SonicWall® Web Application Firewall 3.0

Administration Guide

Contents

1

Overview

This document describes how to configure and use SonicWall® Web Application Firewall (WAF) 3.0. This section provides an overview of the WAF features and functions.

Topics:

What is Web Application Firewall?

SonicWall Web Application Firewall is a software product that can be deployed as a virtual machine or in the cloud. When positioned between a web server and the Internet, it analyzes layer 7 traffic sessions to provide real-time protection of applications from inbound attacks.

The award-winning WAF service enforces defense-in-depth strategy to protect your web applications from the most common threats using a high performance real-time intrusion scanning engine. It offers businesses a complete, affordable, out-of-box compliance solution for web applications that is easy to manage and deploy.

WAF supports OWASP Top Ten and PCI DSS compliance, providing protection against malicious injection and cross-site scripting attacks, credit card and Social Security Number theft, cookie tampering and cross-site request forgery. Dynamic signature updates and Application Profiling that leverages an active learning algorithm protect against known and zero-day vulnerabilities. Virtual Patching using Custom Rules allows you to instantly address a vulnerability and avoid attacks that happen while waiting for a security hotfix. WAF supports IP Reputation services and Rate Limiting features to block automated and brute-force attacks. Stacked authentication, including 2-factor authentication, one-time passwords, and SSL client certificate authentication, combined with access policies, provides granular access control to the web applications.

Highlights:

- Secures web applications against advanced web attacks including OWASP Top Ten
- Layer 7 Load Balancing and Health Monitoring features provides accelerated application delivery and high availability of your applications
- Denial of service (DoS) protection, Rate Limiting and Botnet protection with Remediation blocks automated brute-force attacks

See Types of Web Attacks on page 6 for more information about the types of attacks that SonicWall WAF protects against.

Types of Web Attacks

The top-10 vulnerabilities for web applications are tracked by OWASP, an open source community that focuses its efforts on improving the security of web applications. SonicWall WAF protects against these top-10 vulnerabilities, defined in 2017 as follows:

OWASP Top Ten Vulnerabilities

Name	Description
A1:2017 - Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017 - Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017 - Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017 - XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017 - Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017 - Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
A7:2017 - Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

OWASP Top Ten Vulnerabilities (Continued)

Name	Description
A9:2017 - Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017 - Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Slowloris Protection

In addition to the top-10 threats listed above, WAF protects against **Slowloris** HTTP Denial of Service attacks. This means that WAF 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 WAF protects against the OWASP top-10 and Slowloris types of attacks, see the How Does Web Application Firewall Prevent Attacks? on page 10.

Application Profiling

Application Profiling 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, Web Application Firewall 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

PDF reporting is supported for Web Application Firewall monitoring and PCI DSS 6.5 and 6.6 compliance. You can generate the reports on the **Web Security > Status** page. The timeline for generating the data published in the reports is configurable on the **Dashboard > Monitoring** page.

Benefits of Web Application Firewall

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

Companies using WAF 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 WAF signature updates.

Resources accessed using offloaded web apps can be vulnerable due to a variety of reasons ranging from badly designed architecture to programming errors. WAF provides an effective way to prevent a hacker from exploiting these vulnerabilities by providing real-time protection to web applications deployed in the internal network and backend servers.

Deploying WAF 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.

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. WAF provides a convenient, cost-effective solution.

WAF is easy to configure. 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 are Policies Created and Used in WAF?

The SonicWall WAF web-based management interface provides granular control of access to hosts and web applications protected by WAF. Access policies provide different levels of access to the resources that are accessible using WAF.

There are three levels of policies:

- **Global policies** are configured from the **Local Users** or **Local Groups** page by editing the **Global Policies** entry that appears at the top of the tables on both pages.
- **Group policies** are configured from the **Local Groups** page by editing a local group and adding a policy for it.
- **User policies** are configured from the **Local Users** page by editing a local user and adding a policy for it.

You can block and permit access to a resource by creating access policies for an IP address, an IP address network, all addresses, or a URL.

The policy hierarchy is:

- User policies take precedence over group policies.
- Group policies take precedence over global policies.
- If two or more user, group or global policies are configured, the most specific policy takes precedence.

For example, a policy configured for a single IP address takes precedence over a policy configured for an IP address network. A policy that applies to an IP address network takes precedence over a policy applied to all IP addresses. If two or more IP address network policies are configured, then the smallest address range takes precedence. Policies for URLs are treated the same as policies for individual IP addresses.

How Does One Time Password Work?

The One Time Password feature adds a second layer of login security to the standard username and password. A one-time password is a randomly generated, single-use password. The One Time Password feature requires users to first submit the correct WAF login credentials. After following the standard login procedure, WAF generates a one-time password that is sent to the user at a pre-defined email address. The user must log in to that email account to retrieve the one-time password and type it into the WAF login screen when prompted, before the one-time password expires.

Each one-time password is single-use and expires after a set time period, requiring that a new one-time password be generated after each successful login, canceled or failed login attempt, or login attempt that has timed out, thus reducing the likelihood of a one-time password being compromised.

The administrator can enable the One Time Password feature on a per-user or per-domain basis. To enable the One Time Password feature on a per-user basis, the administrator must edit the user settings in the WAF management interface. The administrator must also enter an external email address for each user who is enabled for One Time Passwords. For users of Active Directory and LDAP, the administrator can enable the One Time Password feature on a per-domain basis.

How Does Web Application Firewall Prevent Attacks?

Web Application Firewall can be configured to log or block detected attacks arriving from the Internet.

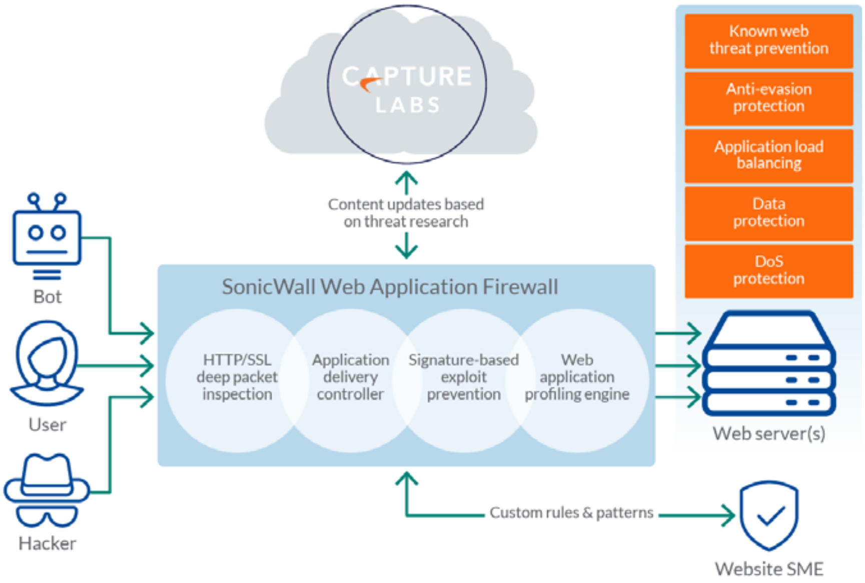
The following sections describe how WAF prevents attacks such as Slowloris or those listed in the OWASP top ten, and how WAF protects against information disclosure, and other capabilities:

- How are Signatures Used to Prevent Attacks? on page 10
- How is Cross-Site Request Forgery Prevented? on page 11
- How is Information Disclosure Prevented? on page 11
- How are Broken Authentication Attacks Prevented? on page 12
- How are Insecure Storage and Communications Prevented? on page 12
- How is Access to Restricted URLs Prevented? on page 12
- How are Slowloris Attacks Prevented? on page 12
- What Type of PCI Compliance Reports Are Available? on page 12
- How Does Cookie Tampering Protection Work? on page 13
- How Does Application Profiling Work? on page 14
- How Does Rate Limiting for Custom Rules Work? on page 14

How are Signatures Used to Prevent Attacks?

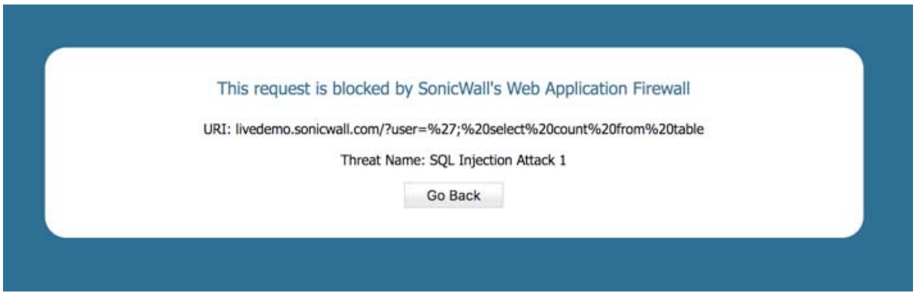
For Cross Site Scripting, Injection Flaws, Malicious File Execution, and Insecure Direct Object Reference vulnerabilities, SonicWall WAF uses a black list of signatures that are known to make web applications vulnerable. New updates to these signatures are periodically downloaded from a SonicWall signature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

How signatures prevent attacks


CAPTURE LABS
Content updates based on threat research
SonicWall Web Application Firewall
HTTP/SSL deep packet inspection
Application delivery controller
Signature-based exploit prevention
Web application profiling engine
Bot
User
Hacker
Known web threat prevention
Anti-evasion protection
Application load balancing
Data protection
DoS protection
Web server(s)
Custom rules & patterns
Website SME

When input arrives from the Internet, WAF 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.

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



This request is blocked by SonicWall's Web Application Firewall

URI: livedemo.sonicwall.com/?user=%27;%20select%20count%20from%20table

Threat Name: SQL Injection Attack 1

This page is customizable under **Web Security > Settings** in the WAF 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, WAF rewrites all URLs contained in a web page.

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 web app, then the user is redirected to the login page for the web app.

How is Information Disclosure Prevented?

WAF 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 WAF reveals this text. These text strings are entered on the **Web Security > Settings** page.

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

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

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

WAF 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. WAF 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 WAF to support strong session management to enhance the authorization requirements for web sites. WAF has strong authentication capabilities with the ability to support One Time Password and client certificate authentication.

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

The **Web Security > Settings > Session Management** 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 WAF and the client. SonicWall WAF also supports HTTPS with the backend web server.

How is Access to Restricted URLs Prevented?

SonicWall WAF supports access policies based on host, subnet, 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?

WAF monitors the rate at which requests are processed and uses timeouts 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 and PCI DSS 6.6 (Version 3.2) are covered in PCI reporting. The administrator can configure WAF to satisfy these PCI requirements.

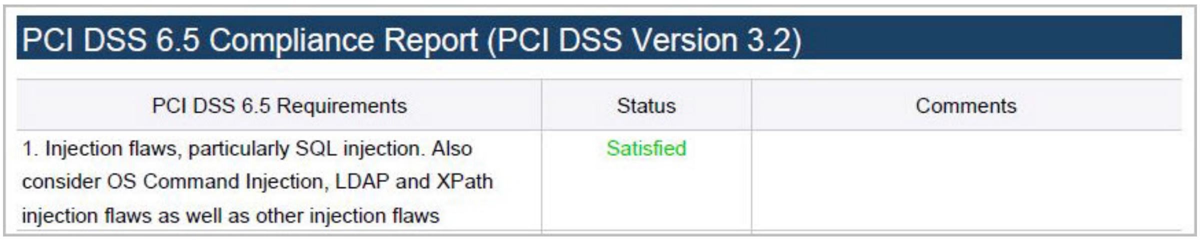
You can generate and download the PCI report file on the **Web Security > Status** page.

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

Web Application Firewall

PCI DSS Compliance Report

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 Version 3.2)

PCI DSS 6.5 Requirements	Status	Comments
1. Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws	Satisfied	

The first column describes the PCI requirement.

The second column displays the status of the PCI requirement under current WAF 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?

WAF 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.

You can configure cookie tampering protection for detection only, for prevention which strips the tampered cookie and logs it, or you can disable cookie tampering protection. You can also configure exclusions for server-side cookies or client-side cookies to allow them to pass without checking for tampering.

This feature is found on the **Web Security > Settings > Cookie Tampering Protection** page.

How Does Application Profiling Work?

The administrator can configure application profiling on the **Web Security > App Profiling** page. Application profiling is performed independently for each web app.

After selecting the web app, you can select the type of application content that you want to profile. You can choose **HTML/XML**, **JSON**, **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.

SonicWall WAF is placed in learning mode and profiling is performed while trusted users are using applications in an appropriate way. WAF records inputs and stores them as URL profiles. You can edit the learned values for a URL if the values are not accurate.

WAF 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 end the profiling and then generate rules from the learned input. If a URL profile has been modified, those changes are incorporated.

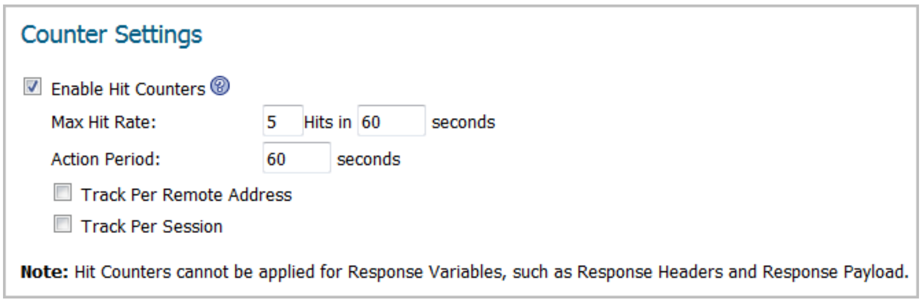
If a rule chain has already been generated from a URL profile in the past, you can overwrite it.

How Does Rate Limiting for Custom Rules Work?

The administrator can configure rate limiting when adding or editing a rule chain from the **Web Security > Custom 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

☑ Enable Hit Counters

Max Hit Rate: 5 Hits in 60 seconds

Action Period: 60 seconds

□ Track Per Remote Address

□ Track Per Session

Note: Hit Counters cannot be applied for Response Variables, such as Response Headers and Response Payload.

Once a rule chain is matched, WAF keeps an internal counter to track how many times the rule chain is matched.

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 WAF. 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

WAF is available on the following platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- VMware ESXi
- Microsoft Hyper-V

For supported versions and system requirements, see the *SonicWall Web Application Firewall Deployment Guide* for the platform, available on the SonicWall Support site at: https://www.sonicwall.com/en-us/support/technical-documentation

2

Using Web Application Firewall Dashboard

The WAF virtual appliance provides configurable monitoring and system tools that enable you to view threat statistics and graphs, and usage data for your appliance. This section describes the Dashboard pages in the SonicWall Web Application Firewall management interface.

Topics:

- Viewing Status and Threats on Dashboard > Monitoring on page 16
- Viewing WAF Usage on Dashboard > System on page 27

Viewing Status and Threats on Dashboard > Monitoring

The **Dashboard > Monitoring** page provides two pages: **Local** and **Global**. Both pages display statistics and graphs for detected threats over time and top-10 threats.

The **Local** page displays web server status statistics, information about your **Licenses** (Web Apps and Data Usage), **Latest Alerts** (Date/Time, User, Message), and a **Web Apps** table.

The **Local** page also shows graphs of the number of requests and the amount of traffic during the selected monitoring period, plus a list of the top 10 botnets.

The **Global** page displays WAF threats detected and prevented over the last six months.

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

- Using the Control Buttons on page 16
- Monitoring on the Local Screen on page 17
- Monitoring on the Global Screen on page 26

Using the Control Buttons

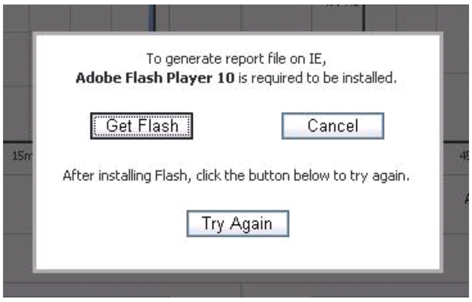
The control buttons on each screen of the **Dashboard > Monitoring** page control the statistics that are displayed. You can use the control buttons to turn streaming updates on or off, refresh the data on the screen, and download a report. The **Streaming Updates** control is displayed at the top right of the screen, and the **REFRESH** and **DOWNLOAD REPORT** buttons are displayed at the bottom right of the page. The **Local** screen provides a **CLEAR statistics** control button at the bottom right under the **WAF Threats Detected & Prevented** section.

The **Local** screen also features a **Monitoring Period** drop-down menu for the **Requests & Traffic** and **WAF Threats Detected & Prevented** sections. You can monitor the activity for the **Last 6 Months**, **Last 12 Hours**, **Last 14 Days**, **Last 21 Days**, and **All in Lists.**

If streaming is turned on, WAF 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** or **Global** 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. On the **Local** screen, click **CLEAR** to empty the **Top 10 Botnets Detected** table.
5. To generate a PDF report with Web Application Firewall statistics, click **DOWNLOAD REPORT**. A popup dialog displays "Your report is ready". Click **DOWNLOAD** to download the report, or **CANCEL** to cancel the request.
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 your browser.

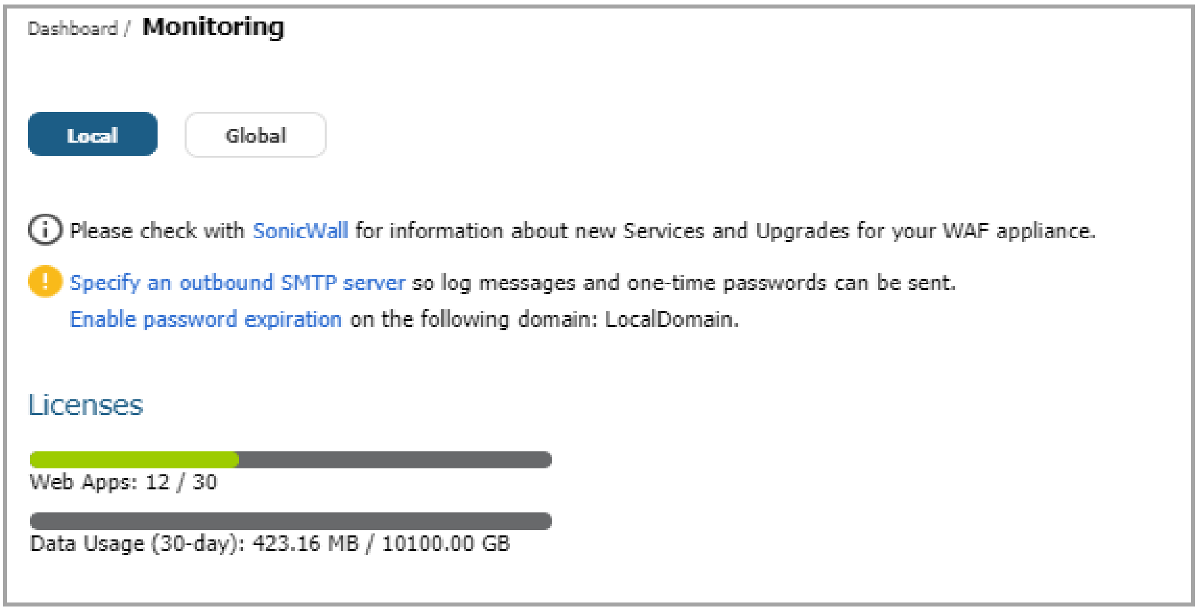


To generate report file on IE,
Adobe Flash Player 10 is required to be installed.

After installing Flash, click the button below to try again.

Monitoring on the Local Screen

The **Dashboard > Monitoring > Local** screen displays notifications and alerts at the top. The **Licenses** progress bars visually display Web App and Data Usage.



Dashboard / **Monitoring**

Local Global

ⓘ Please check with SonicWall for information about new Services and Upgrades for your WAF appliance.

! Specify an outbound SMTP server so log messages and one-time passwords can be sent.
Enable password expiration on the following domain: LocalDomain.

Licenses

Web Apps: 12 / 30

Data Usage (30-day): 423.16 MB / 10100.00 GB

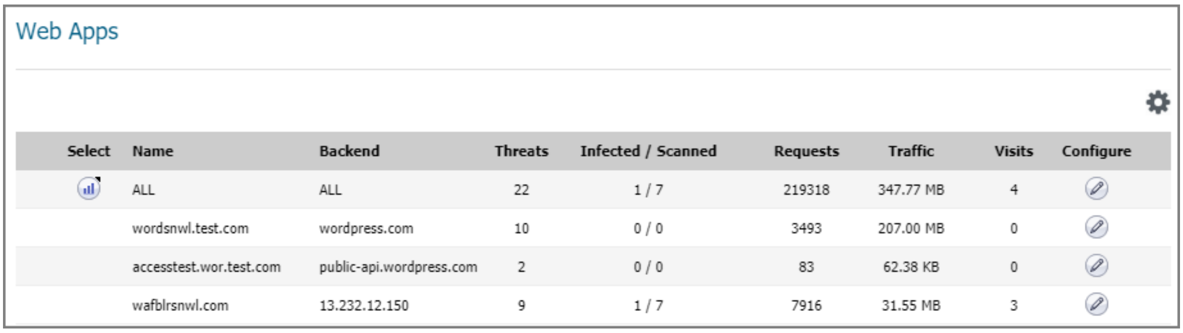
If you have not licensed your firewall, a message appears at the top of the **Monitoring** page. Click the **License Web Application Firewall** link and follow the prompts to license the WAF.

After you register your account, the progress bar starts at green and turns yellow, orange, and then red as the number of available licenses are consumed.

The Web Apps Table displays the list of web applications being monitored. Graphs and statistics are displayed below the **Web Apps** table. The **Configure** icon opens the **Web App Edit** screen.

For more information about WAF licensing, see Configuring System Licenses on page 37.

Web Apps Table



Web Apps

Select	Name	Backend	Threats	Infected / Scanned	Requests	Traffic	Visits	Configure
📊	ALL	ALL	22	1 / 7	219318	347.77 MB	4	✎
	wordsnwl.test.com	wordpress.com	10	0 / 0	3493	207.00 MB	0	✎
	accesstest.wor.test.com	public-api.wordpress.com	2	0 / 0	83	62.38 KB	0	✎
	wafblrsnwl.com	13.232.12.150	9	1 / 7	7916	31.55 MB	3	✎

After the WAF is licensed, a drop-down menu appears when you click the Gear icon on the right in the Web Apps table that provides the following options:

- MANAGE WEB APPS
- EVENTS AND ACCESS LOGS
- CONFIGURE WEB SECURITY
- CONFIGURE BOT SECURITY
- CONFIGURE CAPTURE ATP
- MANAGE EXCLUSIONS

You can click on any row (any application or **ALL**) in the **Web Apps** table to display per-Web App graphs and/or statistics specific to it. The graph icon in the **Graph** column is displayed only on the selected row.

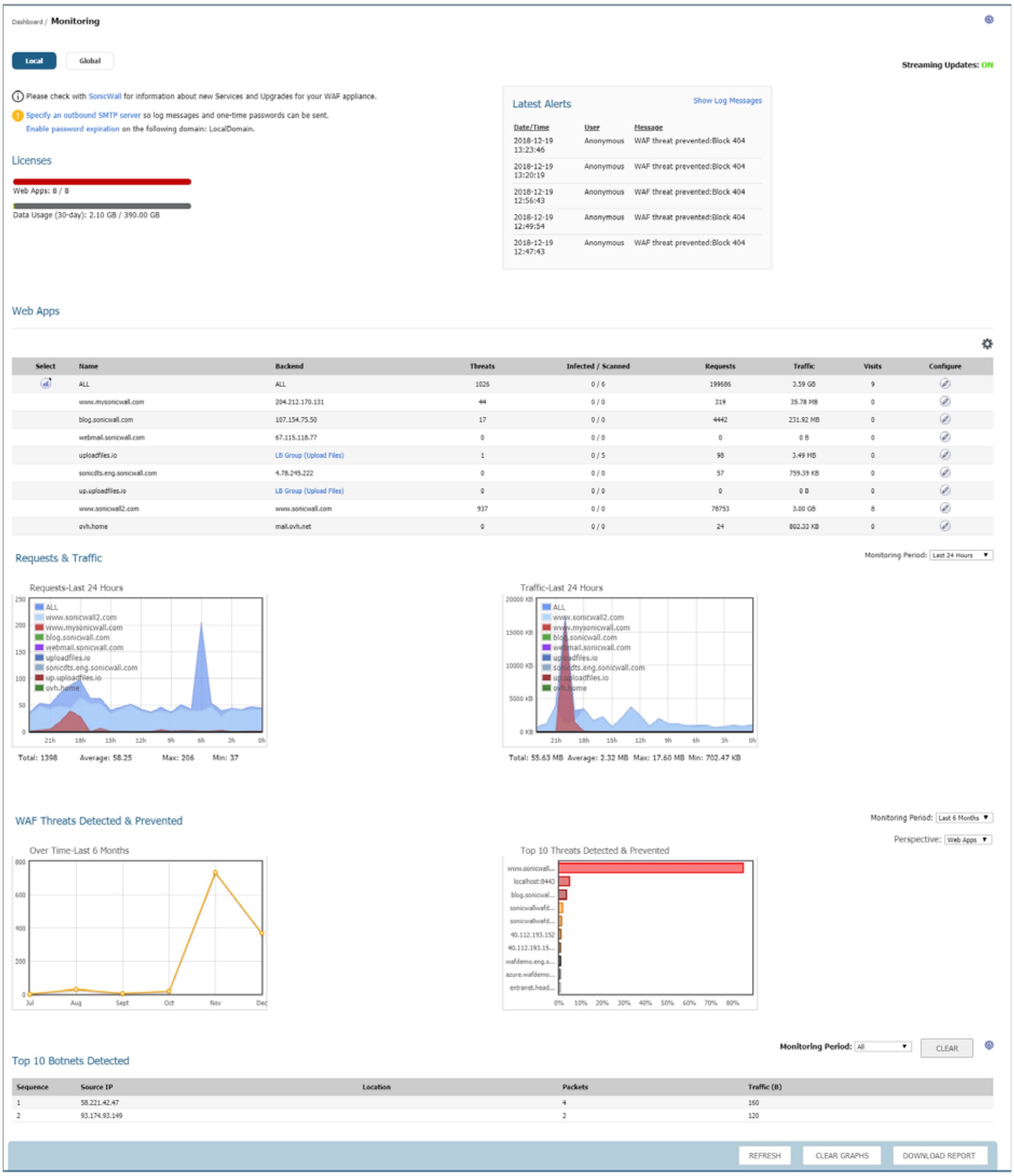
The following graphs and/or statistics are displayed for the selected application or for **ALL**:

- **Requests & Traffic**
    - **Requests**
    - **Traffic**
- **WAF Threats Detected & Prevented**
    - **Over Time-Last 6 Months**
    - **Top 10 Threats Detected & Prevented**
- **Top 10 Botnets Detected**

All offer a choice of the monitoring period. For **WAF Threats Detected & Prevented**, you can display the statistics in list format or as graphs. The **Top 10 Botnets Detected** is displayed as a list.

For more information about configuring a Web App for protection, see Configuring Offloaded Web Apps on page 79.

Dashboard > Monitoring - Local Screen



Dashboard / **Monitoring**

Streaming Updates: ON

Please check with SonicWall for information about new Services and Upgrades for your WAF appliance.

Specify an outbound SMTP server so log messages and one-time passwords can be sent.
Enable password expiration on the following domain: LocalDomain.

Licenses

Web Apps: 8 / 8

Data Usage (30-day): 2.10 GB / 390.00 GB

Latest Alerts

Show Log Messages

Date/Time	User	Message
2018-12-19 13:23:46	Anonymous	WAF threat prevented:Block 404
2018-12-19 13:20:19	Anonymous	WAF threat prevented:Block 404
2018-12-19 12:56:43	Anonymous	WAF threat prevented:Block 404
2018-12-19 12:49:54	Anonymous	WAF threat prevented:Block 404
2018-12-19 12:47:43	Anonymous	WAF threat prevented:Block 404

Web Apps

Select	Name	Backend	Threats	Infected / Scanned	Requests	Traffic	Visits	Configure
●	ALL	ALL	1026	0 / 6	199686	3.59 GB	9	✎
	www.mysonicwall.com	204.212.170.131	44	0 / 0	319	35.78 MB	0	✎
	blog.sonicwall.com	107.154.75.50	17	0 / 0	4442	231.92 MB	0	✎
	webmail.sonicwall.com	67.115.118.77	0	0 / 0	0	0 B	0	✎
	uploadfiles.io	LB Group (Upload Files)	1	0 / 5	98	3.49 MB	0	✎
	sonicdts.eng.sonicwall.com	4.78.245.222	0	0 / 0	57	759.39 KB	0	✎
	up.uploadfiles.io	LB Group (Upload Files)	0	0 / 0	0	0 B	0	✎
	www.sonicwall2.com	www.sonicwall.com	937	0 / 0	78753	3.00 GB	8	✎
	ovh.home	mail.ovh.net	0	0 / 0	24	802.33 KB	0	✎

Requests & Traffic

Monitoring Period: Last 24 Hours ▼

Requests-Last 24 Hours

Total: 1398 Average: 58.25 Max: 206 Min: 37

Traffic-Last 24 Hours

Total: 55.63 MB Average: 2.32 MB Max: 17.60 MB Min: 702.47 KB

WAF Threats Detected & Prevented

Monitoring Period: Last 6 Months ▼

Perspective: Web Apps ▼

Over Time-Last 6 Months

Top 10 Threats Detected & Prevented

Monitoring Period: All ▼

Top 10 Botnets Detected

Sequence	Source IP	Location	Packets	Traffic (B)
1	58.221.42.47		4	160
2	93.174.93.149		2	120

Topics:

- Monitoring Requests & Traffic on page 21
- Monitoring Detected and Prevented Threats on page 22
- Monitoring Detected Botnets on page 25

Monitoring Requests & Traffic

On the **Local** screen, the **Requests & Traffic** section displays two graphs. One graph shows the number of web requests detected over time, and another graph shows the amount of traffic inspected over time.

The **Requests** graph tracks requests sent to all web servers protected by SonicWall WAF as a function of time. Statistics under the graph display total, average, maximum, and minimum number of web server requests within the selected time frame.

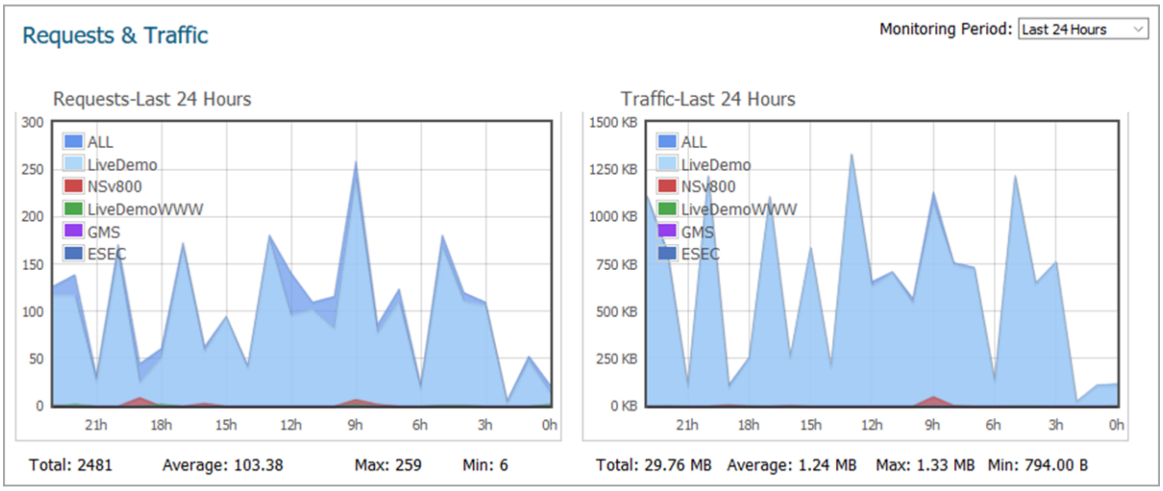
The **Traffic** graph tracks the amount of data transferred and received by the web servers protected by SonicWall WAF as a function of time. Statistics under the graph display total, average, maximum, and minimum amounts of traffic within the selected time frame.

You can view web server requests and traffic 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

The Requests & Traffic For Last 24 Hours image shows a 24 hour period of web server activity.

Requests & Traffic For Last 24 Hours



Requests & Traffic

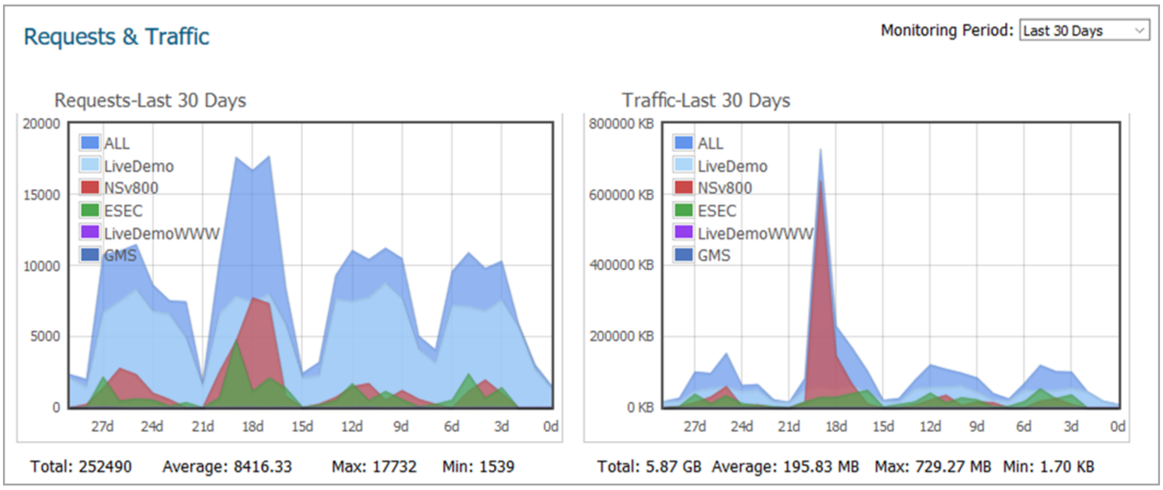
Monitoring Period: Last 24 Hours

Total: 2481 Average: 103.38 Max: 259 Min: 6

Total: 29.76 MB Average: 1.24 MB Max: 1.33 MB Min: 794.00 B

The Requests & Traffic For Last 30 Days image shows a 30 day period of web server activity.

Requests & Traffic For Last 30 Days



Total: 252490 Average: 8416.33 Max: 17732 Min: 1539

Total: 5.87 GB Average: 195.83 MB Max: 729.27 MB Min: 1.70 KB

Monitoring Detected and Prevented Threats

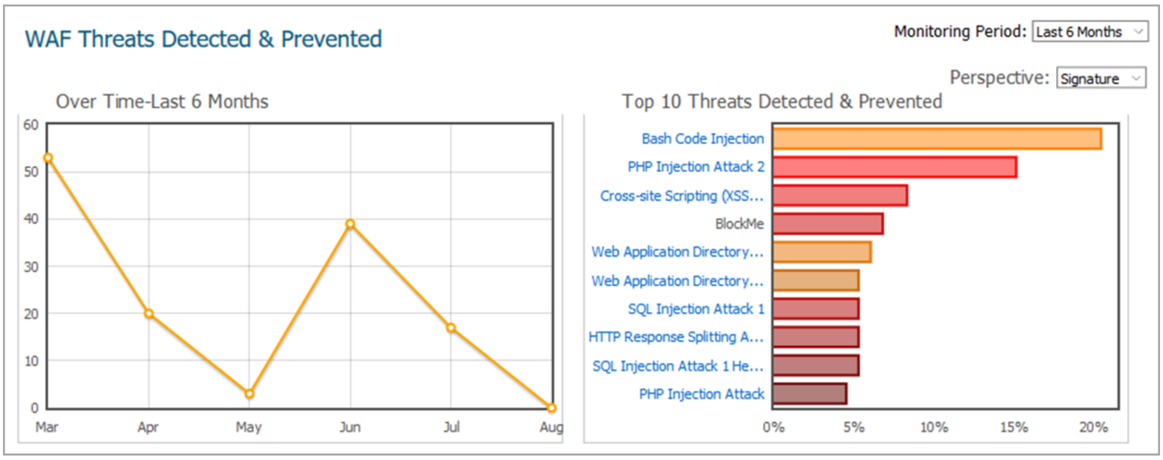
On the **Local** screen, the **WAF Threats Detected & Prevented** section displays graphs indicating the number of detected and prevented threats. Two graphs are presented, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that 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

The Threats Over Last 6 Months image shows an example of the number and severities of threats detected and prevented over the last 6 months.

Threats Over Last 6 Months



WAF Threats Detected & Prevented
Monitoring Period: Last 6 Months
Perspective: Signature
Over Time-Last 6 Months
60
50
40
30
20
10
0
Mar
Apr
May
Jun
Jul
Aug
Top 10 Threats Detected & Prevented
Bash Code Injection
PHP Injection Attack 2
Cross-site Scripting (XSS…
BlockMe
Web Application Directory…
Web Application Directory…
SQL Injection Attack 1
HTTP Response Splitting A…
SQL Injection Attack 1 He…
PHP Injection Attack
0%
5%
10%
15%
20%

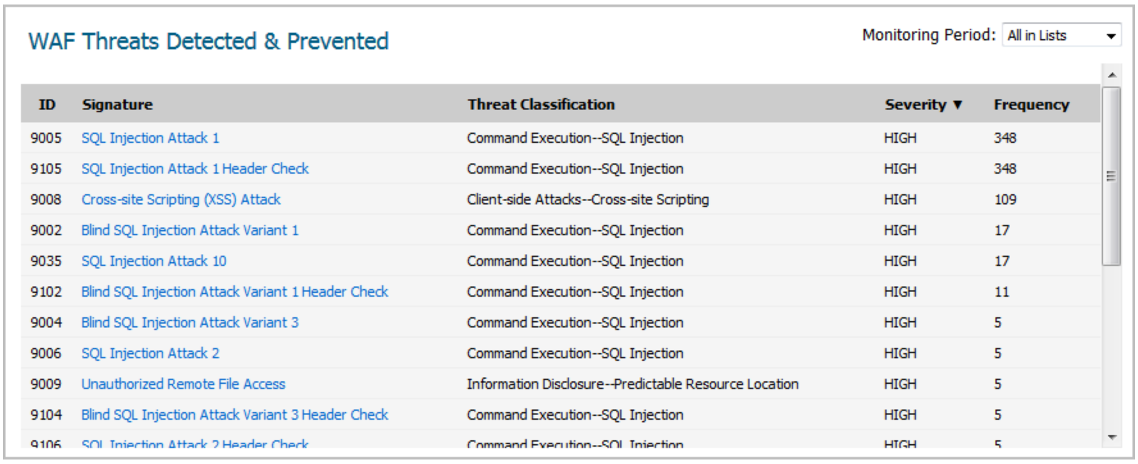
The **Perspective** drop-down list provides options to change the display of the **Top 10 Threats Detected & Prevented** graph between **Signature**, **Severity**, and **Server**. For details, see Changing Perspective on page 24.

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. The Threats in List Format image shows the list format.

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

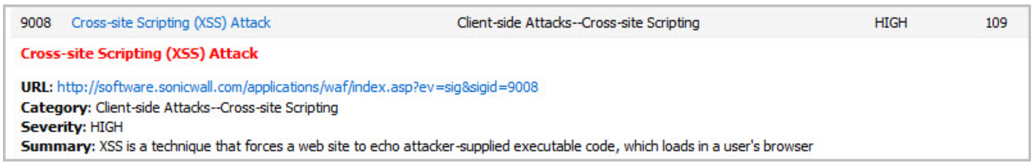
ID	Signature	Threat Classification	Severity ▼	Frequency
9005	SQL Injection Attack 1	Command Execution--SQL Injection	HIGH	348
9105	SQL Injection Attack 1 Header Check	Command Execution--SQL Injection	HIGH	348
9008	Cross-site Scripting (XSS) Attack	Client-side Attacks--Cross-site Scripting	HIGH	109
9002	Blind SQL Injection Attack Variant 1	Command Execution--SQL Injection	HIGH	17
9035	SQL Injection Attack 10	Command Execution--SQL Injection	HIGH	17
9102	Blind SQL Injection Attack Variant 1 Header Check	Command Execution--SQL Injection	HIGH	11
9004	Blind SQL Injection Attack Variant 3	Command Execution--SQL Injection	HIGH	5
9006	SQL Injection Attack 2	Command Execution--SQL Injection	HIGH	5
9009	Unauthorized Remote File Access	Information Disclosure--Predictable Resource Location	HIGH	5
9104	Blind SQL Injection Attack Variant 3 Header Check	Command Execution--SQL Injection	HIGH	5
9106	SQL Injection Attack 2 Header Check	Command Execution--SQL Injection	HIGH	5

To view and hide threat details:

1 On the **Dashboard > Monitoring page**, select **All in Lists** from the **Monitoring Period** drop-down list under **WAF Threats Detected & Prevented**. The list of threats is displayed in a 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



9008	Cross-site Scripting (XSS) Attack	Client-side Attacks--Cross-site Scripting	HIGH	109

Cross-site Scripting (XSS) Attack

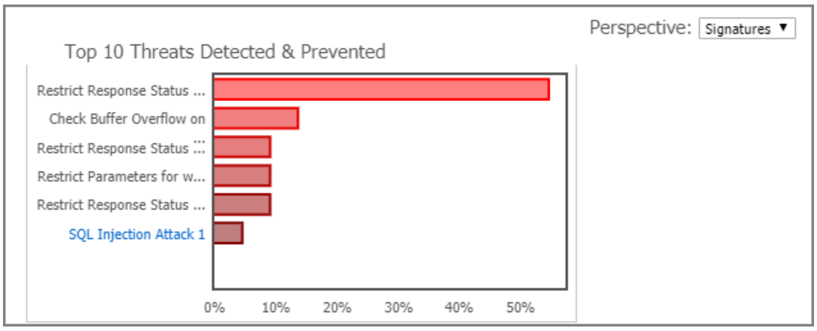
URL: http://software.sonicwall.com/applications/waf/index.asp?ev=sig&sigid=9008
Category: Client-side Attacks--Cross-site Scripting
Severity: HIGH
Summary: XSS is a technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser

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

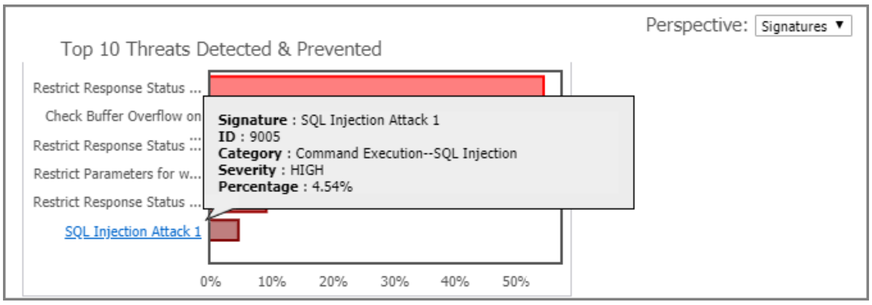
Changing Perspective

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

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

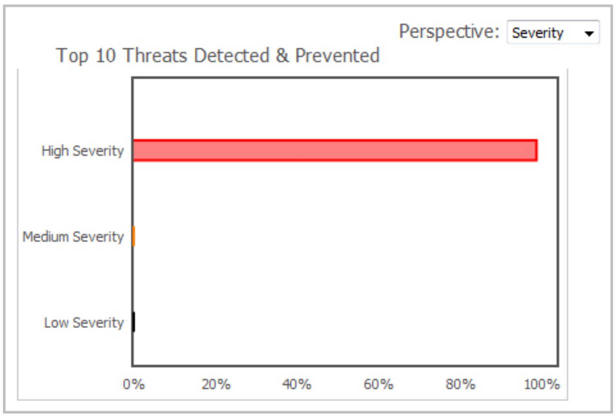

Perspective: Signatures
Top 10 Threats Detected & Prevented
Restrict Response Status ...
Check Buffer Overflow on
Restrict Response Status ...
Restrict Parameters for w...
Restrict Response Status ...
SQL Injection Attack 1
0%
10%
20%
30%
40%
50%

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

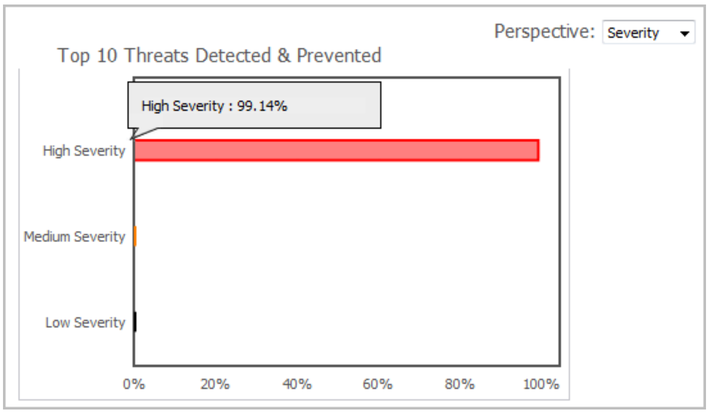

Perspective: Signatures
Top 10 Threats Detected & Prevented
Restrict Response Status ...
Check Buffer Overflow on
Restrict Response Status ...
Restrict Parameters for w...
Restrict Response Status ...
SQL Injection Attack 1
0%
10%
20%
30%
40%
50%

Signature : SQL Injection Attack 1
ID : 9005
Category : Command Execution--SQL Injection
Severity : HIGH
Percentage : 4.54%

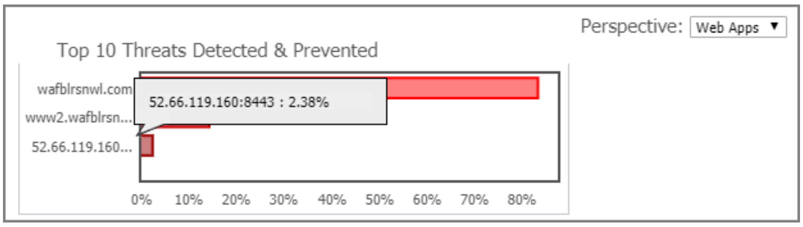
- **Severity** – High, medium, and low severity threats are displayed.



With **Perspective** set to **Severity**, hovering your mouse pointer over the severity level displays the percentage of threats detected for that level of severity during the selected monitoring period.



- **Web Apps** – The web apps can be represented with domain names or IP addresses, listed at the left side of the graph.



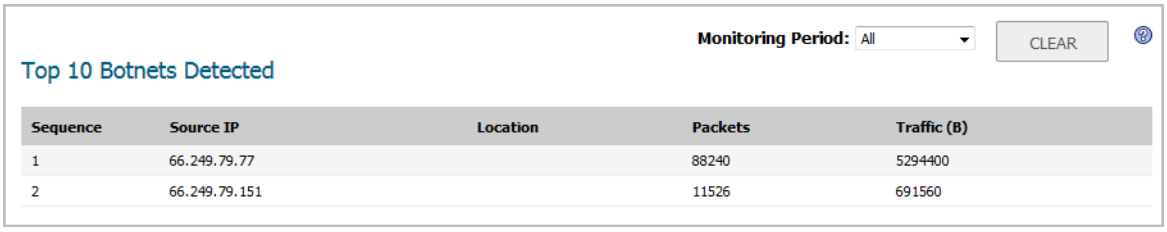
With **Perspective** set to **Web Apps**, hovering your mouse pointer over the web app names or IP address displays the percentage of threats detected for that server.

Monitoring Detected Botnets

On the **Local** screen, the **Top 10 Botnets Detected** section displays a list of the 10 most detected botnets during the selected monitoring period. The following options are available in the **Monitoring Period** drop-down list:

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

Top 10 Botnets Detected



Top 10 Botnets Detected

Sequence	Source IP	Location	Packets	Traffic (B)
1	66.249.79.77		88240	5294400
2	66.249.79.151		11526	691560

The detected botnets are displayed in order of when they were detected, as indicated in the **Sequence** column. The **Source IP** column displays the IP address of the botnet computer. If the geographic location is known, it is displayed in the **Location** column. The **Packets** column displays the number of packets detected, and the **Traffic (B)** column displays the number of bytes from each botnet.

Monitoring on the Global Screen

The **Global** screen on the **Dashboard > Monitoring** page displays statistics and graphs for globally detected and prevented threats reported by all registered and enabled instances of SonicWall Web Application Firewall.

> **NOTE:** This view only displays threat event statistics sent from registered appliances. No sensitive information including customer name, email address, serial number, MSW account is ever shared with other registered appliances.

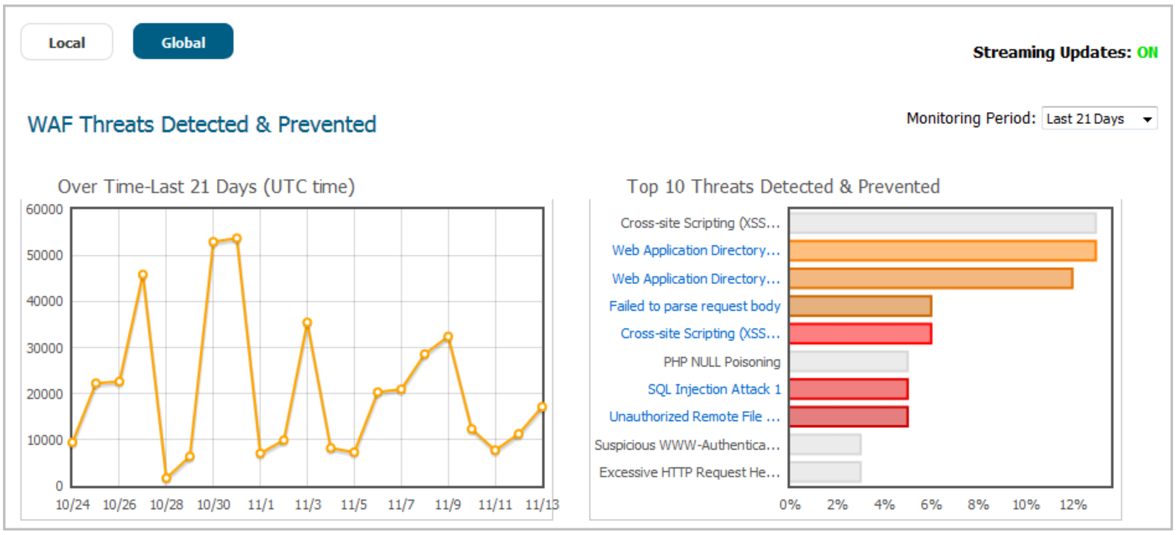
Two graphs are presented under **WAF Threats Detected & Prevented**, one showing the number of threats over time, and the other showing the top ten threats that were detected and prevented during that time frame.

