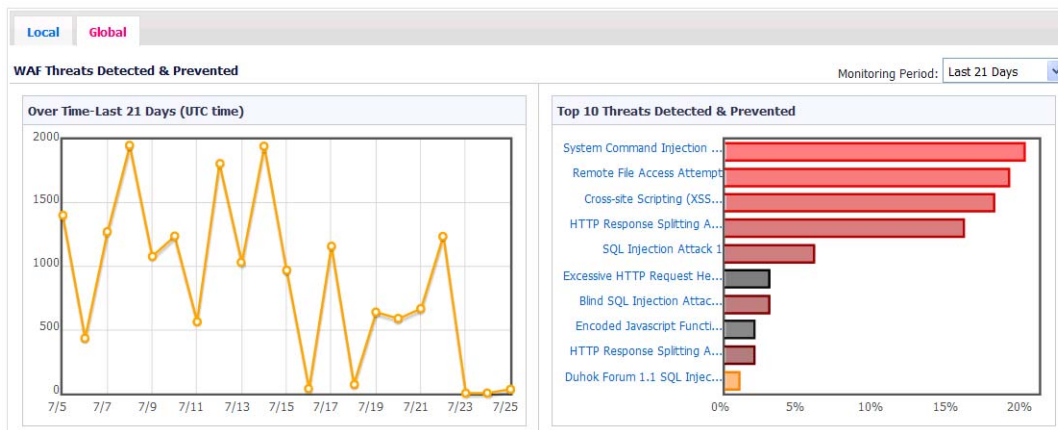
At the top of the **Global** screen, the **Web Application Firewall > Monitoring** page displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that time frame.

You can change the time frame displayed in both graphs by selecting one of the following options from the **Monitoring Period** drop-down list:

- Last 12 Hours
- Last 14 Days
- Last 21 Days
- Last 6 Months

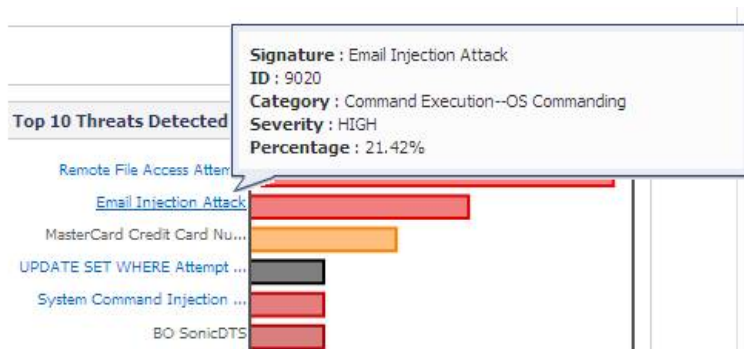
**Threats Over Last 21 Days** shows the number and severities of threats detected and prevented over the last 21 days.

## Threats Over Last 21 Days



Hovering your mouse pointer over the signature ID causes a tooltip to appear with details about the threat.

## Threat Details Tooltip



The local signature database on the appliance is accessed to get detailed threat information, but if the database is not up-to-date, some detailed information for the Top 10 Threats might not be available. In this case, the threat color in the graph is light grey, and the severity is displayed as *unknown* in the tooltip for this threat. The following error message is also displayed below the graphs:

“Warning: Web Application Firewall Signature Database for this device is not current. Please synchronize the Database from the **Web Application Firewall > Status** page”

# Using Web Application Firewall Logs

The **Web Application Firewall > Log** page provides a number of functions, including a flexible search mechanism, and the ability to export the log to a file or email it. The page also provides a way to clear the log. Clicking on a log entry displays more information about the event.

Web Application Firewall / **Log** Export Log Clear Log E-Mail Log

Search  in All Fields Search Exclude Reset

Items per page  Items  to 3 (of 3) « « « « » » » » » »

Time ▼	Priority	Category	Source	Destination	User	Message
2017-02-03 13:02:18	Notice	Web Application Firewall	192.168.200.1	192.168.200.1	System	Signature Database has been updated automatically.
2017-02-03 13:02:16	Notice	Web Application Firewall	192.168.200.1	192.168.200.1	System	WAF signature database has been updated
2017-02-03 13:02:16	Notice	Web Application Firewall	192.168.200.1	192.168.200.1	System	WAF Signature Database Update was downloaded successfully.