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

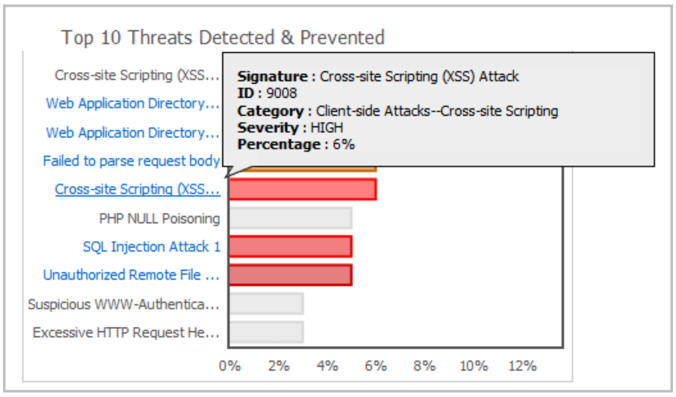
The Threats Over Last 21 Days image shows the number and severities of threats detected and prevented over the last 21 days.

Threats Over Last 21 Days


Local
Global
Streaming Updates: ON
WAF Threats Detected & Prevented
Monitoring Period: Last 21 Days
Over Time-Last 21 Days (UTC time)
60000
50000
40000
30000
20000
10000
0
10/24
10/26
10/28
10/30
11/1
11/3
11/5
11/7
11/9
11/11
11/13
Top 10 Threats Detected & Prevented
Cross-site Scripting (XSS…
Web Application Directory…
Web Application Directory…
Failed to parse request body
Cross-site Scripting (XSS…
PHP NULL Poisoning
SQL Injection Attack 1
Unauthorized Remote File …
Suspicious WWW-Authentica…
Excessive HTTP Request He…
0%
2%
4%
6%
8%
10%
12%

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

Threat Details Tooltip


Top 10 Threats Detected & Prevented
Cross-site Scripting (XSS…
Web Application Directory…
Web Application Directory…
Failed to parse request body
Cross-site Scripting (XSS…
PHP NULL Poisoning
SQL Injection Attack 1
Unauthorized Remote File …
Suspicious WWW-Authentica…
Excessive HTTP Request He…
0%
2%
4%
6%
8%
10%
12%

Signature : Cross-site Scripting (XSS) Attack
ID : 9008
Category : Client-side Attacks--Cross-site Scripting
Severity : HIGH
Percentage : 6%

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 Security > Status** page”.

Viewing WAF Usage on Dashboard > System

The **Dashboard > System** page provides information about Web Application Firewall system usage and utilization over various time periods. Four system monitoring graphs are displayed, as described in the System Monitoring Graph Types table.

System Monitoring Graph Types

Graph	Description
Active Concurrent Users	The number of users who are logged into the WAF virtual appliance at the same time, measured over time by seconds, minutes, hours, or days. This figure is expressed as an integer, for example, 2, 3, or 5.
Bandwidth Usage (Kbps)	Indicates the amount of data per second being transmitted and received by the WAF virtual appliance in Kbps measured over time by seconds, minutes, hours, or days.
CPU Utilization (%)	The amount of capacity usage on the WAF virtual appliance processor being used, measured over time by seconds, minutes, hours, or days. This figure is expressed as a percentage of the total capacity on the CPU.
Memory Utilization (%)	The amount of memory available used by the WAF virtual appliance, measured over time by seconds, minutes, hours, or days. This monitoring graph displays memory utilization as a percentage of the total memory available.

At the top of the page, you can set the **Monitoring Period** to any of:

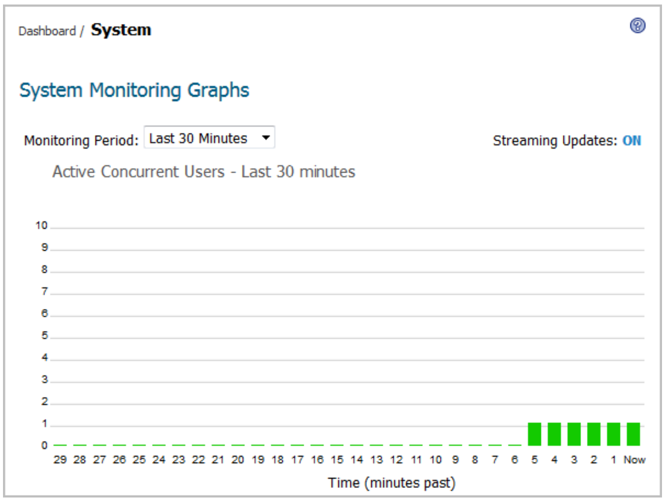
- Last 30 seconds
- Last 30 minutes
- Last 24 hours
- Last 30 days

Control buttons are provided on this page to control the statistics that are displayed. You can use the control buttons to turn streaming updates on or off, refresh the data on the screen, and clear the graphs. The **Streaming Updates** control is displayed at the top of the screen, and the **REFRESH** and **CLEAR GRAPHS** buttons are displayed along the bottom.

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.

Example images for a 30 minute monitoring period are shown below.

Active Concurrent Users Graph


Dashboard / System

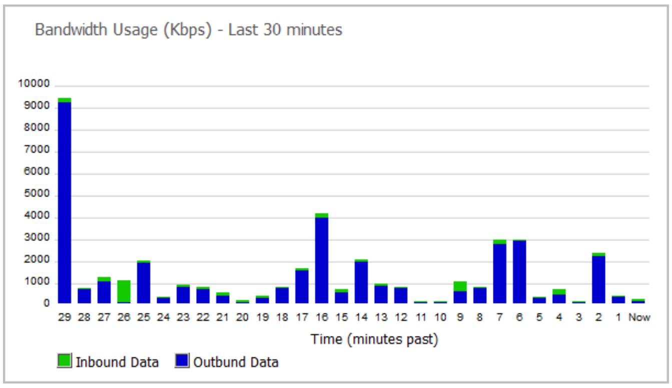
System Monitoring Graphs

Monitoring Period: Last 30 Minutes

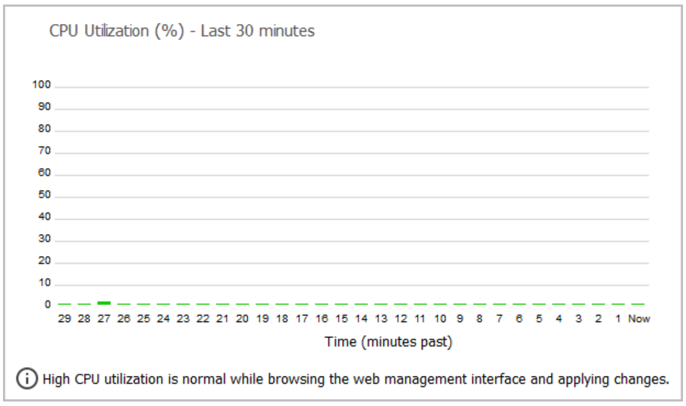
Streaming Updates: ON

Active Concurrent Users - Last 30 minutes
10
9
8
7
6
5
4
3
2
1
0
29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 Now
Time (minutes past)

Bandwidth Usage Graph

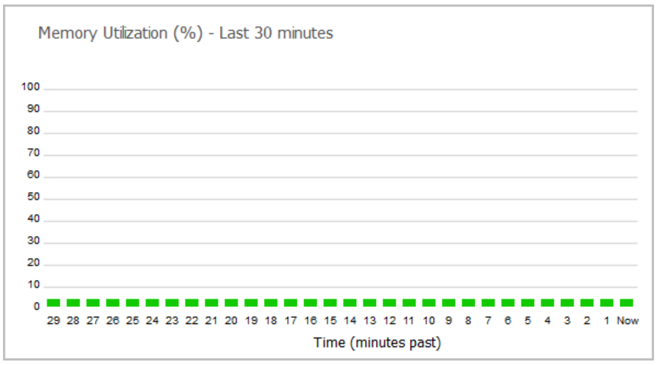


CPU Utilization Graph



ⓘ High CPU utilization is normal while browsing the web management interface and applying changes.

Memory Utilization Graph



System Configuration

This section provides information and configuration tasks specific to the **System** pages in the SonicWall Web Application Firewall management interface, including registering your Web Application Firewall virtual appliance, setting the date and time, configuring system settings, system administration and system certificates.

Topics:

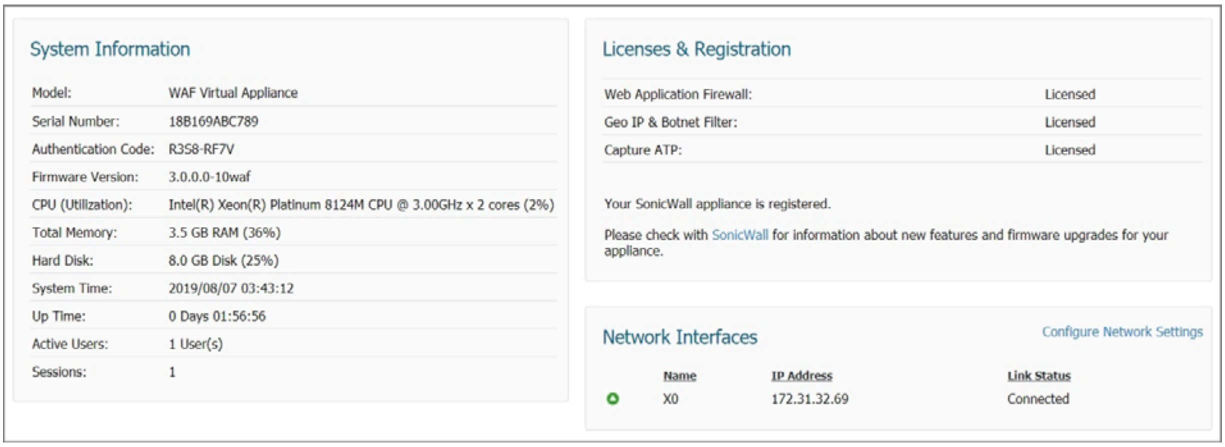
Using the System Status Page

This section provides an overview of the **System > Status** page and a description of the configuration tasks available on this page.

System Status Overview

The **System > Status** page provides the administrator with current system status for the Web Application Firewall virtual appliance, including information and links to help manage the service licenses. This section provides information about the page display and instructions to complete the configuration tasks on the **System > Status** page.

System > Status Page



System Information

Model:	WAF Virtual Appliance
Serial Number:	18B169ABC789
Authentication Code:	R3S8-RF7V
Firmware Version:	3.0.0.0-10waf
CPU (Utilization):	Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz x 2 cores (2%)
Total Memory:	3.5 GB RAM (36%)
Hard Disk:	8.0 GB Disk (25%)
System Time:	2019/08/07 03:43:12
Up Time:	0 Days 01:56:56
Active Users:	1 User(s)
Sessions:	1

Licenses & Registration

Web Application Firewall:	Licensed
Geo IP & Botnet Filter:	Licensed
Capture ATP:	Licensed

Your SonicWall appliance is registered.

Please check with SonicWall for information about new features and firmware upgrades for your appliance.

Network Interfaces

Configure Network Settings

	Name	IP Address	Link Status
●	X0	172.31.32.69	Connected

Overviews of each area of the **System > Status** page are provided in the following sections:

- System Information on page 31
- Licenses & Registration on page 32
- Network Interfaces on page 32

System Information

The **System Information** section displays details about your specific Web Application Firewall virtual appliance. The following information is displayed in this section:

System Information

Field	Description
Model	Set to the model of the WAF Virtual Appliance.
Serial Number	The serial number of the WAF virtual appliance.
Authentication Code	The alphanumeric code used to authenticate the WAF virtual appliance on the registration database at <https://www.mysonicwall.com>.
Firmware Version	The firmware version loaded on the WAF virtual appliance.
CPU (Utilization)	The type of the WAF virtual appliance processor and the average CPU usage over the last 5 minutes.
Total Memory	The amount of RAM on the virtual appliance.
Hard Disk	The size in gigabytes of the hard disk space used by the virtual appliance.
System Time	The current date and time.
Up Time	The number of days, hours, minutes, and seconds, that the WAF virtual appliance has been active since its most recent restart.
Active Users	Total number of authenticated user sessions protected by SonicWall WAF.
Sessions	Total number of user sessions protected by SonicWall WAF for which WAF does not provide user authentication.

Licenses & Registration

The **Licenses & Registration** section indicates the security service license status and the registration status of your WAF virtual appliance. The status of your Geo IP & Botnet Filter license is displayed here.

To register your appliance on MySonicWall and manually enter the registration code in the available field at the bottom of this section, see Manually Registering the WAF Virtual Appliance on page 33.

To register your SonicWall WAF virtual appliance on MySonicWall from the **System > Licenses** page and allow the appliance to automatically synchronize registration and license status with the SonicWall license manager, see Registering WAF from System > Licenses on page 37.

Network Interfaces

The **Network Interfaces** section provides information about all the interface settings on the WAF virtual appliance. The configured IP addresses and current link status are displayed. This section also provides a link to the **Network > IP Configuration** page by clicking **Configure Network Settings**.

Registering Your WAF Virtual Appliance

There are three ways to register your Web Application Firewall virtual appliance:

- Manual Registration – Log in to your MySonicWall account directly from a browser or click the **SonicWall** link on the **System > Status** page to access MySonicWall, enter the appliance serial number and other information there, and then enter the resulting registration code into the field on the **System > Status** page. This manual registration procedure is described in this section.
- Capture Security Center Manual Registration – Log into Capture Security Center (CSC) with your MSW account, enter the two-step verification code sent to your email, and click Verify. Then, Click the WAF tile to navigate to the WAF Dashboard and enter your credentials. Follow the prompts to complete your registration creating your token, entering your serial number, and enabling cloud management. This procedure is described in Configuring Cloud Management on page 50.
- Register from WAF System > Licenses – Use the link on the **System > Licenses** page to access MySonicWall, then enter the serial number and other information into MySonicWall. When finished, your view of the **System > Licenses** page shows that the appliance has been automatically synchronized with the licenses activated on MySonicWall. This procedure is described in Registering WAF from System > Licenses on page 37.

Topics:

Before You Register

Verify that the time, DNS, and default gateway settings on your Web Application Firewall virtual appliance are correct before you register your appliance. These settings are generally configured during the initial Web Application Firewall virtual appliance setup process. To verify or configure the time settings, navigate to the **System > Time** page. To verify or configure the DNS setting or default gateway, navigate to the **Network > IP Configuration** page. For more information about these configuration settings, refer to Setting the Time on page 43, Configuring DNS on page 72, and IP Configuration Settings on page 71

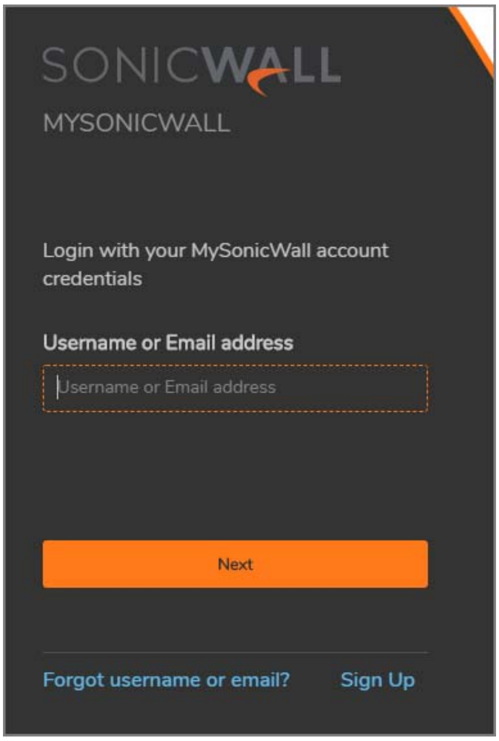
ⓘ **NOTE:** You need a MySonicWall account to register the WAF virtual appliance.

Manually Registering the WAF Virtual Appliance

To manually register your WAF virtual appliance on MySonicWall:

1. If you are not logged into the Web Application Firewall management interface, log in with the administrator username and password you set during initial setup of your Web Application Firewall virtual appliance. The default password for an AWS EC2 instance is the Instance ID. On other deployment types, the administrator credentials default to (*admin* / *password*). For information about configuring the administrator account, refer to the *Deployment Guide* for your WAF platform.
2. Navigate to the **System > Status** page.
3. Record your **Serial Number** and **Authentication Code** from the **System Information** section.
4. Do one of the following to access MySonicWall:
   - Click the **SonicWall** link in the **Licenses & Registration** section.
   - Type http://www.mysonicwall.com into your web browser.

   The MySonicWall **LOGIN** page is displayed.



SONICWALL

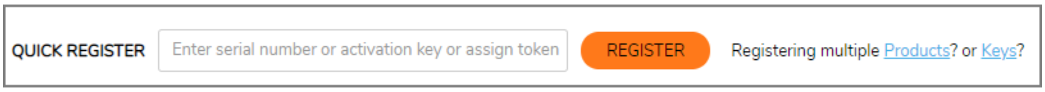
MYSONICWALL

Login with your MySonicWall account credentials

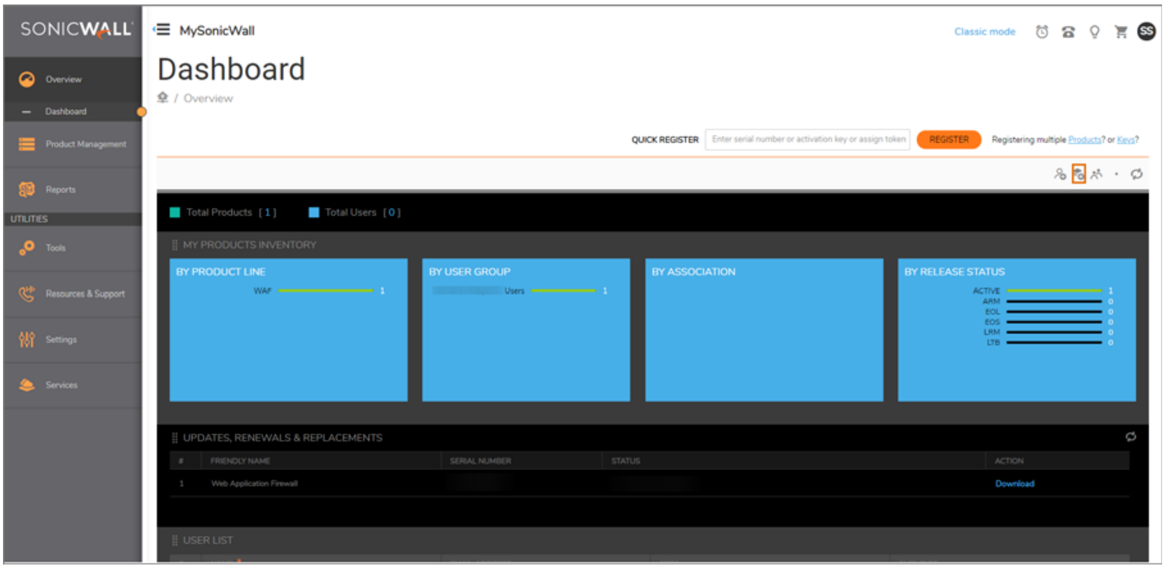
Username or Email address

Username or Email address

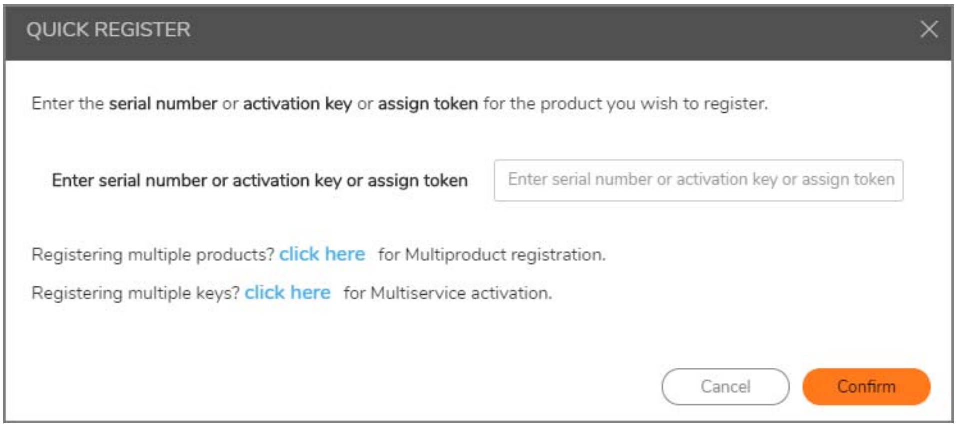
5. Enter your MySonicWall account username or email address and password.
6. You can register your product two ways:
   - Enter your **serial number, or activation key, or assigned token** in the **QUICK REGISTER** text field provided at the top of the **MY PRODUCTS INVENTORY** table on the **Overview > Dashboard** page.
   - Click **REGISTER**.


QUICK REGISTER
Enter serial number or activation key or assign token
REGISTER
Registering multiple Products? or Keys?

- Click the **ADD PRODUCT** icon at the top right of the **MY PRODUCTS INVENTORY** table on the **Overview > Dashboard** page.



- Enter your **serial number, or activation key, or assigned token** in the popup dialog that displays and click **Confirm**.



QUICK REGISTER

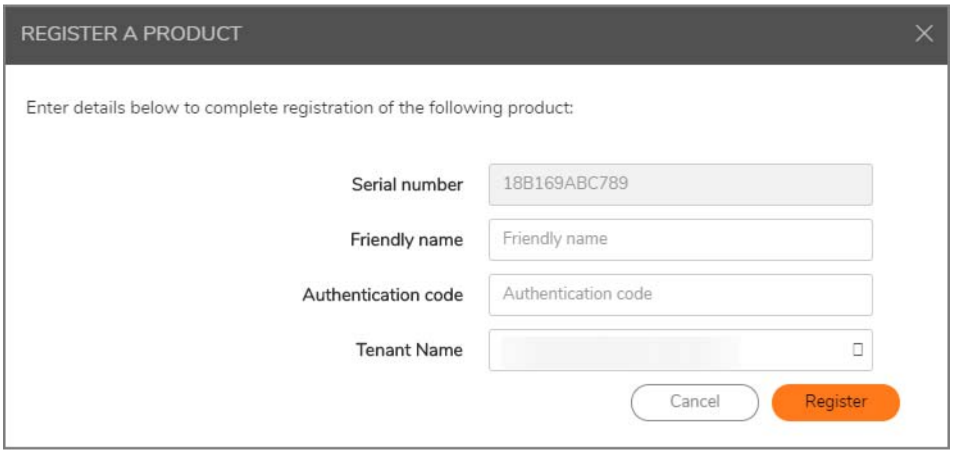
Enter the **serial number** or **activation key** or **assign token** for the product you wish to register.

Enter serial number or activation key or assign token Enter serial number or activation key or assign token

Registering multiple products? click here for Multiproduct registration.

Registering multiple keys? click here for Multiservice activation.

- In the **REGISTER A PRODUCT** popup dialog, enter a descriptive name for your WAF virtual appliance in the **Friendly Name** field.
- Enter your **Authentication Code**.
- Enter the **Tenant Name**.
- Click **REGISTER**.



REGISTER A PRODUCT

Enter details below to complete registration of the following product:

Serial number	18B169ABC789
Friendly name	Friendly name
Authentication code	Authentication code
Tenant Name	

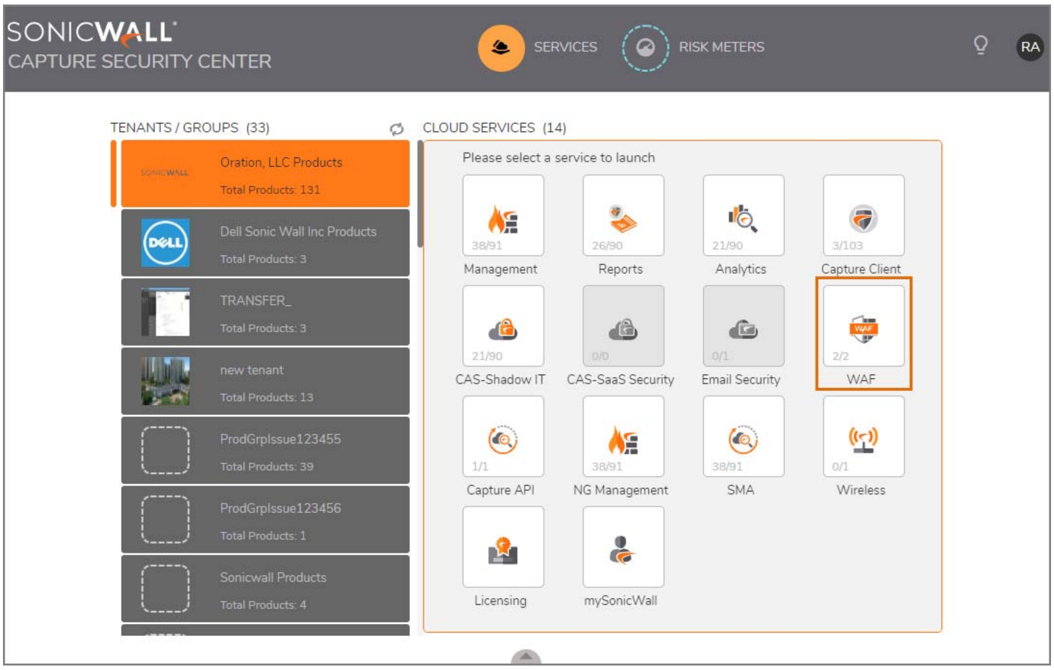
- When the MySonicWall server has finished processing your registration, the Registration Code is displayed along with a statement that your appliance is registered. Click **CONTINUE**.
- On the **System > Status** page of the Web Application Firewall management interface, enter the Registration Code into the field at the bottom of the **Licenses & Registration** section, and then click **Update**.

To manually register your WAF virtual appliance on Capture Security Center:

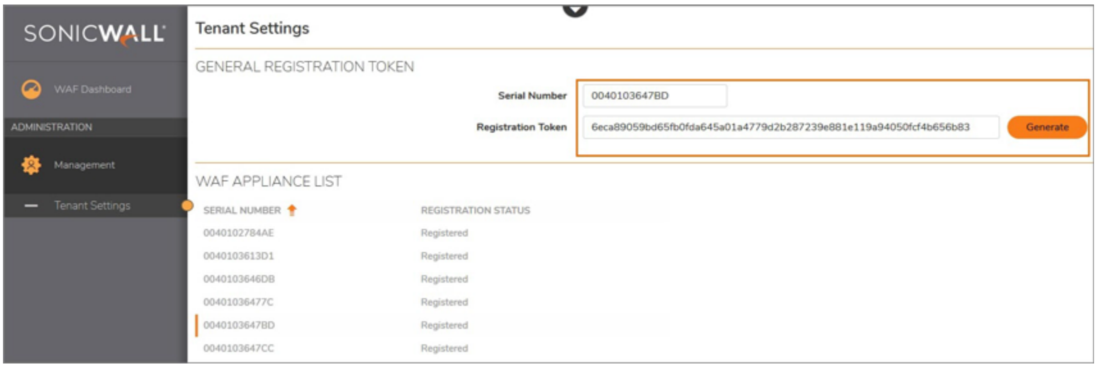
1 Log into **Capture Security Center** with your MSW account.

2 Enter the two-step verification code sent to your email and click **Verify**.

3 Click the **WAF** tile to navigate to the WAF Dashboard and enter your credentials.



4 Create a token for your WAFv registration. Navigate to **WAF Dashboard > Management > Tenant Settings.**



Tenant Settings

GENERAL REGISTRATION TOKEN

Serial Number: 0040103647BD

Registration Token: 6eca89059bd65fb0fda645a01a4779d2b287239e881e119a94050fcf4b656b83

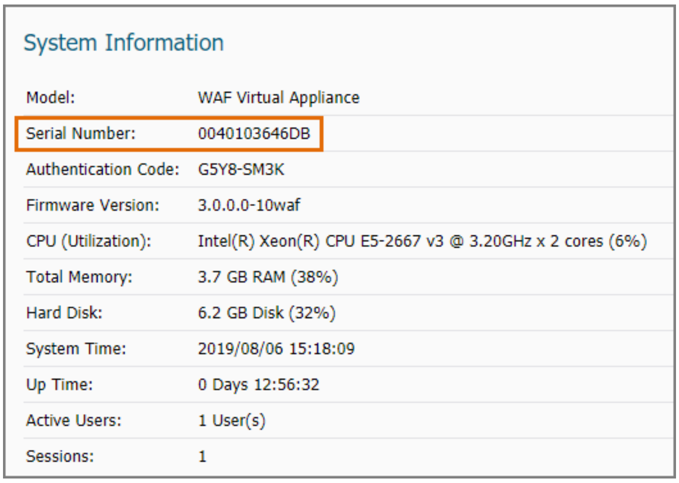
WAF APPLIANCE LIST

SERIAL NUMBER	REGISTRATION STATUS
0040102784AE	Registered
0040103613D1	Registered
0040103646DB	Registered
00401036477C	Registered
0040103647BD	Registered
0040103647CC	Registered

5 In the **GENERAL REGISTRATION TOKEN** section, enter the **Serial Number** of WAFv and the **Registration Token** in the text field provided.

6 Click **Generate**.

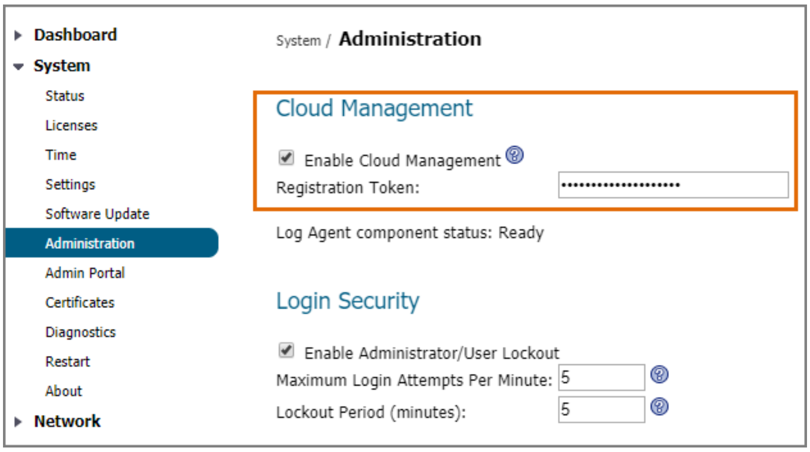
The Serial Number can be found on the **System > Status** page of WAFv. You can also see the **Serial Number** under the **WAF APPLIANCE LIST** section.



System Information

Model:	WAF Virtual Appliance
Serial Number:	0040103646DB
Authentication Code:	G5Y8-SM3K
Firmware Version:	3.0.0.0-10waf
CPU (Utilization):	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz x 2 cores (6%)
Total Memory:	3.7 GB RAM (38%)
Hard Disk:	6.2 GB Disk (32%)
System Time:	2019/08/06 15:18:09
Up Time:	0 Days 12:56:32
Active Users:	1 User(s)
Sessions:	1

7 Copy the generated token to WAFv and check Enable Cloud Management.



System / **Administration**

Cloud Management

☑ Enable Cloud Management

Registration Token: ••••••••••••••••••••

Log Agent component status: Ready

Login Security

☑ Enable Administrator/User Lockout

Maximum Login Attempts Per Minute: 5

Lockout Period (minutes): 5

8 Click **ACCEPT** to save the settings.

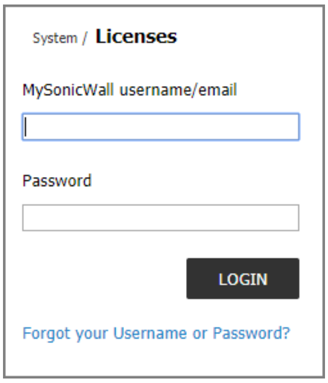
ⓘ **NOTE:** For Cloud WAF Dashboard, the client needs to log in to CSC first to get a WAF console token.

Registering WAF from System > Licenses

On a new Web Application Firewall virtual appliance, you can register your appliance from the **System > Licenses** page.

To register WAF from the System > Licenses page:

1. Log into the Web Application Firewall management interface and navigate to the **System > Licenses** page.
2. Under **Manage Security Services Online**, click the **Activate, Upgrade, or Renew services** link.
3. Enter your **MySonicWall username/email** and **password** into the fields and then click **LOGIN**.



4. The **License Management** page is displayed, with the **Manage Services Online** table.
5. Click **Activate, Upgrade, or Renew** on your existing license.
6. Enter your license key in the spaces provided.
7. Click **LOGIN**.
8. The display changes to inform you that your Web Application Firewall virtual appliance is registered.
9. Click **CONTINUE**.
10. The **License Management** page displays your latest license information.

Configuring System Licenses

This section provides an overview of the **System > Licenses** page and a description of the configuration tasks available on this page. See the following sections:

- System Licenses Overview on page 38
- Security Service and Support Service Summary on page 38
- Licensing Requirements on page 39
- Manage Security Services Online on page 42

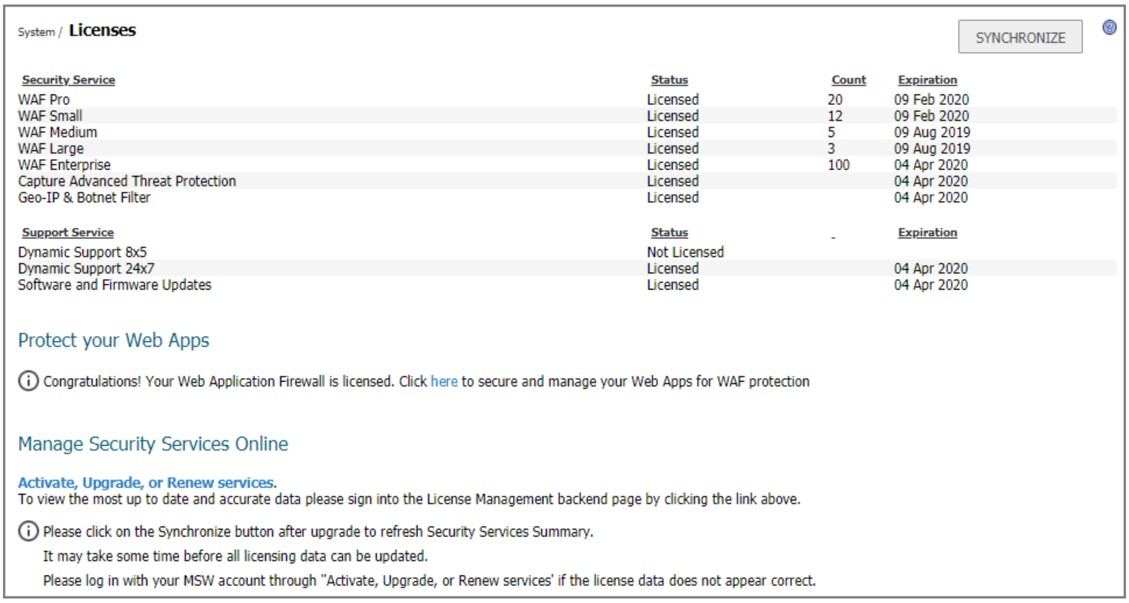
System Licenses Overview

The SonicWall License Manager provides service licensing and related functionality. The License Manager communicates periodically (hourly) with the SonicWall WAF virtual appliance to verify the validity of licenses.

NOTE: Initial registration of the WAF virtual appliance is required for synchronization with the License Manager to work.

The **System > Licenses** page provides a link to activate, upgrade, or renew SonicWall Security Services licenses, including the Geo IP & Botnet Filter license.

System > Licenses Page



System / **Licenses**

Security Service	Status	Count	Expiration
WAF Pro	Licensed	20	09 Feb 2020
WAF Small	Licensed	12	09 Feb 2020
WAF Medium	Licensed	5	09 Aug 2019
WAF Large	Licensed	3	09 Aug 2019
WAF Enterprise	Licensed	100	04 Apr 2020
Capture Advanced Threat Protection	Licensed		04 Apr 2020
Geo-IP & Botnet Filter	Licensed		04 Apr 2020

Support Service	Status	-	Expiration
Dynamic Support 8x5	Not Licensed		
Dynamic Support 24x7	Licensed		04 Apr 2020
Software and Firmware Updates	Licensed		04 Apr 2020

Protect your Web Apps

Congratulations! Your Web Application Firewall is licensed. Click here to secure and manage your Web Apps for WAF protection

Manage Security Services Online

Activate, Upgrade, or Renew services.

To view the most up to date and accurate data please sign into the License Management backend page by clicking the link above.

Please click on the Synchronize button after upgrade to refresh Security Services Summary.

It may take some time before all licensing data can be updated.

Please log in with your MSW account through "Activate, Upgrade, or Renew services' if the license data does not appear correct.

Security Service and Support Service Summary

The **Security Service and Support Service** tables list the WAF license status, the Capture ATP license status, and the Geo-IP & Botnet Filter service license status on the WAF virtual appliance.

The **Security Service** column lists the service names. The **Status** column indicates if the security service is activated (**Licensed**), available for activation (**Not Licensed**), available for free trial, or no longer active (**Expired**).

The **Count** column displays the quantity of available licenses for the Web Application Firewall. See Licensing Requirements on page 39 for more information.

The **Expiration** column displays the expiration date for any licensed service that is time-based.

The information listed in the **Security Service summary** table is updated from the SonicWall licensing server every time the WAF virtual appliance automatically synchronizes with it (hourly), or you can click **SYNCHRONIZE** to synchronize immediately.

NOTE: If the licenses do not update after a synchronize, you might need to restart your WAF virtual appliance. DNS must be configured properly and the appliance should be able to reach the sonicwall.com domain.

Protect Your Web Apps

The **Protect your Web Apps** section displays your WAF license status and provides a link to secure and manage you Web Apps for WAF protection.

Manage Security Services Online

To view the most up to date and accurate data sign into the License Management backend page by clicking the **Activate, Upgrade, or Renew services** link.

> ⓘ **NOTE:** It may take some time before all licensing data can be updated. Log in with your MSW account through **Activate, Upgrade, or Renew services** if the license data does not appear correct.

Licensing Requirements

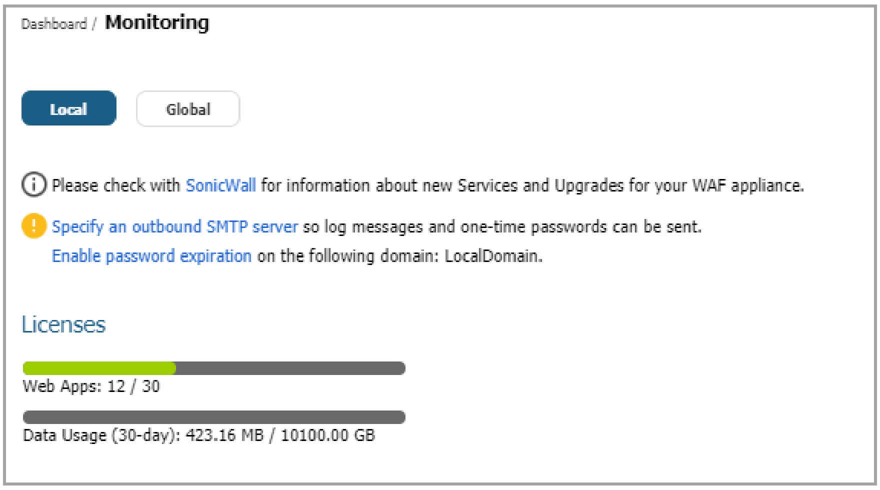
SonicWall WAF uses Web App based licensing for flexibility with sizing and deployment.

Web App based licensing uses a per-website licensing model. This licensing model provides granularity so that you only need to purchase what you need depending on the websites you want to protect.

Under the Web App based licensing model, the WAF appliance synchronizes with the SonicWall backend on an hourly basis and downloads the number of licensed Web Apps of each size. WAF restricts the overall number of Web Apps created on the appliance to the total number of licensed Web Apps across all sizes. Each Web App size is mapped to a capacity limit on the appliance. See the WAF Licensing Structure table, which shows how a website type maps to a capacity limit.

WAF additionally monitors and ensures that the total data transacted does not exceed the total of capacity limits for all licensed Web Apps. WAF does not restrict the data individually for each Web App. Therefore, Web Apps can share this capacity limit.

WAF logs how much data has been transacted every day, displaying the daily traffic on the **Dashboard > Monitoring** page for transparency.



ⓘ Please check with SonicWall for information about new Services and Upgrades for your WAF appliance.

! Specify an outbound SMTP server so log messages and one-time passwords can be sent.
Enable password expiration on the following domain: LocalDomain.

Licenses

Web Apps: 12 / 30

Data Usage (30-day): 423.16 MB / 10100.00 GB

When the rolling 30-day data used exceeds the 30-day limit, the administrator is warned, multiple times if necessary. If data usage exceeds the 30-day limit for 5 consecutive days, Web Security Services are disabled. Web Security is restored as soon as the 30-day rolling data usage is back within limits. Logs and alerts are available to document licensing violations and WAF service deactivation and activation.

ⓘ **NOTE:** Application delivery features continue to function even under license violation to reduce disruption.

The Web App based WAF licensing structure replaces the former model-based WAF tiers and compute capacity based enforcement in WAF 3.0. The new structure is based on the capacity needed by the protected Web Apps or websites. Five capacity based website types are defined: **PRO**, **SMALL**, **MEDIUM**, **LARGE**, **ENTERPRISE**, and **ENTERPRISE Bundle (100 Web Apps)**, as shown in the WAF Licensing Structure table.

WAF Licensing Structure

Website Type	Capacity
PRO	10 GB per month
SMALL	50 GB per month
MEDIUM	200 GB per month
LARGE	500 GB per month
ENTERPRISE	Unlimited GB per month
ENTERPRISE Bundle (100 Web Apps)	Unlimited

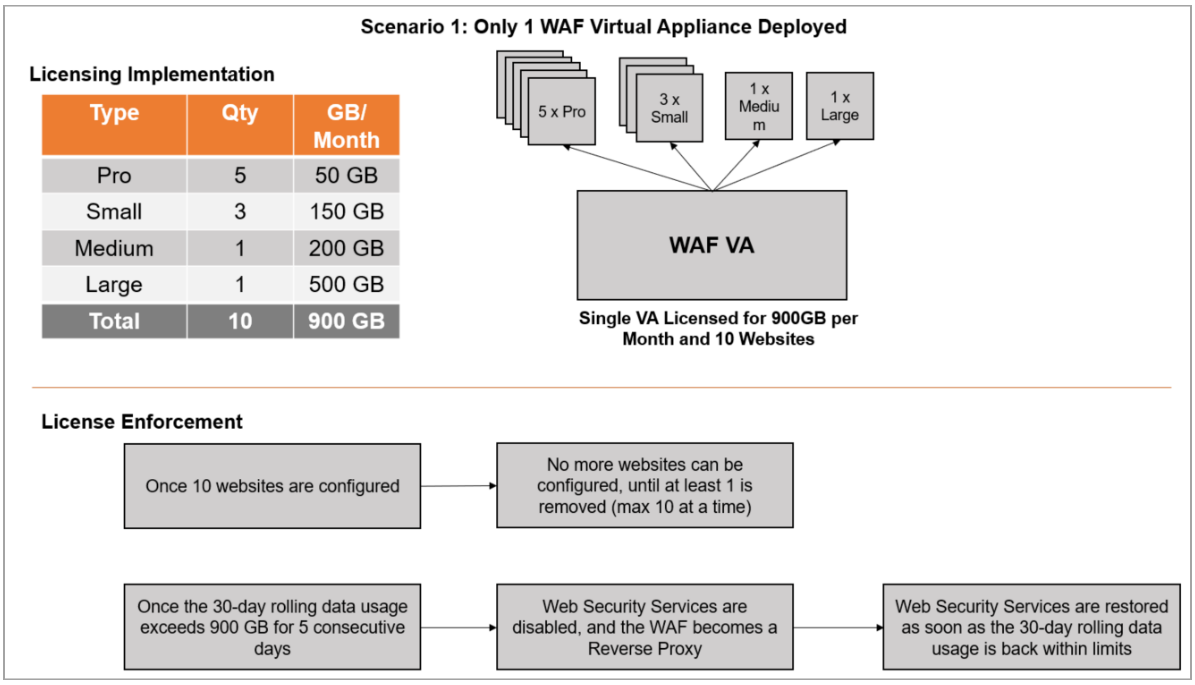
Note the following for deployment of **multiple** WAF virtual appliances:

- If you wish to deploy more than one WAF virtual appliance, you need to determine how to split your total licensed capacity across the appliances.
- Capacity configured on a WAF virtual appliance is considered unique. To configure load balancing or high availability with multiple WAF appliances, you need to purchase multiples of the desired capacity.
- ENTERPRISE web app types are only supported from WAF 2.2.0.3.
- Co-existence of ENTERPRISE web app types with any other web app types (PRO, SMALL, MEDIUM or LARGE) is not supported on the same WAF appliance. If such mixed licensing is desired, ENTERPRISE licenses must be applied to a separate WAF appliance.

The following figures illustrate different licensing scenarios:

- Example with a Single WAF Virtual Appliance
- Example with Multiple WAF Virtual Appliances Using Load Distribution
- Example with Multiple WAF Virtual Appliances Using High Availability

Example with a Single WAF Virtual Appliance



Scenario 1: Only 1 WAF Virtual Appliance Deployed

Licensing Implementation

Type	Qty	GB/ Month
Pro	5	50 GB
Small	3	150 GB
Medium	1	200 GB
Large	1	500 GB
Total	10	900 GB

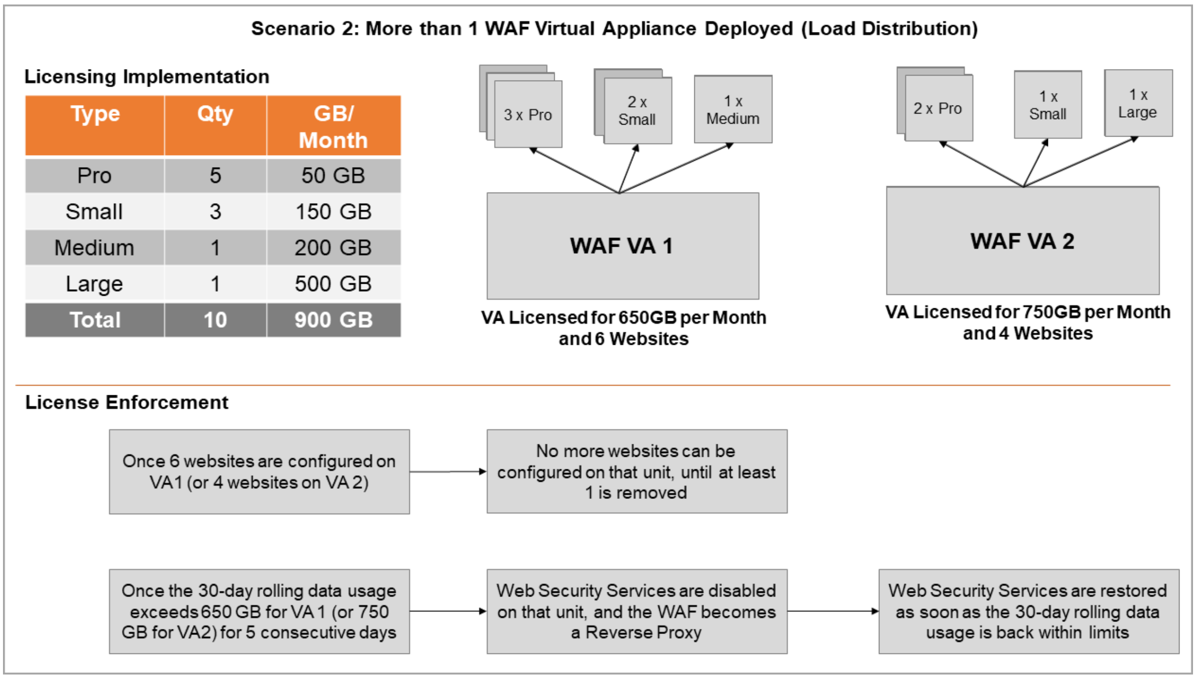
Single VA Licensed for 900GB per Month and 10 Websites

License Enforcement

Once 10 websites are configured → No more websites can be configured, until at least 1 is removed (max 10 at a time)

Once the 30-day rolling data usage exceeds 900 GB for 5 consecutive days → Web Security Services are disabled, and the WAF becomes a Reverse Proxy → Web Security Services are restored as soon as the 30-day rolling data usage is back within limits

Example with Multiple WAF Virtual Appliances Using Load Distribution



Scenario 2: More than 1 WAF Virtual Appliance Deployed (Load Distribution)

Licensing Implementation

Type	Qty	GB/ Month
Pro	5	50 GB
Small	3	150 GB
Medium	1	200 GB
Large	1	500 GB
Total	10	900 GB

VA Licensed for 650GB per Month and 6 Websites

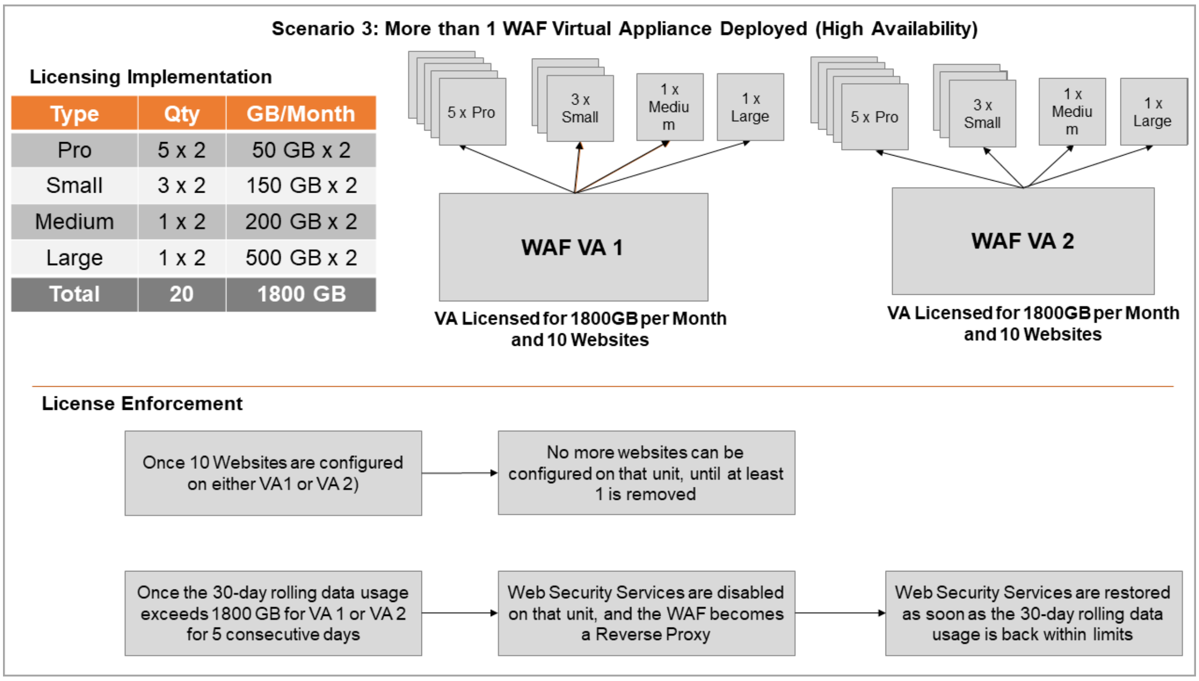
VA Licensed for 750GB per Month and 4 Websites

License Enforcement

Once 6 websites are configured on VA1 (or 4 websites on VA 2) → No more websites can be configured on that unit, until at least 1 is removed

Once the 30-day rolling data usage exceeds 650 GB for VA 1 (or 750 GB for VA2) for 5 consecutive days → Web Security Services are disabled on that unit, and the WAF becomes a Reverse Proxy → Web Security Services are restored as soon as the 30-day rolling data usage is back within limits

Example with Multiple WAF Virtual Appliances Using High Availability



Scenario 3: More than 1 WAF Virtual Appliance Deployed (High Availability)

Licensing Implementation

Type	Qty	GB/Month
Pro	5 x 2	50 GB x 2
Small	3 x 2	150 GB x 2
Medium	1 x 2	200 GB x 2
Large	1 x 2	500 GB x 2
Total	20	1800 GB

VA Licensed for 1800GB per Month and 10 Websites

VA Licensed for 1800GB per Month and 10 Websites

License Enforcement

Once 10 Websites are configured on either VA1 or VA 2) → No more websites can be configured on that unit, until at least 1 is removed

Once the 30-day rolling data usage exceeds 1800 GB for VA 1 or VA 2 for 5 consecutive days → Web Security Services are disabled on that unit, and the WAF becomes a Reverse Proxy → Web Security Services are restored as soon as the 30-day rolling data usage is back within limits

Manage Security Services Online

You can log in to MySonicWall directly from the **System > Licenses** page by clicking the link **Activate, Upgrade, or Renew services**. You can click this link to register your appliance, activate a free 30-day trial, or to purchase additional 1 or 3 year licenses for upgrading or renewing services.

Configuring System Time Settings

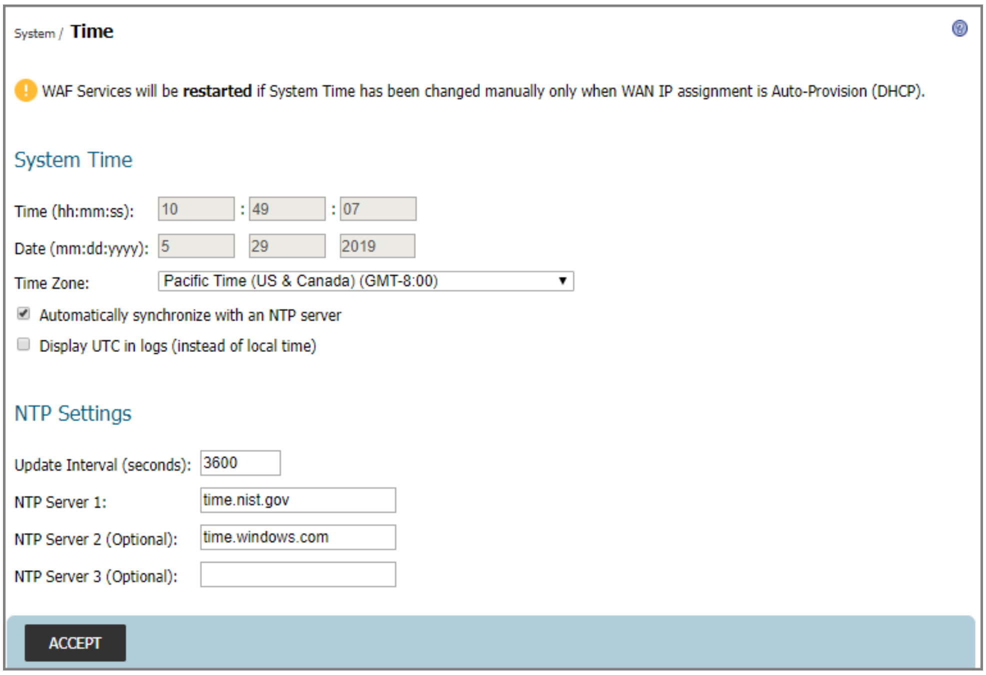
This section provides an overview of the **System > Time** page and a description of the configuration tasks available on this page.

- System Time Overview on page 42
- Setting the Time on page 43
- Enabling Network Time Protocol on page 44

System Time Overview

The **System > Time** page provides the administrator with controls to set the WAF virtual appliance system time, date and time zone, to synchronize with one or more NTP servers, and to set the logs to use Coordinated Universal Time (UTC) if desired.

System > Time Page



System / **Time**

WAF Services will be **restarted** if System Time has been changed manually only when WAN IP assignment is Auto-Provision (DHCP).

System Time

Time (hh:mm:ss): 10 : 49 : 07

Date (mm:dd:yyyy): 5 29 2019

Time Zone: Pacific Time (US & Canada) (GMT-8:00)

☑ Automatically synchronize with an NTP server

□ Display UTC in logs (instead of local time)

NTP Settings

Update Interval (seconds): 3600

NTP Server 1: time.nist.gov

NTP Server 2 (Optional): time.windows.com

NTP Server 3 (Optional):

Setting the Time

The WAF virtual appliance uses the time and date settings to timestamp log events and for other internal purposes.

> **NOTE:** For optimal performance, the WAF virtual appliance must have the correct time and date configured.

To configure the time and date settings:

1 Log into the Web Application Firewall management interface and navigate to the **System > Time** page.

2 Select your time zone in the **Time Zone** drop-down list.

The current time, in 24-hour time format, appears in the **Time (hh:mm:ss)** field and the current date appears in the **Date (mm:dd:yyyy)** field.

3 Alternately, you can manually enter the current time in the **Time (hh:mm:ss)** field and the current date in the **Date (mm:dd:yyyy)** field.

> **NOTE:** If the check box next to **Automatically synchronize with an NTP server** is selected, you cannot manually enter the time and date. To manually enter the time and date, clear the check box.

4 To use Coordinated Universal Time in log entries, select the **Display UTC in logs (instead of local time)** checkbox.

5 Click **ACCEPT** to update the configuration.

Enabling Network Time Protocol

If you enable Network Time Protocol (NTP), then the NTP time settings override the manually configured time settings. The NTP time settings are determined by the NTP server and the time zone that is selected in the **Time Zone** drop-down list.

To set the time and date for the appliance using the Network Time Protocol (NTP):

1. Navigate to the **System > Time** page.
2. Select **Automatically synchronize with an NTP server**.
3. In the NTP Settings section, enter the time interval in seconds to synchronize time settings with the NTP server in the **Update Interval** field. The default update interval is 3600 seconds.
4. Enter the NTP server IP address or fully qualified domain name (FQDN) in the **NTP Server 1** field. The default is **time.nist.gov**.
5. For redundancy, enter a backup NTP server address in the **NTP Server Address 2 (Optional)** and **NTP Server Address 3 (Optional)** fields. The default second server is **time.windows.com**.
6. Click **ACCEPT** to update the configuration.

Configuring System Settings

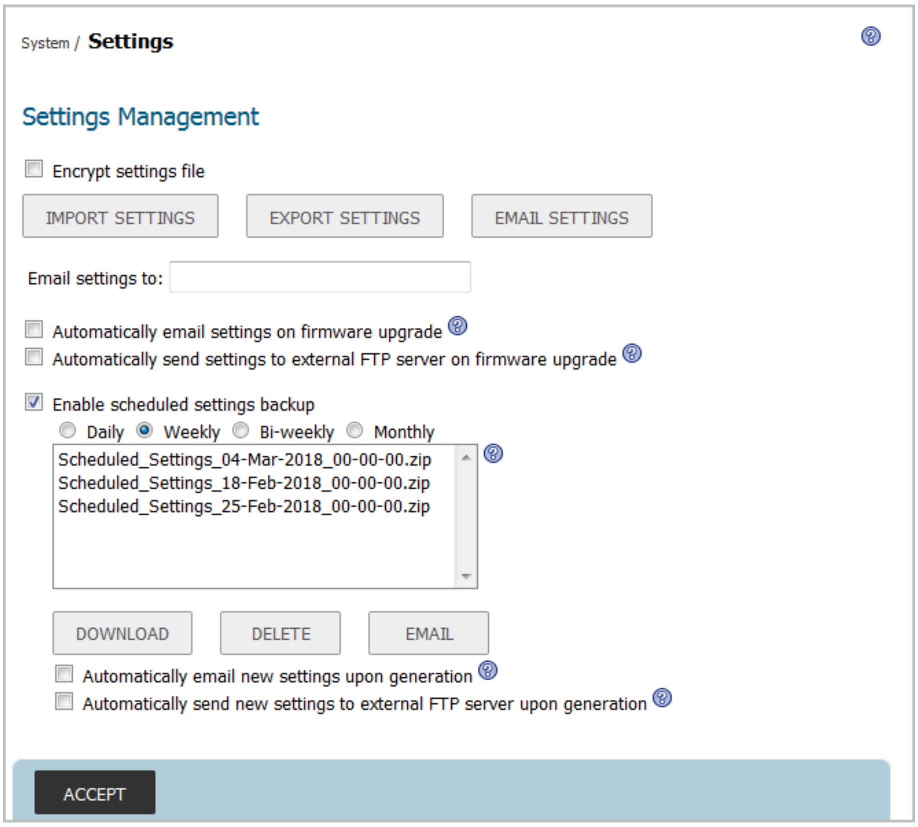
This section provides an overview of the **System > Settings** page and a description of the configuration tasks available on this page.

- System Settings Overview on page 44
- Managing Configuration Files on page 45
- Enabling and Managing Scheduled Backups on page 47

System Settings Overview

The **System** > **Settings** page allows the administrator to import and export the settings of the Web Application Firewall virtual appliance, and provides an option to encrypt the settings files. Options to automatically send your settings to an external FTP server after a firmware upgrade and upon generation are included. You can also schedule automatic settings backups and manage those backups.

System > Settings Page



System / **Settings**

Settings Management

□ Encrypt settings file

Email settings to:

□ Automatically email settings on firmware upgrade

□ Automatically send settings to external FTP server on firmware upgrade

☑ Enable scheduled settings backup

○ Daily ● Weekly ○ Bi-weekly ○ Monthly

Scheduled_Settings_04-Mar-2018_00-00-00.zip
Scheduled_Settings_18-Feb-2018_00-00-00.zip
Scheduled_Settings_25-Feb-2018_00-00-00.zip

□ Automatically email new settings upon generation

□ Automatically send new settings to external FTP server upon generation

Configure the FTP server on the **System > Administration** page to automatically send new settings to the external FTP server. Refer to the Configuring an External FTP/TFTP Server on page 55.

Configure the Mail Server and Mail From Address on the **System > Administration** page to automatically email new settings. See Configuring Log Settings on page 196 for more information.

Managing Configuration Files

Web Application Firewall virtual appliances allow you to save and import file sets that hold the Web Application Firewall configuration settings. These file sets can be saved and uploaded through the **System > Settings** page in the Web Application Firewall management interface.

These tasks are described in the following sections:

- Encrypting the Configuration File on page 46
- Importing a Configuration File on page 46
- Exporting a Backup Configuration File on page 46
- Emailing Configuration Settings on page 47
- Sending Settings to an FTP Server on page 47

Encrypting the Configuration File

For security purposes, you can encrypt the configuration files in the **System > Settings** page. However, if the configuration files are encrypted, they cannot be edited or reviewed for troubleshooting purposes.

To encrypt the configuration files, select **Encrypt settings file** in the **System > Settings** page.

Importing a Configuration File

You can import the configuration settings that you previously exported to a backup configuration file.

To import a configuration file:

1. Navigate to the **System > Settings** page.
2. To import a backup version of the configuration, click **IMPORT SETTINGS**. The **Import Settings** dialog box is displayed.
3. Click **Choose File** to navigate to a location that contains the file (that includes settings) you want to import. The file can be any name, but is named **wafSettings-serialnumber.zip** by default.
4. Click **ACCEPT**. Web Application Firewall imports the settings from the file and configures the virtual appliance with those settings.

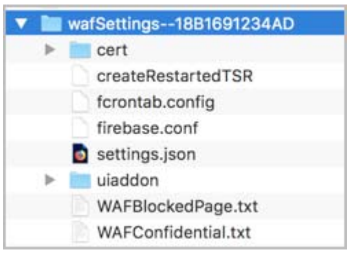
   NOTE: Make sure you are ready to reconfigure your system. After you import the file, the system overwrites the existing settings immediately.

5. After the file has been imported, restart the virtual appliance to make the changes permanent.

Exporting a Backup Configuration File

Exporting a backup configuration file allows you to save a copy of your configuration settings on your local machine. You can then save the configuration settings or export them to a backup file and import the saved configuration file at a later time, if necessary. The backup file is called **wafSettings-serialnumber.zip** by default, and includes the contents shown in the following figure.

Backup Configuration Directory Structure in Zip File



```
▼ wafSettings--18B1691234AD
    ▶ cert
      createRestartedTSR
      fcrontab.config
      firebase.conf
      settings.json
    ▶ uiaddon
      WAFBlockedPage.txt
      WAFConfidential.txt
```

The backup directory structure contains the following elements:

- **ca** folder (not shown) – Contains CA certificates provided by a Certificate Authority.
- **cert** folder – Contains the **default** folder with the default key/certification pair. Also contains key/certification pairs generated by Certificate Signing Requests (CSRs) from the **System > Certificates** page, if any.
- **fcrontab.config** file – Only generated when Schedule TSR is enabled.
- **firebase**.**conf** file – Contains network, DNS and log settings.
- **settings.json** file – Contains user, group, domain and web app settings.

- **uiaddon** folder – Contains a folder for each offloaded web app. Each folder contains web app custom login page messages, if defined, and the default logo or the custom logo for that web app, if one was uploaded.

To export a backup configuration file:

1. Navigate to the **System > Settings** page.
2. To save a backup version of the configuration, click **EXPORT SETTINGS**. The browser you are working in displays a pop-up asking you if you want to open the configuration file.
3. Select the option to **Save** the file.
4. Choose the location to save the configuration file. The file is named **wafSettings-serialnumber.zip** by default, but it can be renamed.
5. Click **Save** to save the configuration file.

Emailing Configuration Settings

You can email the current settings, auto-generated settings on upgrade, and scheduled settings to an email address as another way to back up your system. Specify an email address in the **Email Settings to** field and then click **ACCEPT**. Then, click **EMAIL SETTINGS**.

You can also have the email settings sent automatically upon every firmware upgrade. Select the **Automatically email settings on firmware upgrade** check box and then click **ACCEPT**. The **Mail Server** and **Mail From Address** values must be configured for automated email delivery. See Configuring Email Settings on page 52 for more information.

Sending Settings to an FTP Server

To send the settings to an FTP server after upgrade, select the **Automatically send settings to external FTP server on firmware upgrade** checkbox and then click **ACCEPT**. Configure the FTP server on the **System > Administration** page. Refer to the Configuring an External FTP/TFTP Server on page 55.

Enabling and Managing Scheduled Backups

You can set scheduled backups for your current settings by selecting **Enable scheduled settings backup**. Then, specify the frequency of backups to be scheduled. You can specify for the back ups to occur **Daily**, **Weekly**, **Bi-weekly**, or **Monthly**. Click **ACCEPT** after changing these options. A maximum of 6 backup settings files can be stored, with a total file size of no more than 10MB.

The list of settings backups is displayed in the list box. To manage the list, you can select one or more of the zip files in the list and then use the buttons below the list box as follows:

- Click **DOWNLOAD** to download the files to your management computer.
- Click **DELETE** to delete the files.
- Click **EMAIL** to email the files. The email address must already be configured in the **Email Settings to** field.

Select **Automatically email new settings upon generation** to have emails sent to you with the latest backed up settings after the backup is generated.

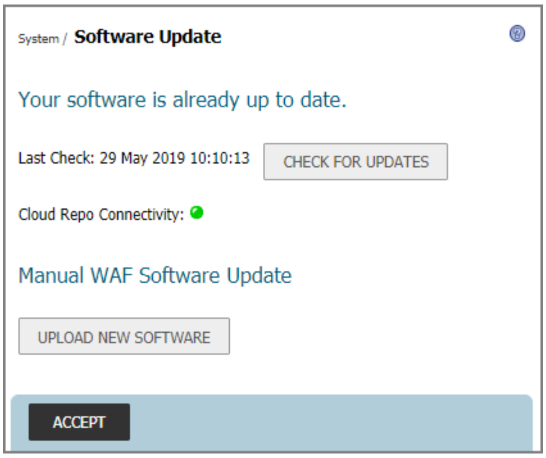
Select **Automatically send new settings to external FTP server upon generation** to have the latest backed up settings sent to an FTP server after the backup is generated.

Click **ACCEPT** after selecting or clearing any check boxes.

Updating System Software

This section provides information about using the **System > Software Update** page to check for software updates and install them.

System > Software Update Page



System / **Software Update**

Your software is already up to date.

Last Check: 29 May 2019 10:10:13

Cloud Repo Connectivity: 🟢

Manual WAF Software Update

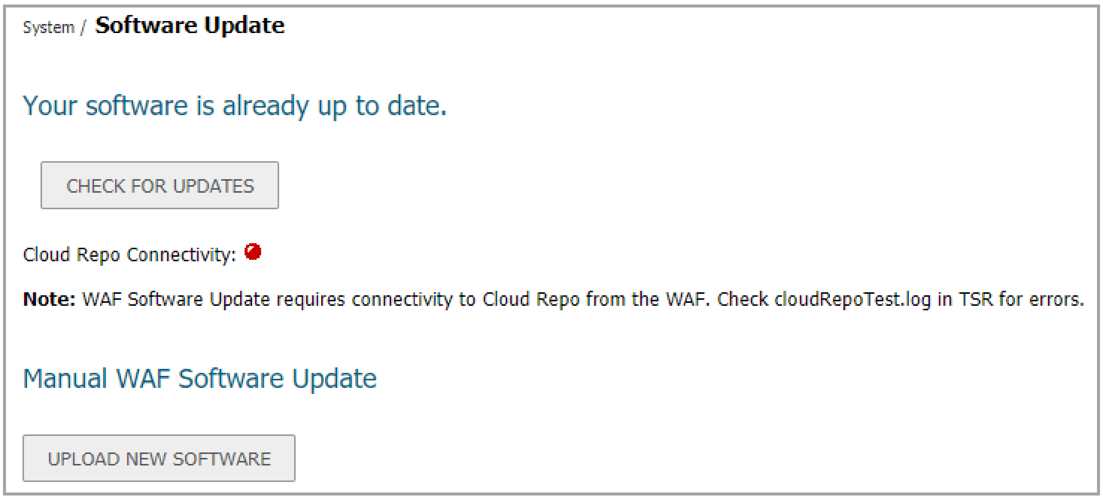
The **System > Software Update** page provides a way to check for WAF software updates. Click the **CHECK FOR UPDATES** button to enable WAF to check for new versions periodically, and automatically downloads new software versions when they become available. The WAF administrator can then install it.

Topics:

- Installing a WAF Software Update on page 48
- When the new version is completely downloaded, click the INSTALL NOW button to install it. on page 49

Installing a WAF Software Update

WAF automatically checks for available software updates and also provides a way to check for them anytime. Cloud Repo Connectivity improves user experience by providing the ability to test repo status and access to the public network, before the WAF software upgrade. A green LED indicates the Cloud Repo is available. A red LED indicates the Cloud Repo is not available and displays an error message.



System / **Software Update**

Your software is already up to date.

Cloud Repo Connectivity: 🔴

Note: WAF Software Update requires connectivity to Cloud Repo from the WAF. Check cloudRepoTest.log in TSR for errors.

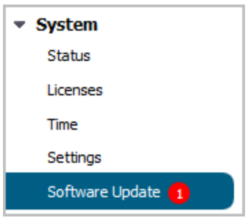
Manual WAF Software Update

NOTE: If the Cloud Repo is not accessible, the WAF software upgrade will fail. If an upgrade fails, check *wafInstall.log* and *wafsystemd.log* in the TSR for more details.

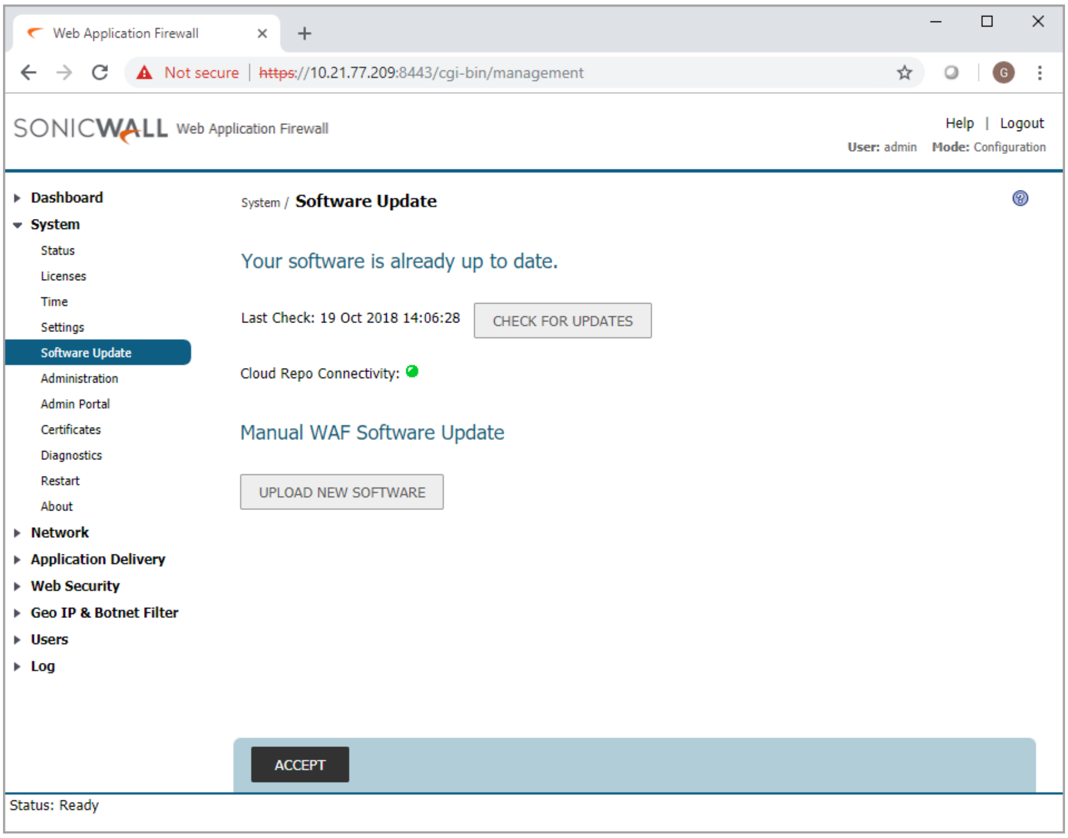
To install a new SonicWall WAF software version:

1. Navigate to the **System > Software Update** page.
2. In the **Your software is already up to date** section of the page, optionally click the **CHECK FOR UPDATES** button to check MySonicWall for a new WAF software version. This allows you to check for a new version between automatic checks.

   If a new version is found, it is downloaded to SonicWall WAF.
3. If the left navigation pane displays a red number next to **Software Updates**, this indicates that a new version of SonicWall WAF is available and has been automatically detected.



   The top section of the page also displays the heading **New Software Version(s) Available**. The new software version is automatically downloaded from MySonicWall.



Your software is already up to date.

Last Check: 19 Oct 2018 14:06:28

Cloud Repo Connectivity: ●

Manual WAF Software Update

Status: Ready

   When the new version is completely downloaded, click the **INSTALL NOW** button to install it.

Manually Uploading and Installing WAF Software

There might be times when you want to use a specific version of SonicWall WAF, but it is not automatically downloaded. You can manually download the version from MySonicWall and then upload it to your WAF and install it.

To manually check for and install new WAF software:

1. Log into your MySonicWall account and download the WAF software to your management computer. This is a signed image file, such as sw_vm_upgrade_image_2.2.0.1-16waf.sig. This update file works with WAF deployments on AWS, Azure, Hyper-V, and VMware.
2. Log into WAF and navigate to the **System > Software Updates** page.
3. Under **Manual WAF Software Update**, click the **UPLOAD NEW SOFTWARE** button.
4. Browse to the saved firmware and click **UPLOAD**.
5. When the new version finishes uploading, click the **INSTALL NOW** button to install it.

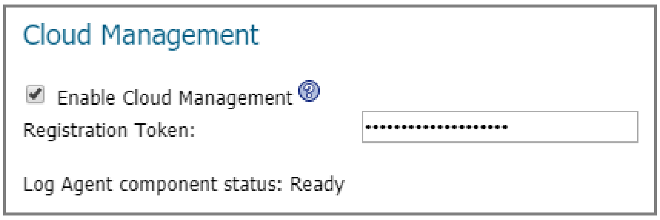
Configuring System Administration Settings

This section provides information about the configuration tasks available on the **System > Administration** page.

- Configuring Cloud Management on page 50
- Configuring Login Security on page 51
- Downloading the Capacity Matrix Report on page 51
- Configuring Web Management Settings on page 52
- Configuring Email Settings on page 52
- Configuring SNMP Settings on page 53
- Configuring an External FTP/TFTP Server on page 55

Configuring Cloud Management

The Cloud Management section provides a way to configure administrator/user access through the cloud and perform basic management tasks. With your registration token, you can subscribe and unsubscribe to different resources.



Cloud Management

☑ Enable Cloud Management

Registration Token: ••••••••••••••••••••••

Log Agent component status: Ready

To enable Cloud Management:

1 Navigate to **System > Administration**.

2 Select **Enable Cloud Management**.

> ⓘ **NOTE:** Cloud Management can be enabled only if components are ready.

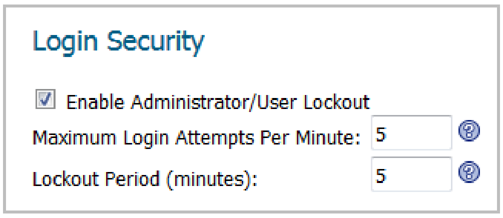
3 In the **Registration Token** field, enter your information.

4 In the **Log Agent component status**, note it should say **Ready**.

5 Click **ACCEPT** to save your changes.

Configuring Login Security

The **Login Security** section provides a way to configure administrator/user lockout for a set period of time (in minutes) after a set number of maximum login attempts per minute. This protects against unauthorized login attempts to the web app.



Login Security

☑ Enable Administrator/User Lockout

Maximum Login Attempts Per Minute: 5

Lockout Period (minutes): 5

To enable the auto lockout feature:

1 Navigate to **System > Administration**.

2 Select **Enable Administrator/User Lockout**.

3 In the **Maximum Login Attempts Per Minute** field, type the number of maximum login attempts allowed before a user is locked out. The default is five attempts. The maximum is 99 attempts.

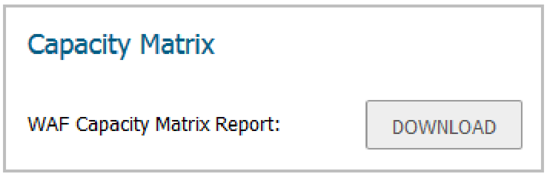
4 In the **Lockout Period (minutes)** field, type a number of minutes to lockout a user who has exceeded the number of maximum login attempts. The default is five minutes. The maximum is 99999 minutes.

5 Click **ACCEPT** to save your changes.

Downloading the Capacity Matrix Report

The Web Application Firewall Capacity Matrix Report is a downloadable PDF file that allows you to view the total number of various connections, interfaces, web apps, domains, groups, users, and so on, available for your specific Web Application Firewall virtual appliance.

On the **System > Administration** page under **Capacity Matrix**, click **DOWNLOAD** to download the report to your local system.

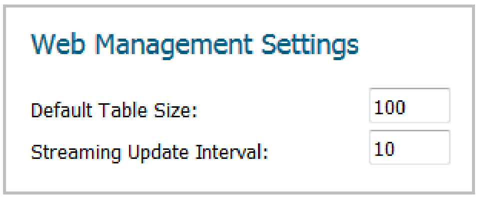


Capacity Matrix

WAF Capacity Matrix Report:

Configuring Web Management Settings

The Web Management Settings section allows the administrator to set the default page size for paged tables and the streaming update interval for dynamically updated tables in the Web Application Firewall management interface.



Web Management Settings

Default Table Size: 100

Streaming Update Interval: 10

The following paged tables are affected by the **Default Table Size** setting:

- **Log > View**

The following dynamically updated tables are affected by the **Streaming Update Interval** setting:

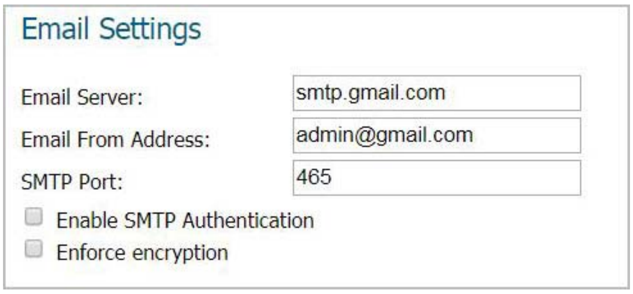
- **Dashboard > Monitoring**
- **Network > Interfaces**
- **Web Security > Status**
- **Geo IP & Botnet Filter > Status**
- **Users > Status**

To set the table page size and streaming update interval:

1. In the **Default Table Size** field, enter the number of rows per page for paged tables in the Web Application Firewall management interface. The default is 100, the minimum is 10, and the maximum is 99,999.
2. In the **Streaming Update Interval** field, enter the number of seconds between updates for dynamically updated tables in the Web Application Firewall management interface. The default is 10, the minimum is 1, and the maximum is 99,999.
3. Click **ACCEPT** to save your changes.

Configuring Email Settings

The **Email Settings** section allows you to configure a mail server and an account to be used as the “mail from” email address. You can also specify the SMTP port, authentication, and encryption settings.



Email Settings

Email Server: smtp.gmail.com

Email From Address: admin@gmail.com

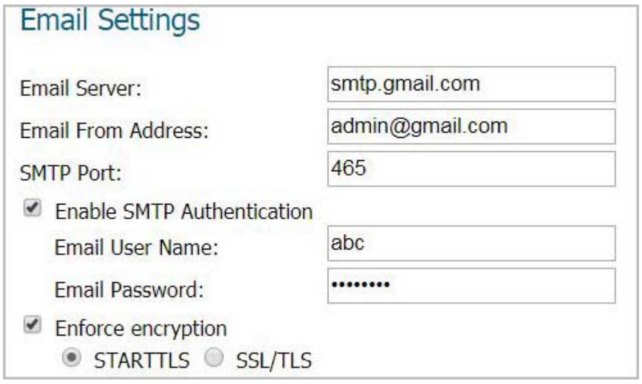
SMTP Port: 465

☐ Enable SMTP Authentication

☐ Enforce encryption

To configure email settings:

1. Navigate to **System > Administration** and scroll down to the **Email Settings** section.
2. In the **Email Server** field, type in the mail server IP address or FQDN.
3. In the **Email From Address** field, type in the email account to appear in the From field when email is sent from the WAF virtual appliance.
4. In the **SMTP Port** field, accept the default 25 or type in a custom port number.
5. Select the **Enable SMTP Authentication** checkbox if you want to enable SMTP authentication. More fields are displayed.



Email Settings

Email Server: smtp.gmail.com

Email From Address: admin@gmail.com

SMTP Port: 465

☑ Enable SMTP Authentication

Email User Name: abc

Email Password: ••••••••

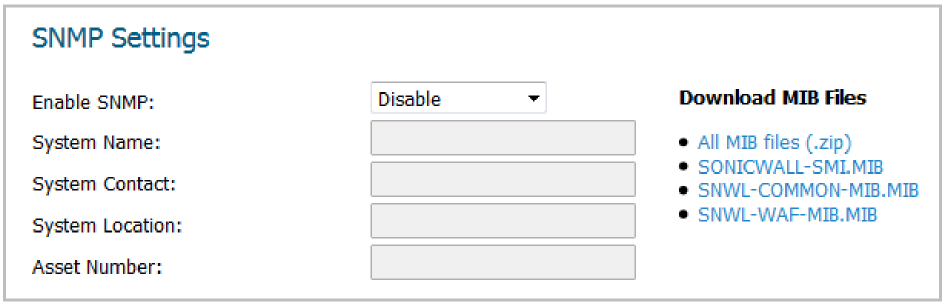
☑ Enforce encryption

● STARTTLS ○ SSL/TLS

6. In the **Email User Name** field, type in the user name for SMTP authentication.
7. In the **Email Password** field, type in the password for SMTP authentication.
8. Select the **Enforce encryption** checkbox if you want to enable encryption. The choices of encryption type are displayed. Select one of:
   - **STARTTLS** – upgrades an existing insecure, plain text connection to a secure one using TLS (or SSL) on the existing port; STARTTLS uses SMTP port 25 or 587
   - **SSL/TLS** – uses SMTP port 465 for SSL or TLS encryption
9. Click **ACCEPT** to save your changes.

Configuring SNMP Settings

The **SNMP Settings** section allows the administrator to enable SNMP and specify SNMP settings for the appliance. A list of downloaded MIBs is displayed to the right of the fields. MIBs can be downloaded from MySonicWall.



SNMP Settings

Enable SNMP: Disable

System Name:

System Contact:

System Location:

Asset Number:

Download MIB Files

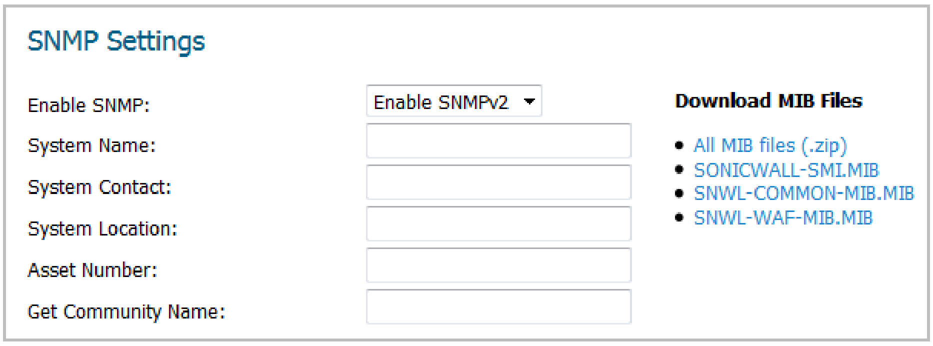
- All MIB files (.zip)
- SONICWALL-SMI.MIB
- SNWL-COMMON-MIB.MIB
- SNWL-WAF-MIB.MIB

To configure the SNMP Settings fields:

1 Navigate to **System > Administration** and scroll down to the **SNMP Settings** section.

2 In the **Enable SNMP** drop-down list, select one of:

- **Enable SNMPv2**



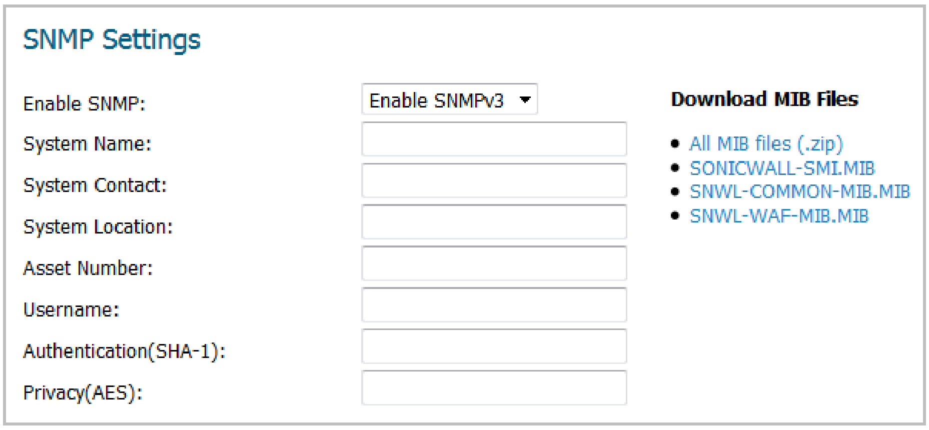
SNMP Settings

Enable SNMP:	Enable SNMPv2
System Name:	
System Contact:	
System Location:	
Asset Number:	
Get Community Name:	

Download MIB Files

- All MIB files (.zip)
- SONICWALL-SMI.MIB
- SNWL-COMMON-MIB.MIB
- SNWL-WAF-MIB.MIB

- **Enable SNMPv3**



SNMP Settings

Enable SNMP:	Enable SNMPv3
System Name:	
System Contact:	
System Location:	
Asset Number:	
Username:	
Authentication(SHA-1):	
Privacy(AES):	

Download MIB Files

- All MIB files (.zip)
- SONICWALL-SMI.MIB
- SNWL-COMMON-MIB.MIB
- SNWL-WAF-MIB.MIB

3 Type the name (FQDN) of the system into the **System Name** field.

4 Type the email address of the system contact into the **System Contact** field.

5 Type the city or other identifying location of the system into the **System Location** field.

6 Type the asset number of the system into the **Asset Number** field. The asset number is defined by the administrator.

7 For SNMPv2, type the public community name into the **Get Community Name** field. This name is used in SNMP GET requests.

8 For SNMPv3:

a In the **Username** field, type the username of the SNMP user who can access the WAF virtual appliance.

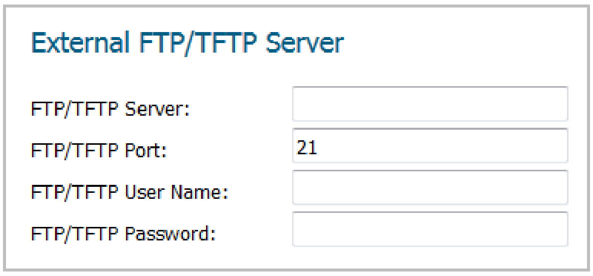
b In the **Authentication(SHA-1)** field, type the password for the SNMP user.

c In the **Privacy(AES)** field, type the privacy password for AES.

9 Click **ACCEPT** to save your changes.

Configuring an External FTP/TFTP Server

The **External FTP/TFTP Server** section allows you to configure an external FTP server to backup your settings and diagnostic data.



External FTP/TFTP Server

FTP/TFTP Server:	
FTP/TFTP Port:	21
FTP/TFTP User Name:	
FTP/TFTP Password:	

To configure the External FTP/TFTP Server settings:

1. Navigate to the **System > Administration** page.
2. In the **External FTP/TFTP Server** section, type the FTP/TFTP server address or FQDN into the **FTP/TFTP Server** field.
3. In the **FTP/TFTP Port** field, accept the default port 21 or type in a custom FTP/TFTP port number.
4. In the **FTP/TFTP User Name** field, type in the user name for the server.
5. In the **FTP/TFTP Password** field, type in the password for the server.
6. Click **ACCEPT** to save your changes.

Configuring a System Admin Portal

The **System > Admin Portal** page provides settings for configuring a management portal for Web Application Firewall. The configuration settings are divided into three screens:

- **General** – The **General** screen allows you to configure **General Settings** for a custom portal by providing the portal name, site title, banner title, login message, and portal URL. This screen also provides a way to configure custom login options for control over what is displayed/loaded on login and logout, HttpOnly security for WAF cookies, HTTP meta tags for cache control, and login uniqueness. **Windows Live Tile Settings** for logo, background color, and site name are also configured on this screen.
- **Server** – The **Server** screen allows users to log in using a different hostname than your default URL.
- **Logo** – The **Logo** screen provides a way to upload a custom logo and to toggle between the default SonicWall logo and a custom uploaded logo. You can also upload a custom favicon from this screen.

Topics:

- Configuring General Settings on page 56
- Configuring Virtual Host Settings on page 58
- Configuring Logo Settings on page 59

The General Settings and Windows Live Tile Settings Fields tables provide a description of the fields you can configure on the **General** screen.

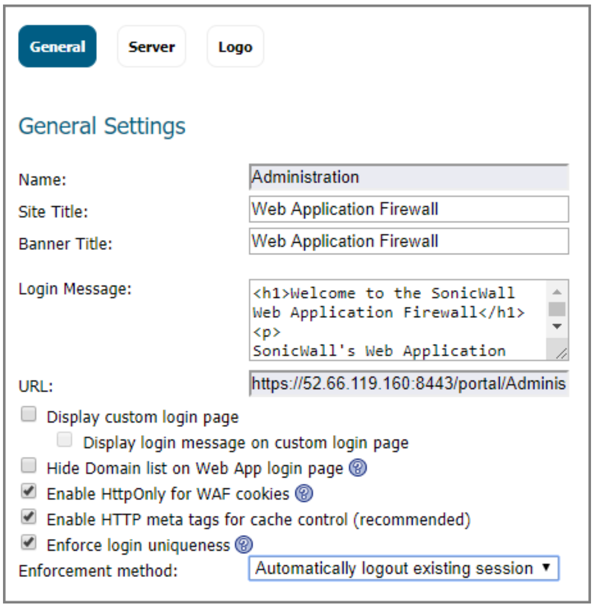
General Settings and Windows Live Tile Settings Fields

Field	Description
Name	The title used to refer to this portal. It is for internal reference only, and is not displayed to users.
Site Title	The title that appears on the web browser title bar of users access this portal.
Banner Title	The welcome text that appears on top of the portal screen.
Login Message	Optional text that appears on the portal login page above the authentication area.
URL	The URL that is used to access this specific portal.
Display custom login page	Displays the customized login page rather than the default login page for this portal.
Display login message on custom login page	Displays the text specified in the Login Message text box.
Hide Domain list on Web App login page	If enabled, this option replaces the Domain list box on the login page with a text box. The user can then type in the correct domain name. This option is only enabled for portal login through web.
Enable HttpOnly for WAF cookies	WAF cookies are secured using the HTTPOnly flag when this option is enabled. The HTTPOnly flag prevents client-side scripts from accessing the cookies, protecting them from cross-site scripting cookie theft.
Enable HTTP meta tags for cache control	Enables HTTP meta tags in all HTTP/HTTPS pages served to remote users to prevent their browser from caching content. SonicWall recommends enabling this option.
Enforce login uniqueness	If enforced, login uniqueness restricts each account to one session at a time. Select to **Automatically logout existing session** or **Confirm logout of existing session** as the preferred Enforcement Method. If not enforced, each account can have multiple simultaneous sessions.
Enforcement method	Enables you to choose between automatically logging out of the existing session or confirming logout of the existing session.
Small Logo	Specify the link for the small logo. The recommended size is 128 x 128.
Medium Logo	Specify the link for the medium logo. The recommended size is 270 x 270.
Wide Logo	Specify the link for the wide logo. The recommended size is 558 x 270.
Large Logo	Specify the link for the large logo. The recommended size is 558 x 558.
Background Color	Specify the background color for Live Tile. The default setting is #0085C3.
Site Name	Specify the display name for the Live Tile bookmark. The default setting is your web app name.

Configuring General Settings

You can configure the Admin Portal with a customized landing page for authentication. The **General** screen on the **System > Admin Portal** page provides a way to define individual layouts for the portal.

Admin Portal General Screen - General Settings



General Settings

Name: Administration

Site Title: Web Application Firewall

Banner Title: Web Application Firewall

Login Message:

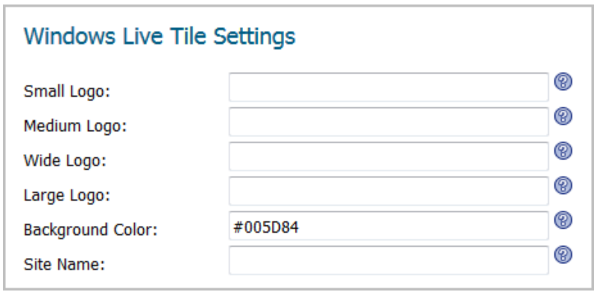
```
<h1>Welcome to the SonicWall
Web Application Firewall</h1>
<p>
SonicWall's Web Application
```

URL: https://52.66.119.160:8443/portal/Adminis

- ☐ Display custom login page
  - ☐ Display login message on custom login page
- ☐ Hide Domain list on Web App login page
- ☑ Enable HttpOnly for WAF cookies
- ☑ Enable HTTP meta tags for cache control (recommended)
- ☑ Enforce login uniqueness

Enforcement method: Automatically logout existing session ▼

Admin Portal General Screen - Windows Live Tile Settings



Windows Live Tile Settings

Small Logo:	
Medium Logo:	
Wide Logo:	
Large Logo:	
Background Color:	#005D84
Site Name:	

To add a portal:

1. Navigate to the **General** screen of the **System > Admin Portal** page. The **General Settings** options are displayed.
2. Enter a descriptive name for the portal in the **Name** field.

   > **NOTE:** Only alphanumeric characters, hyphen (-), and underscore (_) are accepted in the **Name** field. If other types of characters or spaces are entered, the portal name is truncated before the first non-alphanumeric character.

3. Enter the title for the web browser window in the **Site Title** field.
4. To display a banner message to users before they log in to the portal, enter the banner title text in the **Banner Title** field.
5. Enter an HTML compliant message, or edit the default message in the **Login Message** field. This message is shown to users on the custom login page.
6. The **URL** field is automatically populated based on your Web Application Firewall virtual appliance network address and the **Name** field.

7 To enable visibility of your custom logo, message, and title information on the login page, select **Display custom login page**.

> ⓘ **NOTE:** Custom logos can only be added to existing portals. To add a custom logo to a new portal, first complete general portal configuration, then add a logo in Configuring Logo Settings on page 59.

8 To require the user to type in the correct domain name rather than displaying a list, select **Hide Domain list on Web App login page**.

9 To secure WAF cookies with the HTTPOnly flag, select **Enable HttpOnly for WAF cookies**. The HTTPOnly flag prevents client-side scripts from accessing the cookies, protecting them from cross-site scripting cookie theft.

10 Select **Enable HTTP meta tags for cache control** to apply HTTP meta tag cache control directives to the portal. Cache control directives include:

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

These directives help prevent clients browsers from caching Web Application Firewall portal pages and other web content.

> ⓘ **NOTE:** Enabling HTTP meta tags is strongly recommended for security reasons and to prevent out-of-date web pages and data from being stored in the user's web browser cache.

11 Select **Enforce login uniqueness** to restrict each account to a single session at a time. When this option is enabled, select one of the following from the **Enforcement method** drop-down list:

- **Automatically logout existing session** – Automatically logs out the other session.
- **Confirm logout of existing session** – Reminds the user of the existing session and requires confirmation to open the new session, ending the other session.

12 In the **Windows Live Tile Settings** section, specify the link(s) for the **Small** / **Medium** / **Wide** / **Large Logo** to be used with Live Tile.

13 Specify the **Background Color** for Live Tile. If no value is specified, the default color is #0085C3.

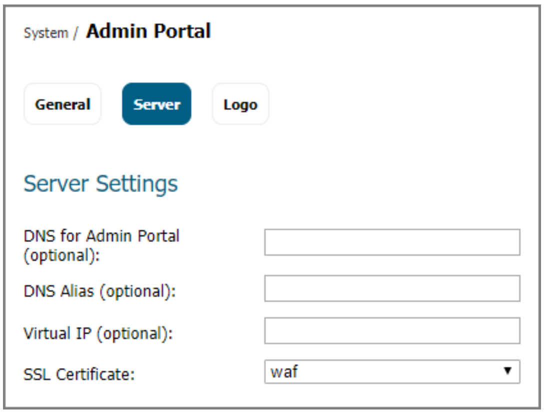
14 Specify the **Site Name** to be displayed for the Live Tile bookmark. If no value is specified, the default is the web app name.

15 Click **ACCEPT** to save changes.

Configuring Virtual Host Settings

Virtual Host settings can be configured for the Admin Portal to use a FQDN or a virtual IP to access the management interface instead of the default IP. For example, the administrators can use **https://waf.company.com:8443** to manage the appliance.

Admin Portal Server Host Screen



Server Settings

DNS for Admin Portal (optional):	
DNS Alias (optional):	
Virtual IP (optional):	
SSL Certificate:	waf

To configure a server host:

1. Navigate to the **Server** screen of the **System > Admin Portal** page. The **Server Settings** options are displayed.
2. Enter a host name in the **DNS for Admin Portal (optional)** field, for example, **sales.company.com**.

   Only alphanumeric characters, hyphen (-) and underscore (_) are accepted in the **DNS for Admin Portal** field.
3. Optionally enter an alias name in the **DNS for Admin Portal** field.
4. Optionally select a **DNS Alias** for this portal.

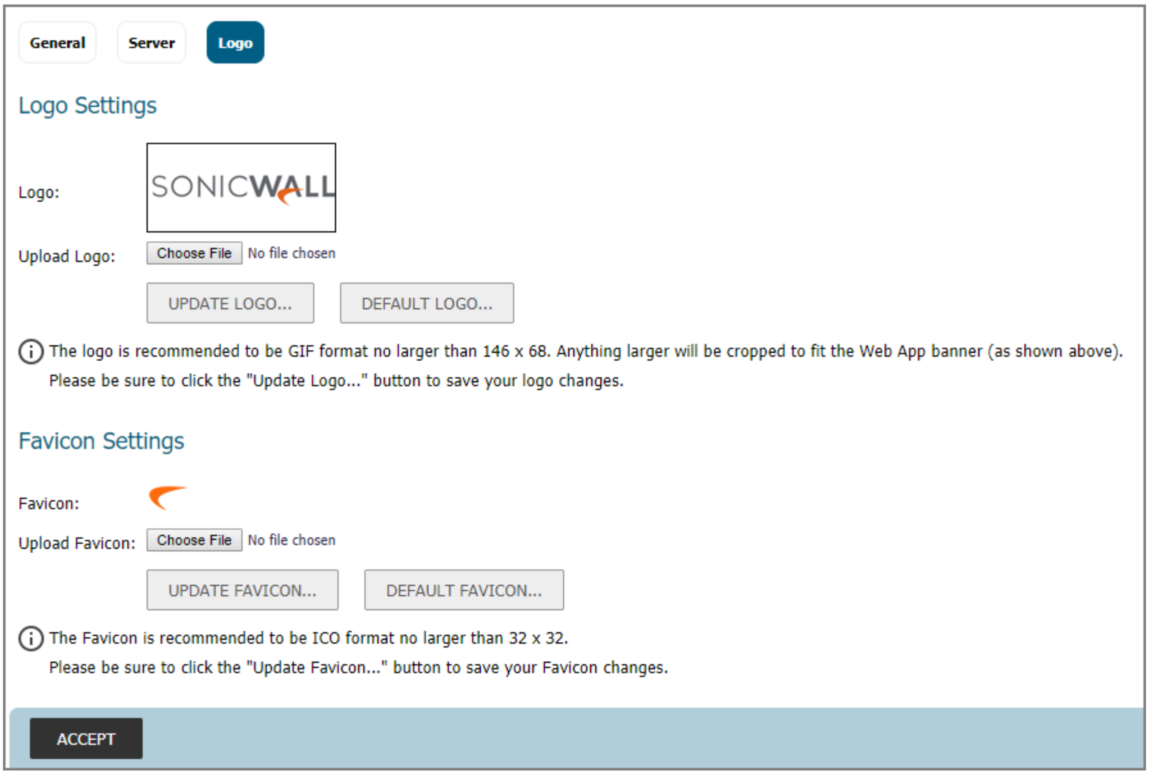
   If your server host implementation uses name-based server hosts — where more than one hostname resides behind a single IP address — choose **All Interfaces** from the server interface.
5. Optionally select a **Virtual IP** address for this portal.
6. If you plan to use a unique security certificate for this sub-domain, select the corresponding port interface address from the **Virtual Host Certificate** list.