See the following sections:

- [Searching the Log](#) on page 63
- [Controlling the Log Pagination](#) on page 63
- [Viewing Log Entry Details](#) on page 64
- [Exporting and Emailing Log Files](#) on page 64
- [Clearing the Log](#) on page 65

## Searching the Log



You can search for a value contained in a certain column of the log table, and can also search for log entries that do **not** contain the specified value.



### *To view and search Web Application Firewall log files:*

- 1 On the **Web Application Firewall > Log** page, type the value to search for into the **Search** field.
- 2 Select the column in which to search from the drop-down list to the right of the **Search** field.
- 3 Do one of the following:
  - To start searching for log entries containing the search value, click **Search**.
  - To start searching for log entries that do not contain the search value, click **Exclude**.
  - To clear the Search field, set the drop-down list back to the default (Time), and display the first page of log entries, click **Reset**.

## Controlling the Log Pagination

### *To adjust the number of entries on the log page and display a different range of entries:*

- 1 On the **Web Application Firewall > Log** page, enter the number of log entries that you want on each page into the **Items per Page** field. The Log page display changes to show the new number of entries.
- 2 To view the log entries beginning at a certain number, type the starting number into the **Item** field and press **Enter** on your keyboard.
- 3 To view the first page of log entries, click the left-most button  in the arrow control pad.
- 4 To view the previous page of log entries, click the left arrow  in the arrow control pad.

- To view the next page of log entries, click the right arrow  in the arrow control pad.
- To view the last page of log entries, click the right-most button  in the arrow control pad.

## Viewing Log Entry Details

The log entry details vary with the type of log entry. The URI (Uniform Resource Indicator) is provided along with the command for detected threats. Information about the agent that caused the event is also displayed. For an explanation of the rather cryptic Agent string, the following Wikipedia page provides a description and links to external sites that can analyze any user agent string: [http://en.wikipedia.org/wiki/User\\_agent](http://en.wikipedia.org/wiki/User_agent)

### To view more details about an individual log entry:

- On the **Web Application Firewall > Log** page, click anywhere on the log entry that you want to view. The details are displayed directly beneath the entry.

2009-02-06 14:54:52	Critical	10.0.61.71	192.168.200.20	admin	WAF threat detected: System Command Injection Variant 1
<b>More Detail</b>					
<b>URI :</b> http://www.google.com/?cmd=tracert					
<b>Agent :</b> Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; InfoPath.1)					

- To collapse the details for a log entry, click again on the entry.

## Exporting and Emailing Log Files

You can export the current contents of the Web Application Firewall log to a file, or email the log contents by using the buttons in the top right corner of the **Web Application Firewall > Log** page.

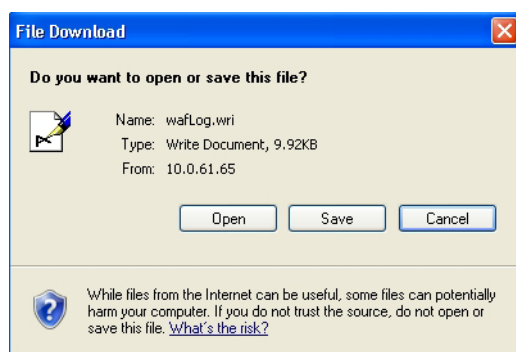
Exported files are saved with a **.wri** file name extension, and open with Wordpad, by default.

Emailed files are automatically sent to the address configured on the **Log > Settings** page of the SonicWall SMA management interface. If no address is configured, the Status line at the bottom of the browser will display an error message when you click the **E-Mail Log** button on the **Web Application Firewall > Log** page.

**Status: Error: No destination e-mail address has been configured. Please check your log settings.**

### To export or email the log:

- To export the log contents, click the **Export** button in the top right corner of the **Web Application Firewall > Log** page. The File Download dialog box is displayed.





- 2 In the File Download dialog box, do one of the following:
  - To open the file, click **Open**.
  - To save the file, click **Save**, then browse to the folder where you want to save the file and click **Save**.
- 3 To email the log contents, click the **E-Mail Log** button in the top right corner of the **Web Application Firewall > Log** page. The log contents are emailed to the address specified in the **Log > Settings** page.