   Unless you have a certificate for each virtual host domain name, or if you have purchased a *.domain SSL certificate, your users might see a **Certificate host name mismatch** warning when they log in to the Virtual Host portal.
7. Click **ACCEPT** to save changes.

Configuring Logo Settings

The **Logo** screen on the **System > Admin Portal** page provides a way to upload a custom logo and to toggle between the default SonicWall logo and a custom uploaded logo. You can also upload a custom favicon from this screen. You must add the portal before you can upload a custom logo or custom favicon.

Admin Portal Logo Screen



Logo Settings

Logo:

Upload Logo: Choose File No file chosen

ⓘ The logo is recommended to be GIF format no larger than 146 x 68. Anything larger will be cropped to fit the Web App banner (as shown above). Please be sure to click the "Update Logo..." button to save your logo changes.

Favicon Settings

Favicon:

Upload Favicon: Choose File No file chosen

ⓘ The Favicon is recommended to be ICO format no larger than 32 x 32. Please be sure to click the "Update Favicon..." button to save your Favicon changes.

To add a custom logo:

1 Navigate to the **Logo** screen of the **System > Admin Portal** page. The **Logo Settings** and **Favicon Settings** options are displayed.

2 Under **Logo Settings**, click **Choose File** by the **Upload Logo** field. The file browser window displays.

3 Select an appropriate-sized .gif format logo in the file browser and click **Open**.

> ⓘ **NOTE:** SonicWall recommends GIF format. Anything larger than 146x68 pixels is cropped to fit the designated logo space on the page.

4 Click **UPDATE LOGO** to transfer the logo to the Web Application Firewall virtual appliance.

5 Click **DEFAULT LOGO** to revert to the default SonicWall logo.

6 Click **ACCEPT** to save changes.

To add a custom favicon:

1 Navigate to the **Logo** screen of the **System > Admin Portal** page. The **Logo Settings** and **Favicon Settings** options are displayed.

2 Under **Favicon Settings**, click **Choose File** by the **Upload Favicon** field. The file browser window displays.

3 Select an appropriate-sized ICO format favicon in the file browser and click **Open**.

> ⓘ **NOTE:** SonicWall recommends ICO format for the custom favicon, no larger than 32x32 pixels.

4 Click **UPDATE FAVICON** to transfer the favicon to the Web Application Firewall virtual appliance.

5 Click **DEFAULT FAVICON** to revert to the default SonicWall logo.

6 Click **ACCEPT** to save changes.

Managing System Certificates

The **System > Certificates** page allows the administrator to import server certificates and additional CA (Certificate Authority) certificates and perform other related tasks. This section describes the configuration tasks available on this page.

ⓘ **NOTE:** The Managing System Certificates section is not mandatory when using the Let's Encrypt service for automated certificate management. Certificates can be managed as part of the configuration of Application Offloading process, see Adding an Offloaded Web App on page 80.

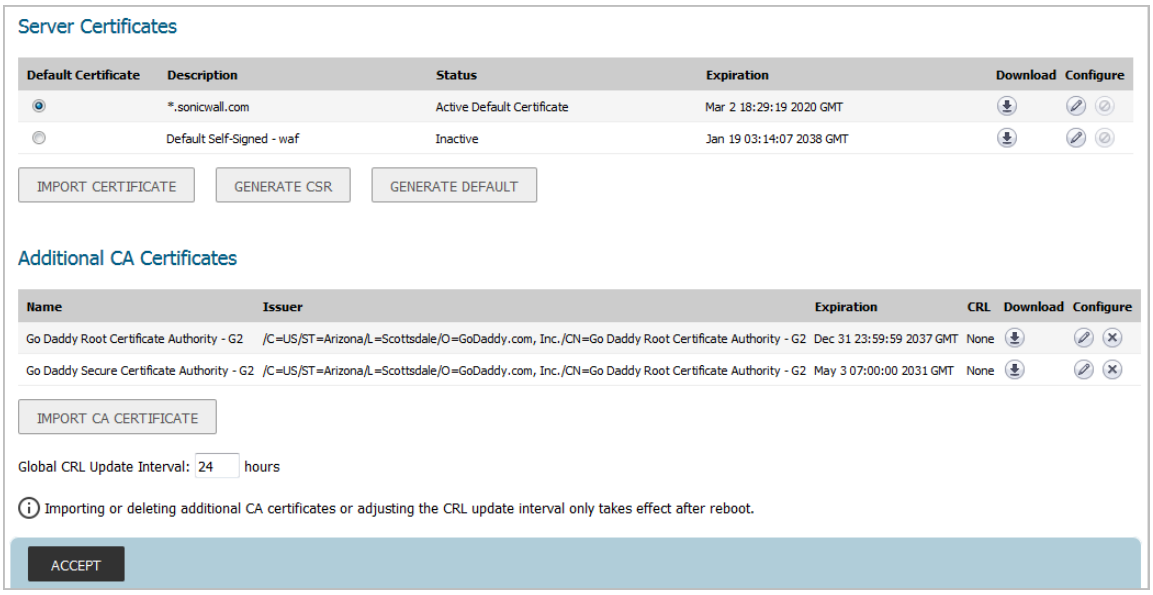
ⓘ **NOTE:** Importing or deleting additional CA certificates or adjusting the CRL update interval only takes effect after reboot.

- System Certificates Overview on page 61
- Certificate Management on page 62
- Generating a Certificate Signing Request on page 62
- Viewing and Editing Certificate Information on page 63
- Deleting a Certificate on page 64
- Importing a Certificate on page 64
- Adding Additional CA Certificates on page 65
- Using System Diagnostics on page 65

System Certificates Overview

In addition to importing certificates, the **System > Certificates** page provides a way to generate a certificate signing request and to generate a default self-signed certificate.

System > Certificates Page



Server Certificates

Default Certificate	Description	Status	Expiration	Download	Configure
●	*.sonicwall.com	Active Default Certificate	Mar 2 18:29:19 2020 GMT	⤓	✎ ⊘
○	Default Self-Signed - waf	Inactive	Jan 19 03:14:07 2038 GMT	⤓	✎ ⊘

Additional CA Certificates

Name	Issuer	Expiration	CRL	Download	Configure
Go Daddy Root Certificate Authority - G2	/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	None	⤓	✎ ⊗
Go Daddy Secure Certificate Authority - G2	/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2	May 3 07:00:00 2031 GMT	None	⤓	✎ ⊗

Global CRL Update Interval: 24 hours

ⓘ Importing or deleting additional CA certificates or adjusting the CRL update interval only takes effect after reboot.

Server Certificates

The Server Certificates section allows the administrator to import and configure a server certificate, to generate a CSR (certificate signing request), and to generate a default, self-signed certificate.

A server certificate is used to verify the identity of the Web Application Firewall virtual appliance. The appliance presents its server certificate to the user's browser when the user accesses the login page. Each server certificate contains the name of the server to which it belongs.

There is always one self-signed certificate (self-signed means that it is generated by the Web Application Firewall virtual appliance, not by a real CA), and there could be multiple certificates imported by the administrator. If the administrator has configured multiple web apps, it is possible to associate a different certificate with each web app. For example, **waf.test.sonicwall.com** might also be reached by pointing the browser to **waf2.test.sonicwall.com**. Each of those web apps can have its own certificate. This is useful to prevent the browser from displaying a certificate mismatch warning, such as "This server is abc, but the certificate is xyz, are you sure you want to continue?"

A CSR is a certificate signing request. When preparing to get a certificate from a CA, you first generate a CSR with the details of the certificate. Then the CSR is sent to the CA with any required fees, and the CA sends back a valid signed certificate.

Additional CA Certificates

The Additional CA Certificates section allows the administrator to import additional certificates from a Certificate Authority server, either inside or outside of the local network. The certificates are in PEM encoded format for use with chained certificates, for example, when the issuing CA uses an intermediate (chained) signing certificate.

The imported additional certificates only take effect after restarting the Web Application Firewall virtual appliance.

Certificate Management

The Web Application Firewall virtual appliance comes with a pre-installed self-signed X509 certificate for SSL functions. A self-signed certificate provides all the same functions as a certificate obtained through a well-known certificate authority (CA), but presents an "untrusted root CA certificate" security warning to users until the self-signed certificate is imported into their trusted root store. This import procedure can be completed by the user by clicking **Import Certificate** after authenticating.

The alternative to using the self-signed certificate is to generate a certificate signing request (CSR) and to submit it to a well-known CA for valid certificate issuance. Well-known CAs include RapidSSL (www.rapidssl.com), Verisign (www.verisign.com), and Thawte (www.thawte.com).

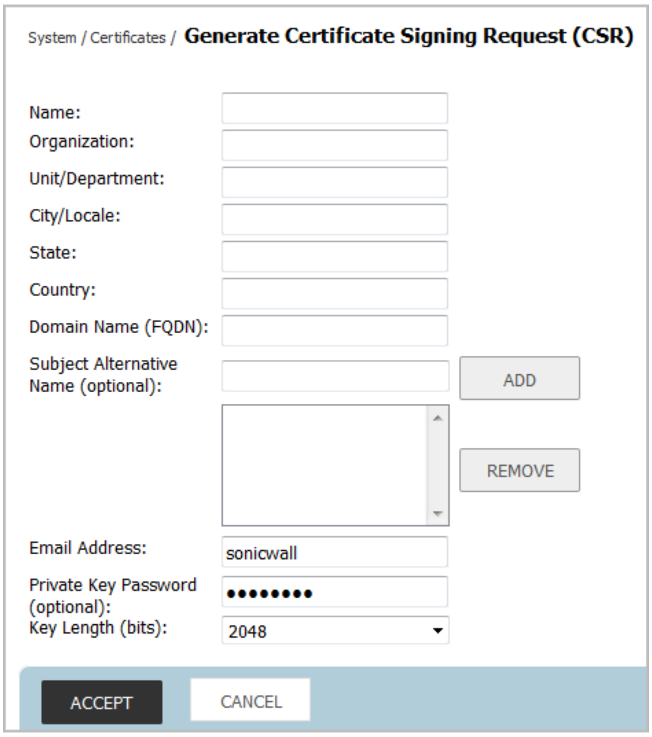
Generating a Certificate Signing Request

To get a valid certificate from a widely accepted CA such as RapidSSL, Verisign, or Thawte, you must generate a Certificate Signing Request (CSR) for your Web Application Firewall virtual appliance.

To generate a certificate signing request:

1 Navigate to the **System > Certificates** page.

2 Click **GENERATE CSR** to generate a CSR and Certificate Key. The **Generate Certificate Signing Request** dialog box is displayed.



System / Certificates / **Generate Certificate Signing Request (CSR)**

Name:	
Organization:	
Unit/Department:	
City/Locale:	
State:	
Country:	
Domain Name (FQDN):	
Subject Alternative Name (optional):	
Email Address:	sonicwall
Private Key Password (optional):	••••••••
Key Length (bits):	2048

3 Fill in the fields in the dialog box and click **ACCEPT**.

NOTE: The Subject Alternative Name (SAN)/Unified Communications Certificate (UCC) can be included in the request.

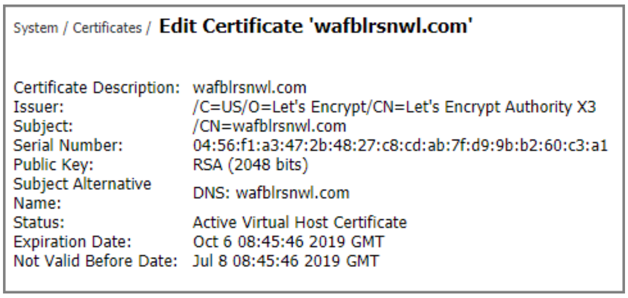
4 If all information is entered correctly, a **csr.zip** file is created. Save this .zip file to disk. You need to provide the contents of the **server.csr** file, found within this zip file, to the CA.

Viewing and Editing Certificate Information

The **System > Certificates** page lists the currently loaded SSL certificates.

To view certificate and issuer information and edit the Common Name in the certificate:

1 On the **System > Certificates** page, click the configure icon in the row for the certificate. The **Edit Certificate** window is displayed, showing issuer and certificate subject information.



System / Certificates / **Edit Certificate 'wafblrsnwl.com'**

Certificate Description:	wafblrsnwl.com
Issuer:	/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
Subject:	/CN=wafblrsnwl.com
Serial Number:	04:56:f1:a3:47:2b:48:27:c8:cd:ab:7f:d9:9b:b2:60:c3:a1
Public Key:	RSA (2048 bits)
Subject Alternative Name:	DNS: wafblrsnwl.com
Status:	Active Virtual Host Certificate
Expiration Date:	Oct 6 08:45:46 2019 GMT
Not Valid Before Date:	Jul 8 08:45:46 2019 GMT

2 Click **ACCEPT** to submit the changes.

Deleting a Certificate

You can delete an expired or incorrect certificate. Delete the certificate by clicking the **Delete** icon in the row for the certificate, on the **System > Certificates** page.

NOTE: A certificate that is currently active cannot be deleted. To delete a an active certificate, upload and enable another SSL certificate, then delete the now-inactive certificate on the **System > Certificates** page.

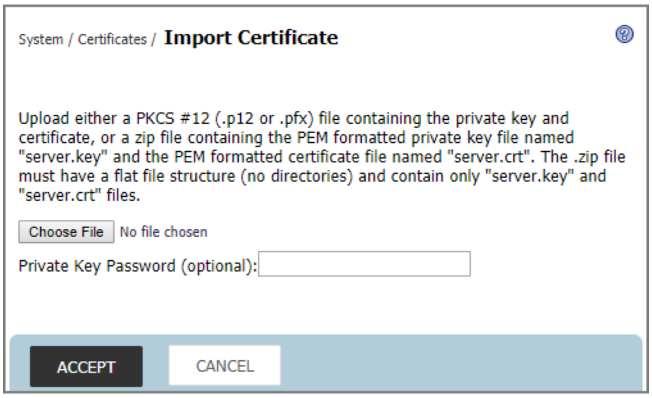
Importing a Certificate

When importing a certificate you must upload either a **PKCS #12** (**.p12** or **.pfx**) file containing the private key and certificate, or a zip file containing the PEM-formatted private key file named **server.key** and the PEM-formatted certificate file named **server.crt**. The **.zip** file must have a flat file structure (no directories) and contain only **server.key** and **server.crt** files.

To import a certificate:

1 Navigate to the **System** > **Certificates** page.

2 Click **IMPORT CERTIFICATE**. The Import Certificate dialog box is displayed.



System / Certificates / **Import Certificate**

Upload either a PKCS #12 (.p12 or .pfx) file containing the private key and certificate, or a zip file containing the PEM formatted private key file named "server.key" and the PEM formatted certificate file named "server.crt". The .zip file must have a flat file structure (no directories) and contain only "server.key" and "server.crt" files.

Private Key Password (optional):

3 Click **Choose File**.

4 Locate the server certificate. If uploading from a PKCS #12 file, select the **.p12** or **.pfx** file from your disk or network drive. If uploading a zipped file containing the private key and certificate select the **.zip** file from your disk or network drive. Any filename is accepted, but it must have the “.zip” extension. The zipped file should contain a certificate file named **server.crt** and a certificate key file named **server.key**. The key and certificate must be at the root of the zip, or the file is not uploaded.

5 Click **Upload**.

6 Click **ACCEPT**.

After the certificate has been uploaded, the certificate is displayed in the Certificates list in the **System > Certificates** page.

ⓘ **NOTE:** Private keys might require a password.

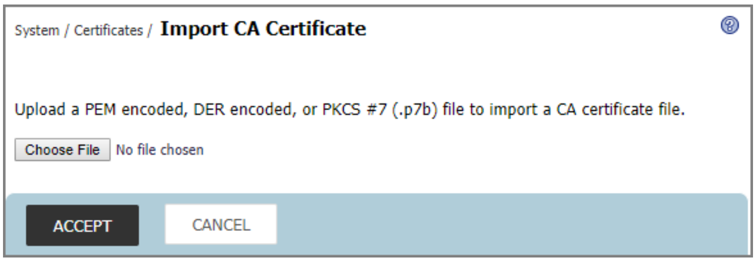
Adding Additional CA Certificates

You can import additional CA certificates for use with chained certificates, for example, when the issuing CA uses an intermediate (chained) signing certificate. To import a CA certificate file, upload a **PEM-encoded**, **DER-encoded**, or **PKCS #7** (**.p7b**) file.

To add additional certificates in PEM format:

1 Navigate to the **System > Certificates** page.

2 Under **Additional CA Certificates**, click **IMPORT CA CERTIFICATE** section. The **Import CA Certificate** dialog box is displayed.



System / Certificates / **Import CA Certificate**

Upload a PEM encoded, DER encoded, or PKCS #7 (.p7b) file to import a CA certificate file.

3 Click **Choose File**.

4 Locate the PEM-encoded, DER-encoded, or PKCS #7 CA certificate file on your disk or network drive and select it. Any filename is accepted.

5 Click **Upload**.

6 Click **ACCEPT**.

After the certificate has been uploaded, the CA certificate is displayed in the Additional CA Certificates list in the **System > Certificates** page.

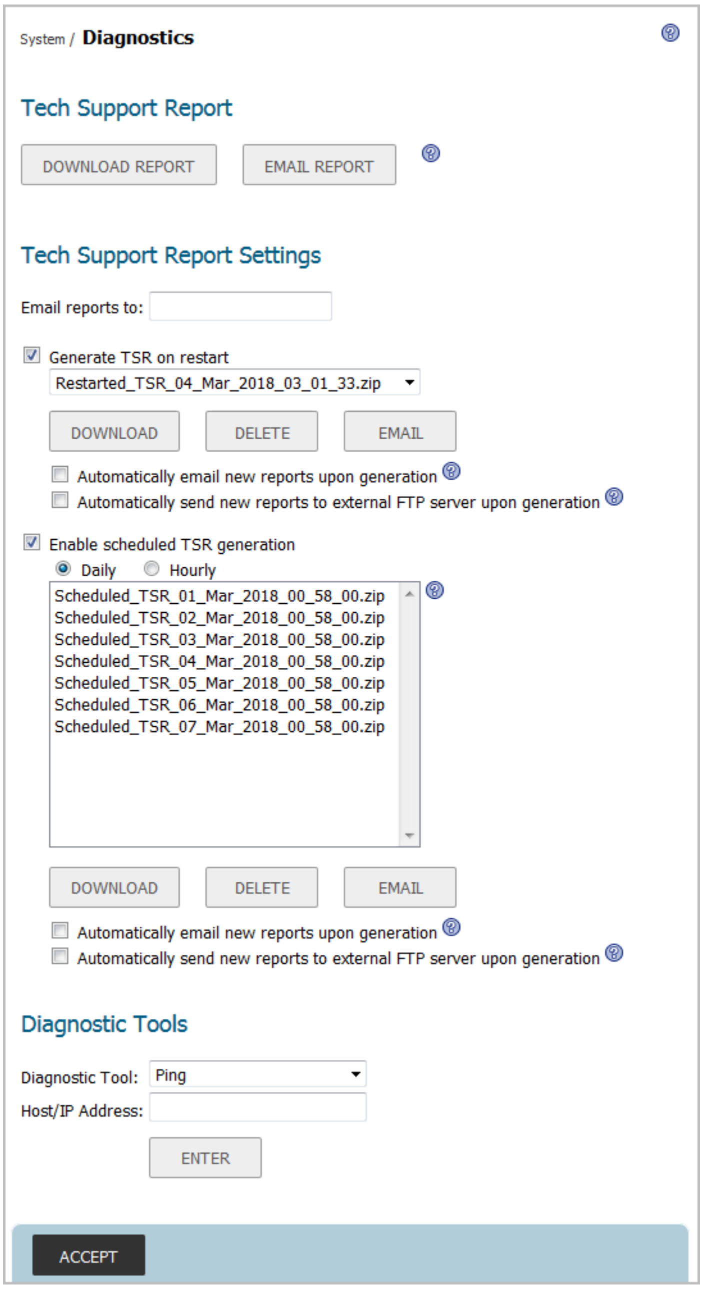
7 To add the new CA certificate to the web server’s active CA certificate list, the web server must be restarted. Restart the Web Application Firewall virtual appliance to restart the web server.

Using System Diagnostics

This section provides an overview of the **System > Diagnostics** page and a description of the configuration tasks available.

- System Diagnostics Overview on page 66
- Downloading & Generating the Tech Support Report on page 67
- Performing Diagnostic Tests on page 68

System > Diagnostics Page



System / **Diagnostics**

Tech Support Report

Tech Support Report Settings

Email reports to:

☑ Generate TSR on restart

Restarted_TSR_04_Mar_2018_03_01_33.zip

□ Automatically email new reports upon generation

□ Automatically send new reports to external FTP server upon generation

☑ Enable scheduled TSR generation

● Daily ○ Hourly

Scheduled_TSR_01_Mar_2018_00_58_00.zip
Scheduled_TSR_02_Mar_2018_00_58_00.zip
Scheduled_TSR_03_Mar_2018_00_58_00.zip
Scheduled_TSR_04_Mar_2018_00_58_00.zip
Scheduled_TSR_05_Mar_2018_00_58_00.zip
Scheduled_TSR_06_Mar_2018_00_58_00.zip
Scheduled_TSR_07_Mar_2018_00_58_00.zip

□ Automatically email new reports upon generation

□ Automatically send new reports to external FTP server upon generation

Diagnostic Tools

Diagnostic Tool: Ping

Host/IP Address:

System Diagnostics Overview

The **System > Diagnostics** page allows the administrator to download or email a tech support report and complete basic network diagnostics.

Options to automatically email the TSR or send the TSR to an external FTP server after a restart and upon generation are included. Configure the email settings or FTP server in the **System > Administration** page to automatically send the TSR to an external FTP server. See Configuring Email Settings on page 52 or Configuring an External FTP/TFTP Server on page 55 for more information.

Downloading & Generating the Tech Support Report

Downloading a Tech Support Report records system information and settings that are useful to SonicWall Technical Support when analyzing system behavior. The following options are available for Tech Support Reports:

- **DOWNLOAD REPORT**—Click this button and confirm the download in the popup dialog. Click **Save** to save the report. The Tech Support Report is saved as a .zip file, containing graphs, event logs and other technical information about your Web Application Firewall virtual appliance.
- **EMAIL REPORT—** Click to email the TSR report to the Email address specified in the **Email Reports to** field.
- **Generate TSR on restart**—Enable this option by selecting the check box. When enabled, the Web Application Firewall virtual appliance generates a new TSR upon every restart. The latest report generated from an appliance restart is available in the drop-down list, prefaced with “Restarted_TSR_.”
    - **DOWNLOAD**—This button allows you to download the latest Restarted Tech Support Report to your local system.
    - **DELETE**—This button allows you to delete the latest Restarted Tech Support Report.
    - **EMAIL**—Click this button to email the latest Restarted Tech Support Report to the values specified in the **Mail Server** field on the **System** > **Administration** page.
    - **Automatically email new reports upon generation**—Select this check box to enable automatic emailing of the latest Restarted Tech Support Report. You must specify the **Mail Server** and **Mail From Address** fields on the **System** > **Administration** page for automated email delivery.
    - **Automatically send new reports to external FTP server upon generation**—Select this check box to enable the latest Restarted Tech Support Report to be sent to the configured FTP server. You must specify the **FTP Server** fields on the **System** > **Administration** page for automated forwarding.
    - After selecting or clearing any check box, click **ACCEPT** to save your changes.
- **Enable scheduled TSR generation**—Select this check box to enable scheduled Tech Support Reports. After enabling, you can either have them generated **Hourly** or **Daily**. Note that a maximum of 12 TSRs are stored, with a total file size not exceeding 50 MB. Scheduled Tech Support Reports are mostly used for diagnostics or troubleshooting purposes by a SonicWall technician, if needed.
    - **DOWNLOAD**—This button allows you to download the latest scheduled Tech Support Reports to your local system.
    - **DELETE**—This button allows you to delete the latest scheduled Tech Support Reports.
    - **EMAIL**—Click this button to email the latest scheduled Tech Support Reports to the values specified in the **Mail Server** field on the **Log** > **Settings** page.
    - **Automatically email new reports upon generation**—Select this check box to enable automatic emailing of the latest scheduled Tech Support Reports. You must specify the **Mail Server** and **Mail From Address** fields on the **System** > **Administration** page for automated email delivery.
    - **Automatically send new reports to external FTP server upon generation**—Select this check box to enable the latest scheduled Tech Support Reports to be sent to the configured FTP server. You must specify the **FTP Server** fields on the **System** > **Administration** page for automated forwarding.
    - After selecting or clearing any check box, click **ACCEPT** to save your changes.

Enabling Scheduled TSR Generation

To enable scheduled Tech Support Reports:

1. Go to **System > Diagnostics**.
2. Click **Enable scheduled TSR generation**.
3. Then enter https://<WAFv Hostname>:8443/cgi-bin/diag in the URL field of your browser.

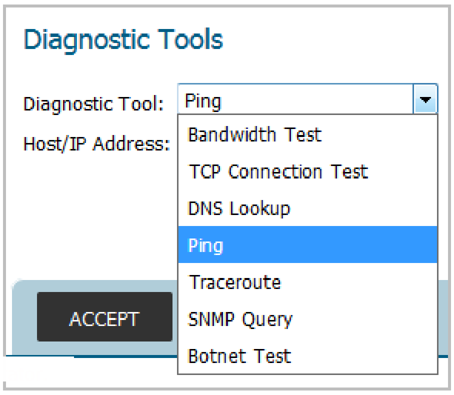
Performing Diagnostic Tests

Diagnostic tools allows the administrator to test Web Application Firewall connectivity by performing a ping, TCP connection test, DNS lookup, Traceroute, or botnet test for a specific IP address or web site. You can also do a bandwidth test between the Web Application Firewall virtual appliance and your local computer, or do an SNMP query to display information about the virtual appliance.

You can do these diagnostic tests on the Web Application Firewall virtual appliance in the **System > Diagnostics** page.

To run a diagnostic test:

1. Navigate to the **System** > **Diagnostics** page.
2. In the **Diagnostic Tool** drop-down list, select **Bandwidth Test**, **TCP Connection Test**, **DNS Lookup**, **Ping**, **Traceroute**, **SNMP Query**, or **Botnet Test**.



The Diagnostic Tools table describes the diagnostic tools and their functions.

Diagnostic Tools

Diagnostic Tool	Function
Bandwidth Test	Measures the upload and download speed of the network connection between your computer and the Web Application Firewall virtual appliance.
TCP Connection Test	Tests the connectivity of a port that is specified by appending a colon and port number to the host name or IP address (for example, 10.9.9.19:83 or www.myhost.com:83. If no port is specified, port 80 is tested.
DNS Lookup	Translates a DNS name to an IP address and vice versa.
Ping	Tests the connection to a host or IP address.
Traceroute	Identifies the route and number of hops needed to connect to a host or IP address.

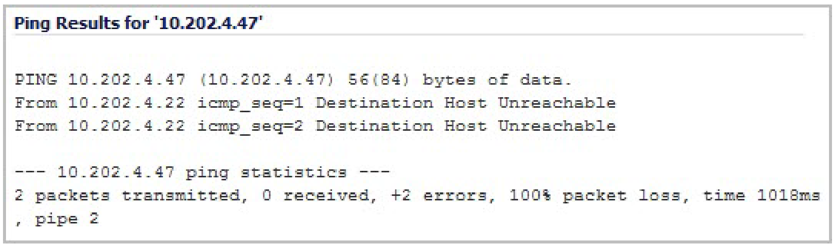
Diagnostic Tools

Diagnostic Tool	Function
SNMP Query	Looks up SNMP information from the selected MIB. SNMP must be enabled (**System > Administration** page) before a query can be completed. In the **SNMP MIB** drop-down list, select the MIB for which to display the values.
Botnet Test	Identifies whether an IP address is a Botnet IP address.

3 If prompted for additional information like a **Host** or **IP Address**, type in the requested information.

4 Click **ENTER**.

The results display at the bottom of the page.



Ping Results for '10.202.4.47'

```
PING 10.202.4.47 (10.202.4.47) 56(84) bytes of data.
From 10.202.4.22 icmp_seq=1 Destination Host Unreachable
From 10.202.4.22 icmp_seq=2 Destination Host Unreachable

--- 10.202.4.47 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1018ms
, pipe 2
```

Restarting the System

The **System > Restart** page allows the administrator to restart the Web Application Firewall virtual appliance. Restarting takes one or two minutes and causes all current users to be disconnected.

To restart the Web Application Firewall virtual appliance:

1 Navigate to **System > Restart**.

2 Click **RESTART**.

3 In the confirmation dialog box, click **OK**.

Using the System About Page

The **System** > **About** page provides the **End-User Product Agreement** for using the Web Application Firewall virtual appliance. For more information regarding the End-User Product Agreement, refer to https://www.sonicwall.com/legal/.

Click **DOWNLOAD** to download a copy of the SonicWall WAF copyright Information.

Links to the SonicWall Support page and the SonicWall Blog and Community page are provided at the bottom of the **System** > **About** page.

4

Network Configuration

This section provides information and configuration tasks specific to the **Network** pages in the SonicWall Web Application Firewall management interface.

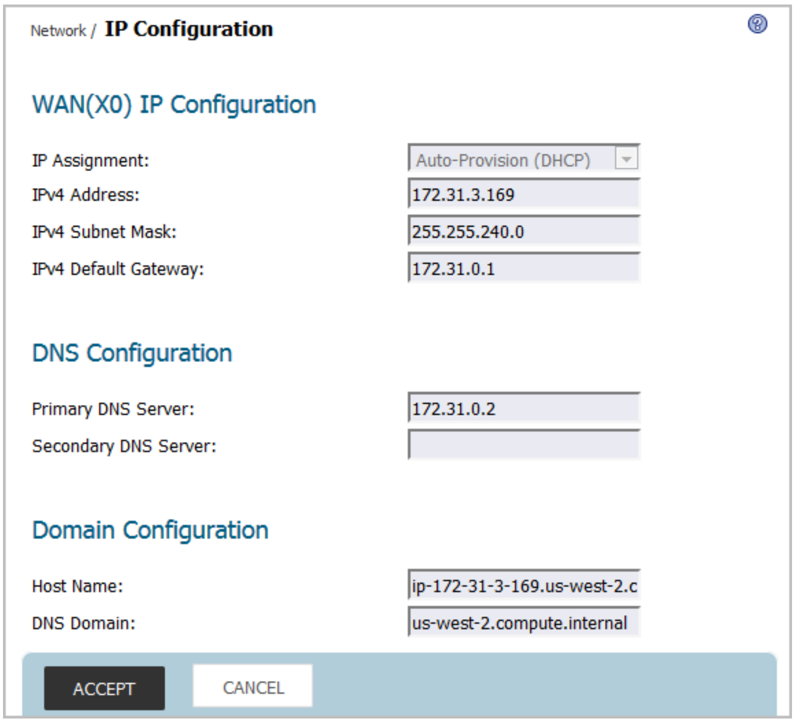
Topics:

- IP Configuration Settings on page 71
- Advanced Configuration Settings on page 73

IP Configuration Settings

The **Network > IP Configuration** page provides settings for WAN, DNS, and domain configuration.

Network > IP Configuration Page



Network / **IP Configuration**

WAN(X0) IP Configuration

IP Assignment:	Auto-Provision (DHCP)
IPv4 Address:	172.31.3.169
IPv4 Subnet Mask:	255.255.240.0
IPv4 Default Gateway:	172.31.0.1

DNS Configuration

Primary DNS Server:	172.31.0.2
Secondary DNS Server:	

Domain Configuration

Host Name:	ip-172-31-3-169.us-west-2.c
DNS Domain:	us-west-2.compute.internal

Topics:

- Configuring the WAN IP on page 72
- Configuring DNS on page 72
- Configuring the Domain on page 73

Configuring the WAN IP

To configure the WAN IP Configuration settings:

1. Navigate to the **Network > IP Configuration** page.

   Under **WAN(X0) IP Configuration**, the **IP Assignment** field is set to **Auto-Provision (DHCP)** by default for AWS and MS Azure deployments and cannot be changed. On ESXi and MS Hyper-V deployments, the default setting is **Static**, but you can change it to **Auto-Provision (DHCP)**.

   If **Static** is selected, then the other fields are editable.

2. For **IPv4 Address**, type in the IPv4 address for the WAN (X0) interface of your Web Application Firewall virtual appliance.
3. For **IPv4 Subnet Mask**, type in the IPv4 subnet mask, such as 255.255.255.0, for the WAN (X0) interface of your Web Application Firewall virtual appliance.
4. For **IPv4 Default Gateway**, type in the IPv4 default gateway address for the WAN (X0) interface of your Web Application Firewall virtual appliance.
5. Click **ACCEPT** to save your changes.

   WAF validates that the **IPv4 Default Gateway** is reachable, and displays the error message “Unable to reach IPv4 Default Gateway” under the field, if not.

   WAF automatically redirects to the new IP address if **IP Assignment** is changed from **Auto-Provision (DHCP)** to **Static** or if **IPv4 Address** or **IPv4 Subnet Mask** were changed.

   If WAF fails to get an IP address when **IP Assignment** is changed from **Static** to **Auto-Provision (DHCP)**, WAF restarts and recovers to the previous static IP configuration settings.

   If **IP Assignment** is **Auto-Provision (DHCP)** and System Time is manually changed, WAF services are restarted.

Configuring DNS

To configure the DNS Configuration settings:

1. Navigate to the **Network > IP Configuration** page.
2. Under **DNS Configuration**, in the **Primary DNS Server** field, type in the main DNS server IP address for your Web Application Firewall virtual appliance.
3. In the **Secondary DNS Server** field, optionally type in the secondary DNS server IP address for your Web Application Firewall virtual appliance.
4. Click **ACCEPT** to save your changes.

   When DNS settings are changed, WAF validates that MySonicWall and the SonicWall License Manager are reachable. If not, a confirmation dialog allows you to continue with the settings or cancel the change.

Configuring the Domain

To configure the Domain Configuration settings:

1. Navigate to the **Network > IP Configuration** page.
2. Under **Domain Configuration**, in the **Host Name** field, type in the host name for your Web Application Firewall virtual appliance.
3. In the **DNS Domain** field, type in the domain name for your Web Application Firewall virtual appliance.
4. Click **ACCEPT** to save your changes.

Advanced Configuration Settings

The **Network > Advanced Configuration** page provides more network settings on three screens: **Interfaces**, **Host Resolution**, and **Routes**.

Topics:

- Configuring Advanced Interface Settings on page 73
- Configuring Host Resolution Settings on page 74
- Configuring Network Routes on page 75

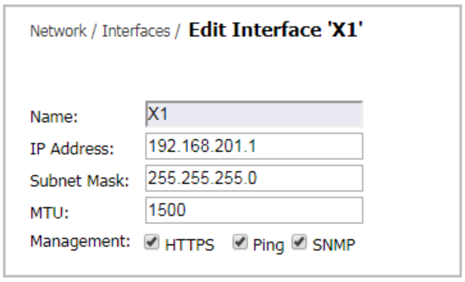
Configuring Advanced Interface Settings

You can configure the maximum transmission unit (MTU) size and management access settings, as well as changing the basic interface settings, on the **Interfaces** screen.

ⓘ **NOTE:** Use the **Network > IP Configuration** page to configure initial interface settings. See Configuring the WAN IP on page 72.

To configure advanced interface settings:

1. Navigate to the **Interfaces** screen on the **Network > Advanced Configuration** page.
2. In the table in the **Interfaces** section, click the edit icon in the **Configure** column of the row containing the interface you want to edit. The Edit Interface dialog is displayed.



Network / Interfaces / **Edit Interface 'X1'**

Name: X1
IP Address: 192.168.201.1
Subnet Mask: 255.255.255.0
MTU: 1500
Management: ☑ HTTPS ☑ Ping ☑ SNMP

The X0 interface is not editable here, but can be configured on the **Network > IP Configuration** page.

3. Make any changes needed to the basic interface settings fields, including **Name**, **IP Address**, and **Subnet Mask**.

4 In the **MTU** field, type in the maximum transmission unit size in bytes. This is the maximum packet size that Web Application Firewall will send on this interface.

5 For **Management**, select the checkboxes for the allowed types of management access to Web Application Firewall on this interface:

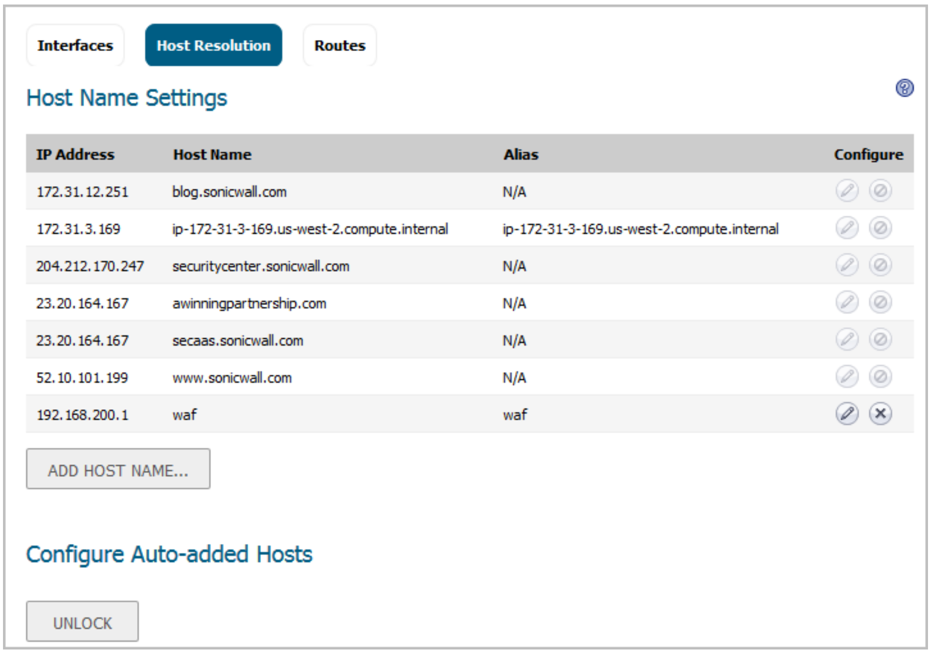
- **HTTPS** – to allow management access from a browser
- **Ping** – to respond to pings
- **SNMP** – to allow SNMP access

6 Click **ACCEPT** to save your changes.

Configuring Host Resolution Settings

The **Host Resolution** screen displays the mapping between IP addresses and host names in the same network as Web Application Firewall. You can add settings for a host or edit existing settings for your configured hosts. Some hosts are automatically added by the system, and these are not configurable unless you click the **UNLOCK** button.

Host Resolution Screen



IP Address	Host Name	Alias	Configure
172.31.12.251	blog.sonicwall.com	N/A	✎ ⊘
172.31.3.169	ip-172-31-3-169.us-west-2.compute.internal	ip-172-31-3-169.us-west-2.compute.internal	✎ ⊘
204.212.170.247	securitycenter.sonicwall.com	N/A	✎ ⊘
23.20.164.167	awinningpartnership.com	N/A	✎ ⊘
23.20.164.167	secaas.sonicwall.com	N/A	✎ ⊘
52.10.101.199	www.sonicwall.com	N/A	✎ ⊘
192.168.200.1	waf	waf	✎ ✕

Adding or Editing Host Name Settings

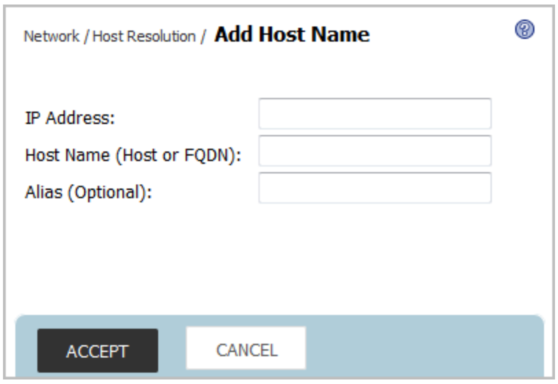
To add or edit settings for a host:

1 Navigate to the **Host Resolution** screen on the **Network > Advanced Configuration** page.

2 Do one of the following:

- Click **ADD HOST NAME** to add a host.
- Click the edit icon in the Configure column of a host entry you want to edit.

The **Add Host Name** or **Edit Host Name** dialog opens. Both dialogs have the same options.



Network / Host Resolution / **Add Host Name**

IP Address:

Host Name (Host or FQDN):

Alias (Optional):

3 In the **IP Address** field, type in or edit the IP address of the host.

4 In the **Host Name (Host or FQDN)** field, type in or edit the host name or fully qualified domain name of the host.

5 In the **Alias (Optional)** field, optionally enter a descriptive name for the host.

6 Click **ACCEPT** to save your changes.

Configuring Auto-Added Hosts

The Host Resolution screen typically displays several entries for hosts that have been automatically added by the system. Normally, these do not display an edit button in the **Configuration** column.

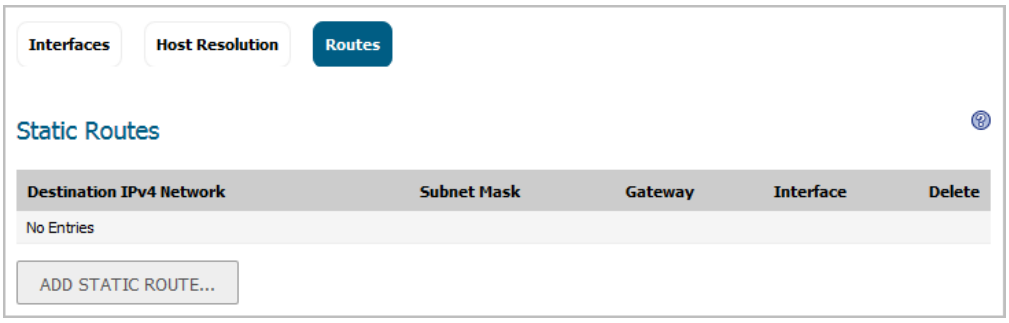
You can make changes to these entries by clicking the **UNLOCK** button under **Configure Auto-added Hosts** in the **Network > Advanced Configuration** page.

This is not recommended, as it could lead to bad host configuration.

Configuring Network Routes

The **Routes** screen on the **Network > Advanced Configuration** page lists any static routes, including the destination network, subnet mask, gateway, and interface settings. You can add a static route or delete an existing route.

Routes Screen

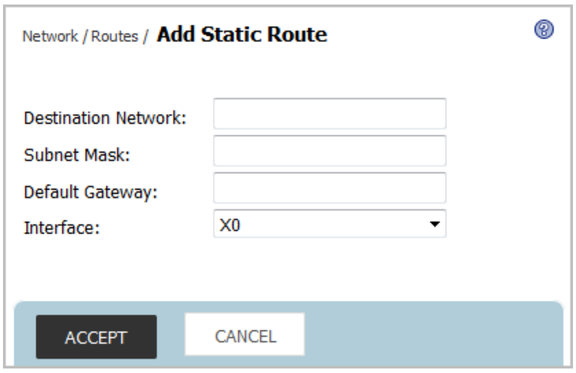


Static Routes

Destination IPv4 Network	Subnet Mask	Gateway	Interface	Delete
No Entries				

To add a static route:

1. Navigate to the **Routes** screen on the **Network > Advanced Configuration** page.
2. Click the **ADD STATIC ROUTE** button. The **Add Static Route** dialog opens.



Network / Routes / **Add Static Route**

Destination Network:	
Subnet Mask:	
Default Gateway:	
Interface:	X0

3. In the **Destination Network** field, type in the IPv4 network address. It should not be a host address, but should only contain the network portion of the address.
4. In the **Subnet Mask** field, enter the mask for the destination network, such as 255.255.255.0.
5. In the **Default Gateway** field, enter the IP address of the default gateway for the destination network.
6. In the **Interface** field, select the Web Application Firewall interface from which traffic is sent when sending to the destination network.
7. Click **ACCEPT** to save your changes.

To delete a static route:

1. On the **Routes** screen on the **Network > Advanced Configuration** page, click the delete icon in the **Delete** column for the route you want to delete.
2. Click **OK** in the confirmation dialog.

5

Application Delivery Configuration

This section provides information and configuration tasks specific to the **Application Delivery** pages in the SonicWall Web Application Firewall management interface.

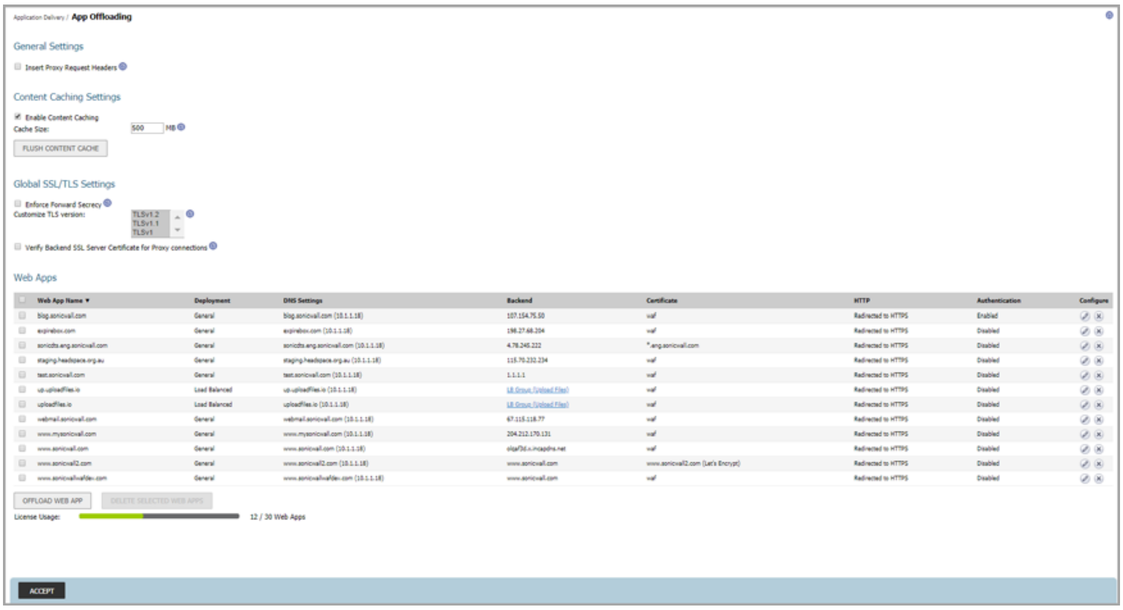
Topics:

- Configuring App Offloading on page 77
- Configuring Load Balancing on page 97

Configuring App Offloading

The **Application Delivery > App Offloading** page provides settings related to web applications, including proxy request headers, content caching, encryption, and offloading web applications.

App Offloading Page



Application Delivery / **App Offloading**

General Settings

☐ Insert Proxy Request Headers

Content Caching Settings

☑ Enable Content Caching

Cache Size: 500 MB

Global SSL/TLS Settings

☐ Enforce Forward Secrecy

Customize TLS version: TLSv1.2 TLSv1.1 TLSv1

☐ Verify Backend SSL Server Certificate for Proxy connections

Web Apps

☐	Web App Name ▾	Deployment	DNS Settings	Backend	Certificate	HTTP	Authentication	Configure
☐	blog.sonicwall.com	General	blog.sonicwall.com (10.1.1.18)	107.154.75.50	waf	Redirected to HTTPS	Enabled	✎ ✕
☐	expirebox.com	General	expirebox.com (10.1.1.18)	198.27.68.204	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	sonicdts.eng.sonicwall.com	General	sonicdts.eng.sonicwall.com (10.1.1.18)	4.78.245.222	*.eng.sonicwall.com	Redirected to HTTPS	Disabled	✎ ✕
☐	staging.headspace.org.au	General	staging.headspace.org.au (10.1.1.18)	115.70.232.234	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	test.sonicwall.com	General	test.sonicwall.com (10.1.1.18)	1.1.1.1	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	up-uploadfiles.io	Load Balanced	up-uploadfiles.io (10.1.1.18)	LB Group (Upload Files)	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	uploadfiles.io	Load Balanced	uploadfiles.io (10.1.1.18)	LB Group (Upload Files)	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	webmail.sonicwall.com	General	webmail.sonicwall.com (10.1.1.18)	67.115.118.77	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	www.mysonicwall.com	General	www.mysonicwall.com (10.1.1.18)	204.212.170.131	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	www.sonicwall.com	General	www.sonicwall.com (10.1.1.18)	olga/3d.x.incapdns.net	waf	Redirected to HTTPS	Disabled	✎ ✕
☐	www.sonicwall2.com	General	www.sonicwall2.com (10.1.1.18)	www.sonicwall.com	www.sonicwall2.com (Let's Encrypt)	Redirected to HTTPS	Disabled	✎ ✕
☐	www.sonicwallwafdev.com	General	www.sonicwallwafdev.com (10.1.1.18)	www.sonicwall.com	waf	Redirected to HTTPS	Disabled	✎ ✕

License Usage: 12 / 30 Web Apps

Topics:

- App Offloading Overview on page 78
- Configuring General Settings on page 78
- Configuring Content Caching Settings on page 79
- Configuring Global SSL/TLS Settings on page 79
- Configuring Offloaded Web Apps on page 79

App Offloading Overview

Application offloading provides secure access to both internal and publicly hosted web applications. An application offloading web app is configured with an associated virtual host acting as a proxy for the backend web application.