## Clearing the Log

You can remove all entries from the Web Application Firewall log on the **Web Application Firewall > Log** page. The entries on the page are removed, and any attempt to export or email the log file while it is still empty will cause a confirmation dialog box to display.



### *To clear the Web Application Firewall log:*

- 1 On the top right corner of the **Web Application Firewall > Log** page, click **Clear**.
- 2 Click **OK** in the confirmation dialog box.

## Configuring an Application Offloading Portal

Because Web Application Firewall is used most often to protect an Application Offloading portal, this section provides a summary of how to configure such a portal. The SonicWall SMA/SRA appliance administrator can configure web (HTTP) or secure web (HTTPS) offloaded applications to allow user access to web-based resources and applications such as Sharepoint, Microsoft OWA Premium, or Domino Web Access.

Application Offloading should support any application using HTTP/HTTPS. SonicWall SMA has limited support for applications using web services and no support for non-HTTP protocols wrapped within HTTP.

The application should not contain hard-coded self-referencing URLs. If these are present, the Application Offloading proxy must rewrite the URLs. Since web site development does not usually conform to HTML standards, the proxy can only do a best-effort translation when rewriting these URLs. Specifying hard-coded, self-referencing URLs is not recommended when developing a web site because content developers must modify the web pages whenever the hosting server is moved to a different IP or hostname.

For example, if the backend application has a hard-coded IP address and scheme within URLs as follows, Application Offloading must rewrite the URL.

```
<a href="http://1.1.1.1/doAction.cgi?test=foo">
```

For detailed configuration information, see the *SonicWall SMA Application Offloading and HTTP(S) Bookmarks Feature Guide* or the *SMA 8.6 Administration Guide* at: <http://www.sonicwall.com>

The **Application Offloading Portal Settings** table shows appropriate Application Offloading portal settings when the portal is providing Web Application Firewall protection to remotely accessed internal sites and to public sites.

## Application Offloading Portal Settings

Application Offloading Portal Settings	For Remote Access to an Internal Site	For Remote Access to a Public Site
DNS Configuration	Split DNS	Public DNS
Authentication	Enabled	Disabled (likely)
Access Policies	User/Group/Global	Global
SSL VPN Domains	Enabled	None
Login Customization	Optional	None
Custom Logo	Optional	None

SonicWall recommends using the same FQDN for the Virtual Host Name and the application server site to avoid the need for URL rewriting.

### To offload a Web application and create a portal for it:

1. Navigate to **Portals > Portals** and go to the **Virtual Host** section. The Virtual Host Settings screen opens. This allows you to access the Portal directly.

2. Enter a descriptive name in the **Virtual Host Domain Name** field.
3. On the **Offloading** tab, select **Enable Load Balancing** for load balancing among offloaded application servers.
4. Select one of the following from the **Scheme** drop-down list:
  - **Web (HTTP)** – access the Web application using HTTP (default scheme)
  - **Secure Web (HTTPS)** – access the Web application using HTTPS
  - **Auto (HTTP/HTTPS)** – allows the user to determine the actual scheme used to talk to the backend server when accessing an offloading portal. Access is still under the control of the access policy.

When using the Auto scheme, users can type <http://www.example.virtual.host.com> or <https://www.example.virtual.host.com> in browser's address bar to test this feature. Even scheme set to Auto, it's still under the control of the access policy.

**CAUTION:** It is the Administrator's responsibility to configure the correct scheme used to talk to the backend server. Auto (HTTP/HTTPS) Scheme can operate only if HTTP access is enabled for the Virtual Host (under the Virtual Host tab) and authentication is disabled (under the Offloading tab) that can be insecure. Therefore, you are prompted to click OK to enable HTTP for Virtual Host.