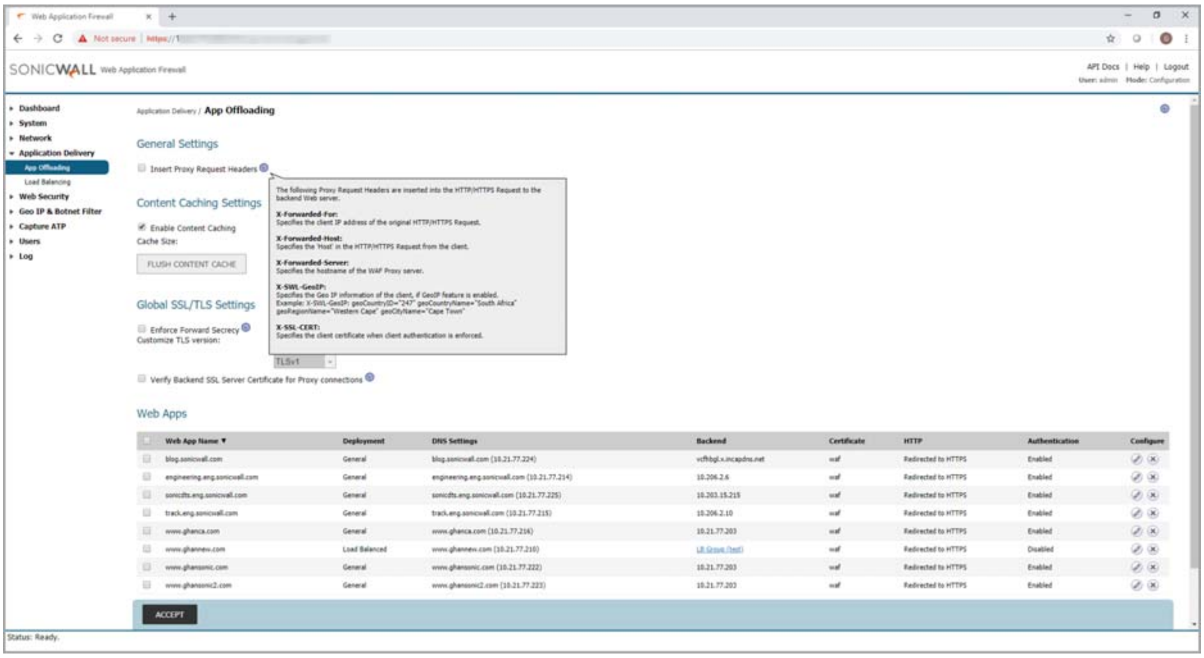
The administrator can enforce strong authentication and access policies for specific users or groups. For instance, in an organization certain guest users might need Two-factor or Client Certificate authentication to access Outlook Web Access (OWA), but are not allowed to access OWA public folders. If authentication is enabled, multiple layers of advanced authentication features such as One Time Password, Client Certificate Authentication and Single Sign-On can be applied on top of each other for the offloaded web app.

The web app must be configured with a virtual host and a suitable domain. It is possible to disable authentication and access policy enforcement for such an offloaded web app.

Web transactions can be centrally monitored by viewing the logs. In addition, Web Application Firewall can protect these web apps from any unexpected intrusion, such as cross-site scripting or SQL injection.

Configuring General Settings

The **General Settings** section of the **Application Delivery > App Offloading** page provides the **Insert Proxy Request Headers** option.



General Settings

□ Insert Proxy Request Headers

The following Proxy Request Headers are inserted into the HTTP/HTTPS Request to the backend Web server.

X-Forwarded-For:
Specifies the client IP address of the original HTTP/HTTPS Request.

X-Forwarded-Host:
Specifies the 'Host' in the HTTP/HTTPS Request from the client.

X-Forwarded-Server:
Specifies the hostname of the WAF Proxy server.

X-SWL-GeoIP:
Specifies the Geo IP information of the client, if GeoIP feature is enabled.
Example: X-SWL-GeoIP: geoCountryID="247" geoCountryName="South Africa" geoRegionName="Western Cape" geoCityName="Cape Town"

X-SSL-CERT:
Specifies the client certificate when client authentication is enforced.

Content Caching Settings

☑ Enable Content Caching
Cache Size:

Global SSL/TLS Settings

□ Enforce Forward Secrecy
Customize TLS version: TLSv1

□ Verify Backend SSL Server Certificate for Proxy connections

Web Apps

□	Web App Name ▼	Deployment	DNS Settings	Backend	Certificate	HTTP	Authentication	Configure
□	blog.sonicwall.com	General	blog.sonicwall.com (10.21.77.224)	vcfhbgl.x.incapdns.net	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	engineering.eng.sonicwall.com	General	engineering.eng.sonicwall.com (10.21.77.214)	10.206.2.6	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	sonicdts.eng.sonicwall.com	General	sonicdts.eng.sonicwall.com (10.21.77.225)	10.203.15.215	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	track.eng.sonicwall.com	General	track.eng.sonicwall.com (10.21.77.215)	10.206.2.10	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	www.ghanca.com	General	www.ghanca.com (10.21.77.216)	10.21.77.203	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	www.ghannew.com	Load Balanced	www.ghannew.com (10.21.77.210)	LB Group (test)	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	www.ghansonic.com	General	www.ghansonic.com (10.21.77.222)	10.21.77.203	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	www.ghansonic2.com	General	www.ghansonic2.com (10.21.77.223)	10.21.77.203	waf	Redirected to HTTPS	Enabled	✎ ⊗

Select the **Insert Proxy Request Headers** checkbox to insert the following types of headers into the HTTP/HTTPS requests to the backend web server:

- **X-Forwarded-For** – Specifies the client IP address of the original HTTP/HTTPS request.
- **X-Forwarded-Host** – Specifies the “Host” in the HTTP/HTTPS request from the client.
- **X-Forwarded-Server** – Specifies the host name of the web app.
- **X-SWL-GeoIP** – Specifies the Geo IP information of the client, if GeoIP feature is inabled. Example: X-SWL-GeoIP: geoCountryID=″247″ geoCountryName=″SouthAfrica″ geoRegionName=″Western Cape″ geoCityName=″CapeTown″
- **X-SSL-CERT** – Specifies the client certificate when client authentication is enforced.

To enable insertion of proxy request headers:

1 Navigate to the **Application Delivery > App Offloading** page.

2 Select the **Insert Proxy Request Headers** checkbox.

3 Click **ACCEPT** to save your changes.

Configuring Content Caching Settings

The **Content Caching Settings** section of the **Application Delivery > App Offloading** page provides the **Enable Content Caching** and **Cache Size** options, and provides a button to flush the content cache.

To configure settings or flush the cache:

1 Navigate to the **Application Delivery > App Offloading** page.

2 **Enable Content Caching** is selected by default. You can disable it by clearing the checkbox. Note that changing the **Enable Content Cache** setting restarts Web Application Firewall services, including the web server.

3 In the **Cache Size** field, define the size of the content cache. The default size is 500 MB, the minimum is 100 MB, and the maximum is 2048 MB.

4 To flush the content cache, click the **FLUSH CONTENT CACHE** button.

5 Click **ACCEPT** to save your changes.

Configuring Global SSL/TLS Settings

The **Global SSL/TLS Settings** section of the **Application Delivery > App Offloading** page provides options for configuring Secure Sockets Layer (SSL) and Transport Layer Security (TLS) settings globally.

To configure the global SSL/TLS settings:

1 Navigate to the **Application Delivery > App Offloading** page.

2 Select the **Enforce Forward Secrecy** checkbox to allow current information to be kept secret, even if the private key is compromised in the future. Some older browsers that do not support Forward Secrecy might not be able to connect to the Web Application Firewall virtual appliance. The performance of this feature can decline depending on the ciphers that the client browser supports.

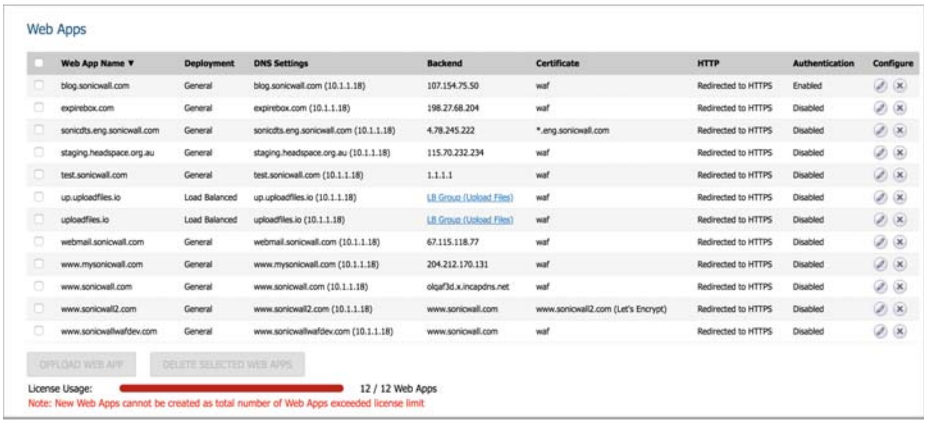
3 In the **Customize TLS version** drop-down list, select the TLS version that is supported by the web server. The default is TLSv1.2 and TLSv1.1, but this option provides a way to change it due to special security reasons. The selected TLS version is used for communication between clients and the web server.

4 Select the **Verify Backend SSL Server Certificate for Proxy connections** checkbox to drop the connection if the backend SSL/TLS server certificate is not trusted. The verification depth is 10. Alert level log messages are also generated when this option is enabled.

5 Click **ACCEPT** to save your changes.

Configuring Offloaded Web Apps

The **Web Apps** section of the **Application Delivery > App Offloading** page displays the list of currently offloaded web applications protected by SonicWall WAF. The table shows the web app name, the type of deployment, DNS settings, the backend IP address of the web app, the web app’s certificate name, HTTP information such as redirection to HTTPS, and whether or not authentication is enabled for the web app. The **Configure** column provides edit and delete buttons for each offloaded web app. The color-coded **License Usage** progress bar visually displays the number of available licenses. If the number of web apps exceeds the license limit, the **OFFLOAD WEB APP** feature is disabled and a message will appear under the progress bar indicating the number of web apps exceeds the license limit and no new apps can be created.



Web Apps

□	Web App Name ▼	Deployment	DNS Settings	Backend	Certificate	HTTP	Authentication	Configure
□	blog.sonicwall.com	General	blog.sonicwall.com (10.1.1.18)	107.154.75.50	waf	Redirected to HTTPS	Enabled	✎ ⊗
□	expirebox.com	General	expirebox.com (10.1.1.18)	198.27.68.204	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	sonicdts.eng.sonicwall.com	General	sonicdts.eng.sonicwall.com (10.1.1.18)	4.78.245.222	*.eng.sonicwall.com	Redirected to HTTPS	Disabled	✎ ⊗
□	staging.headspace.org.au	General	staging.headspace.org.au (10.1.1.18)	115.70.232.234	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	test.sonicwall.com	General	test.sonicwall.com (10.1.1.18)	1.1.1.1	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	up.uploadfiles.io	Load Balanced	up.uploadfiles.io (10.1.1.18)	LB Group (Upload Files)	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	uploadfiles.io	Load Balanced	uploadfiles.io (10.1.1.18)	LB Group (Upload Files)	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	webmail.sonicwall.com	General	webmail.sonicwall.com (10.1.1.18)	67.115.118.77	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	www.mysonicwall.com	General	www.mysonicwall.com (10.1.1.18)	204.212.170.131	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	www.sonicwall.com	General	www.sonicwall.com (10.1.1.18)	olqaf3d.x.incapdns.net	waf	Redirected to HTTPS	Disabled	✎ ⊗
□	www.sonicwall2.com	General	www.sonicwall2.com (10.1.1.18)	www.sonicwall.com	www.sonicwall2.com (Let's Encrypt)	Redirected to HTTPS	Disabled	✎ ⊗
□	www.sonicwallwafdev.com	General	www.sonicwallwafdev.com (10.1.1.18)	www.sonicwall.com	waf	Redirected to HTTPS	Disabled	✎ ⊗

License Usage: 12 / 12 Web Apps

Note: New Web Apps cannot be created as total number of Web Apps exceeded license limit

The progress bar will turn green, yellow, orange and red as the number of available licenses goes down.

> **NOTE:** If 30-day data usage exceeds the limit on any day, the license progress bar shows the usage has exceeded the 30-day limit and a log alert indicates 30-day data usage exceeds the 30-day data limit. Please contact SonicWall to review your licenses.

> **NOTE:** If data usage exceeds the limit for 5 consecutive days, the WAF security service becomes disabled and the website is unprotected until the 30-day usage is within the 30-day licensed limit. The licenses progress bar on the Dashboard page also shows that the 30-day data usage has exceeded the 30-day data limit. A log alert indicates that the WAF service has been disabled due to data usage exceeding the license limits. Please contact SonicWall for assistance.

Topics:

- Adding an Offloaded Web App on page 80
- Editing an Offloaded Web App on page 84
- Deleting an Offloaded Web App on page 93

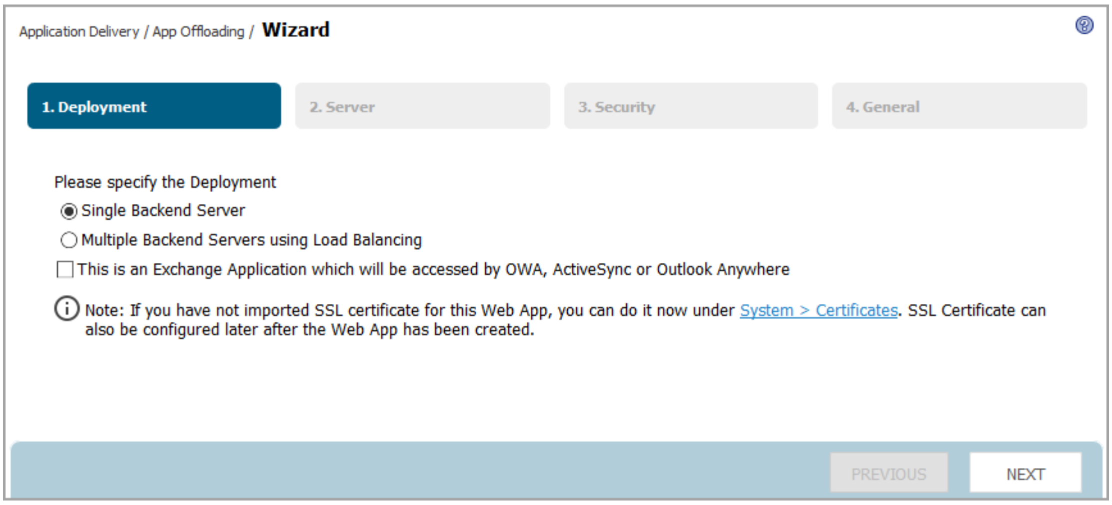
Adding an Offloaded Web App

The **OFFLOAD WEB APP** button launches a wizard that provides detailed tooltips to assist you in configuring the offloaded web app.

To add an offloaded web app:

1 Navigate to the **Application Delivery > App Offloading** page.

2 Click the **OFFLOAD WEB APP** button below the **Web Apps** table. The first screen of the wizard is displayed.



Application Delivery / App Offloading / **Wizard**

Please specify the Deployment

● Single Backend Server

○ Multiple Backend Servers using Load Balancing

□ This is an Exchange Application which will be accessed by OWA, ActiveSync or Outlook Anywhere

Note: If you have not imported SSL certificate for this Web App, you can do it now under System > Certificates. SSL Certificate can also be configured later after the Web App has been created.

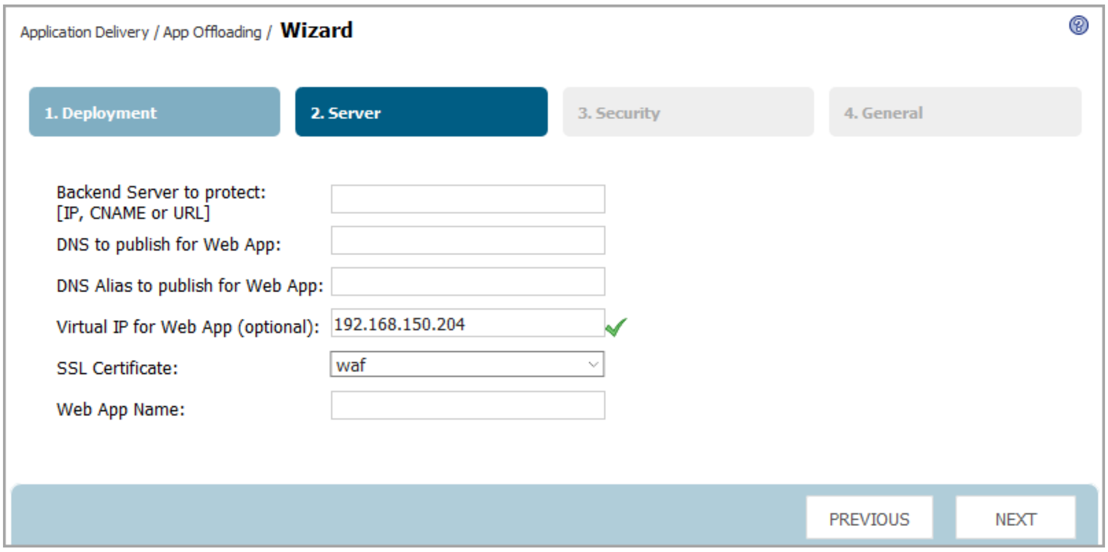
3 In the **1. Deployment** screen, select the type of deployment:

- **Single Backend Server** – Choose this option when you have only one backend server or a resource to protect. This deployment type is displayed as ***General*** in the **Web Apps** table on the **Application Delivery > App Offloading** page.
- **Multiple Backend Servers using Load Balancing** – Choose this option when your backend web application is hosted as a cluster of web servers. WAF can be additionally be used as an application load balancer. A Load Balancing Group needs to be created ahead of time from the **Application Delivery > Load Balancing** page. This deployment type is displayed as ***Load Balancing*** in the **Web Apps** table on the **Application Delivery > App Offloading** page.

4 Select the **This is an Exchange Application which will be accessed by OWA, ActiveSync or Outlook Anywhere** check box if the offloaded application will be accessed in this way. SonicWall WAF will proxy the authentication performed by ActiveSync or Outlook Anywhere, but will not require separate authentication. For OWA, WAF will enforce a second layer of authentication.

5 Optionally click the **System > Certificates** link in the Note to jump to that page and import the SSL certificate for this web app.

6 Click **NEXT**. The second screen of the wizard is displayed.



Application Delivery / App Offloading / **Wizard**

Backend Server to protect: [IP, CNAME or URL]:

DNS to publish for Web App:

DNS Alias to publish for Web App:

Virtual IP for Web App (optional): 192.168.150.204

SSL Certificate: waf

Web App Name:

7 In the **2. Server** screen in the **Backend Server to protect** field, type in one of:

- ***IP address*** of the backend server where the web app is hosted, such as ***192.168.200.101***
- ***CNAME*** of the backend server where the web app is hosted, such as ***elb-mail.company.com***
- ***URL*** of the backend server where the web app is hosted, such as ***https://elb-mail.company.com:8443/owa***
- ***Virtual IP address*** or ***CNAME record*** of the load balancer, if the web app is load balanced by multiple backend servers

> **NOTE:** WAF resolves the FQDN of the backend server dynamically with DNS caching enabled. This allows ongoing access to the web app even if its public IP address changes.

8 In the **DNS to publish for Web App** field, type in the DNS name that users can use to access the web app.

> **NOTE:** Once the web app is configured, publish a DNS record so users are redirected to the WAF for protection. The DNS name and DNS alias should resolve to the web app's public IP address.

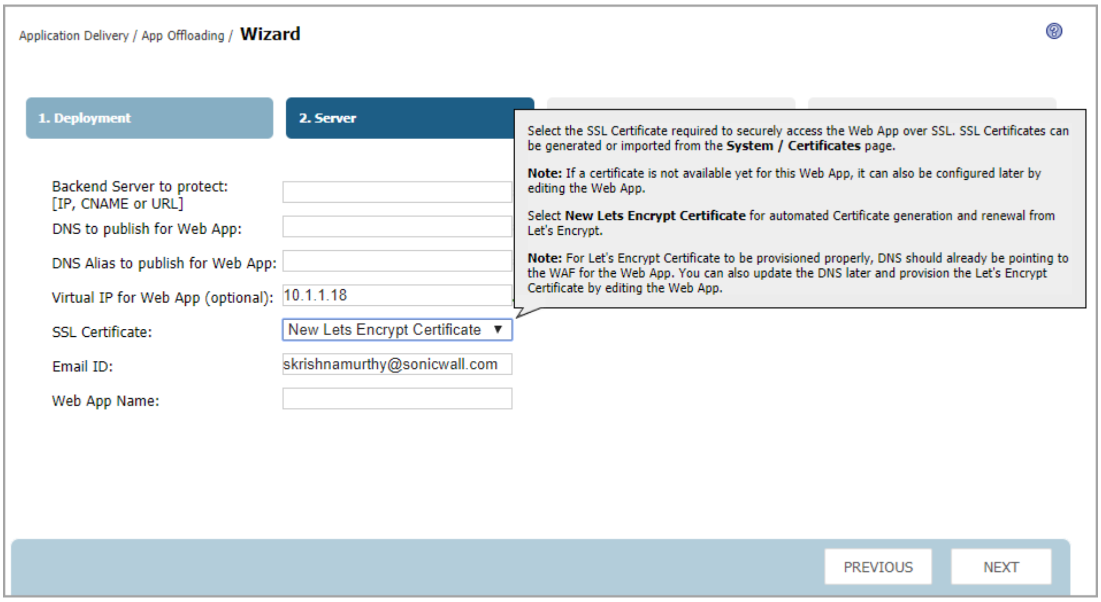
9 In the **DNS Alias to publish for Web App** field, optionally type in the DNS alias that users can use to access the web app. The DNS Alias provides another way to access the web app, and is mapped to the DNS name.

> **NOTE:** Once the web app is configured, publish a DNS record so users are redirected to the WAF for protection. The DNS name and DNS alias should resolve to the web app's public IP address.

10 In the **Virtual IP for Web App** field, optionally type in the virtual IP address for the web app. You can specify a custom port, if desired, such as in ***192.168.201.100:444***. Multiple web apps can be configured using the same virtual IP address.

When using this field, a DNS record should be published to resolve the DNS name and alias to this virtual IP address rather than to the WAF's WAN IP address.

11 For **SSL Certificate**, select the applicable certificate from the drop-down list. The default is the self-signed certificate listed on the **System > Certificates** page.



Backend Server to protect: [IP, CNAME or URL]

DNS to publish for Web App:

DNS Alias to publish for Web App:

Virtual IP for Web App (optional): 10.1.1.18

SSL Certificate: New Lets Encrypt Certificate ▼

Email ID: skrishnamurthy@sonicwall.com

Web App Name:

Select the SSL Certificate required to securely access the Web App over SSL. SSL Certificates can be generated or imported from the **System / Certificates** page.

Note: If a certificate is not available yet for this Web App, it can also be configured later by editing the Web App.

Select **New Lets Encrypt Certificate** for automated Certificate generation and renewal from Let's Encrypt.

Note: For Let's Encrypt Certificate to be provisioned properly, DNS should already be pointing to the WAF for the Web App. You can also update the DNS later and provision the Let's Encrypt Certificate by editing the Web App.

You can generate or import SSL certificates on the **System > Certificates** page. If a certificate is not yet available for this web app, you can configure it later by editing the web app from the **Web Apps** table.

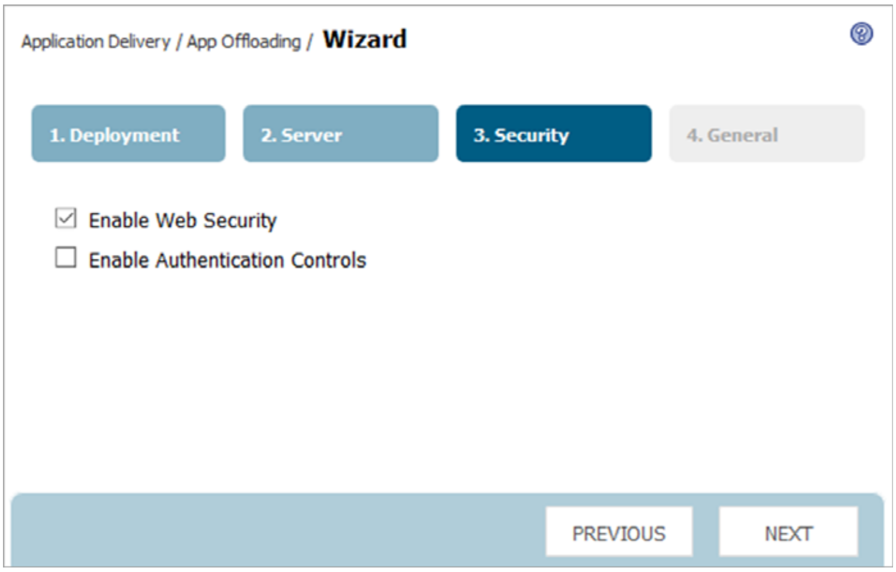
For automated certificate generation and renewal from Let's Encrypt, select **New Let's Encrypt Certificate** from the drop-down menu. Let's Encrypt certificates are valid for 90 days and can be managed from the **System > Certificates** page. WAF has a scheduled task for automatic renewal of Let's Encrypt certificates, which runs every Monday at midnight. If any Let’s Encrypt certificates are nearing the expiration date, those certificates are automatically renewed. Let’s Encrypt success and error messages are logged. If the Let's Encrypt option was not selected at the time of web app creation, you can edit the web app to select it. This generates a Let's Encrypt certificate for an existing web app.

ⓘ **NOTE:** For Let’s Encrypt to work, the domain name must be registered and DNS must be updated to direct the requests through WAF.

If the domain name is not registered already and you attempt to create a Let's Encrypt certificate, the web app creation succeeds using the WAF default certificate and provides a detailed error message. If Let's Encrypt certificate generation fails for some reason, web app creation succeeds using the default certificate and provides an appropriate message.

12 Type a friendly name for the application into the **Web App Name** field.

13 Click **NEXT**. The third screen of the wizard is displayed.


Application Delivery / App Offloading / **Wizard**

1. Deployment | 2. Server | 3. Security | 4. General

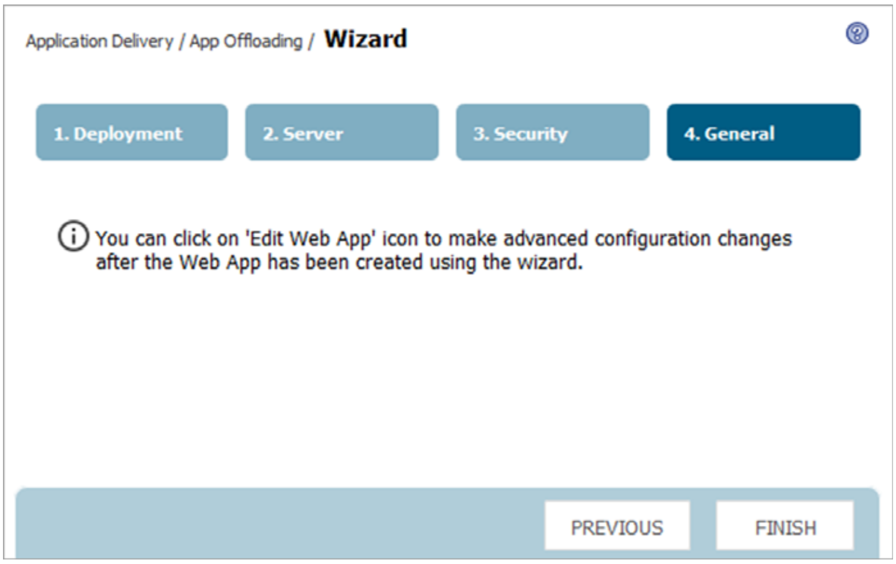
☑ Enable Web Security

☐ Enable Authentication Controls

14 In the **3. Security** screen, select the **Enable Web Security** check box to enable the core security features of Web Application Firewall.

15 Select the **Enable Authentication Controls** check box to require users to authenticate before accessing this application.

16 Click **NEXT**. The fourth screen of the wizard is displayed.



You can click on 'Edit Web App' icon to make advanced configuration changes after the Web App has been created using the wizard.

17 In the **4. General** screen, a message informs you to click the Edit Web App icon to make advanced configuration changes after the web app has been created using the wizard.

18 Click **FINISH**.

Editing an Offloaded Web App

To edit an existing offloaded web app:

1 Navigate to the **Application Delivery > App Offloading** page.

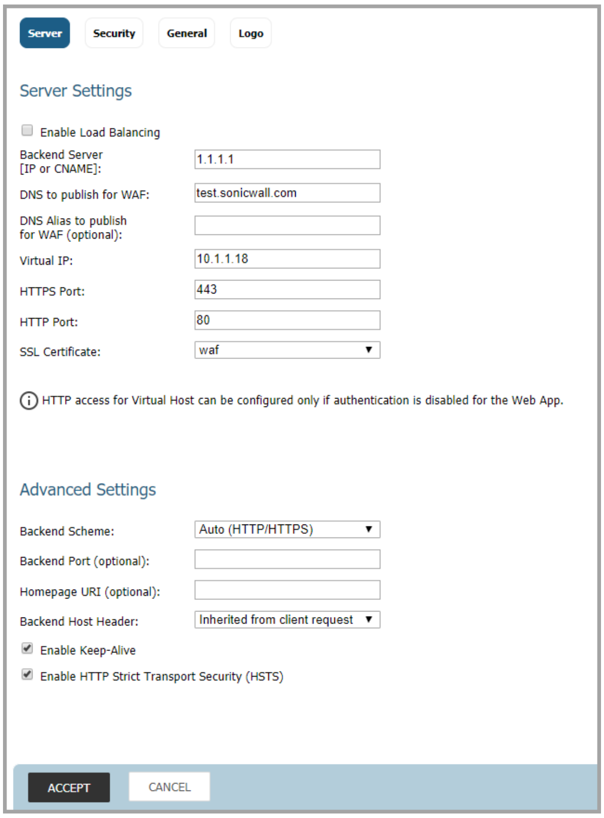
2 In the table under **Web Apps**, click the edit button in the **Configure** column for the app you want to edit.

The page changes to display the editable settings, divided into four screens. You can click the buttons along the top to display the screen you want, then click **ACCEPT** after making changes on that screen:

- Server –
  - The **Server Settings** section contains settings for the backend server IP address, DNS name, DNS alias, Virtual IP address, HTTP port, HTTPS port, and SSL certificate.
  - The **Advanced Settings** section, contains settings for the backend scheme, backend port, homepage URI, backend host header, and to enable keep-alive.
- Security – Contains settings for enabling security, Capture ATP, access policies, authentication, anonymous session tracking, exchange web app, forward secrecy, certificate verification, and version of SSL/TLS.
- General – Contains settings for the application name and login page settings if authentication controls are enabled for this offloaded application.
- Logo – Contains settings for the logo and favicon.

Server

3 On the **Server** screen under **Server Settings**, select the **Enable Load Balancing** check box to load-balance this offloaded application.



Server Settings

☐ Enable Load Balancing

Backend Server [IP or CNAME]:	1.1.1.1
DNS to publish for WAF:	test.sonicwall.com
DNS Alias to publish for WAF (optional):	
Virtual IP:	10.1.1.18
HTTPS Port:	443
HTTP Port:	80
SSL Certificate:	waf ▼

ⓘ HTTP access for Virtual Host can be configured only if authentication is disabled for the Web App.

Advanced Settings

Backend Scheme:	Auto (HTTP/HTTPS) ▼
Backend Port (optional):	
Homepage URI (optional):	
Backend Host Header:	Inherited from client request ▼

☑ Enable Keep-Alive

☑ Enable HTTP Strict Transport Security (HSTS)

4 For **Backend Server [IP or CNAME]**, type in the IP address or CNAME of the backend server to protect. If the backend web application is load balanced by multiple backend servers, type in the Virtual IP address or CNAME record of the load balancer.

5 In the **DNS to publish for WAF** field, type in the DNS name that users can use to access the web app.

Once the web app is configured, publish a DNS record so users are redirected to the WAF for protection. The DNS name and DNS alias should resolve to the web app's public IP address.

6 In the **DNS Alias to publish for WAF** field, optionally type in the DNS alias that users can use to access the web app. The DNS Alias provides another way to access the web app, and is mapped to the DNS name.

Once the web app is configured, publish a DNS record so users are redirected to the WAF for protection. The DNS name and DNS alias should resolve to the web app's public IP address.

7 In the **Virtual IP** field, type in the virtual IP address for the web app. Multiple web apps can be configured using the same virtual IP address.

When using this field, a DNS record should be published to resolve the DNS name and alias to this virtual IP address rather than to the web app's public IP address.

8 For **HTTPS Port**, type in the custom, secure port used to access the web app. The default is ***443***.

9 For **HTTP Port**, type in the custom port used to access the web app. The default is ***80***.

10 For **SSL Certificate**, select the applicable certificate from the drop-down list. This certificate is required to securely access the web app over SSL. The default is the self-signed certificate on the **System > Certificates** page.

You can generate or import SSL certificates on the **System > Certificates** page.

11 To enable unsecured HTTP access to the virtual host, select the **Enable HTTP access** check box.

12 On the **Server** screen under **Advanced Settings**, select the scheme for connecting to the backend server from the **Backend Scheme** drop-down list. Select one of the following schemes:

- **Web (HTTP)** – access the backend server using HTTP
- **Secure Web (HTTPS)** – access the backend server using HTTPS
- **Auto (HTTP/HTTPS)** – allows the user to determine whether HTTP or HTTPS is used to talk to the backend server when accessing an offloaded web app. When **Auto (HTTP/HTTPS)** is selected, WAF uses the same protocol (HTTP or HTTPS) in the request to the backend as the user used in the request to WAF. Access is still under the control of the access policy.

> **NOTE:** It is the administrator’s responsibility to configure the correct scheme used to talk to the backend server. The **Auto (HTTP/HTTPS)** scheme can operate only if HTTP and HTTPS access are enabled for the backend server.

13 For **Backend Port (optional)**, optionally type in the specific port number for accessing the backend server.

14 For **Homepage URI (optional)**, optionally type in the full URI for the home page of the offloaded application. This is the landing page for the user.

For example, ***/exch/test.cgi?key1=value1&key2=value2***.

15 For **Backend Host Header**, if the backend server can only accept requests with a specific DNS name or Host header, select the Host header to send to the backend server from the drop-down list. The choices are:

- **Inherited from client request (default)** – reuse the same Host header from the client request
- **DNS of the Web App** – use the domain name configured above in **Server Settings** in the **DNS to publish for WAF** field as the Host header
- **Backend Server Host** – use the configured Backend Server IP or CNAME as the Host header

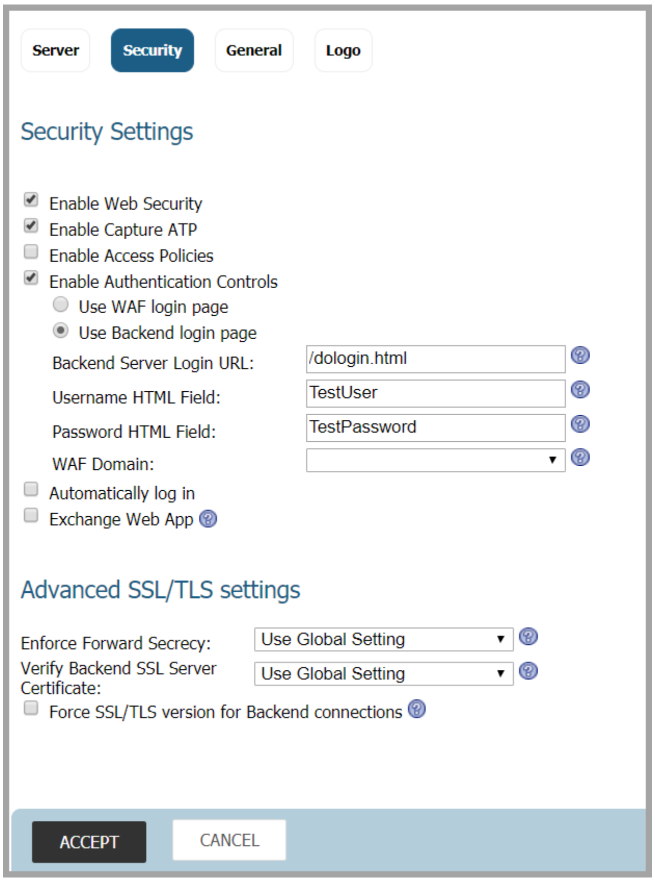
16 Select the **Enable Keep-Alive** check box to allow browsers to reuse the connection for several requests to save resources. If disabled, the TCP connection will be closed after every request.

17 Select the **Enable HTTP Strict Transport Security (HSTS)** check box to allow web servers to declare that web browsers (or other complying user agents) should interact with it using only secure HTTPS connections, and never via the insecure HTTP protocol. This flag is enforced on the client side when there is a valid certificate for the Web App and the SSL session is trusted. Once this flag is enforced, it can only be disabled if the Web App has a valid SSL certificate and SSL session is trusted.

18 Click **ACCEPT** to save changes.

Security

19 On the **Security** screen, under **Security Settings**, select the **Enable Web Security** check box to enable all core web security features. If disabled, no security features will be enforced, and WAF acts like a proxy.



Security Settings

☑ Enable Web Security
☑ Enable Capture ATP
□ Enable Access Policies
☑ Enable Authentication Controls
○ Use WAF login page
● Use Backend login page
Backend Server Login URL: /dologin.html
Username HTML Field: TestUser
Password HTML Field: TestPassword
WAF Domain:
□ Automatically log in
□ Exchange Web App

Advanced SSL/TLS settings

Enforce Forward Secrecy: Use Global Setting
Verify Backend SSL Server Certificate: Use Global Setting
□ Force SSL/TLS version for Backend connections

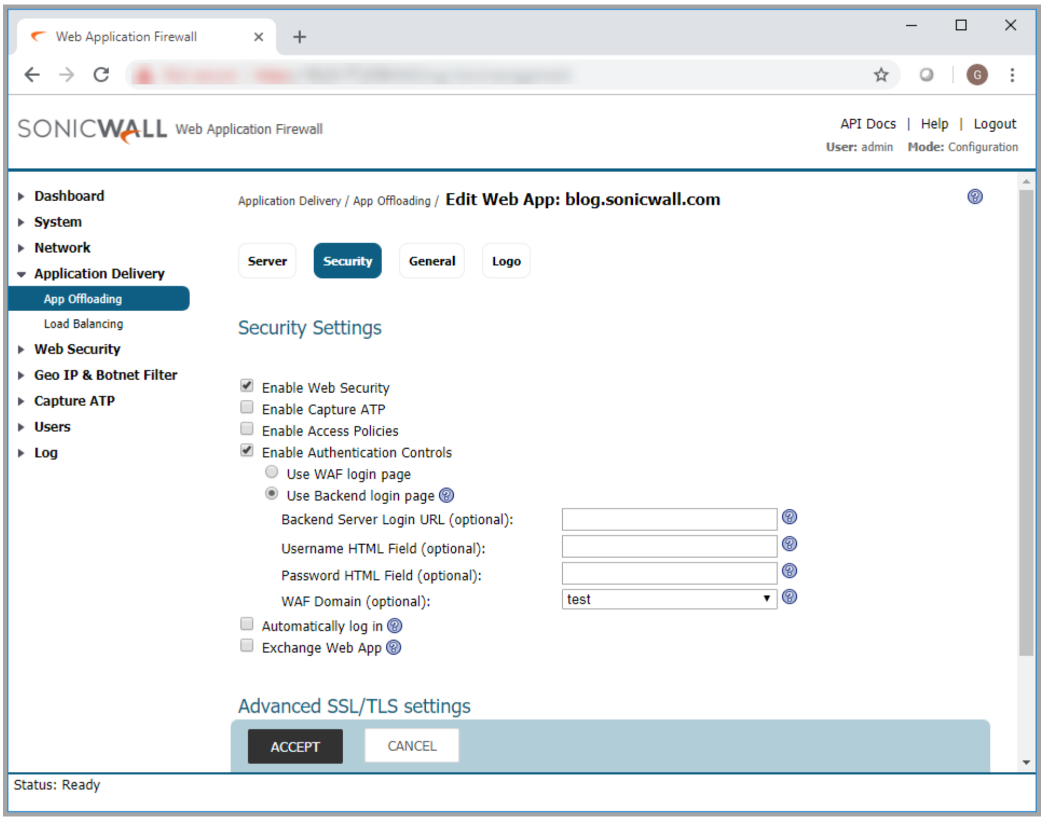
20 Select the **Enable Capture ATP** check box to have WAF enable Web Application file scanning.

21 Select the **Enable Access Policies** check box to have Web Application Firewall enforce configured group and user access policies for this offloaded web app.

22 Select the **Enable Authentication Controls** check box to have WAF require users to authenticate before accessing the offloaded web app. If this option is selected:

- The **Enable Anonymous Session Tracking** option is hidden and the login settings are available for configuration on the **General** screen.
- The **Use WAF login page** option is displayed. Optionally, select this option to use the WAF login page.

  ⓘ **NOTE:** If this option is left blank, the WAF will try to auto-populate the fields when the first end user authentication happens.



Application Delivery / App Offloading / **Edit Web App: blog.sonicwall.com**

Security Settings

☑ Enable Web Security
□ Enable Capture ATP
□ Enable Access Policies
☑ Enable Authentication Controls
○ Use WAF login page
● Use Backend login page

Backend Server Login URL (optional):	
Username HTML Field (optional):	
Password HTML Field (optional):	
WAF Domain (optional):	test

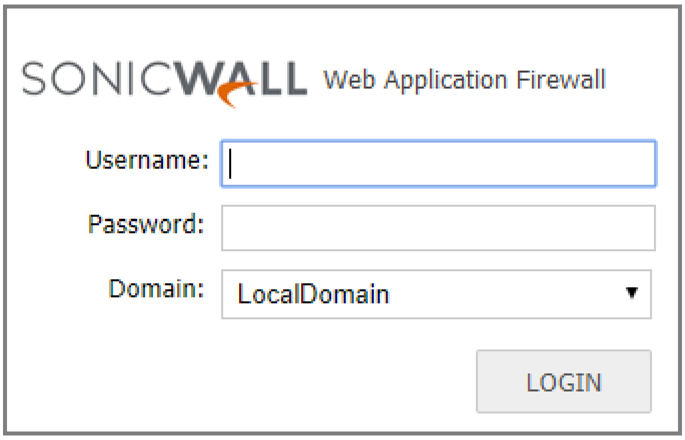
□ Automatically log in
□ Exchange Web App

Advanced SSL/TLS settings

Status: Ready

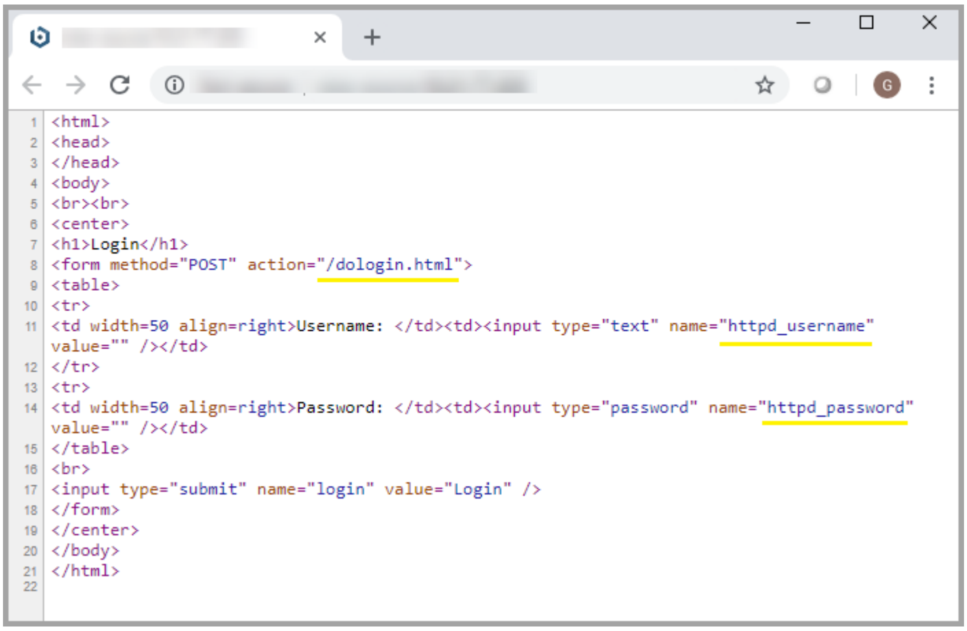
Select this option to display the following choices:

- **Backend Server Login URL -** optionally, select this as the backend URL that the login POST request will be sent to. You must configure the backend server URL before you can configure usernames and passwords.



Username:	
Password:	
Domain:	LocalDomain

- **Username HTML Field -** optionally, enter the HTML field for the username on the login page. To get the values of the Username HTML field names, view the HTML source of the backend login page.



```
<html>
<head>
</head>
<body>
<br><br>
<center>
<h1>Login</h1>
<form method="POST" action="/dologin.html">
<table>
<tr>
<td width=50 align=right>Username: </td><td><input type="text" name="httpd_username" value="" /></td>
</tr>
<tr>
<td width=50 align=right>Password: </td><td><input type="password" name="httpd_password" value="" /></td>
</table>
<br>
<input type="submit" name="login" value="Login" />
</form>
</center>
</body>
</html>
```

- **Password HTML Field -** optionally, enter the HTML field for the password on the login page. To get the values of the Password HTML field names, view the HTML source of the backend login page.
- **WAF Domain -** optionally, enter the WAF domain previously configured for this app. The WAF domain is a local domain that should be created for this web app before configuring the backend login page.

- The **Automatically log in** option is displayed. Select the check box to display the following choices for automatic login:
  - **Use WAF account credentials**
  - **Use custom credentials**

    If you select this option, type the custom credentials for automatically accessing the web app into the displayed fields:
    - **Username**
    - **Password**
    - **Domain**
- The **Exchange Web App** option is displayed. Select the check box to have SonicWall WAF proxy the authentication performed by ActiveSync or Outlook Anywhere, without separate authentication by WAF. For OWA, WAF will enforce a second layer of authentication.

23 If the **Enable Authentication Controls** option is not selected, you can select the **Enable Anonymous Session Tracking** check box. This option allows you to track sessions anonymously for this offloaded web app when users are not authenticated by WAF. Session tracking is necessary for security features including CSRF protection, cookie tampering protection, and the session-based hit counter. Clients must be able to support cookies set by SonicWall WAF. If clients cannot supports those cookies, disable this option.

24 On the **Security** screen under **Advanced SSL/TLS settings**, select the desired setting from the **Enforce Forward Secrecy** drop-down list. Available options are: **Use Global Setting**, **Enabled**, or **Disabled**.

Forward secrecy allows current information to be kept secret even if the private key is compromised in the future.

25 Select the desired setting from the **Verify Backend SSL Server Certificate** drop-down list. Available options are: **Use Global Setting**, **Enabled**, or **Disabled**. If enabled, the connection to the backend SSL/TLS server is dropped if the server's certificate is not trusted. The verification depth is 10.

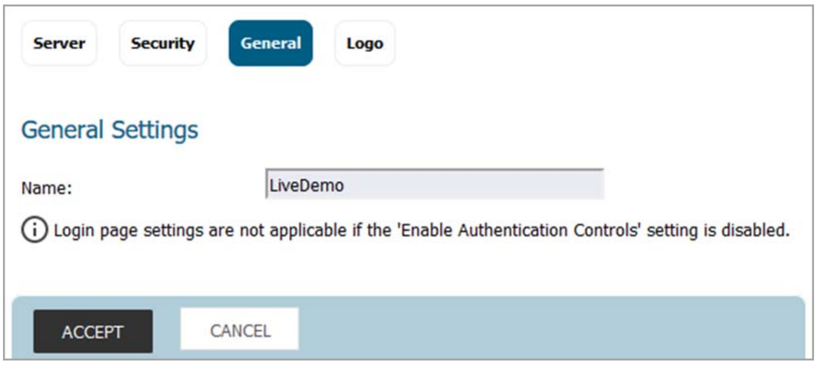
26 To specify the SSL/TLS version to use for communication between the virtual host and the backend server, select **Force SSL/TLS version for Backend connections** and then select the desired version from the **SSL/TLS versions** drop-down list. Available options are: **TLSv1.2** (default), **TLSv1.1**, **TLSv1**.

ⓘ **NOTE:** Forcing older versions of the SSL/TLS protocol is strongly discouraged for security reasons.

27 Click **ACCEPT** to save changes.

General

28 On the **General** screen, only the **Name** option is available if **Enable Authentication Controls** option is not selected on the **Security** screen. Type in the desired name for the offloaded web app.

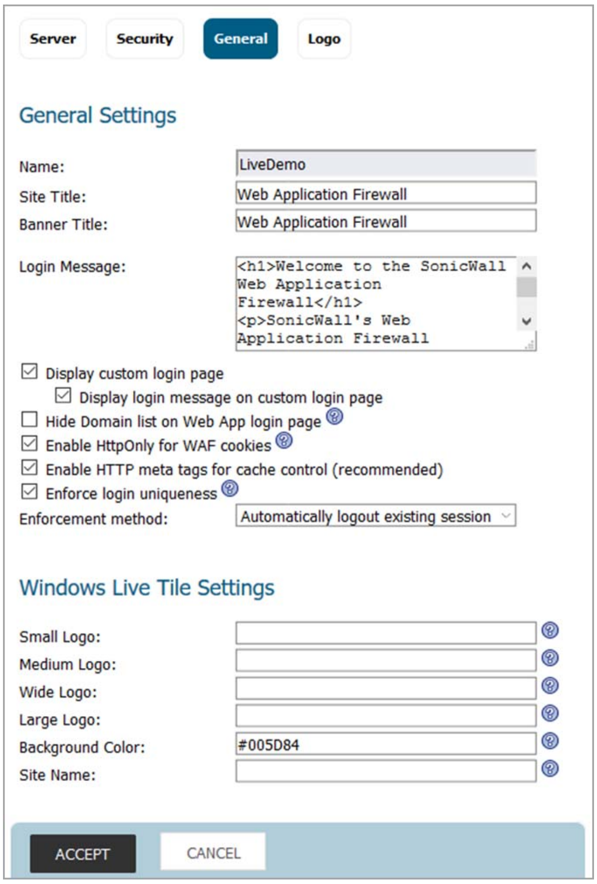


General Settings

Name: LiveDemo

ⓘ Login page settings are not applicable if the 'Enable Authentication Controls' setting is disabled.

If the **Enable Authentication Controls** option is selected on the **Security** screen, multiple login-related options are displayed on the **General** screen.



General Settings

Name: LiveDemo

Site Title: Web Application Firewall

Banner Title: Web Application Firewall

Login Message:

```
<h1>Welcome to the SonicWall
Web Application
Firewall</h1>
<p>SonicWall's Web
Application Firewall
```

☑ Display custom login page

☑ Display login message on custom login page

□ Hide Domain list on Web App login page

☑ Enable HttpOnly for WAF cookies

☑ Enable HTTP meta tags for cache control (recommended)

☑ Enforce login uniqueness

Enforcement method: Automatically logout existing session

Windows Live Tile Settings

Small Logo:

Medium Logo:

Wide Logo:

Large Logo:

Background Color: #005D84

Site Name:

29 Enter a descriptive name for the offloaded app in the **Name** field.

30 Enter the title for the offloaded app browser window in the **Site Title** field.

31 To display a banner message to users before they access the offloaded app, enter the banner title text in the **Banner Title** field.

32 Enter an HTML compliant message, or edit the default message in the **Login Message** field. This message is shown to users on the custom login page.

33 To enable visibility of your custom logo, message, and title information on the login page, select **Display custom login page** and **Display login message on custom login page**.

> ⓘ **NOTE:** Custom logos can be added to existing offloaded apps.

34 To require the user to type in the correct domain name rather than displaying a list, select **Hide Domain list on Web App login page**.

35 To secure WAF cookies with the HTTPOnly flag, select **Enable HttpOnly for WAF cookies**. The HTTPOnly flag prevents client-side scripts from accessing the cookies, protecting them from cross-site scripting cookie theft.

36 Select **Enable HTTP meta tags for cache control (recommended)** to apply HTTP meta tag cache control directives to the web app. Cache control directives include:

```
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
```

These directives help prevent client browsers from caching Web Application Firewall offloaded application pages and other web content.

> **NOTE:** Enabling HTTP meta tags is strongly recommended for security reasons and to prevent out-of-date web pages and data from being stored in the user’s web browser cache.

37 Select **Enforce login uniqueness** to restrict each account to a single session at a time. When this option is enabled, select one of the following from the **Enforcement method** drop-down list:

- **Automatically logout existing session** – Automatically logs out the other session.
- **Confirm logout of existing session** – Reminds the user of the existing session and requires confirmation to open the new session, ending the other session.

38 On the **General** screen in the **Windows Live Tile Settings** section, specify the link(s) for the **Small** / **Medium** / **Wide** / **Large Logo** to be used with Live Tile.

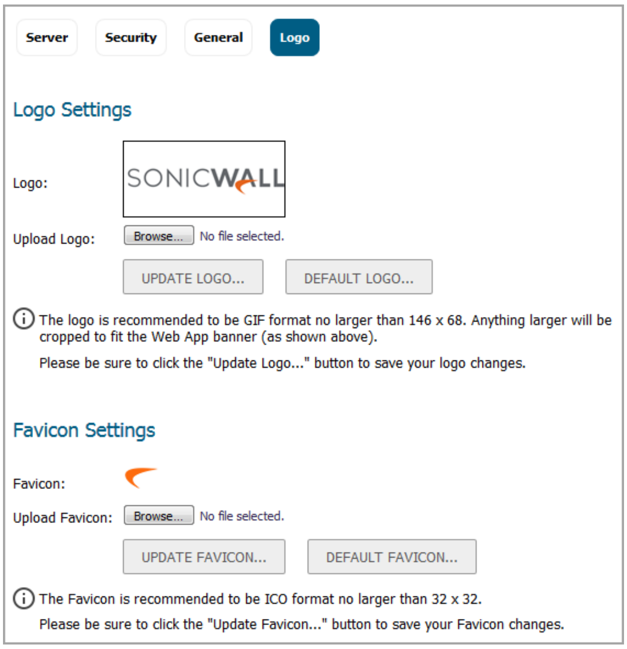
39 Specify the **Background Color** for Live Tile. If no value is specified, the default color is #0085C3.

40 Specify the **Site Name** to be displayed for the Live Tile bookmark. If no value is specified, the default is the web app name.

41 Click **ACCEPT** to save changes.

Logo

42 On the **Logo** screen, under **Logo Settings**, click **Browse** by the **Upload Logo** field.



Logo Settings

Logo:

Upload Logo: No file selected.

The logo is recommended to be GIF format no larger than 146 x 68. Anything larger will be cropped to fit the Web App banner (as shown above).

Please be sure to click the "Update Logo..." button to save your logo changes.

Favicon Settings

Favicon:

Upload Favicon: No file selected.

The Favicon is recommended to be ICO format no larger than 32 x 32.

Please be sure to click the "Update Favicon..." button to save your Favicon changes.

43 Select an appropriately-sized .gif format logo in the file browser window and then click **Open**.

> **NOTE:** SonicWall recommends GIF format. Anything larger than 146x68 pixels is cropped to fit the designated logo space on the page.

44 Select **Light** or **Dark** from the **Background** drop-down list. Select a background shade that helps set off your logo from the rest of the login page.

45 Click **UPDATE LOGO**.

46 Under **Favicon Settings**, click **Browse** by the **Upload Favicon** field. The file browser window displays.

47 Select an appropriate-sized ICO format favicon in the file browser window and then click **Open**.

ⓘ | **NOTE:** SonicWall recommends ICO format for the custom favicon, no larger than 32x32 pixels.

48 Click **UPDATE FAVICON**.

49 Click **ACCEPT** to save changes.

Deleting an Offloaded Web App

You can delete one or more offloaded web applications on the **Application Delivery > App Offloading** page.

To delete a single offloaded web app:

1 In the table under **Web Apps**, click the delete button in the **Configure** column for the app you want to delete.

2 Click **OK** in the confirmation dialog.

To delete multiple offloaded web apps:

1 In the table under **Web Apps**, select the check boxes to the left of one or more offloaded web apps that you want to delete.

2 Click the **DELETE SELECTED WEB APPS** button.

3 Click **OK** in the confirmation dialog.

Configuring Seamless Multi-Factor Authentication

The multi-factor authentication feature enables authentication for a specific URL, extends WAF's authentication to public websites, identifies users classified as "Anonymous", and enforces access policies. Seamless multi-factor authentication is achieved by selecting **Backend Login Page** for Authentication. This configuration allows a website owner to present the website's login page for authentication instead of WAF's login page providing users with a seamless login experience. This feature also allows a website to enable a second factor of authentication without any changes to the website. For example, if One Time Password (OTP) is enabled, the OTP login is presented seamlessly after the user logs into the Backend website.

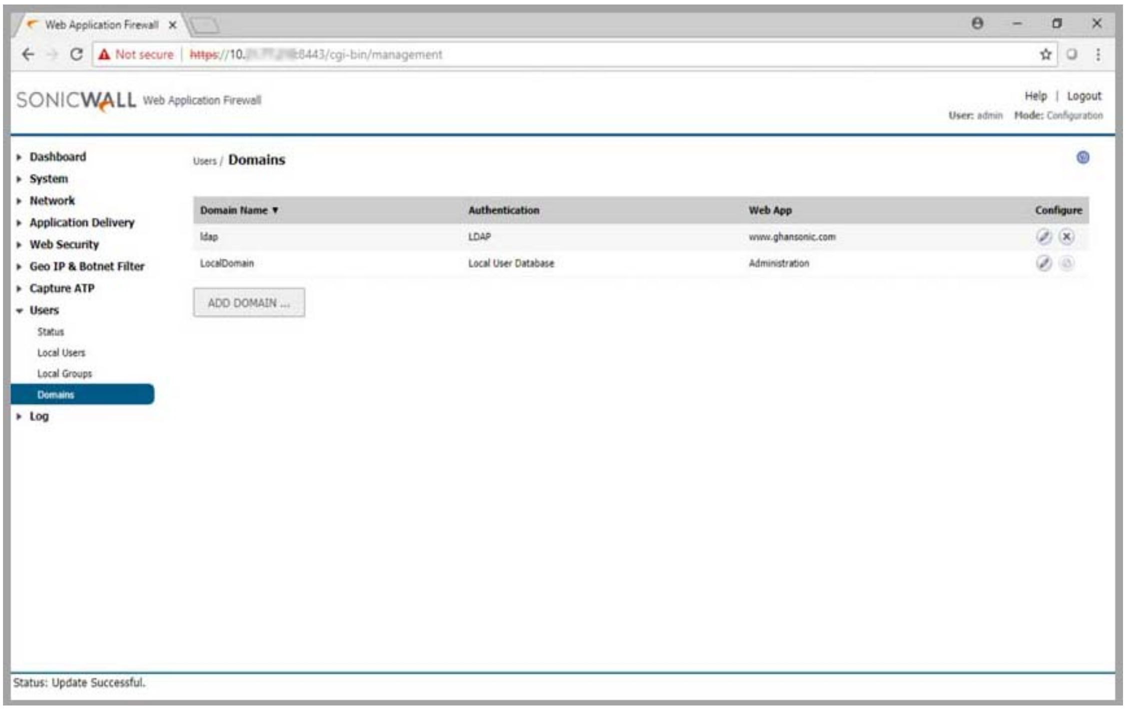
In order to enable the anonymous identification feature, you must configure the user-name, password, and domain fields on the backend login page. The WAF intercepts the login request to the website's login page, sends the authentication/login request to the configured external authentication server and authenticates the user. If the authentication succeeds, WAF creates the user in the WAF database.

The logged in user is now listed on the **Users > Status** page. If OTP or another two factor authentication method has been configured for the WAF's domain, after the user overcomes the first form-based login challenge, the user has to login using the OTP code. If the login fails, the user is redirected to a WAF login error page.

To configure seamless multi-factor identification:

1 Log into the WAF as an administrator and navigate to **Users > Domains.**

2 Configure an external domain (e.g. LDAP server) and bind it to a web application.



Users / Domains

Domain Name ▼	Authentication	Web App	Configure
ldap	LDAP	www.ghansonic.com	
LocalDomain	Local User Database	Administration	

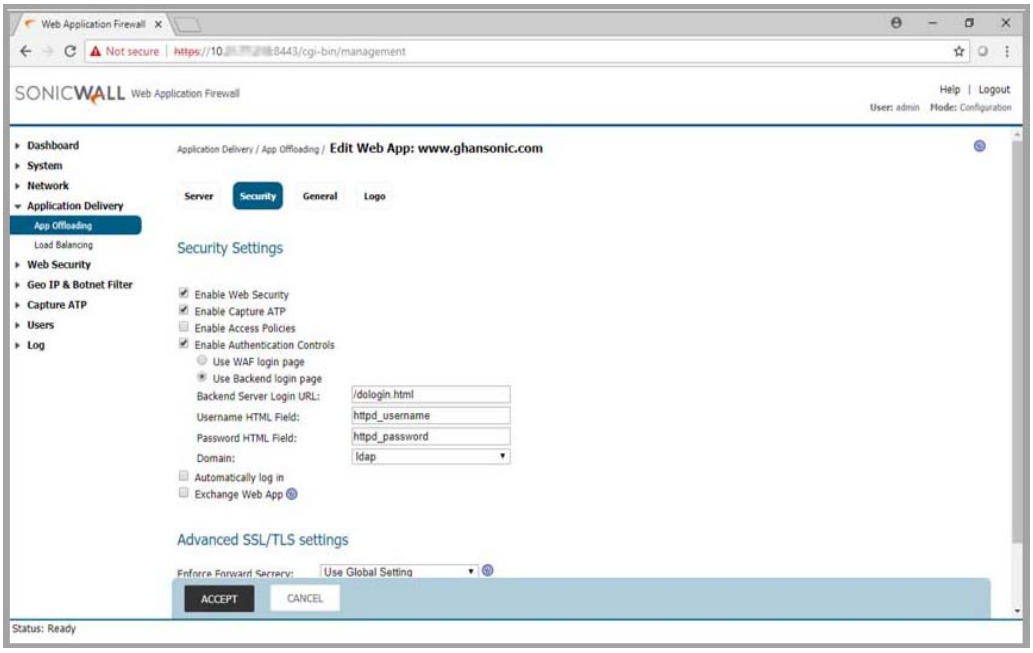
Status: Update Successful.

3 Navigate to **Application Delivery > App Offloading** and scroll down to find the domain you configured in the previous step.

4 Click the **edit** icon. The **Edit Web App** page displays.

5 Click the **Security** tab then select **Use Backend login page**. Selecting this setting enables **Seamless multi-factor authentication** by delivering a backend login page for authentication, instead of WAF's standard login page.

6 Enter the **Backend Server Login URL**, **Username HTML Field**, **Password HTML Field**, and **WAF Domain** in the fields provided. Configure the backend server so that the home page is the backend login page and then access the web app to verify backend login page is used for authentication.



Application Delivery / App Offloading / Edit Web App: www.ghansonic.com

Security Settings

☑ Enable Web Security
☑ Enable Capture ATP
□ Enable Access Policies
☑ Enable Authentication Controls
○ Use WAF login page
● Use Backend login page
Backend Server Login URL: /dologin.html
Username HTML Field: httpd_username
Password HTML Field: httpd_password
Domain: ldap
□ Automatically log in
□ Exchange Web App

Advanced SSL/TLS settings

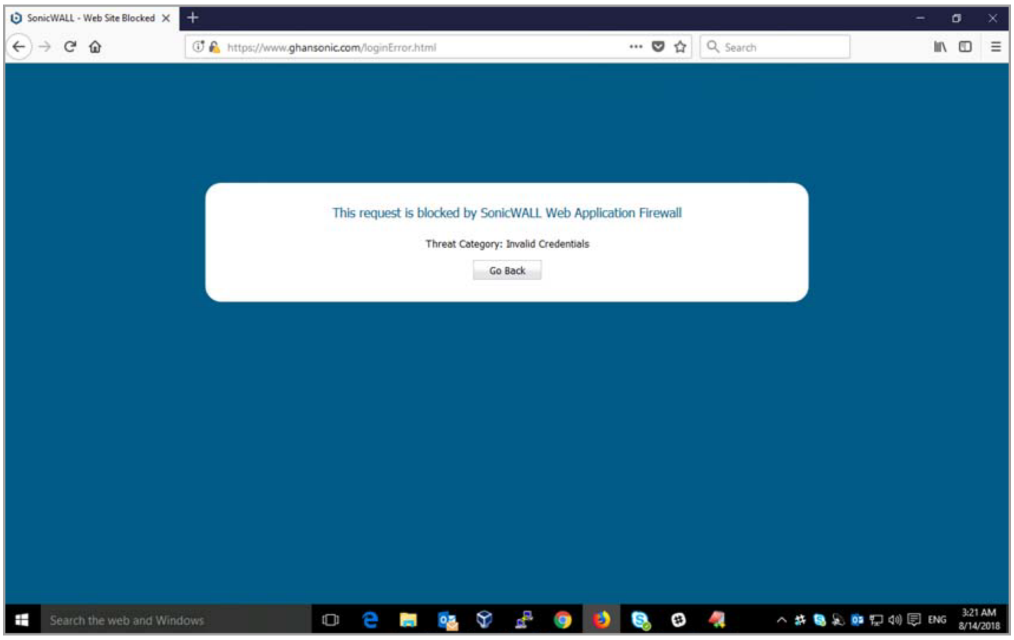
Enforce Forward Secrecy: Use Global Setting

Status: Ready

The backend login page is displayed. To enable the **Logout** button, navigate to **Security > Settings** and select **Secure Session Logout**. If you click the **Logout** button in the top right corner, an error will be displayed since you have not yet logged in.

> **NOTE:** The **Logout** button is present when the Security Session Logout feature is enabled from the **Web Security > Settings** page.

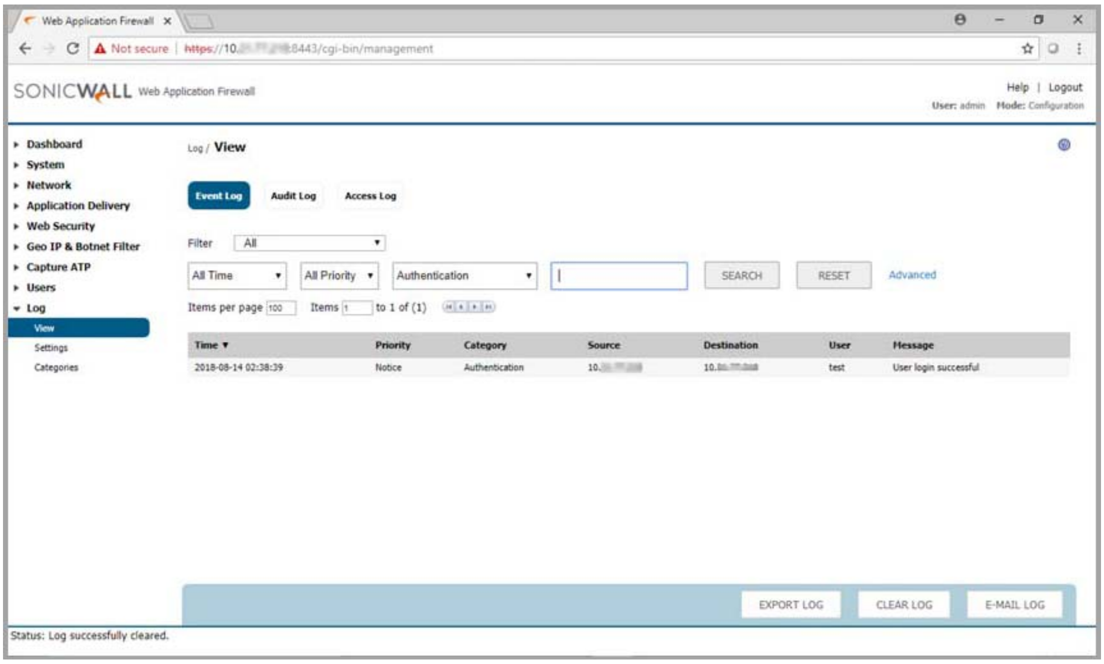
Enter the **Username** and **Password** credentials into the fields provided and then click **Login**. If the credentials are correct, the backend landing page is displayed. If the credentials are not correct, an error page is displayed.


SonicWALL - Web Site Blocked
https://www.ghansonic.com/loginError.html
Search
Search the web and Windows
ENG
3:21 AM
8/14/2018

This request is blocked by SonicWALL Web Application Firewall

Threat Category: Invalid Credentials

7 Navigate to **Log > View > Event Log** to see the user session in the Event Log.



Filter: All

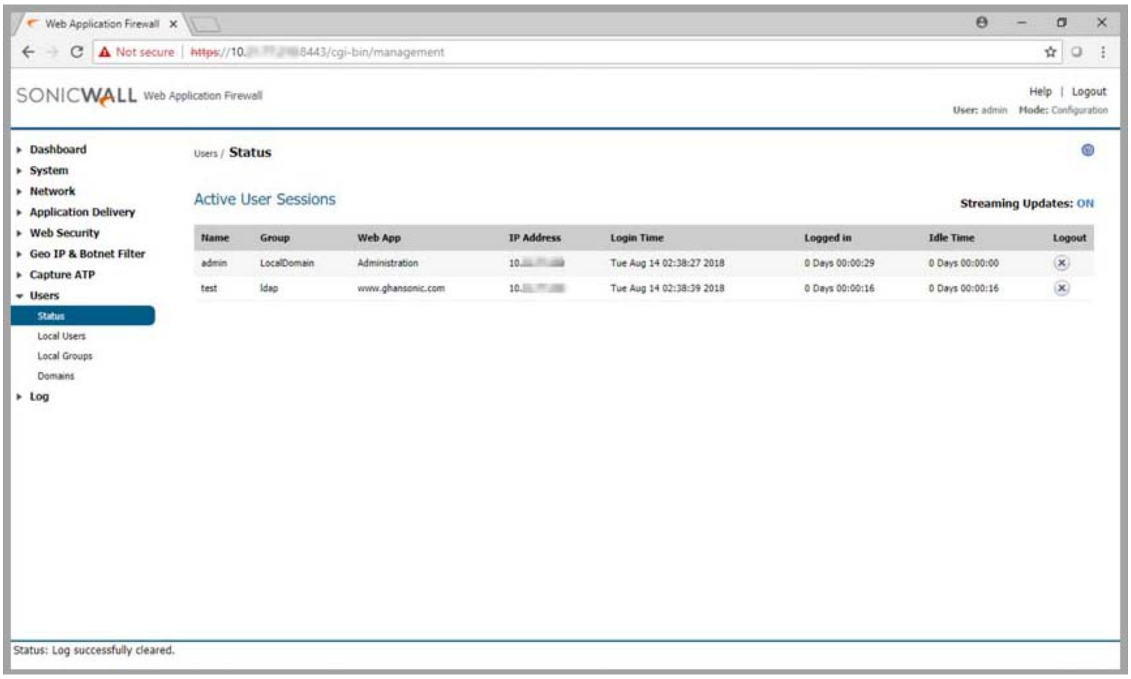
All Time | All Priority | Authentication

Items per page 100 Items 1 to 1 of (1)

Time ▼	Priority	Category	Source	Destination	User	Message
2018-08-14 02:38:39	Notice	Authentication	10.[redacted]	10.[redacted]	test	User login successful

Status: Log successfully cleared.

8 Navigate to **Users > Status** to see the user session in the active user sessions.



Users / **Status**

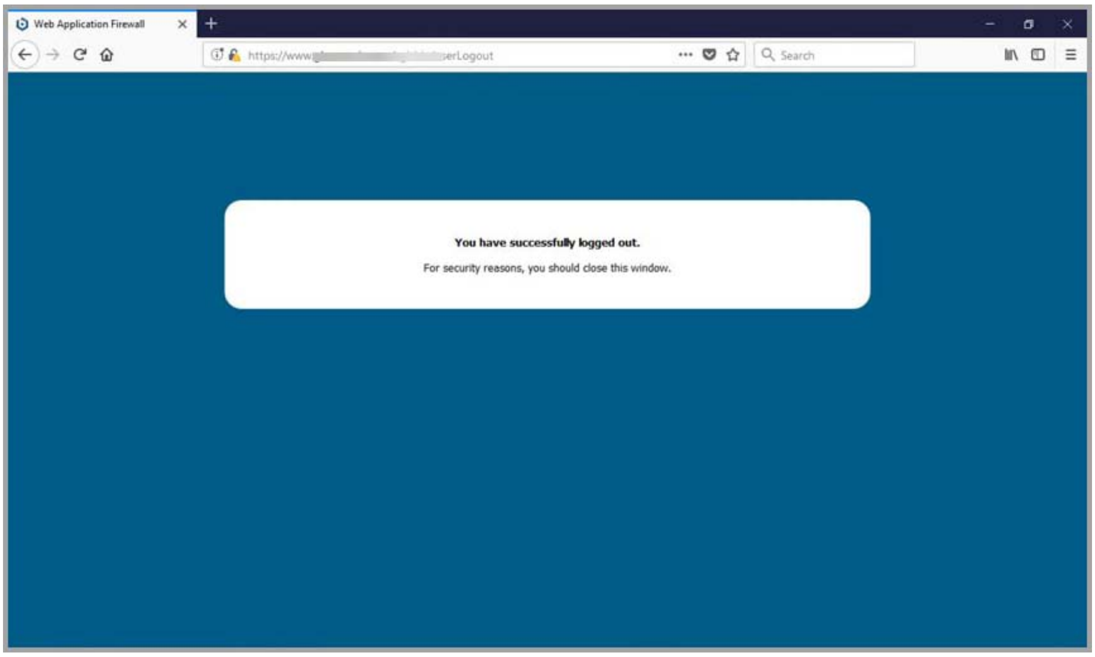
Active User Sessions

Streaming Updates: ON

Name	Group	Web App	IP Address	Login Time	Logged in	Idle Time	Logout
admin	LocalDomain	Administration	10.[redacted]	Tue Aug 14 02:38:27 2018	0 Days 00:00:29	0 Days 00:00:00	☒
test	ldap	www.ghansonic.com	10.[redacted]	Tue Aug 14 02:38:39 2018	0 Days 00:00:16	0 Days 00:00:16	☒

Status: Log successfully cleared.

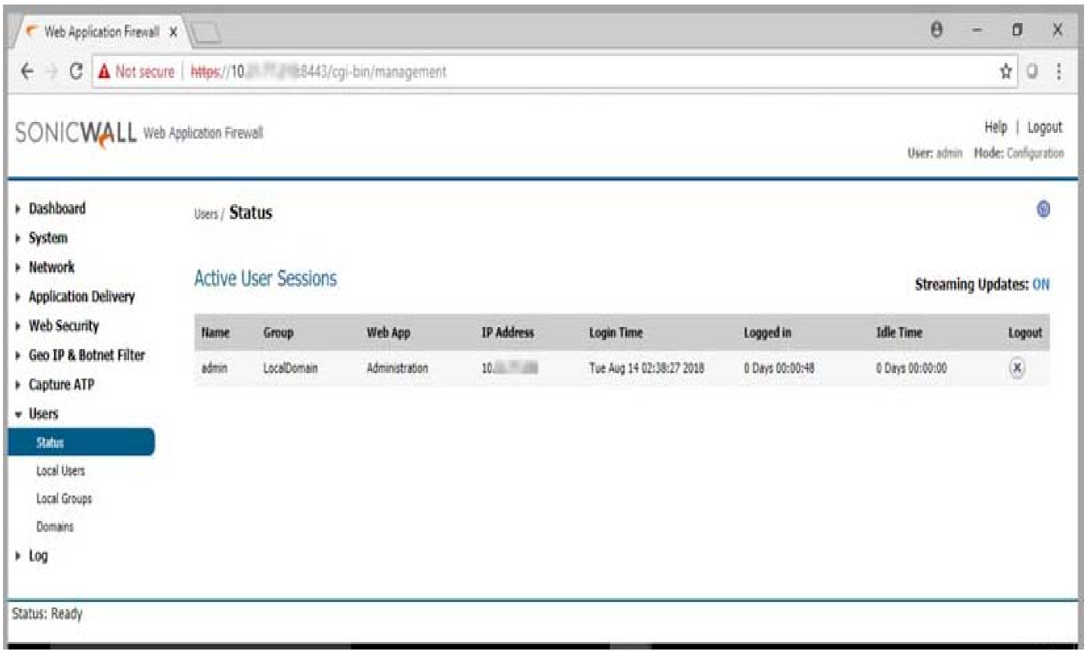
9 When the user clicks the **Logout** button, the **WAF logout** page displays.



You have successfully logged out.

For security reasons, you should close this window.

10 When the user logs out, the user is removed from the active user sessions on the **Users > Status** page.



Users / **Status**

Active User Sessions

Streaming Updates: ON

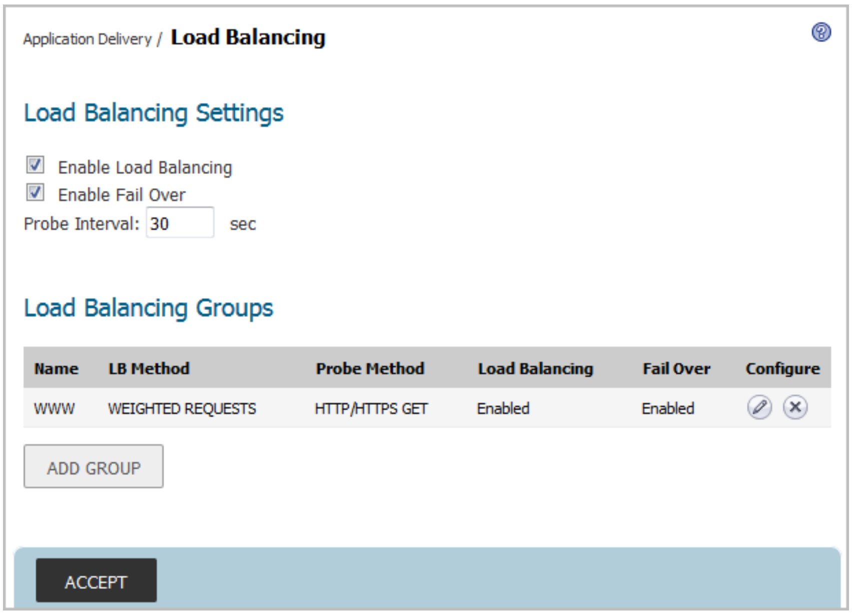
Name	Group	Web App	IP Address	Login Time	Logged in	Idle Time	Logout
admin	LocalDomain	Administration	10.[redacted]	Tue Aug 14 02:38:27 2018	0 Days 00:00:48	0 Days 00:00:00	☒

Configuring Load Balancing

The **Application Delivery > Load Balancing** page allows you to configure backend web servers for a load balanced deployment. This page provides options to enable load balancing, enable fail over, and set the probe interval. You can configure load balancing groups and view any existing load balancing groups.

NOTE: This feature also requires a load balanced offloaded web application with virtual IP address to be configured in the **Application Delivery > App Offloading** page.

Application Delivery > Load Balancing Page



Application Delivery / **Load Balancing**

Load Balancing Settings

☑ Enable Load Balancing

☑ Enable Fail Over

Probe Interval: 30 sec

Load Balancing Groups

Name	LB Method	Probe Method	Load Balancing	Fail Over	Configure
WWW	WEIGHTED REQUESTS	HTTP/HTTPS GET	Enabled	Enabled	✎ ☒

Topics:

- Configuring Load Balancing Settings on page 98
- Configuring Load Balancing Groups on page 98

Configuring Load Balancing Settings

The following table lists the configuration options under the **Load Balancing Settings** section. Additional per-group configuration options are described in Configuring Load Balancing Groups on page 98.

Load Balancing Settings

Option	Description
Enable Load Balancing	Enables/disables the load balancing feature across all currently active groups.
Enable Fail Over	Enables/disables all probing, monitoring, and failover features.
Probe Interval	Determines the frequency (in seconds) at which the load balancing feature checks the status of backend nodes.

Configuring Load Balancing Groups

The **Load Balancing Groups** section of the **Application Delivery > Load Balancing** page displays the list of existing load balancing groups. The table shows the group name, the load balancing method, the probe method, whether load balancing is currently enabled or disabled, and whether fail over is currently enabled or disabled. The **Configure** column provides edit and delete buttons for each load balancing group.

Topics:

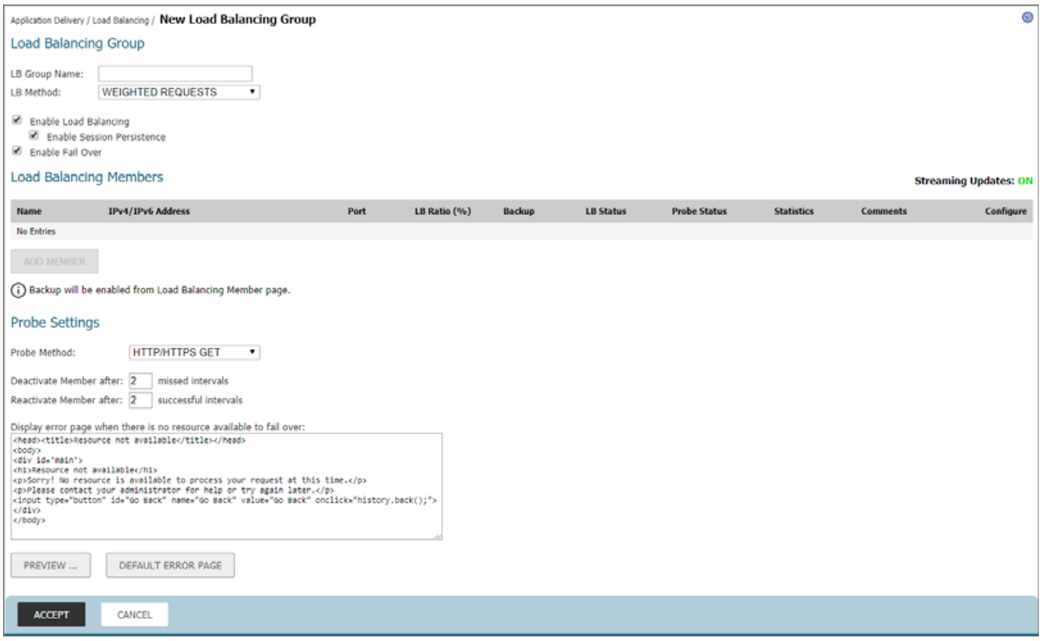
- Configuring Load Balancing Groups on page 98
- Adding a Load Balancing Group on page 99
- Configuring Probe Settings on page 102
- Adding Load Balancing Members on page 103

Adding a Load Balancing Group

To add a load balancing group:

1 Navigate to the **Application Delivery > Load Balancing** page.

2 Click the **ADD GROUP** button. The **Load Balancing Group** configuration page displays.



Application Delivery / Load Balancing / **New Load Balancing Group**

Load Balancing Group

LB Group Name:
LB Method: WEIGHTED REQUESTS ▾

☑ Enable Load Balancing
☑ Enable Session Persistence
☑ Enable Fail Over

Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
No Entries									

ⓘ Backup will be enabled from Load Balancing Member page.

Probe Settings

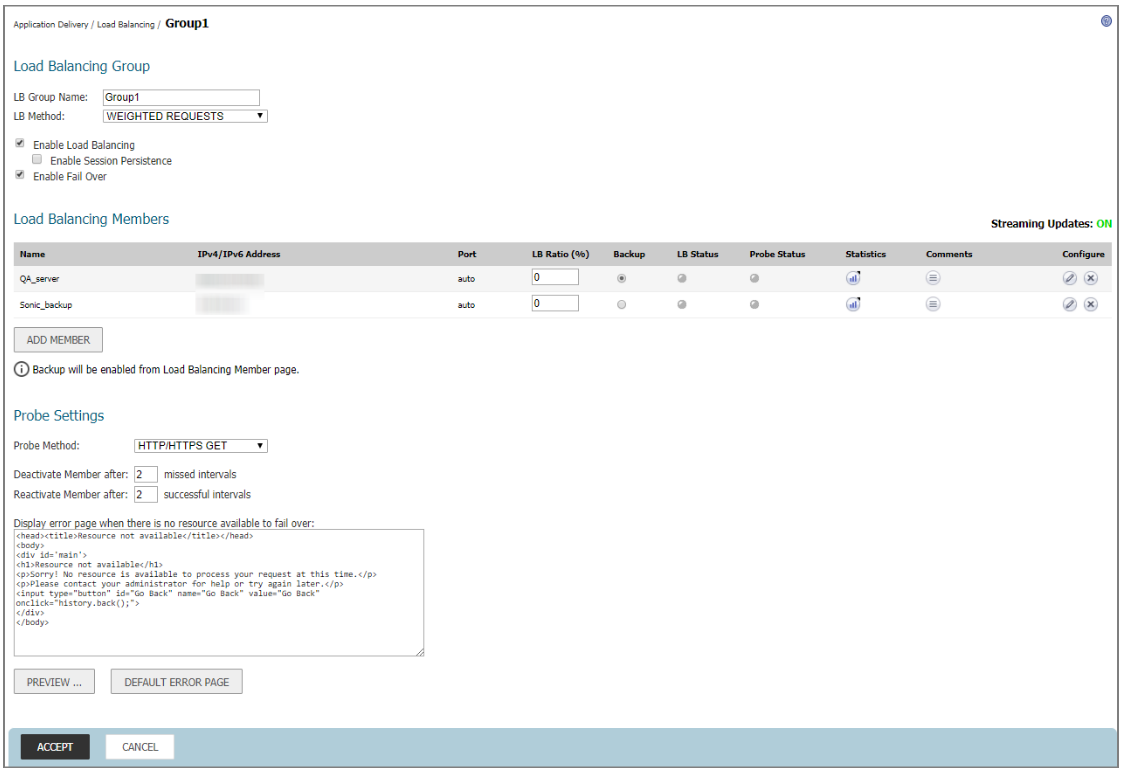
Probe Method: HTTP/HTTPS GET ▾

Deactivate Member after: 2 missed intervals
Reactivate Member after: 2 successful intervals

Display error page when there is no resource available to fail over:

```
<head><title>Resource not available</title></head>
<body>
<div id='main'>
<h1>Resource not available</h1>
<p>Sorry! No resource is available to process your request at this time.</p>
<p>Please contact your administrator for help or try again later.</p>
<input type="button" id="Go Back" name="Go Back" value="Go Back" onclick="history.back();">
</div>
</body>
```

3 In the **Load Balancing Group** section, enter a descriptive **LB Group Name** for this load balancing group.



Application Delivery / Load Balancing / **Group1**

Load Balancing Group

LB Group Name: Group1
LB Method: WEIGHTED REQUESTS ▾

☑ Enable Load Balancing
☐ Enable Session Persistence
☑ Enable Fail Over

Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
QA_server	[redacted]	auto	0	●	●	●			
Sonic_backup	[redacted]	auto	0	○	●	●			

ⓘ Backup will be enabled from Load Balancing Member page.

Probe Settings

Probe Method: HTTP/HTTPS GET ▾

Deactivate Member after: 2 missed intervals
Reactivate Member after: 2 successful intervals

Display error page when there is no resource available to fail over:

```
<head><title>Resource not available</title></head>
<body>
<div id='main'>
<h1>Resource not available</h1>
<p>Sorry! No resource is available to process your request at this time.</p>
<p>Please contact your administrator for help or try again later.</p>
<input type="button" id="Go Back" name="Go Back" value="Go Back"
onclick="history.back();">
</div>
</body>
```

4 Select a load balancing method from the **LB Method** drop-down list. Options include:

- **WEIGHTED REQUESTS** – Keeps track of the number of incoming requests (including successfully completed requests) to decide which member should handle the next incoming request. The LB Ratio decides the percentage distribution.
- **LEAST REQUESTS** – Keeps track of the number of incoming requests (excluding successfully completed requests) that are currently being serviced to decide which Member should handle the next incoming request.

5 Select **Enable Load Balancing** to enable this group for load balancing.

6 The **Enable Session Persistence** option is automatically selected when the group is enabled. This option allows you to enable continuous user sessions by forwarding the "requests" part of the same session to the same backend member.

7 Select **Enable Failover** to enable probing, monitoring, and failover features.

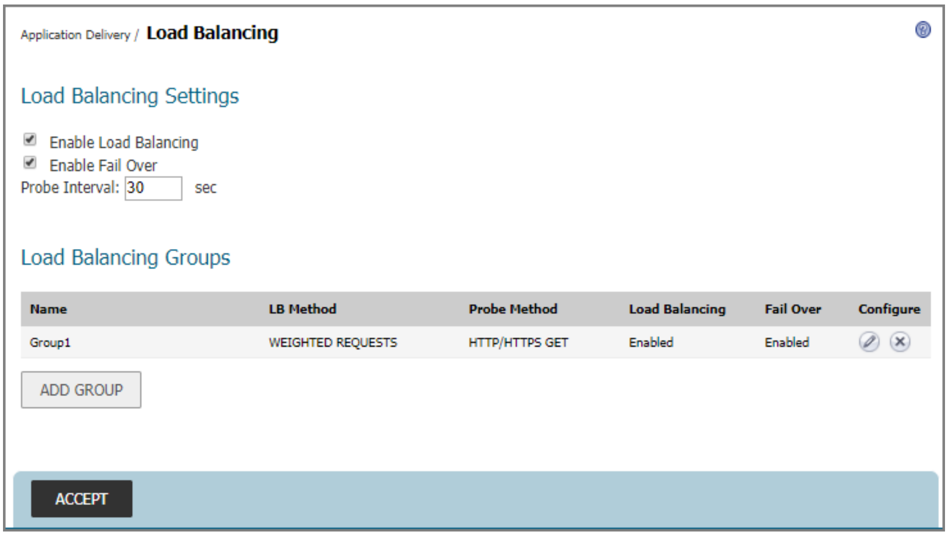
> **NOTE:** It is important to ensure that the same member receives all cookies to keep the user authenticated. However, for improved performance in certain situations, all backend members might be able to accept the session cookies of all users. In this case, you can turn off Session persistence. The Load Balancer then strictly adheres to the LB method and LB factors in distributing the load.

8 Proceed to Configuring Probe Settings on page 102 and then click **ACCEPT** to add the group. You cannot add load balancing group members during creation of a new load balancing group. To add members to an existing group, see Adding Load Balancing Members on page 103.

Configuring Load Balancing Groups

To configure Load Balancing Groups:

1 Click the **Edit** icon on the right of the **Load Balancing Groups** table.



Application Delivery / **Load Balancing**

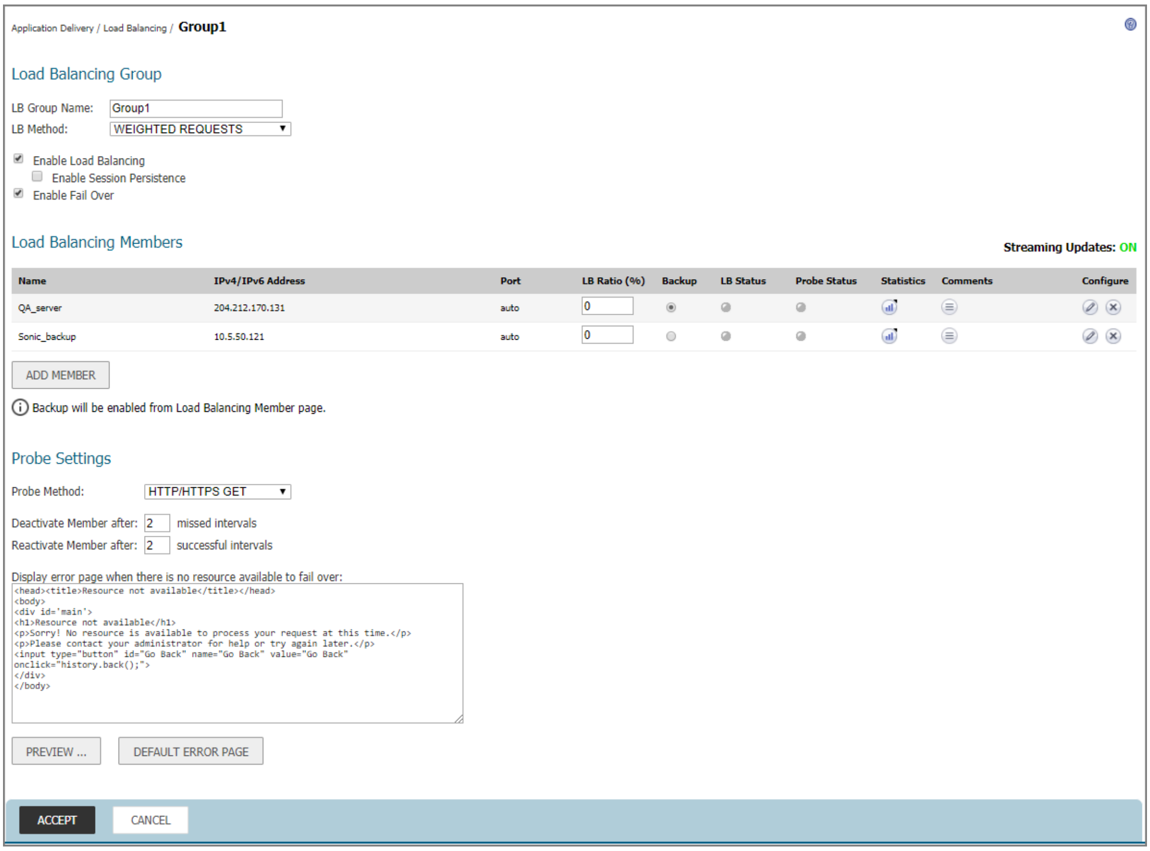
Load Balancing Settings

☑ Enable Load Balancing
☑ Enable Fail Over
Probe Interval: 30 sec

Load Balancing Groups

Name	LB Method	Probe Method	Load Balancing	Fail Over	Configure
Group1	WEIGHTED REQUESTS	HTTP/HTTPS GET	Enabled	Enabled	✎ ⊗

The **Application Delivery / Load Balancing / Group1** page displays showing you the **Load Balancing Members t**hat belong to **Group1**.



Application Delivery / Load Balancing / **Group1**

Load Balancing Group

LB Group Name: Group1
LB Method: WEIGHTED REQUESTS ▾

☑ Enable Load Balancing
☐ Enable Session Persistence
☑ Enable Fail Over

Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
QA_server	204.212.170.131	auto	0	◉	●	●	📊	☰	✎ ✕
Sonic_backup	10.5.50.121	auto	0	○	●	●	📊	☰	✎ ✕

ⓘ Backup will be enabled from Load Balancing Member page.

Probe Settings

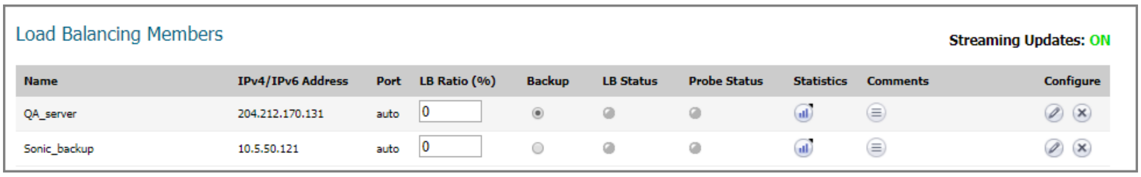
Probe Method: HTTP/HTTPS GET ▾

Deactivate Member after: 2 missed intervals
Reactivate Member after: 2 successful intervals

Display error page when there is no resource available to fail over:

```
<head><title>Resource not available</title></head>
<body>
<div id='main'>
<h1>Resource not available</h1>
<p>Sorry! No resource is available to process your request at this time.</p>
<p>Please contact your administrator for help or try again later.</p>
<input type="button" id="Go Back" name="Go Back" value="Go Back"
onclick="history.back();">
</div>
</body>
```

The **Load Balancing Members** of **Group1** are shown in the middle section table.



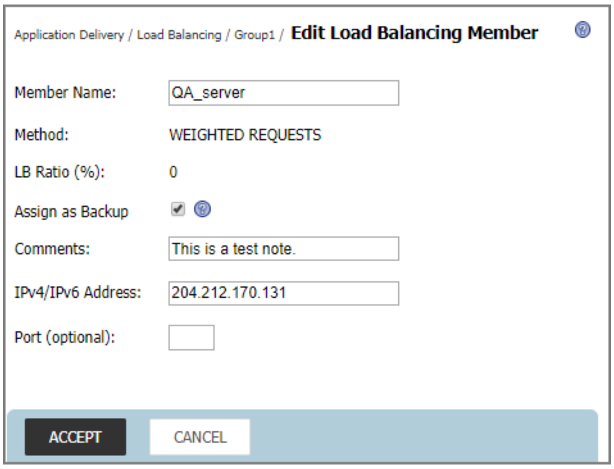
Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
QA_server	204.212.170.131	auto	0	◉	●	●	📊	☰	✎ ✕
Sonic_backup	10.5.50.121	auto	0	○	●	●	📊	☰	✎ ✕

2 Click the **Edit** icon on the right of the **Load Balancing Members** table to configure the member you want.

The **Edit Load Balancing Member** screen displays.



Application Delivery / Load Balancing / Group1 / **Edit Load Balancing Member**

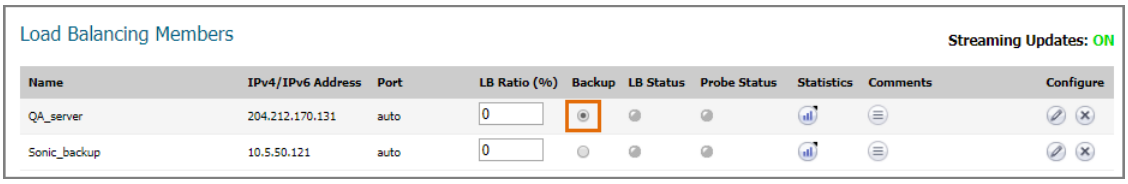
Member Name:	QA_server
Method:	WEIGHTED REQUESTS
LB Ratio (%):	0
Assign as Backup	☑
Comments:	This is a test note.
IPv4/IPv6 Address:	204.212.170.131
Port (optional):	

3 Verify that the information in the text fields is correct and check the box next to **Assign as Backup**.

> **NOTE:** Backup is not supported when Session Persistence is enabled for the Load Balancing Group. Disable Session Persistence for the Group to enable Backup.

4 Click **ACCEPT** to save your changes.

5 Confirm that you have assigned the Member as backup by making sure the radio button under the **Backup** column and in the member row is enabled.



Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
QA_server	204.212.170.131	auto	0	◉	●	●			
Sonic_backup	10.5.50.121	auto	0	○	●	●			

Refer to the table below for more information about the Load Balancing Members table columns:

Load Balancing Members

Column Name	Description
Name	The descriptive **LB Group Name** for your load balancing group.
IPv4/IPv6 Address	The numeric backend HTTP(S) server IP address of your system on the Internet.
Port	The hardware interface by which your system is connected to the backend server. The default value for an HTTPS connection is 443.
LB Ratio (%)	The load balancing quantity.
Backup	The configuration of any of the server members in the Group as Backup.
LB Status	The state or condition of your load balancing data.
Probe Status	The state of your inquiry method, whether it is **HTTP/HTTPS GET, TCP CONNECT, or ICMP PING**.
Statistics	The numerical data of your load balancing
Comments	Any note you type in the Add Load Balancing Member window Comments field.
Configure	The setting of the load balancing group.

Configuring Probe Settings

To configure probe settings for a load balancing group:

1 In the **Probe Settings** section of the **Load Balancing Group** screen, select a **Probe Method** from the drop-down list. Options include:

- **HTTP/HTTPS GET** – The Load Balancer sends an HTTP(S) GET request periodically (based on the configured probe interval) to confirm that the HTTP response status code is not greater than or equal to 500 to ensure there are no web server errors. This is the most reliable method to determine if a web server is alive. This method ignores SSL Certificate warnings while probing.
- **TCP CONNECT** – The Load Balancer completes a 3-way TCP handshake periodically to monitor the health of a backend node.
- **ICMP PING** – The Load Balancer sends a simple ICMP Ping request to monitor if a backend node is alive.

2 In the **Deactivate Member after** field, enter the number of **missed intervals** required to fail the node. The default value is 2.

3 In the **Reactivate Member after** field, enter the number of **successful intervals** required to reinstate the node as functional. The default value is 2.

4 In the **Display error page when there is no resource available to fail over** text box, enter a custom message or web page to display in the event that all of the configured backend nodes have failed. HTML formatting is allowed in this field.

5 Click the **PREVIEW** button to see how your error page will appear.

6 To set the current customized page as the default error page, click the **DEFAULT ERROR PAGE** button and then click **OK** in the confirmation dialog.

7 Click **ACCEPT** to save your changes.

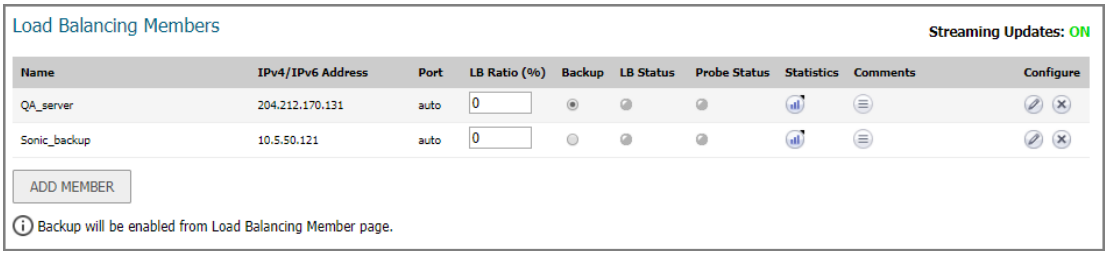
Adding Load Balancing Members

ⓘ **NOTE:** You must create a Load Balancing group before you can begin adding members to the group.

To add members to a load balancing group:

1 On the **Application Delivery > Load Balancing** page, click the edit button in the **Configure** column to add a member to that load balancing group.