- **Generic (SSL Offloading)** – use SSL offloading to access custom SSL applications (non-HTTP(S) applications)
- 5 Enter the host name or private IP address of the backend host into the **Application Server Host** field.
  - 6 Optionally enter the IPv6 address of the backend host into the **Application Server IPv6 Address** field.
  - 7 In the **Port Number (optional)** field, optionally enter a custom port number to use for accessing the application.
  - 8 In the **Homepage URI (optional)** field, optionally enter a URI to a specific resource on the Web server to which the user is forwarded the first time the user tries to access the Application Offloading Portal. This is a string in the form of: **/exch/test.cgi?key1=value1&key2=value2**

When this field is configured, it redirects the user to the Web site's home page the first time the user accesses the portal. This happens only when the user is accessing the site with no URL path (that is, when accessing the root folder, for example: <https://www.google.com/>). This is not an alias for the root folder. The user can edit the URL to go back to the root folder.

The key=value pairs allow you to specify URL query parameters in the URL. You can use these for any Web site that does not have a default redirect from the root folder to the home page URL. Outlook Web Access is one example, but note that most public sites do have a default redirect.

- a Under Security Settings, select **Enable Web Application Firewall** to enable the feature.
  - b Select **Disable Authentication Controls, Access Policies, and CSRF Protection (if enabled)** if you need no authentication, access policies, or CSRF protection enforced. This is useful for publicly hosted Web sites.
  - a To configure ActiveSync authentication, clear **Disable Authentication Controls** to display the authentication fields. Select **Enable ActiveSync authentication** and then type the default domain name. The default domain name is not used when the domain name is set in the email client's setting.
- 9 Select **Automatically Login** to configure Single Sign-On settings.

The screenshot shows the 'Security Settings' configuration page. It includes several checkboxes: 'Disable Access Policies', 'Disable Authentication Controls', 'Share session with other local applications', and 'Automatically log in'. Under 'Automatically log in', there are radio buttons for 'Use SSL VPN account credentials' (selected), 'Use Login Domain for SSO', and 'Use custom credentials'. There is also a checkbox for 'Forms-based Authentication' which is checked, with input fields for 'User Form Field', 'Password Form', and 'Field:'. At the bottom, there are checkboxes for 'Enable Email Clients Authentication' and 'Enforce ActiveSync Provision:', with a dropdown menu set to 'Use Global Setting'.

- 10 For automatic login using SSO, select one of the following radio buttons:

- **Use SSL-VPN account credentials** – allow log in to the offloaded application using the credentials configured on the SonicWall SMA/SRA appliance.

- **Use custom credentials** – displays **Username**, **Password**, and **Domain** fields where you can enter the custom credentials for the application or use dynamic variables. For the **Password** field, enter the custom password to be passed, or leave the field blank to pass the current user's password to the offloaded application portal. For the other fields, dynamic variables can be used, such as those shown in the following table:

### Supported dynamic variables

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN%\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%

- 11 If you selected **Automatically Login**, select **Forms-based Authentication** to configure Single Sign-On for forms-based authentication.

- Configure the **User Form Field** to be the same as the 'name' and 'id' attribute of the HTML element representing User Name in the Login form, for example:

```
<input type=text name='userid'>
```

- Configure the **Password Form Field** to be the same as the 'name' or 'id' attribute of the HTML element representing Password in the Login form, for example:

```
<input type=password name='PASSWORD' id='PASSWORD' maxlength=128>
```

- 12 In the **Virtual Host** section, set a host name for the application in the **Virtual Host Domain Name** field, and optionally enter a descriptive alias in the **Virtual Host Alias** field.

If you need to associate a certificate to this host, you should additionally set a virtual interface and import the relevant SSL certificate. You could avoid creating a virtual interface by importing a wildcard certificate for all virtual hosts on the SonicWall SMA/SRA appliance.

See the *SonicWall Secure Mobile Access 8.6 Administration Guide* for more instructions on configuring the fields in this section.

- 13 If authentication is disabled for this portal, you have the option to **Enable HTTP access** for this Application Offloaded Portal. This feature is useful for setting up offloading in trial deployments.

#### Virtual Host Settings

Virtual Host Domain Name:

Virtual Host Alias (optional):

Virtual Host Interface:


Virtual Host IP Address:


Virtual Host IPv6 Address:

**Note:** Portals must have unique Virtual Host IP Addresses (if specified).

Virtual Host Certificate:

Enable Keep-Alive

Enable Virtual Host Domain SSO 

Shared Domain Name:  

- 14 Click **Accept**. You are returned to the **Portals > Portals** page where you see the Web application listed as an **Offloaded Web Application** under Description.