2 In the **Load Balancing Members** section of the group configuration page, click **ADD MEMBER**.



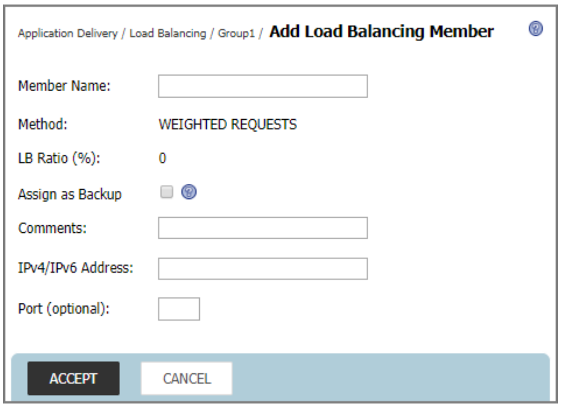
Load Balancing Members

Streaming Updates: ON

Name	IPv4/IPv6 Address	Port	LB Ratio (%)	Backup	LB Status	Probe Status	Statistics	Comments	Configure
QA_server	204.212.170.131	auto	0	●	●	●			
Sonic_backup	10.5.50.121	auto	0	○	●	●			

ⓘ Backup will be enabled from Load Balancing Member page.

The **Add Load Balancing Member** screen displays.



Application Delivery / Load Balancing / Group1 / **Add Load Balancing Member**

Member Name:	
Method:	WEIGHTED REQUESTS
LB Ratio (%):	0
Assign as Backup	□
Comments:	
IPv4/IPv6 Address:	
Port (optional):	

3 Enter a **Member Name** to uniquely identify this member within the Load Balancing Group.

4 Check the box next to **Assign as Backup** if you want to configure a server as backup.

5 Enter a friendly name or description on the **Comments** field to identify this group.

6 Enter the backend HTTP(S) server IP address in the **IPv4/IPv6 Address** field.

7 Enter the **Port** for the backend server. The default value for an HTTPS connection is 443.

8 Click **ACCEPT** to add this member to the group.

6

Web Security Configuration

This section provides information and configuration tasks specific to the **Web Security** pages in the SonicWall Web Application Firewall management interface.

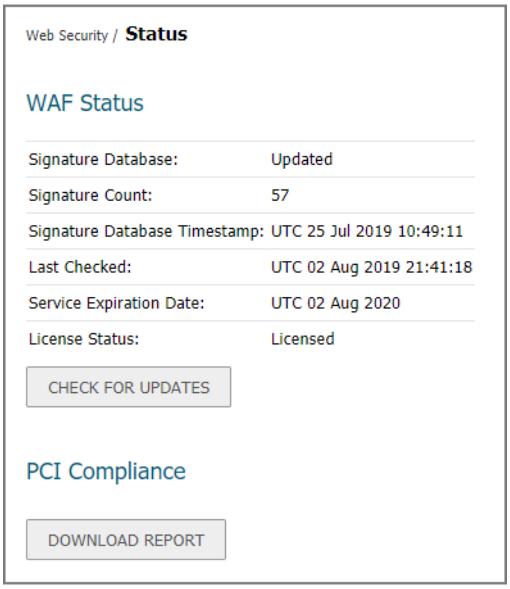
Topics:

- Using the Web Security Status Page on page 105
- Configuring Web Security Settings on page 106
- Configuring Web Security Signatures on page 118
- Configuring Web Security Custom Rules on page 122
- Configuring Web Security App Profiling on page 135
- Viewing the Web Security Licensing Page on page 138

Using the Web Security Status Page

The **Web Security > Status** page provides status information about the Web Application Firewall service and signature database, and displays the license status and expiration date. This page provides a way to download the latest signatures from the SonicWall online database and to generate and download a PCI compliance report.

Web Security > Status Page



Web Security / **Status**

WAF Status

Signature Database:	Updated
Signature Count:	57
Signature Database Timestamp:	UTC 25 Jul 2019 10:49:11
Last Checked:	UTC 02 Aug 2019 21:41:18
Service Expiration Date:	UTC 02 Aug 2020
License Status:	Licensed

PCI Compliance

Topics:

- Viewing Status and Synchronizing Signatures on page 106
- Downloading a PCI Compliance Report on page 106

Viewing Status and Synchronizing Signatures

To view the status of the signature database, service license, and update signatures:

1 Navigate to **Web Security > Status**. The **WAF Status** section displays the following information:
   - Status of updates to the signature database
   - Signature count
   - 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 Click **CHECK FOR UPDATES** to check the backend database for updated signatures.

> ⓘ **NOTE:** The **Web Security > Settings** page provides an option to update and apply new signatures automatically.

Downloading a PCI Compliance Report

To download a PCI Compliance report:

1 Navigate to **Web Security > Status** page.

2 Under **PCI Compliance**, click **DOWNLOAD REPORT**.

3 Click on your downloaded **PCIReport.pdf** document to see your **WAF PCI DSS Compliance Report**.

Configuring Web Security Settings

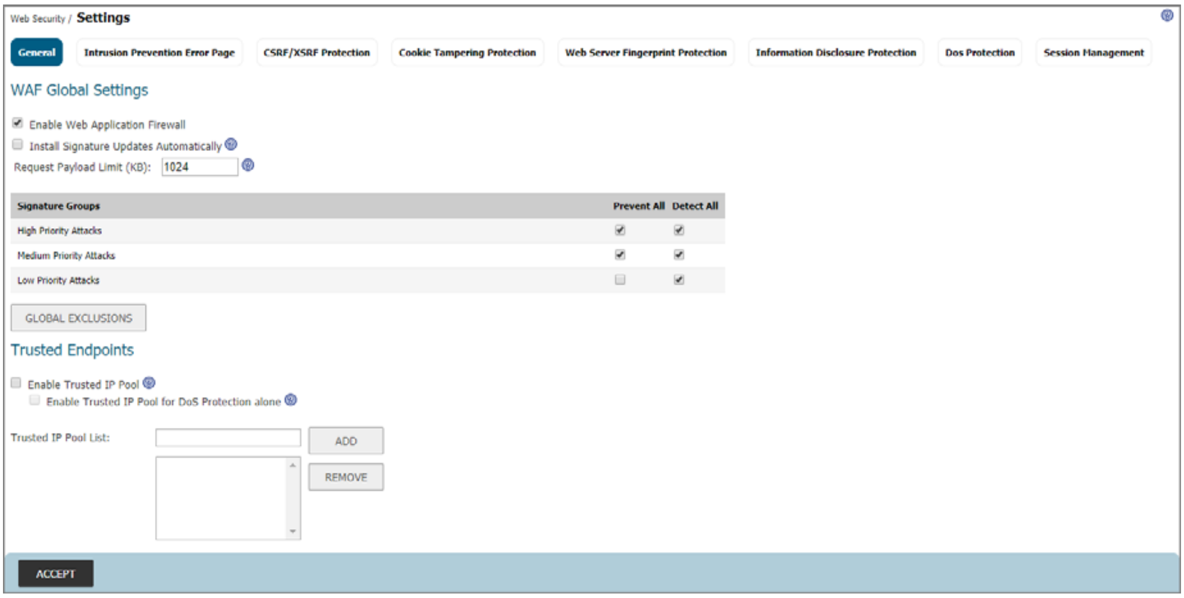
The **Web Security > Settings** page provides eight screens. Click the buttons along the top to display the screen you want, then click **ACCEPT** after making changes on that screen.

Topics:

Configuring General Settings

The **General** screen of the **Web Security > Settings** page allows you to globally enable and disable Web Application Firewall, enable automatic signature updates, specify detection or prevention for high, medium, and low priority attack classes, and set up global exclusions and trusted endpoints.

Web Security > Settings > General Screen



Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management

WAF Global Settings

☑ Enable Web Application Firewall

☐ Install Signature Updates Automatically

Request Payload Limit (KB): 1024

Signature Groups	Prevent All	Detect All
High Priority Attacks	☑	☑
Medium Priority Attacks	☑	☑
Low Priority Attacks	☐	☑

Trusted Endpoints

☐ Enable Trusted IP Pool

☐ Enable Trusted IP Pool for DoS Protection alone

Trusted IP Pool List:

To enable and activate Web Application Firewall, you must select the check box to globally enable it and select at least one of the check boxes in the **Signature Groups** table. The settings in the **WAF Global 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** check box to temporarily disable Web Application Firewall without losing any of your custom configuration settings.

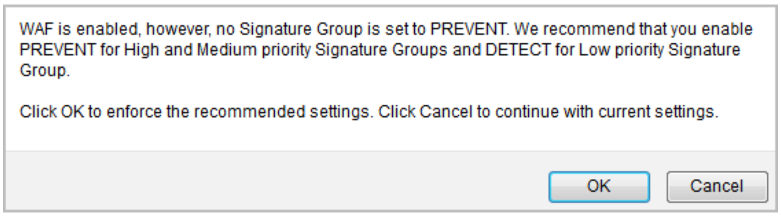
You can enable automatic signature updates so that new signatures are automatically downloaded and applied when available. A log entry is generated for each automatic signature update. If a signature is deleted during automatic updating, its associated Exclusion List is also removed. A log entry is generated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

To configure WAF global settings:

1 Navigate to the **General** screen of the **Web Security > Settings** page.

2 To globally enable SonicWall WAF, select the **Enable Web Application Firewall** check box.

3 A warning dialog box is displayed if none of the signature groups have **Prevent All** already selected.



WAF is enabled, however, no Signature Group is set to PREVENT. We recommend that you enable PREVENT for High and Medium priority Signature Groups and DETECT for Low priority Signature Group.

Click OK to enforce the recommended settings. Click Cancel to continue with current settings.

4 Click **OK** in the dialog box to set the high and medium priority signature groups to **Prevent All**, or click **Cancel** to leave the settings as they are or to manually continue the configuration.

5 Select the **Install Signature Updates Automatically** check box to enable new signatures to be automatically downloaded and installed when available. New signatures take effect immediately.

6 For **Request Payload Limit (KB)**, leave the default of 1024 or select another value in the field. The minimum is 10 and the maximum is 102400.

This limits the size of the request body in kilobytes. If the body size exceeds the limit, the request will be blocked. This limit does not apply to files uploaded through WAF. It applies only to content included inline in the request body, such as POST parameters, plain text, XML, and JSON. File uploads have a 1GB limit.

7 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 check boxes.

8 Select the desired level of protection for **Medium Priority Attacks** in the Signature Groups table.

9 Select the desired level of protection for **Low Priority Attacks** in the Signature Groups table.

10 Optionally configure Global Exclusions and Trusted Endpoints. See Configuring Global Exclusions on page 108 and Configuring Trusted Endpoints on page 109.

11 Click **ACCEPT** to save your changes.

Configuring Global Exclusions

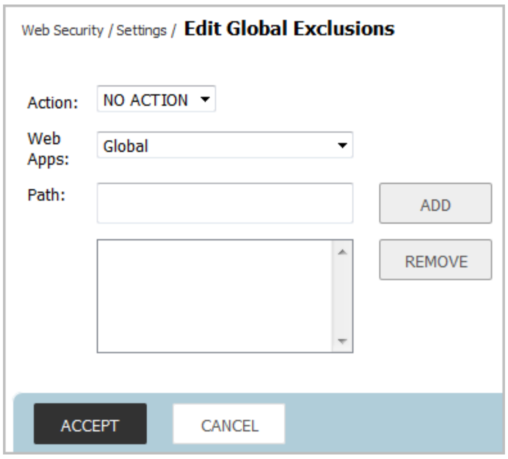
There are three ways that you can exclude specific web applications from currently configured global WAF settings. You can completely disable Web Application Firewall for certain apps, you can lower the action level from Prevent to Detect for certain apps, or you can set Web Application Firewall to take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

To configure global exclusions:

1 Navigate to the **General** screen of the **Web Security > Settings** page.

2 Click **GLOBAL EXCLUSIONS**.

In the **Edit Global Exclusions** page, the action you set overrides the signature group settings for the resources configured on this page.


Web Security / Settings / **Edit Global Exclusions**

Action: NO ACTION

Web Apps: Global

Path:

3 Select one of the following from the **Action** drop-down list:

- **DISABLE** – Disables Signature Groups, Custom Rules, and App Profiling rules for the path of web apps listed in Global Exclusions settings.
- **DETECT** – Lowers the action level from prevention to detection and logging for the web application.
- **NO ACTION** – The Global Exclusion settings will be ignored, but remain intact and can be turned on for other actions later.

4 Select the web application to exclude from the **Web Apps** drop-down list. Select **Global** to apply the exclusion to all web apps in the list.

5 In the **Path** field, optionally type in a path to a particular folder or HTML file. If a path is configured, then the exclusion is recursively applied to all subfolders and files. For instance, if **Path** is set to **webmail.company.com/exchange**, then all files and folders under **exchange** are also excluded.

6 Click **ADD** to move the path into the list box.

7 Repeat Step 5 and Step 6 to add more paths to this exclusion.

8 Click **ACCEPT** in the **Edit Global Exclusions** page.

9 Click **ACCEPT** in the **Web Security > Settings** page to save your changes.

Configuring Trusted Endpoints

The options under **Trusted Endpoints** on the **General** screen of the **Web Security > Settings** page provide a way to create a “white list” of trusted hosts.

For trusted hosts in the list, access to a web application from the host is automatically profiled for the following if the web app is in profiling state:

- **Form Based CSRF Protection** – if CSRF Protection is enabled for the web app
- **App Profiling**

To configure trusted endpoints:

1 Navigate to the **General** screen of the **Web Security > Settings** page.

2 In the **Trusted Endpoints** section, select the **Enable Trusted IP Pool** check box. When you click on this check box, you **Enable Trusted IP Pool for DoS Protection alone**.

Web Security features and DOS protection are disabled for trusted hosts. **When Enable Trusted IP Pool for DoS Protection alone** is checked, only DOS protection is disabled and Web Security features are still enforced.

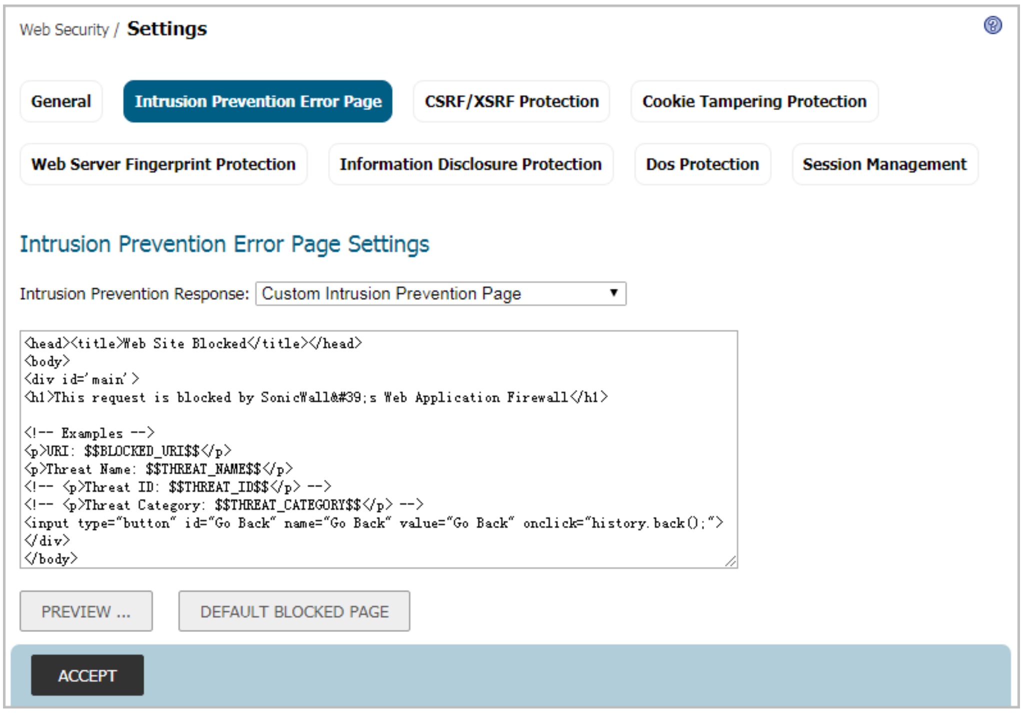
3 In the **Trusted IP Pool List** field, type in an IP address for a trusted host and then click **ADD** to add it to the list box. You can add up to 32 host IP addresses to the **Trusted IP Pool List**.

4 Click **ACCEPT** to save your changes.

Configuring the Intrusion Prevention Error Page

The **Intrusion Prevention Error Page** screen of the **Web Security > Settings** page provides a way to create a custom error page to be displayed when an intrusion prevention occurs.

Web Security > Settings > Intrusion Prevention Error Page Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
Intrusion Prevention Error Page Settings
PREVIEW ...
DEFAULT BLOCKED PAGE
ACCEPT

Intrusion Prevention Response: Custom Intrusion Prevention Page ▾

```
<head><title>Web Site Blocked</title></head>
<body>
<div id='main'>
<h1>This request is blocked by SonicWall&#39;s Web Application Firewall</h1>

<!-- Examples -->
<p>URI: $$BLOCKED_URI$$</p>
<p>Threat Name: $$THREAT_NAME$$</p>
<!-- <p>Threat ID: $$THREAT_ID$$</p> -->
<!-- <p>Threat Category: $$THREAT_CATEGORY$$</p> -->
<input type="button" id="Go Back" name="Go Back" value="Go Back" onclick="history.back();">
</div>
</body>
```

To configure the Intrusion Prevention Error Page settings:

1 Navigate to the **Intrusion Prevention Error Page** screen of the **Web Security > Settings** page.

2 In the **Intrusion Prevention Response** drop-down list, select the custom page option or the desired error response code to be displayed when blocking an intrusion attempt. The choices are:

- **Custom Intrusion Prevention 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**

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 **PREVIEW**.

5 To reset the current customized error page to the default error page, click **DEFAULT BLOCKED PAGE** and then click **OK** in the confirmation dialog box.

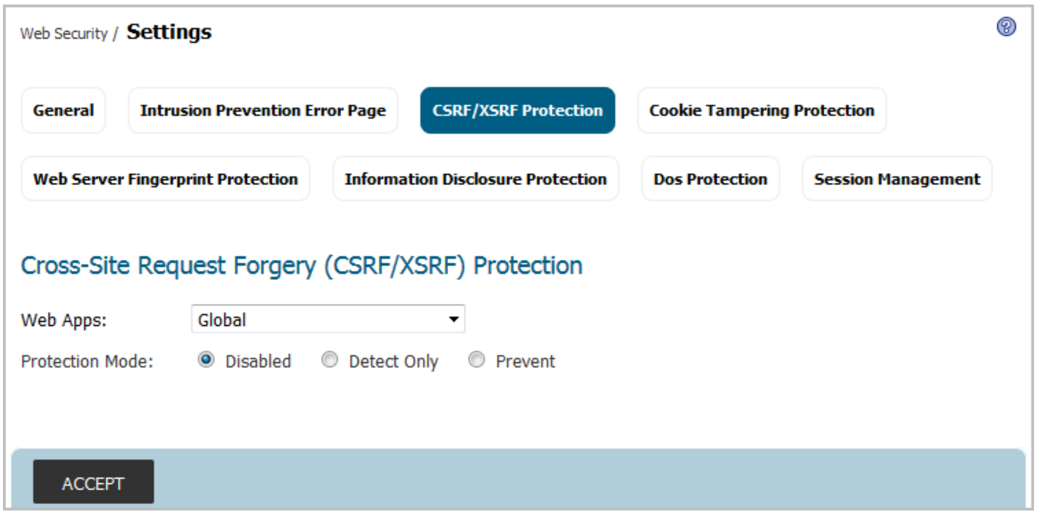
6 Click **ACCEPT** to save your changes.

Configuring CSRF/XSRF Protection

The **CSRF/XSRF Protection** screen of the **Web Security > Settings** page provides settings for Cross-Site Request Forgery (CSRF/XSRF) protection. You can set the same level of protection for all web apps, or configure it for each web app independently.

When a web app is used by users, the CSRF settings page lists every URL that is a candidate for CSRF protection. The enforcement happens only when the administrator marks the candidates for prevention.

Web Security > Settings > CSRF/XSRF Protection Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
ACCEPT

Cross-Site Request Forgery (CSRF/XSRF) Protection

Web Apps: Global

Protection Mode: ● Disabled ○ Detect Only ○ Prevent

To configure the CSRF/XSRF Protection settings:

1 Navigate to the **CSRF/XSRF Protection** screen of the **Web Security > Settings** page.

2 In the **Web Apps** drop-down list, select the web app to which these CSRF protection settings apply. To make these CSRF settings the default for all web applications, select **Global**.

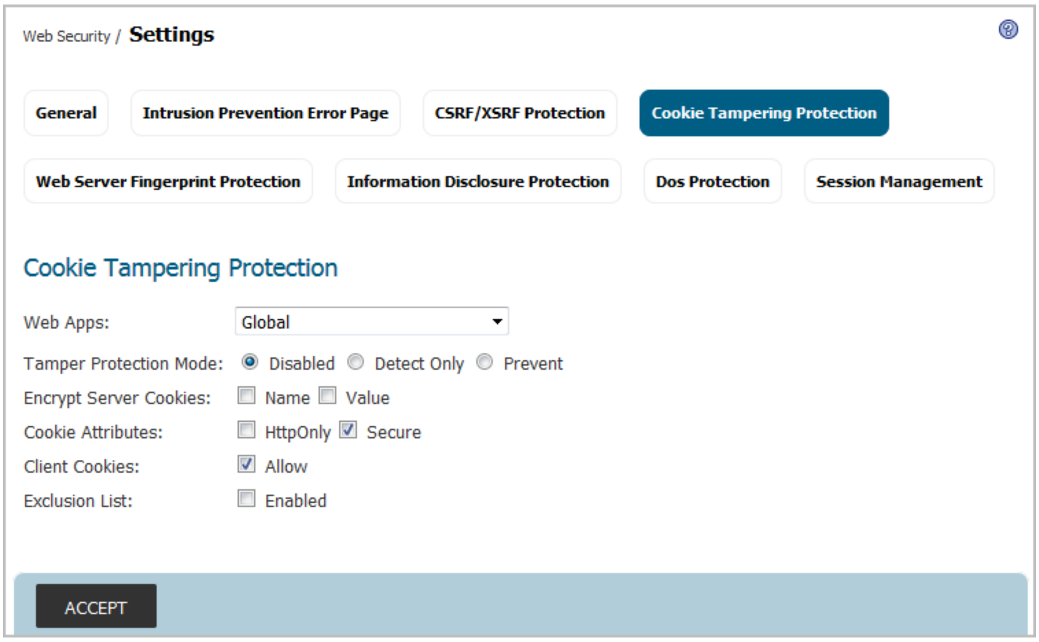
3 For **Protection Mode**, select the desired level of protection against CSRF attacks. Select **Disabled** to disable CSRF protection, select **Detect Only** to log these attacks, or select **Prevent** to log and block them.

4 Click **ACCEPT** to save your changes.

Configuring Cookie Tampering Protection

The **Cookie Tampering Protection** screen of the **Web Security > Settings** page provides settings for cookie tampering protection. You can set the same level of protection for all web apps, or configure it for each web app independently.

Web Security > Settings > Cookie Tampering Protection Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
ACCEPT

Cookie Tampering Protection

Web Apps: Global

Tamper Protection Mode: ● Disabled ○ Detect Only ○ Prevent

Encrypt Server Cookies: □ Name □ Value

Cookie Attributes: □ HttpOnly ☑ Secure

Client Cookies: ☑ Allow

Exclusion List: □ Enabled

To configure the Cookie Tampering Protection settings:

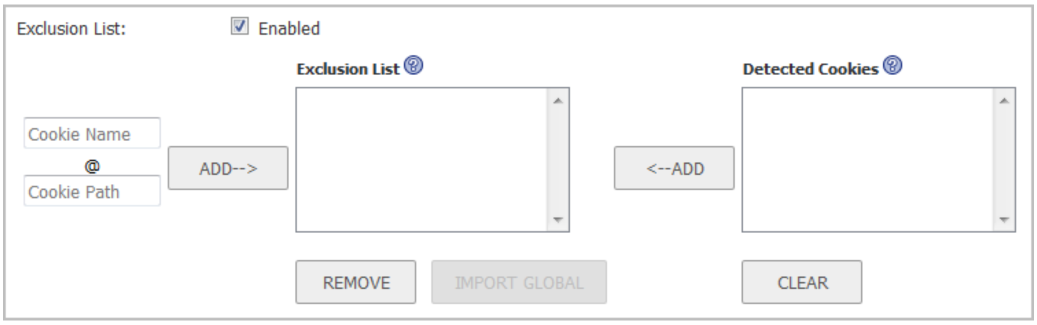
1. Navigate to the **Cookie Tampering Protection** screen of the **Web Security > Settings** page.
2. In the **Web Apps** drop-down list, select the application offloaded web app to which these protection settings apply. To make these settings the default for all web applications, select **Global**.
3. For **Tamper Protection Mode**, select the desired level of protection against cookie tampering attacks. Select one of the following:
   - **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 web app. This option is not available when **Global** is selected in the **Web Apps** drop-down list.

   Cookie tampering protection ensures that cookies set by the protected web application are not tampered with or modified by the clients. If **Prevent** is selected, a request with a tampered cookie is blocked. If **Detect** is selected, the event is logged.
4. For **Encrypt Server Cookies**, select the **Name** check box to encrypt the cookie name, and select the **Value** check box to encrypt the values of the cookies. This affects client-side script behavior because it makes encrypted cookie names or values unreadable. Only server-side cookies are encrypted by these options.
5. For **Cookie Attributes**, select the **HttpOnly** check box to append the *HTTPOnly* attribute to server-side cookies, and/or select the **Secure** check box to append the *Secure* attribute to server-side cookies. The *HTTPOnly* attribute prevents 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 *Secure* attribute 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.

6 For **Client Cookies**, select the **Allow** check box only when the web application needs ***all*** of the client cookies. When disabled, client-side cookies are not allowed to be sent to the backend systems. You can add the needed cookies to the **Exclusion List** below. This option does not affect server-side cookies.

7 For **Exclusion List**, select the **Enabled** check box to configure a cookie exclusion list. The display changes to expose more configuration fields.



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.

8 In the **Cookie Name** field, type in the name or ID of the cookie. This entry is case-sensitive.

9 In the **Cookie Path** field, type in the path to the cookie name you just entered. The path is also case-sensitive.

> **NOTE:** Cookies with the same name and different paths are treated as different cookies. You can leave the path empty if there are multiple cookies with the same name and different paths; an empty path represents all paths. If a path is specified, it includes all subfolders and all paths starting with the same specified path. For example, ***/path*** includes ***/path/subpath*** and ***/pathtail***.

10 Click **ADD-->** to add the cookie name and path (if any) to the **Exclusion List** box.

11 Optionally remove entries from the **Exclusion List** box by selecting them and then clicking **REMOVE**.

12 The **Detected Cookies** list box contains all cookies set by the client. Optionally select one or more and then click **<--ADD** to add those cookies to the **Exclusion List** box. Cookies beginning with **C:** are client cookies and those beginning with **S:** are server cookies.

13 Optionally click **CLEAR** to remove all entries from the **Detected Cookies** list box.

14 Click **ACCEPT** to save your changes.

Configuring Web Server Fingerprint Protection

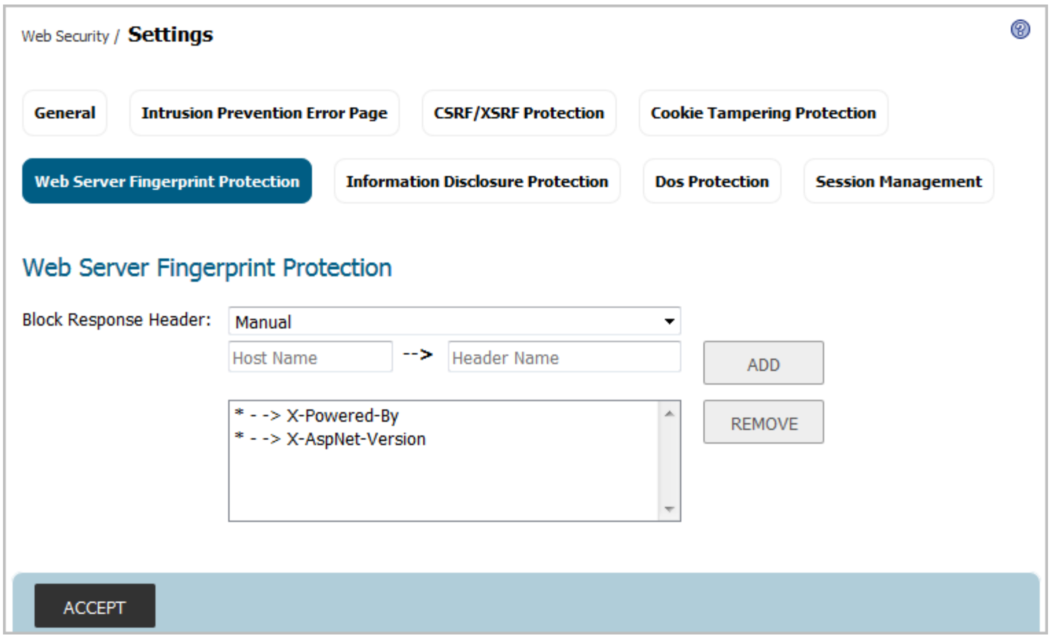
The **Web Server Fingerprint Protection** screen of the **Web Security > Settings** page provides settings for removing headers from web server responses. This prevents information about the web server from being disclosed to a bad actor who could use it to determine how to penetrate the server.

Some essential headers like *Content-Type* and *Connection* are generated by Web Application Firewall and cannot be removed.

The following headers are always obfuscated or removed by default:

- *Date*
- *Server*
- *X-Pad*

Web Security > Settings > Web Server Fingerprint Protection Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
Web Server Fingerprint Protection
Host Name
Header Name
ADD
REMOVE
ACCEPT

Block Response Header: Manual

Host Name --> Header Name

* - -> X-Powered-By
* - -> X-AspNet-Version

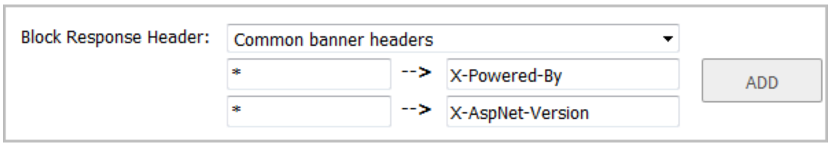
To configure the Web Server Fingerprint Protection settings:

1 Navigate to the **Web Server Fingerprint Protection** screen of the **Web Security > Settings** page.

2 In the **Block Response Header** drop-down list, select one of the following header types and fill in the fields:

> **NOTE:** Asterisks in the **Host Name** fields indicate all hosts. To block the response header for a single offloaded web application, put its virtual host domain name or virtual host IP address value into the **Host Name** field.

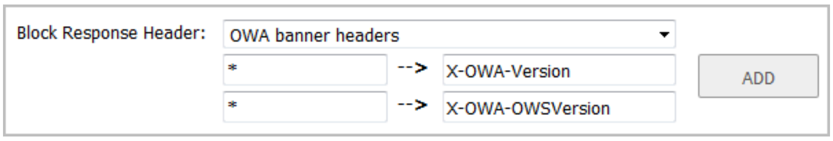
- **Common banner headers** – The display changes to show two common headers, *X-Powered-By* and *X-AspNet_Version* in the **Header Name** fields.



Block Response Header: Common banner headers

* --> X-Powered-By
* --> X-AspNet-Version

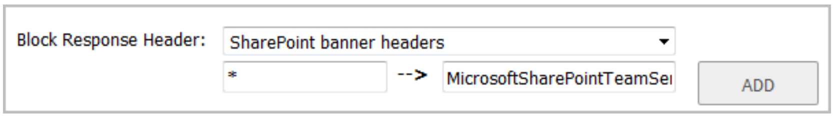
- **OWA banner headers** – The display changes to show two Outlook Web Access headers, X-OWA-Version and X-OWA-OWSVersion in the **Header Name** fields.



Block Response Header: OWA banner headers

* --> X-OWA-Version
* --> X-OWA-OWSVersion

- **SharePoint banner headers** – The display changes to show one SharePoint header, MicrosoftSharePointTeamServices in the **Header Name** field.

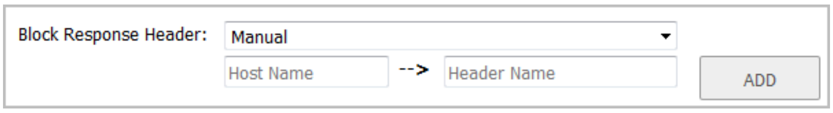


Block Response Header: SharePoint banner headers

* --> MicrosoftSharePointTeamSe

- **Manual** – The display shows a single **Host Name** field and **Header Name** field. Type an asterisk into the **Host Name** field to indicate all hosts, or type in the virtual host domain name or virtual host IP address value to block the response header for a single offloaded web application.

  Type the desired response header to block into the **Header Name** field.



Block Response Header: Manual

Host Name --> Header Name

3 Click **ADD** to add the entry or entries to the list box.

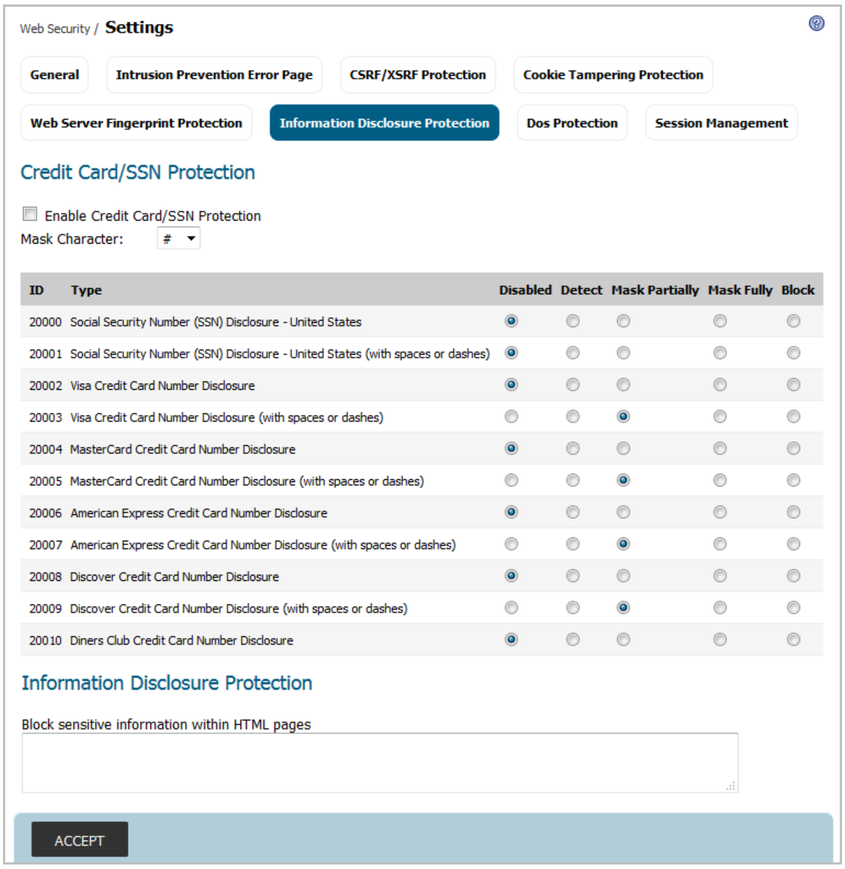
4 To remove entries from the list box, select one or more and then click **REMOVE**.

5 Click **ACCEPT** to save your changes.

Configuring Information Disclosure Protection

The **Information Disclosure Protection** screen of the **Web Security > Settings** page provides settings to prevent 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.

Web Security > Settings > Information Disclosure Protection Screen



Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management

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	●	○	○	○	○
20001	Social Security Number (SSN) Disclosure - United States (with spaces or dashes)	●	○	○	○	○
20002	Visa Credit Card Number Disclosure	●	○	○	○	○
20003	Visa Credit Card Number Disclosure (with spaces or dashes)	○	○	●	○	○
20004	MasterCard Credit Card Number Disclosure	●	○	○	○	○
20005	MasterCard Credit Card Number Disclosure (with spaces or dashes)	○	○	●	○	○
20006	American Express Credit Card Number Disclosure	●	○	○	○	○
20007	American Express Credit Card Number Disclosure (with spaces or dashes)	○	○	●	○	○
20008	Discover Credit Card Number Disclosure	●	○	○	○	○
20009	Discover Credit Card Number Disclosure (with spaces or dashes)	○	○	●	○	○
20010	Diners Club Credit Card Number Disclosure	●	○	○	○	○

Information Disclosure Protection

Block sensitive information within HTML pages

To configure Information Disclosure Protection settings:

1. Navigate to the **Information Disclosure Protection** screen of the **Web Security > Settings** page.

   The table in the **Credit Card/SSN Protection** section 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.

2. Select the **Enable Credit Card/SSN Protection** check box.

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 done.
   - **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. In the **Information Disclosure Protection** section under the table, type confidential text strings that should not be revealed on any web site protected by Web Application Firewall into the **Block sensitive information within HTML pages** text box. 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.

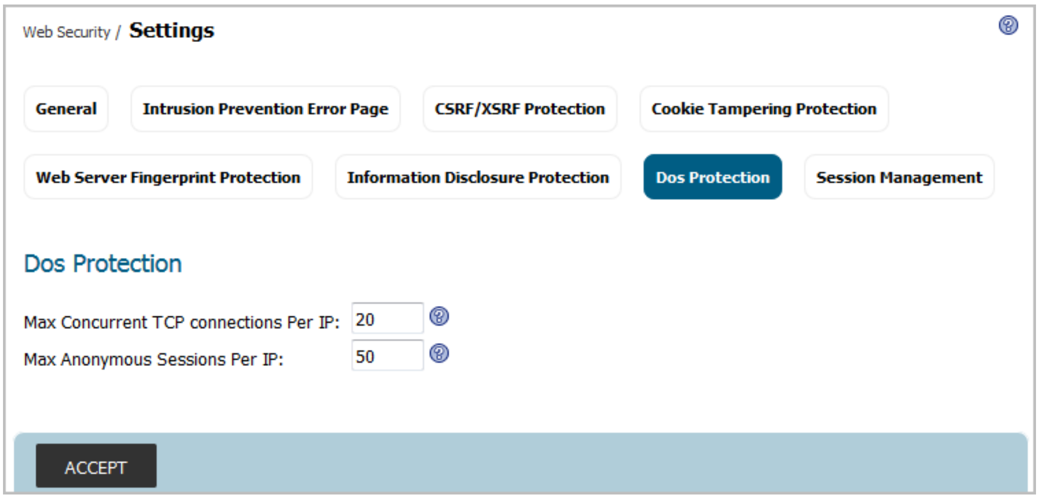
   You can also configure patterns to block in web server responses using the Custom Rules feature. See Configuring Web Security Custom Rules on page 122.

6. Click **ACCEPT** to save your changes.

Configuring Dos Protection

The **Dos Protection** screen of the **Web Security > Settings** page provides settings to prevent Denial of Service attacks.

Web Security > Settings > DOS Protection Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
ACCEPT

Dos Protection

Max Concurrent TCP connections Per IP: 20

Max Anonymous Sessions Per IP: 50

To configure Dos Protection settings:

1 Navigate to the **Dos Protection** screen of the **Web Security > Settings** page.

2 In the **Max Concurrent TCP connections Per IP** field, type in a number between 20 and 10000. This is the maximum number of concurrent TCP connections that a client can open with the WAF web server. The default is 20.

3 In the **Max Anonymous Sessions Per IP** field, type in a number between 20 and 1000. This is the maximum number of anonymous sessions that a client can create with the WAF web server. The default is 50.

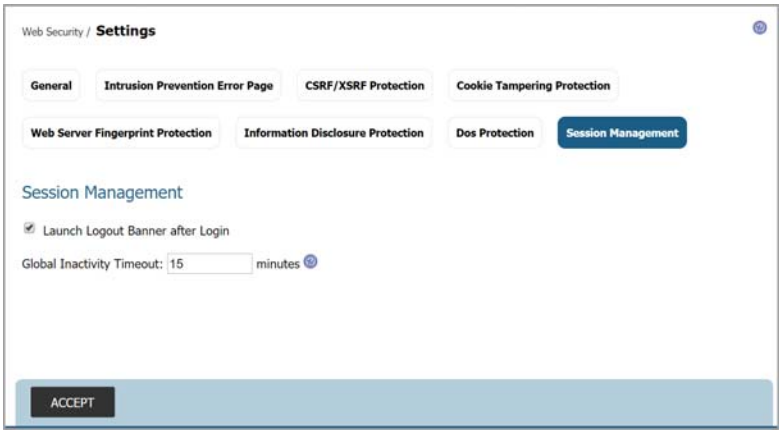
> ⓘ **NOTE:** To disable session-based DOS protection for an application, clear the **Enable Anonymous Session Tracking** check box on the **Application Delivery > App Offloading > Edit Web App** screen for the application.

4 Click **ACCEPT** to save your changes.

Configuring Session Management

The **Session Management** screen of the **Web Security > Settings** page provides settings to control user sessions on the WAF web server.

Web Security > Settings > Session Management Screen


Web Security / Settings
General
Intrusion Prevention Error Page
CSRF/XSRF Protection
Cookie Tampering Protection
Web Server Fingerprint Protection
Information Disclosure Protection
Dos Protection
Session Management
ACCEPT

Session Management

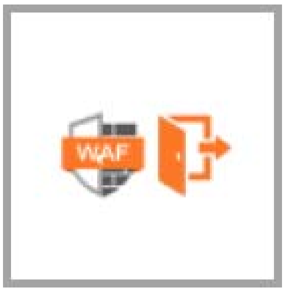
☑ Launch Logout Banner after Login

Global Inactivity Timeout: 15 minutes

To configure session management settings:

1 Navigate to the **Session Management** screen of the **Web Security > Settings** page.

2 Select the **Launch Logout Banner after Login** check box to enable the session logout WAF logo banner and logout button.



When this check box is enabled, the banner and logout button appear in the top-right corner and on the web app page.

> ⓘ **NOTE:** The banner can be dragged from the top-right corner to another position at the top of the page.

3 In the **Global Inactivity Timeout** field, select the number of inactive minutes allowed before the user is logged out. The timeout value can be any number between 1 and 525,600. This setting can be overridden by Group or User settings.

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

4 Click **ACCEPT** to save your changes.

Configuring Web Security Signatures

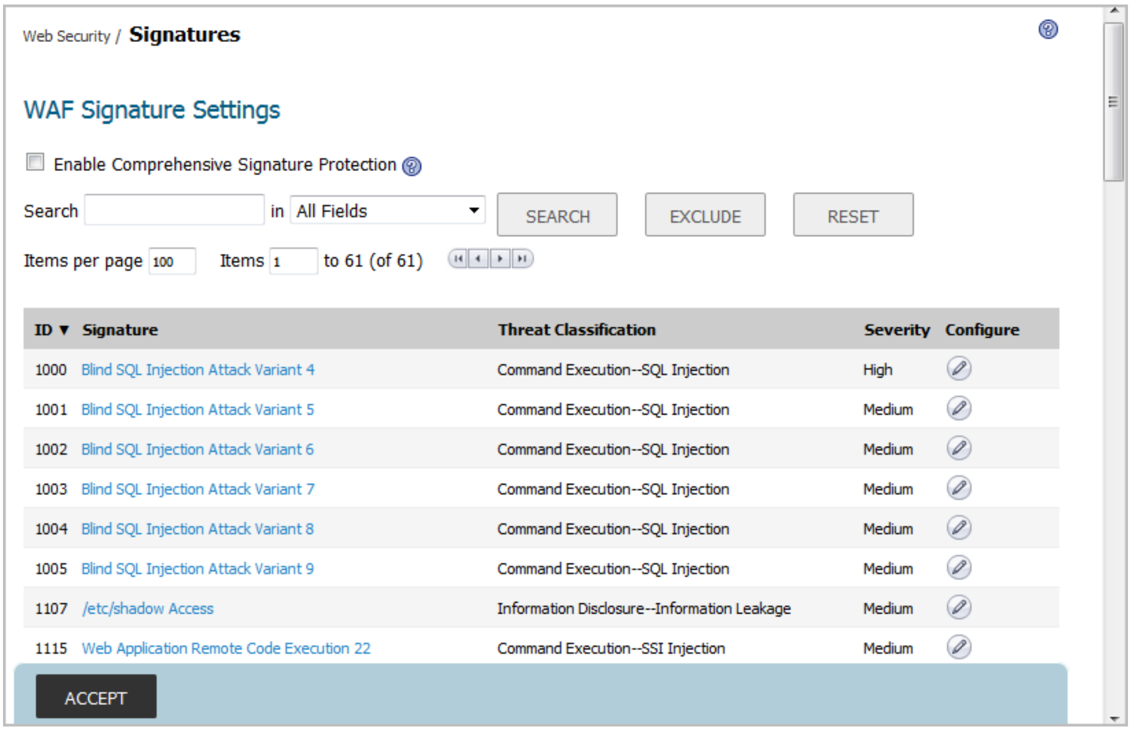
The **Web Security > Signatures** page allows you to configure custom handling or exclusion of certain hosts on a per-signature basis. You can use signature-based exclusions to apply exclusions for all hosts for each signature. See Configuring Signature Based Custom Handling and Exclusions on page 119.

You can also revert back to using the global settings for the signature group to which a signature belongs without losing the configuration details of existing exclusions. See Reverting a Signature to Global Settings on page 121.

On the **Web Security > 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.

The list of signatures can be sorted by the contents of any column in ascending or descending order by clicking the column heading. In addition, signatures can be divided into pages and filtered by searching for a key word. The default is 50 signatures per page.

Web Security > Signatures Page



Web Security / **Signatures**

WAF Signature Settings

□ Enable Comprehensive Signature Protection

Search [ ] in All Fields

Items per page 100 Items 1 to 61 (of 61)

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	✎
1107	/etc/shadow Access	Information Disclosure--Information Leakage	Medium	✎
1115	Web Application Remote Code Execution 22	Command Execution--SSI Injection	Medium	✎

To configure WAF signature settings:

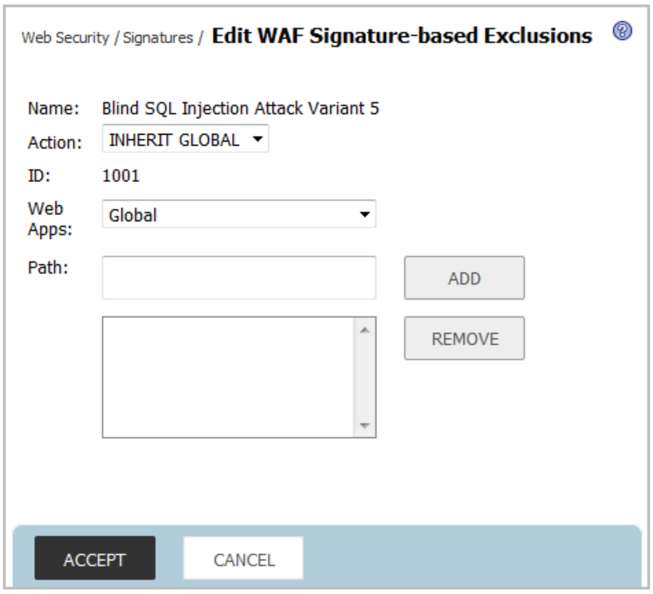
1. Navigate to the **Web Security > Signatures** page.
2. Select the **Enable Comprehensive Signature Protection** check box to protect application specific signatures and low severity signatures for higher security. By default, all the critical signatures for your websites are already protected.
3. 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.
4. Click **EXCLUDE** to display only signatures that do not contain the key word in the **Search** field. All matches are highlighted.
5. Click **RESET** to display all signatures.
6. Change the **Items per page** field to display more or fewer signatures in the table.
7. Click the arrow buttons to page forward or back, or to jump to the first or last page of signatures.
8. Click **ACCEPT** to save your changes.

Configuring Signature Based Custom Handling and Exclusions

You can disable inspection for a signature in traffic to an individual offloaded web application, or for all web apps. You can also change the handling of detected threats for an individual web app or for all web apps. 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 offloaded web apps. If no web apps are configured, the action is applied to the signature itself and acts as a global setting for all web apps. This change blocks access to a web app 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 Security > Settings** page.

Web Security > Edit WAF Signature-Based Exclusions Screen



Web Security / Signatures / **Edit WAF Signature-based Exclusions**

Name: Blind SQL Injection Attack Variant 5

Action: INHERIT GLOBAL

ID: 1001

Web Apps: Global

Path:

To configure exclusions or custom handling for a signature:

1. Navigate to the **Web Security > Signatures** page and click the edit button in the **Configure** column for the signature you want to exclude or customize.
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 web apps listed in this exclusion
   - **DETECT** – Detect and log threats matching this signature from web apps listed in this exclusion, but do not block access to the web apps
   - **PREVENT** – Log and block host access for threats matching this signature from web apps listed in this exclusion
   - **INHERIT GLOBAL** – The Signature-based Exclusion settings for the resources configured on this page will be ignored, but remain intact and can be turned on for other actions later.
3. To apply this action globally to all web apps, select **Global** from the **Web Apps** drop-down list. To apply this action to an individual web app, type in the virtual host domain name as it appears in the offloaded web application configuration. This can be a host name or an IP address.
4. In the **Path** field, you can configure a path to a particular folder or file along with the web app. 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 **Web Apps** is set to **webmail.yourcompany.com/exchange**, then all files and folders under **exchange** are also excluded.
5. If you specified a **Path**, click **ADD** to move the path into the list box. Optionally add more paths in the same way.
6. Click **ACCEPT** in the **Edit WAF Signature-based Exclusions** screen.
7. Click **ACCEPT** in the **Web Security > Signatures** page to save your changes.

To change a customized or excluded signature back to the global signature group settings, see Reverting a Signature to Global Settings on page 121.

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 web app names and paths in place in case you need to re-enable the exclusion.

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

1 Navigate to the **Web Security > Signatures** page and click the edit button in the **Configure** column for the signature that you wish to change.

1 In the **Edit WAF Signature-based Exclusions** screen, select **INHERIT GLOBAL** from the **Action** drop-down list.

2 In the **Web Apps** field, select **Global** to revert to global signature settings for all web apps. To apply this action to an individual web app, select its name in the **Web Apps** field.