<input type="checkbox"/>	Portal Name ▼	Description	Virtual Host Settings	Configure
<input type="checkbox"/>	OWA	Offloaded Web Application	webmail.example.com	
<input type="checkbox"/>	sales	Secure Mobile Access	sales	
<input type="checkbox"/>	VirtualOffice	Secure Mobile Access	105	

ADD PORTAL ...    OFFLOAD WEB APPLICATION ...    DELETE SELECTED PORTALS

- 15 If you have not disabled authentication, navigate to the **Portals > Domains** page and create a domain for this portal.
- 16 Update your DNS server for this virtual host domain name and alias (if any).

**i** | **NOTE:** In the future, without a WAF license, Anonymous Application Offloading access will not be supported. Activate a WAF subscription or use the trial version from the **System > Licenses** page.

# Verifying and Troubleshooting Web Application Firewall

One way to verify the correct configuration of Web Application Firewall is by viewing the **Web Application Firewall > Monitoring** page. This page displays statistics and graphs for detected/prevented threats over time and top 10 threats. The **Local** screen also displays Web server status statistics and graphs of the number of requests and the amount of traffic during the selected monitoring period. With normal use and exposure to the Internet, you should begin to see statistics within a day of activation.

You can also find helpful information in both the **Log > View** page and **Web Application Firewall > Log** page. This section lists some of the relevant log messages and provides an explanation or suggestions for actions in those cases.

## Log > View Messages

The following messages can be viewed from the **Log > View** page:

- License Manager SSL connection failed - Restarting the appliance could be necessary  
Test the connectivity to **licensemanager.sonicwall.com** from the **System > Diagnostics** page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.
- License Manager Failed to resolve host. Check DNS.  
Test the connectivity to **licensemanager.sonicwall.com** from the **System > Diagnostics** page using the **Ping** and **DNS Lookup** diagnostic utilities to ensure that there is connectivity to the backend server.
- License Manager Peer Identity failed - Check certificates and time  
The License Manager server or the signature database server may not have a valid SSL Certificate.
- License Manager Reset called  
The device licenses have been reset. Navigate to the **System > Licenses** page to activate, upgrade or renew licenses.

## Web Application Firewall > Log and Log > View Messages

The following messages can be viewed from the **Web Application Firewall > Log** page and the **Log > View** page:

- WAF signature database update failed: No signatures were found in the update  
The download for the database update completed, but no suitable signatures were found in the database.
- WAF signature database update failed: Old signature timestamp found in the update  
The timestamp found in the database update from the License Manager is older than what was originally advertised before the download for the update started.
- WAF signature database update failed: Error occurred while processing the update

There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.

- WAF signature database update failed: Error occurred while downloading the WAF signature database update

There was a general error in downloading and processing the database update. This is possible if the data in the update does not conform to the signature parser schema.

- WAF signature database update was downloaded successfully. The new database contains <num> rules  
Signature database download was successful. The new database contains <num> number of rules. A rule is an internal property which will be used by SonicWall to determine how many signatures were downloaded.

**i** **NOTE:** You can select the **Apply Signature Updates Automatically** option on the **Web Application Firewall > Settings** page to apply new signatures automatically. If this option is not selected, you must click the **Apply** button that appears on the **Web Application Firewall > Status** page after a successful download. After the database has been successfully applied, all of the signatures within the new database can be found on the **Web Application Firewall > Signatures** page.

- WAF signature database has been updated

The signature database update was applied after the administrator clicked on the **Apply** button on the **Web Application Firewall > Status** page.

- WAF engine is being started with the factory default signature database

The Web Application Firewall engine will be using the factory default signature database for traffic inspection. This may imply that no new signatures were found since the firmware update. If an attempt to download is revealed in the logs earlier, then this message could also imply that the update could not be processed successfully due to database errors and as a precautionary measure the factory default database has been used.

## SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.



# About This Document

## Legend



**WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.



**CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



**IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SonicWall SMA Web Application Firewall Feature Guide  
Updated - March 2018  
Software Version - 8.6  
232-004278-00 Rev A

## Copyright © 2018 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

## Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
SonicWall Inc. Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035