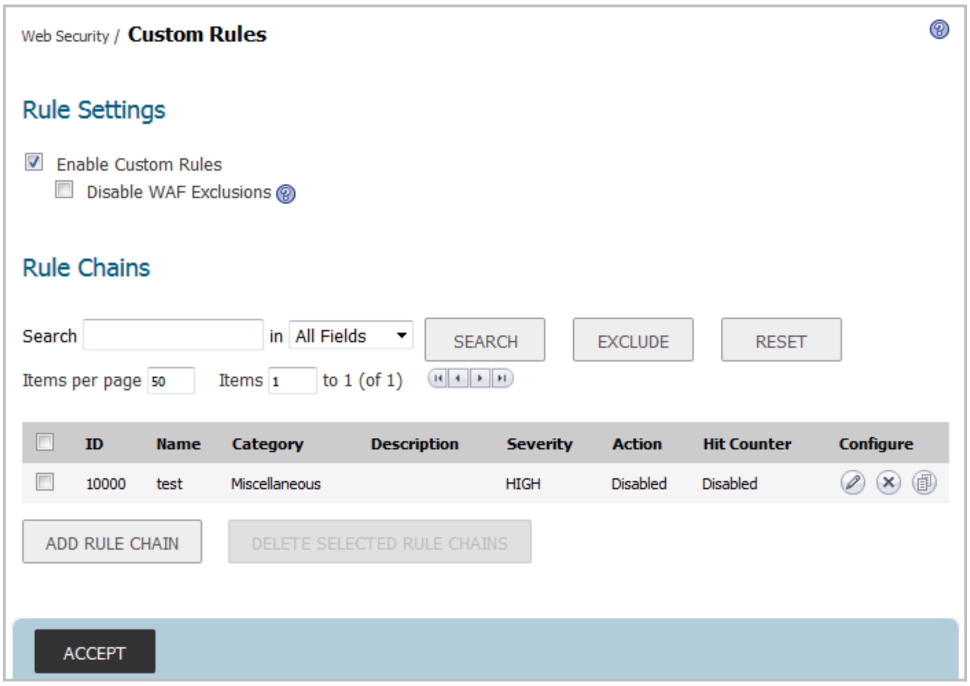
3 Click **ACCEPT** to save your changes.

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.

Configuring Web Security Custom Rules

The **Web Security > Custom Rules** page allows you to configure custom rules with all the same properties as the signatures in the SonicWall signature database.

Web Security > Custom Rules Page



Web Security / **Custom Rules**

Rule Settings

☑ Enable Custom Rules

□ Disable WAF Exclusions

Rule Chains

Search in All Fields

Items per page 50 Items 1 to 1 (of 1)

□	ID	Name	Category	Description	Severity	Action	Hit Counter	Configure
□	10000	test	Miscellaneous		HIGH	Disabled	Disabled	

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.

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 virtual host. One rule in the chain is configured to match the URI or web app virtual 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 host. When the request is blocked, the user sees a custom block page. The **Dashboard > Monitoring** page also shows the activity in the graphs.

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.

> **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.

To configure settings on the Custom Rules page:

1 Navigate to the **Web Security > Custom Rules** page.

2 Select the **Enable Custom Rules** check box to globally enable the custom rules feature.

3 Select the **Disable WAF Exclusions** check box if you want to apply the custom rules to WAF administrator pages.

> ⓘ **NOTE:** By default, some critical WAF administrator pages are excluded from custom rules to prevent inadvertent admin lockout. Be sure that the admin login will not be blocked before enabling the **Disable WAF Exclusions** option.

4 In the **Rule Chains** section, to display only rule chains 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.

5 Click **EXCLUDE** to display only rule chains that do not contain the key word in the **Search** field. All matches are highlighted.

6 Click **RESET** to display all rule chains.

7 Change the **Items per page** field to display more or fewer rule chains in the table.

8 Click the arrow buttons to page forward or back, or to jump to the first or last page of rule chains.

9 Click **ACCEPT** to save your changes.

Adding or Editing a Rule Chain

You can add a new rule chain manually by clicking **ADD RULE CHAIN** or by cloning an existing rule chain by clicking the clone button in the **Configure** column of an existing rule chain and then editing it.

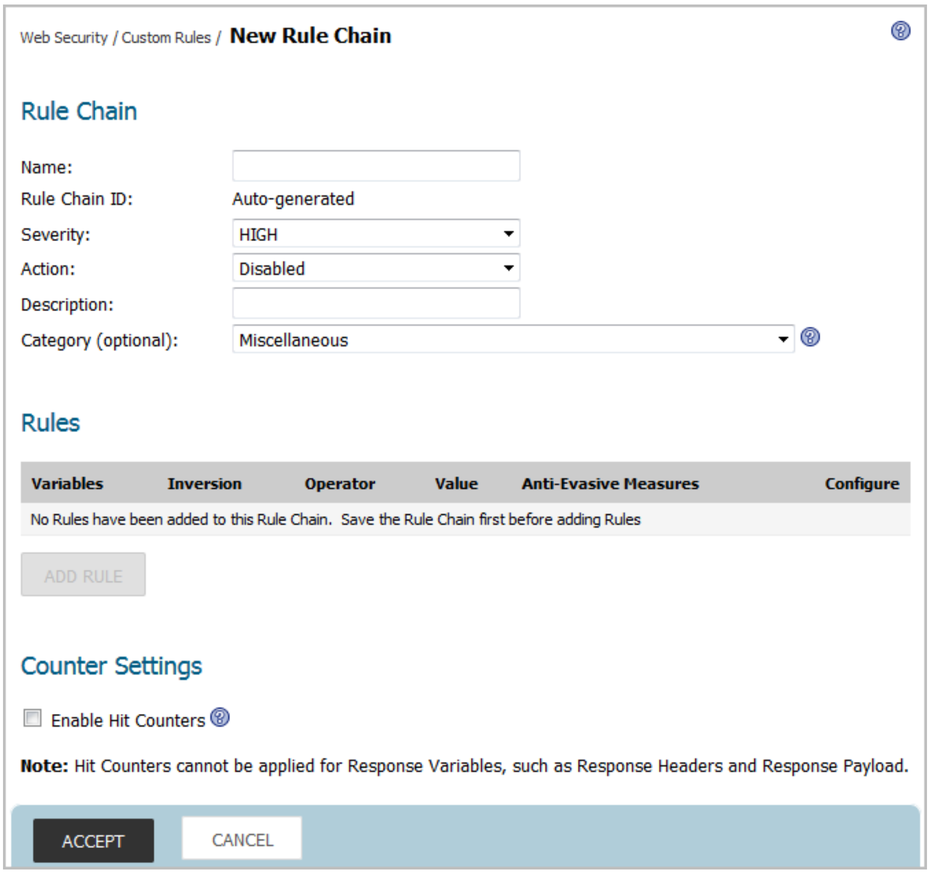
You can configure rate limiting when adding or editing a rule chain. When rate limiting is enabled for a rule chain, the action for the rule chain is triggered only when the number of matches within a configured time period is above the configured threshold.

To add, edit, or clone a rule chain and configure it, including for rate limiting:

1 Navigate to the **Web Security > Custom Rules** page.

2 In the **Rule Chains** section, do one of the following:

- Click **ADD RULE CHAIN**. The **New Rule Chain** screen is displayed.



Web Security / Custom Rules / **New Rule Chain**

Rule Chain

Name:	
Rule Chain ID:	Auto-generated
Severity:	HIGH
Action:	Disabled
Description:	
Category (optional):	Miscellaneous

Rules

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
No Rules have been added to this Rule Chain. Save the Rule Chain first before adding Rules					

Counter Settings

□ Enable Hit Counters

Note: Hit Counters cannot be applied for Response Variables, such as Response Headers and Response Payload.

- Click the edit button in the **Configure** column of an existing rule chain. The displayed screen is very similar to the **New Rule Chain** screen, except that some fields already show the configured values.
- Click the clone button in the **Configure** column of an existing rule chain and then click **OK** in the confirmation dialog. The displayed screen is very similar to the **New Rule Chain** screen, except that some fields already show the configured values.

3 In the **Name** field, type in a descriptive name for the rule chain.

4 For **Severity**, select **HIGH**, **MEDIUM**, or **LOW** from the drop-down list, depending on the severity associated with this rule chain.

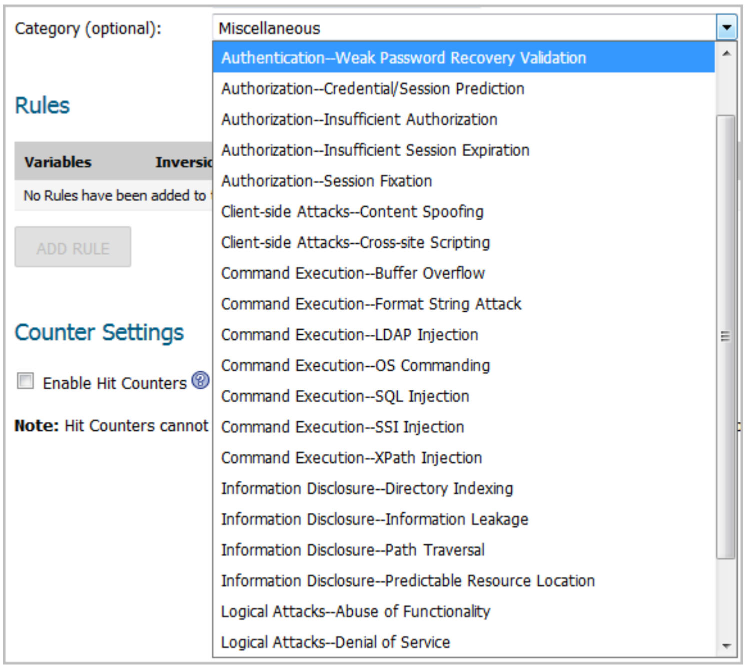
5 For **Action**, select **Disabled**, **Detect Only**, or **Prevent** from the drop-down list.

- **Disabled** – The rule chain should not take effect.
- **Detect Only** – Allow the traffic, but log it.
- **Prevent** – Block traffic that matches the rule and log it.

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

6 In the **Description** field, type in a description of what the rule chain matches or other information.

7 Optionally select a category for this rule chain from the **Category** drop-down list. The default is **Miscellaneous**. This field is for informational purposes, and does not change the way the rule chain is applied.



Category (optional): Miscellaneous

Rules

Variables	Inversic
No Rules have been added to	

Counter Settings

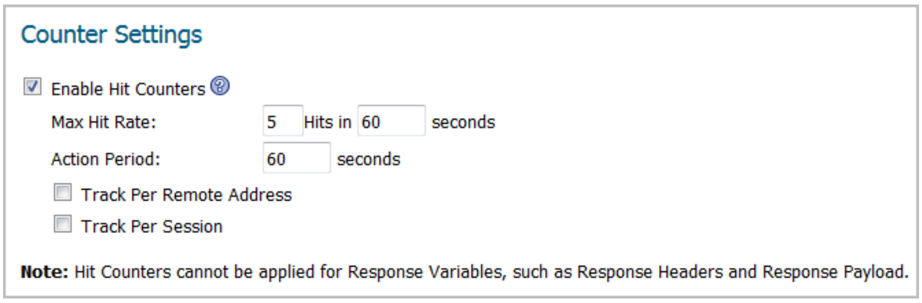
□ Enable Hit Counters

Note: Hit Counters cannot

- Authentication--Weak Password Recovery Validation
- Authorization--Credential/Session Prediction
- Authorization--Insufficient Authorization
- Authorization--Insufficient Session Expiration
- Authorization--Session Fixation
- Client-side Attacks--Content Spoofing
- Client-side Attacks--Cross-site Scripting
- Command Execution--Buffer Overflow
- Command Execution--Format String Attack
- Command Execution--LDAP Injection
- Command Execution--OS Commanding
- Command Execution--SQL Injection
- Command Execution--SSI Injection
- Command Execution--XPath Injection
- Information Disclosure--Directory Indexing
- Information Disclosure--Information Leakage
- Information Disclosure--Path Traversal
- Information Disclosure--Predictable Resource Location
- Logical Attacks--Abuse of Functionality
- Logical Attacks--Denial of Service

8 Skip the **Rules** section for now. Rules can only be added to an existing rule chain.

9 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.



Counter Settings

☑ Enable Hit Counters

Max Hit Rate: 5 Hits in 60 seconds

Action Period: 60 seconds

□ Track Per Remote Address

□ Track Per Session

Note: Hit Counters cannot be applied for Response Variables, such as Response Headers and Response Payload.

10 In the **Max Hit Rate** field for **Hits**, enter the number of matches for this rule chain that must occur before the selected action is triggered.

11 In the **Max Hit Rate** field for **seconds**, enter the time period during which the configured number of rule chain matches must occur before the selected action is triggered.

12 In the **Action Period** field, enter the number of seconds during which the action for this rule chain is performed after being triggered.

13 Select the **Track Per Remote Address** check box 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 Web Application Firewall. 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.

14 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.

15 Click **ACCEPT** to save your changes. A **Rule Chain ID** is automatically generated.

Deleting a Rule Chain

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

To delete a rule chain:

1. Navigate to the **Web Security > Custom Rules** page.
2. In the table under **Rule Chain**, click the delete button in the **Configure** column for the rule chain you want to delete.
3. Click **OK** in the confirmation dialog box.
4. Click **ACCEPT** to save your changes.

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.

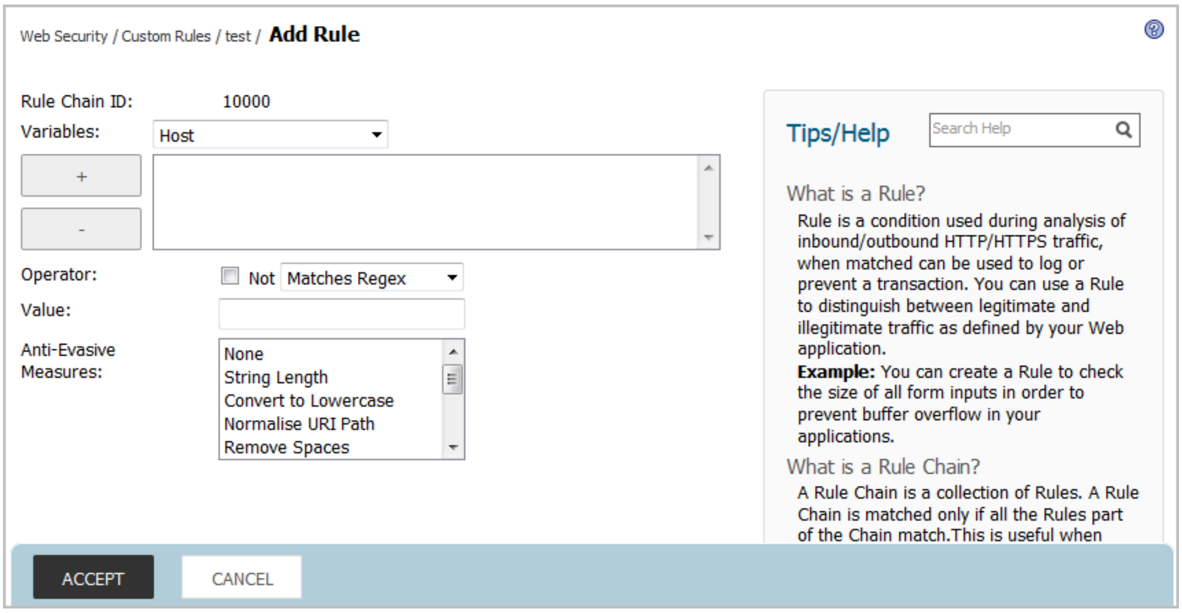
Rules allow the administrator to employ both a positive security model and a negative security model. In a positive security model, policies are written only to allow known traffic and block everything else.

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 129 for more information about variables.
- **Operators** – These are arithmetic and string operators. The **Not** check box is an inversion operator used to match any value except the configured condition. See About Operators on page 131 for more information about the operators.
- **Value** – This entity can be a number, literal string, or a regular expression that is compared with the scanned target. 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 measures beyond those supported by the **Operators** field, especially to enforce Anti-Evasive protection. See About Anti-Evasive Measures on page 131 for more information about these measures.

Web Security > Custom Rules - Add Rule Screen



Web Security / Custom Rules / test / **Add Rule**

Rule Chain ID: 10000

Variables: Host

Operator: □ Not Matches Regex

Value:

Anti-Evasive Measures: None, String Length, Convert to Lowercase, Normalise URI Path, Remove Spaces

What is a Rule?

Rule is a condition used during analysis of inbound/outbound HTTP/HTTPS traffic, when matched can be used to log or prevent a transaction. You can use a Rule to distinguish between legitimate and illegitimate traffic as defined by your Web application.

Example: You can create a Rule to check the size of all form inputs in order to prevent buffer overflow in your applications.

What is a Rule Chain?

A Rule Chain is a collection of Rules. A Rule Chain is matched only if all the Rules part of the Chain match.This is useful when

The following sections provide detailed information about rules:

- Adding or Editing a Rule on page 127
- Cloning a Rule on page 128
- Deleting a Rule on page 128
- About the Tips/Help Sidebar on page 128
- About Variables on page 129
- About Operators on page 131
- About Anti-Evasive Measures on page 131
- Example Use Cases for Rules on page 133

Adding or Editing a Rule

See Example Use Cases for Rules on page 133 for examples.

To add or edit a rule in a rule chain:

1. Navigate to the **Web Security > Custom Rules** page.
2. In the **Rule Chains** section, click the edit icon in the **Configure** column for the rule chain on which you want to add or edit a rule. The page for that rule chain opens.
3. Click **ADD RULE** to add a new rule, or click the edit icon in the **Configure** column for the rule you want to edit.
4. In the **Add Rule** page or the page for the edited rule, select a variable from the **Variables** drop-down list. See About the Tips/Help Sidebar on page 128 and About Variables on page 129 for information about the available variables.
5. 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).

6 Click the '+' (plus) button to add the variable to the rule. Repeat Step 4 through Step 6 to add more variables.

To delete a variable, select it in the large text box and click the '-' (minus) button.

7 Select a string or arithmetic operator from the **Operators** drop-down list. To complete the inverse operation, select **Not**. See About Operators on page 131 for information about the available operators.

8 In the **Value** field, type in the value to be compared with the selected variable(s) in the scanned HTTP(S) input. If you selected the **Matches Keyword** operator, you can compare the input against multiple values by typing in each value separated by a space. Each value is compared individually.

9 Select one or more measures from the **Anti-Evasive Measures** list. Hold **Ctrl** on your keyboard while clicking to select multiple measures. See About the Tips/Help Sidebar on page 128 and About Anti-Evasive Measures on page 131 for information about anti-evasive measures.

10 Click **ACCEPT** to save your changes.

Cloning a Rule

To clone a rule:

1 On the **Web Security > Custom Rules** page, click the edit icon in the **Configure** column for the rule chain which contains the rule you want to clone. The page for that rule chain opens.

2 Click the clone icon in the **Configure** column 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 on page 127.

Deleting a Rule

To delete a rule from a rule chain:

1 On the **Web Security > Custom Rules** page, click the edit icon in the **Configure** column for the rule chain from which you want to delete a rule. The page for that rule chain opens.

2 Click the delete icon in the **Configure** column for the rule you want to delete.

3 Click **OK** in the confirmation dialog box.

4 Click **ACCEPT** to save your changes.

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.
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	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. To match against some aspect of the entire list of parameter values, such as the number of parameter values, leave the selection field empty. 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.
Parameter Names	Yes	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. To match against some aspect of the entire list of parameter names, leave the selection field empty. To match against the name of a particular parameter, specify the parameter name in the selection field to the right of the colon.
Remote Address	No	Refers to the client's IP address. This variable allows you to allow or block access from certain IP addresses.

Variables for Use in Rules

Variable Name	Collection	Description
Request Header Values	Yes	Refers to the collection of all HTTP(S) request header values for the current request. To match against some aspect of the entire list of request header values, leave the selection field empty. To match against a particular header value, specify the name of the header in the selection field to the right of the colon. For example, to block Ajax requests, select **Request Header Values** as the Variable, specify **X-Request-With** in the selection text box, and specify **ajax** in the **Value** field.
Request Header Names	Yes	Refers to the collection of all HTTP(S) request header names for the current request. To match against some aspect of the entire list of request 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. For example, to block requests that are not referred by a trusted host, select **Request Header Names** as the **Variable**, specify **Referrer** in the selection text box, enter the host names or IP addresses of the trusted hosts in the **Value** field, select the **Not** check box and select the **Matches Keyword** operator.
Response Header Values	Yes	Refers to the collection of all HTTP(S) response header values for the current request. To match against some aspect of the entire list of response header values, leave the selection field empty. To match against a particular header value, specify the name of the header in the selection field to the right of the colon.
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.
Server Hostname	No	Refers to the virtual host name of the web server 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.
Server Address	No	Refers to the IP address of the web server 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 string operators. The **Not** check box is an inversion operator that 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**.

Rule Operators 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 **Value** field.
Equals String	String	The scanned variable(s) match the alphanumeric string in the **Value** field exactly.
=	Arithmetic	The scanned variable is equal to the content of the **Value** field.
>	Arithmetic	The scanned variable is greater than the content of the **Value** field.
>=	Arithmetic	The scanned variable is greater than or equal to the content of the **Value** field.
<	Arithmetic	The scanned variable is less than the content of the **Value** field.
<=	Arithmetic	The scanned variable is less than or equal to the content of the **Value** field.
Matches Keyword	String	One or more of the scanned variables matches one of the keywords in the **Value** field. If multiple keywords are specified, they should be separated by spaces.
Matches Regex	String	One or more of the scanned variables matches the regular expression in the **Value** field. An example of a regular expression that matches any four decimal numbers is **\d{4}**.
Member of (CSV)	String	One or more of the scanned variables matches one of the comma separated values in the **Value** field.

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** measure 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 measures to choose from in the **Anti-Evasive Measures** field, including the **None** measure 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

Measure	Description
None	Use the **None** 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 **String Length** measure 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 **Convert to Lowercase** 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 **Value** field are all in lowercase. This is an anti-evasive measure to prevent hackers from changing case to bypass the rule.
Normalize URI Path	Use the **Normalize URI Path** 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 www.eshop.com/././//login.aspx is converted to www.eshop.com/login.aspx. This is an anti-evasive measure to prevent hackers from adding invalid references in the URI to bypass the rule.
Remove Spaces	Use the **Remove Spaces** 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.
Base64 Decode	Use the **Base64 Decode** measure to decode base64 encoded data before the comparison is made according to the rule. 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. This is an anti-evasive measure to prevent hackers from using base64 encoding of their input to bypass the rule.
Hexadecimal Decode	Use the **Hexadecimal Decode** measure to decode hexadecimal encoded data before the comparison is made according to the rule. This is an anti-evasive measure to prevent hackers from using hexadecimal encoding of their input to bypass the rule.
URL Decode URL Decode (Unicode)	Use the **URL Decode** measure to decode URL encoded strings in the input. Use the **URL Decode (Unicode)** 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. **NOTE**: Do not use these measures against an input that has been decoded already. 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. For example, the URI www.eshop.com/hack+URL%3B is converted to www.eshop.com/hack URL by this operator before the comparison is made.
Trim	Use the **Trim** 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. This is an anti-evasive measure to prevent hackers from adding spaces before and after the input data to bypass the rule.

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.

Topics:

- Example – Positive Security Model: Blocking a Form Submission with Unwanted Parameters on page 134
- Example – Negative Security Model: Blocking Malicious Input to a Form on page 134
- Example – Using URL Decode and None on page 134
- Example – Using Convert to Lowercase and URL Decode with Parameter Values on page 135
- Example – Using String Length and URL Decode with Parameter Values:ID on page 135

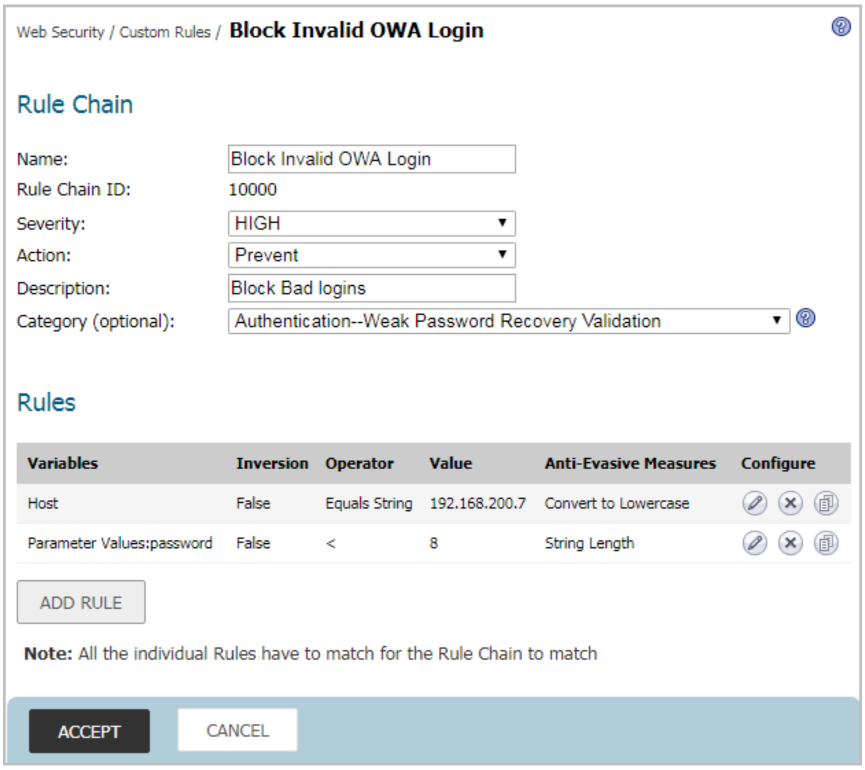
Example – Positive Security Model: Blocking Bad Logins

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 web server for the web app. 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



Web Security / Custom Rules / **Block Invalid OWA Login**

Rule Chain

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

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

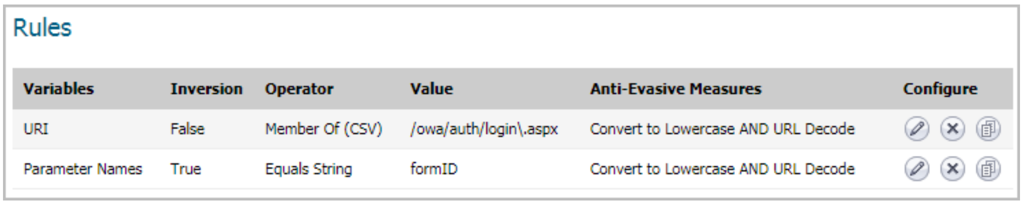
Note: All the individual Rules have to match for the Rule Chain to match

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:

1 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 check box selected.

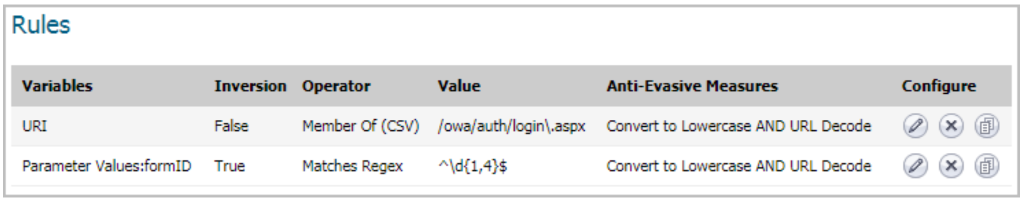


Rules

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Member Of (CSV)	/owa/auth/login\.aspx	Convert to Lowercase AND URL Decode	✎ ⊗ ⧉
Parameter Names	True	Equals String	formID	Convert to Lowercase AND URL Decode	✎ ⊗ ⧉

2 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 regular expression **^\d{1,4}$** which matches anything that consists of one to four digits. The **Not** inversion check box is selected to change the rule to match anything that does not consist of one to four digits.



Rules

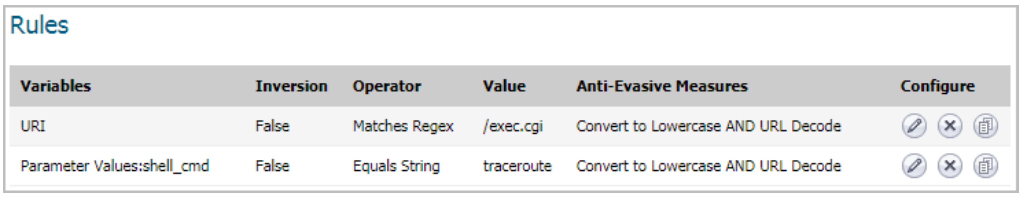
Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Member Of (CSV)	/owa/auth/login\.aspx	Convert to Lowercase AND URL Decode	✎ ⊗ ⧉
Parameter Values:formID	True	Matches Regex	^\d{1,4}$	Convert to Lowercase AND URL Decode	✎ ⊗ ⧉

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, **traceroute**.



Rules

Variables	Inversion	Operator	Value	Anti-Evasive Measures	Configure
URI	False	Matches Regex	/exec.cgi	Convert to Lowercase AND URL Decode	✎ ⊗ ⧉
Parameter Values:shell_cmd	False	Equals String	traceroute	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 might attempt to sneak those characters into the request by completing URL encoding on the characters before adding them to the request. The URI then contains **%0D** and **%0A** characters that could be used to launch an HTTP response splitting attack. The **URL Decode** and/or **URL Decode (Unicode)** measures 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/aaa%20bbb/ and the **URL Decode** measure is selected, the scanned URI becomes http://www.host.com/aaa bbb/ after decoding that 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 **aaa bbb** in order to block such a request. Because the backend application accepts case-insensitive inputs (aaa bbb and AAA BBB), the hacker can pass **aaa BBB** in the request and evade the rule. To prevent this evasion, the administrator specifies **Convert to Lowercase** as an anti-evasive measure and configures the value as **aaa bbb** 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 **aaa%20BBB**, which is the URL encoded version typically used by browsers. To prevent this evasion, the administrator specifies **URL Decode** as the anti-evasive measure to apply to the request entity. The input **aaa%20BBB** is URL decoded to **aaa BBB**. If the input is already **aaa BBB**, then URL decoding is not applied.

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

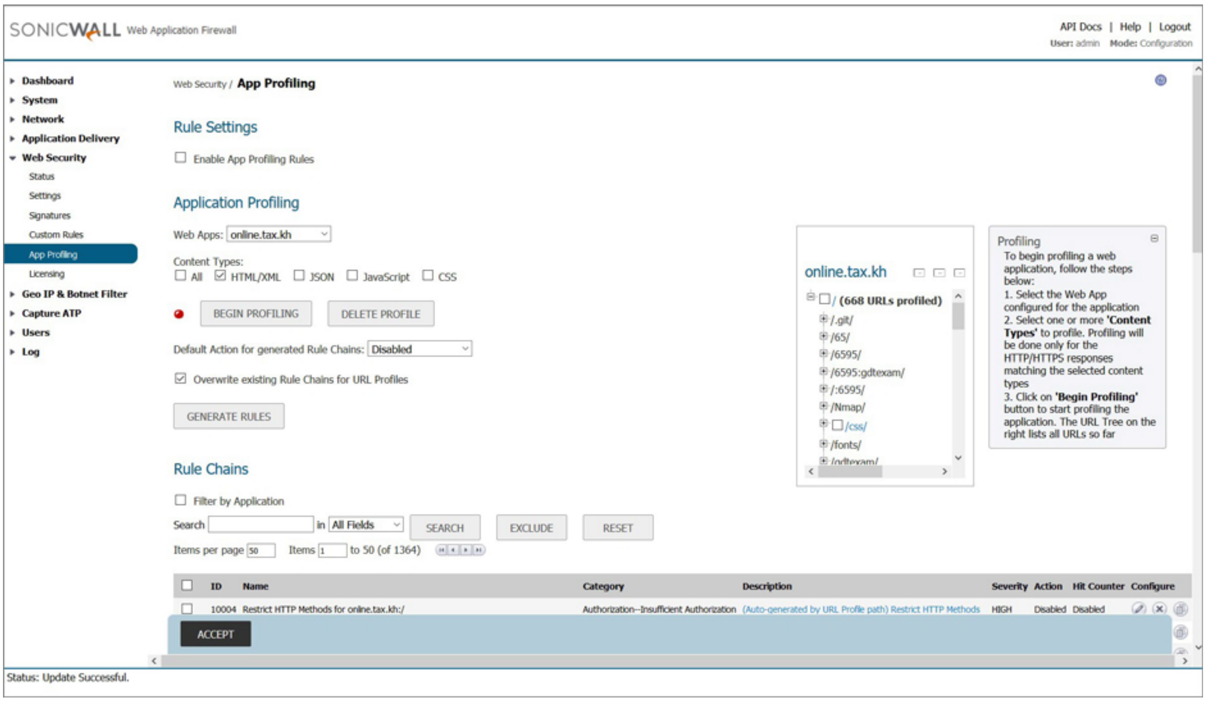
Comparing against a decoded input allows the administrator to use the **String Length** measure to check the length of the input against the matching variable. For example, if a web application ID parameter should not be more than four characters, the administrator could select **Parameter Values** in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

Configuring Web Security App 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 Web Application Firewall 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, you can use the “learned” URL profiles to generate rule chains that prevent malicious misuse of the applications.

Web Security > App Profiling Page



SONICWALL Web Application Firewall

API Docs | Help | Logout
User: admin Mode: Configuration

Web Security / **App Profiling**

Rule Settings

□ Enable App Profiling Rules

Application Profiling

Web Apps: online.tax.kh

Content Types:
□ All ☑ HTML/XML □ JSON □ JavaScript □ CSS

● BEGIN PROFILING DELETE PROFILE

Default Action for generated Rule Chains: Disabled

☑ Overwrite existing Rule Chains for URL Profiles

GENERATE RULES

online.tax.kh

□ / (668 URLs profiled)
- /.git/
- /65/
- /6595/
- /6595:gdtexam/
- /:6595/
- /Nmap/
- □ /css/
- /fonts/
- /gdtexam/

Profiling
To begin profiling a web application, follow the steps below:
1. Select the Web App 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

Rule Chains

□ Filter by Application

Search [ ] in All Fields SEARCH EXCLUDE RESET

Items per page 50 Items 1 to 50 (of 1364)

□	ID	Name	Category	Description	Severity	Action	Hit Counter	Configure
□	10004	Restrict HTTP Methods for online.tax.kh:/	Authorization--Insufficient Authorization	(Auto-generated by URL Profile path) Restrict HTTP Methods	HIGH	Disabled	Disabled	

ACCEPT

Status: Update Successful.

To configure application profiling and automatically generate rules:

1 Navigate to the **Web Security > App Profiling** page.

2 In the **Rule Settings** section, select the **Enable App Profiling Rules** check box.

3 In the **Application Profiling** section, select the application to be profiled from the **Web Apps** drop-down list.

4 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.
- **JSON** – Appropriate for an application written using JavaScript Object Notation (JSON).
- **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.

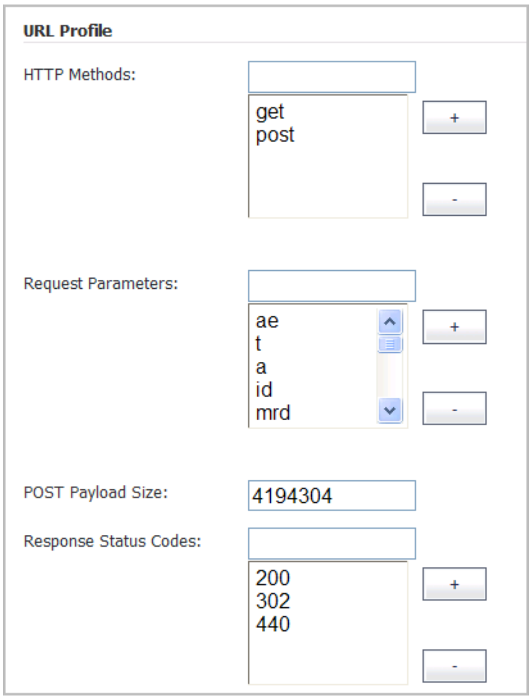
5 Click **BEGIN PROFILING** to start the “learning” process. Trusted users should be using the selected application during the active profiling period. As soon as you click it, the **BEGIN PROFILING** button changes to **END PROFILING**. Profiling continues until you click **END PROFILING**.

During profiling, Web Application Firewall records inputs and stores them as URL profiles. The URL profiles are listed as a tree structure on the **Web Security > App Profiling** page in the **Application Profiling** section. Only the URLs presented as hyperlinks are accessible URLs on the backend server.

6 After a period of time adequate to record inputs from normal application use, click **END PROFILING** to stop the profiling process.

7 Optionally click any of the links in the URL profile tree display to edit the learned values for that URL if the values are not accurate. Click ⤢ to expand all URLs at that level in the tree. You can also click ⟳ to refresh all URLs in the list or click ⊗ to delete a selected URL.

The editing page for the clicked URL is displayed.



URL Profile

HTTP Methods: get, post

Request Parameters: ae, t, a, id, mrd

POST Payload Size: 4194304

Response Status Codes: 200, 302, 440

8 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.

9 Click **ACCEPT** when finished editing. Repeat for other URLs as needed.

10 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 are disabled rather than active.
- **Detect Only** – Content triggering the generated rule is detected and logged.
- **Prevent** – Content triggering the generated rule is blocked and logged.

11 Select the **Overwrite existing Rule Chains for URL Profiles** check box to overwrite rule chains that have already been generated from a URL profile.

12 Click **GENERATE RULES** 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.

13 If you do not want to accept the generated rule chains, click the **DELETE SELECTED RULE CHAINS** button in the **Rule Chains** section under the rule chain list. All of the automatically added rule chains are pre-selected right after generation for easy deletion of the group.

14 In the **Rule Chains** section, to display only rule chains 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.

15 Click **EXCLUDE** to display only rule chains that do not contain the key word in the **Search** field. All matches are highlighted.

16 Click **RESET** to display all rule chains.

17 Change the **Items per page** field to display more or fewer rule chains in the table.

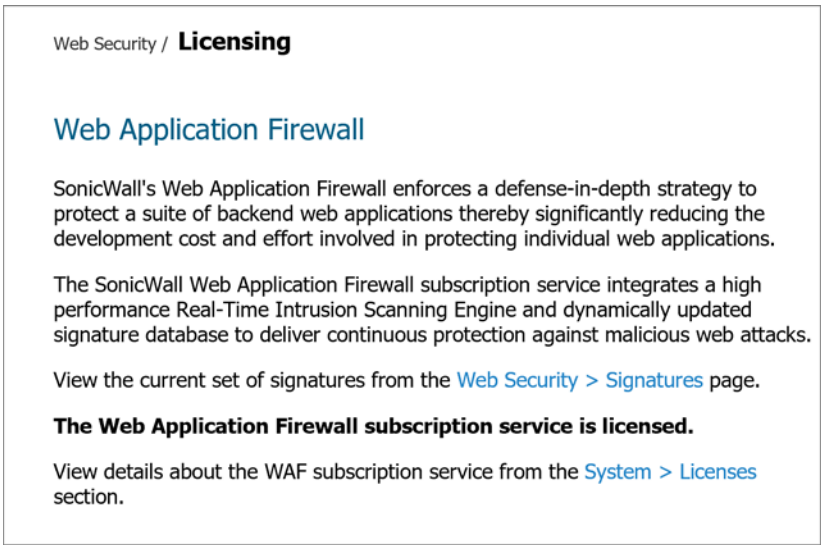
18 Click the arrow buttons to page forward or back, or to jump to the first or last page of rule chains.

19 Click **ACCEPT** to save your changes.

Viewing the Web Security Licensing Page

The **Web Security > Licensing** page displays a brief product description and provides links to the **Web Security > Signatures** and **System > Licenses** pages.

Web Security > Licensing Page



Web Security / **Licensing**

Web Application Firewall

SonicWall's Web Application Firewall enforces a defense-in-depth strategy to protect a suite of backend web applications thereby significantly reducing the development cost and effort involved in protecting individual web applications.

The SonicWall Web Application Firewall subscription service integrates a high performance Real-Time Intrusion Scanning Engine and dynamically updated signature database to deliver continuous protection against malicious web attacks.

View the current set of signatures from the Web Security > Signatures page.

The Web Application Firewall subscription service is licensed.

View details about the WAF subscription service from the System > Licenses section.

7

GeoIP & Botnet Filter Configuration

This section provides information and configuration tasks specific to the **Geo IP & Botnet Filter** pages in the SonicWall Web Application Firewall management interface. The Geo IP feature enables administrators to monitor and enforce policies effectively based on the geographical locations of remote users. The Botnet Filter feature enforces a strong and anti-evasive defense against any rogue activity from Botnets using a dynamically updated database maintained by SonicWall. Botnets pose huge security risks such as Denial of Service (DoS) attacks and Data Leakage. They are hard to identify and control because of the transient nature of their origins. The Geo IP and Botnet Filter features are disabled by default.

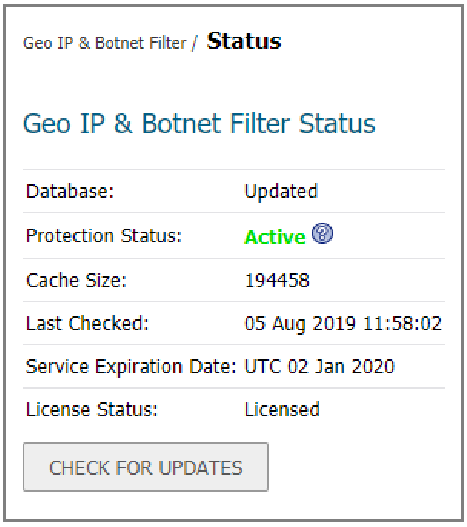
Topics:

- Viewing and Updating Geo IP & Botnet Filter Status on page 139
- Configuring Geo IP & Botnet Filter Settings on page 140
- Configuring Geo IP & Botnet Filter Policies on page 143
- Viewing Geo IP & Botnet Filter Licensing on page 146

Viewing and Updating Geo IP & Botnet Filter Status

The **Geo IP & Botnet Filter > Status** page provides status information about the SonicWall WAF Geo IP & Botnet Filter database, protection status, and cache size, and displays the license status and service expiration date. This page allows you to check for updates and download the latest data from the SonicWall online database.

Geo IP & Botnet Filter > Status Page



Geo IP & Botnet Filter / **Status**

Geo IP & Botnet Filter Status

Database:	Updated
Protection Status:	Active
Cache Size:	194458
Last Checked:	05 Aug 2019 11:58:02
Service Expiration Date:	UTC 02 Jan 2020
License Status:	Licensed

To view the status of the database, service license, and update the database:

1 Navigate to **Geo IP & Botnet Filter > Status**. The **Geo IP & Botnet Filter Status** section displays the following information:

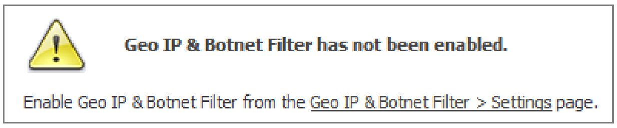
- **Database** shows the status of updates to the database.
- **Protection Status** shows whether the backend server is connected (**Active**) or not (**Offline**).

> ⓘ **NOTE: Protection Status** should display **Active**. If **Offline**, check your network settings and ensure that the following data servers are not blocked:
>
> - https://smagbdata.global.sonicwall.com
> - https://geoipdata.global.sonicwall.com

- **Cache Size** shows the total number of Geo IP and Botnet entries. Geo IP cache contains location information entries for IP and IP Range. Botnet cache contains IP entries. All caches are managed automatically by the server.
- **Last Checked** displays the timestamp of when the system last checked for available updates to the database.
- **Service Expiration Date** shows the license expiration date of the Geo IP & Botnet Filter service.
- **License Status** identifies whether the Geo IP & Botnet Filter service is licensed. The Geo IP & Botnet Filter is a subscription service that includes a free trial.

2 Click **CHECK FOR UPDATES** to check the backend database for updates. When **CHECK FOR UPDATES** is clicked, the server immediately checks for new database updates on the backend server.

When the Geo IP & Botnet Filter is licensed but disabled, the **Status** page displays a warning that contains a link to the **Settings** page where the feature can be enabled:



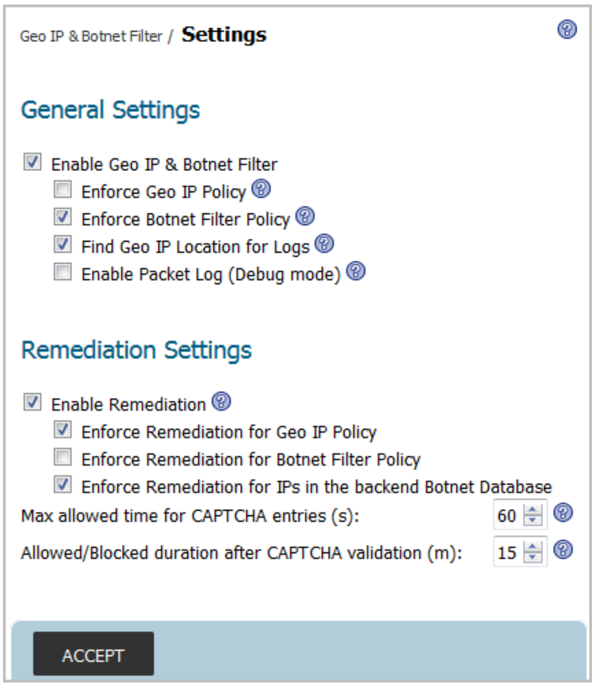
Geo IP & Botnet Filter has not been enabled.

Enable Geo IP & Botnet Filter from the Geo IP & Botnet Filter > Settings page.

Configuring Geo IP & Botnet Filter Settings

The **Geo IP & Botnet Filter > Settings** page allows you to globally enable and disable the Geo IP & Botnet Filter service, enable and disable policies, set log options, and enforce remediation using CAPTCHA.

Geo IP & Botnet Filter > Settings Page



Geo IP & Botnet Filter / **Settings**

General Settings

☑ Enable Geo IP & Botnet Filter
- □ Enforce Geo IP Policy
- ☑ Enforce Botnet Filter Policy
- ☑ Find Geo IP Location for Logs
- □ Enable Packet Log (Debug mode)

Remediation Settings

☑ Enable Remediation
- ☑ Enforce Remediation for Geo IP Policy
- □ Enforce Remediation for Botnet Filter Policy
- ☑ Enforce Remediation for IPs in the backend Botnet Database

Max allowed time for CAPTCHA entries (s): 60

Allowed/Blocked duration after CAPTCHA validation (m): 15

Topics:

- Configuring General Settings on page 141
- Configuring Remediation Settings on page 142

Configuring General Settings

The **General** screen of the **Geo IP & Botnet Filter > Settings** page allows you to globally enable and disable Geo IP & Botnet Filter, enable and disable Geo IP policies and Botnet policies, and configure log options.

To configure general settings:

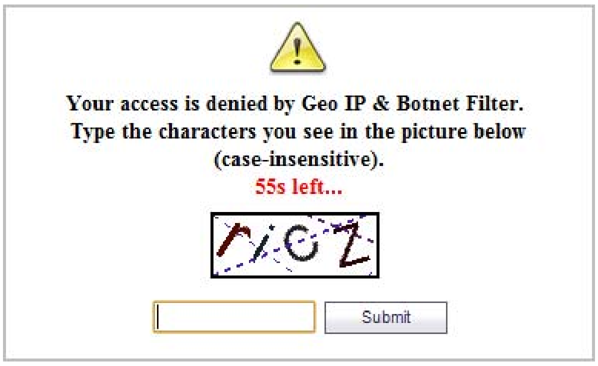
1. Navigate to **Geo IP & Botnet Filter > Settings | General Settings**.
2. Select the **Enable Geo IP & Botnet Filter** check box to globally enable Geo IP & Botnet Filter, or clear the check box to globally disable it.
3. Select the **Enforce Geo IP Policy** check box to globally enable Geo IP policies that you have configured, or clear the check box to globally disable them.
4. Select the **Enforce Botnet Filter Policy** check box to enable enforcing Botnet Filter policies. If this is disabled, Botnet IP addresses from the SonicWall database are not blocked, however, they are still detected and included in the Botnet Filter Statistics.
5. Select the **Find Geo IP Location for Logs** check box to add a **Location** column to the **Log > View** page that identifies the location of users’ source IP addresses. Mousing over an icon in the **Location** column displays the City (if applicable), Region, and Country of the source IP.
6. Select the **Enable Packet Log (Debug mode)** check box to generate log entries for allowed or denied packets. This option is for debug purposes only. Enabling the Packet Log makes logs increase rapidly if the log level is set to Debug.
7. Click **ACCEPT** to save your changes.

Configuring Remediation Settings

The **Geo IP & Botnet Filter > Settings | Remediation Settings** page allows you to globally enable and disable remediation, and enforce remediation for Geo IP policies, Botnet policies, and IP addresses in the backend Botnet Database. You can also set durations for CAPTCHA.

If remediation is enabled and enforced, users must use CAPTCHA to gain access. Remediation provides valid users an opportunity to prove that they are real users rather than “bots” and be allowed access.

For web access, users are redirected to the CAPTCHA page, as shown in the following figure. A countdown timer tells the time that remains for the user to complete remediation. The user must finish remediation within the allotted time, otherwise the user IP address is added to the block list and all access from that IP address is blocked for a period of time.



Your access is denied by Geo IP & Botnet Filter.
Type the characters you see in the picture below (case-insensitive).
55s left...

If remediation is successful within the verification time, the user is directed to the requested page. A CAPTCHA session is then created to record the remediation status. During the valid duration, all access from the IP address is allowed. After the valid duration, the CAPTCHA session expires. If the user is still logged in, access is not interrupted, but after the user login session expires the CAPTCHA session is deleted and remediation is required again.

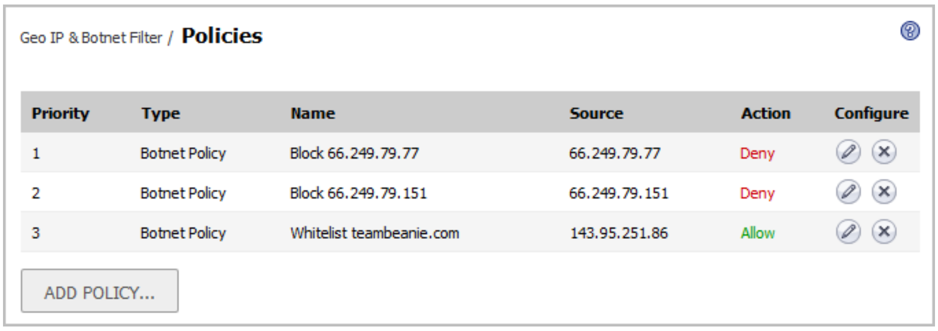
To enable Remediation and configure the settings:

1. Navigate to **Geo IP & Botnet Filter > Settings | Remediation Settings**.
2. Select the **Enable Remediation** check box to globally enable remediation using CAPTCHA, or clear the check box to globally disable it. If enabled, denied users cannot access resources protected by the appliance without CAPTCHA-based remediation.
3. Select the **Enforce Remediation for Geo IP Policy** check box to globally enforce remediation for Geo IP policies that you have configured. Using this option, remediation can be enforced separately for the IP addresses defined by your Geo IP Policy.
4. Select the **Enforce Remediation for Botnet Filter Policy** check box to globally enforce remediation for the Botnet Filter Policy.
5. Select the **Enforce Remediation for IPs in the backend Botnet Database** check box to globally enforce remediation for IP addresses in the backend Botnet Database.
6. In the **Max allowed time for CAPTCHA entries (s)** field, enter the number of seconds that the user has to complete Remediation. The minimum/maximum range is 30-300 seconds, the default is 60 seconds.
7. In the **Allowed/Blocked duration after CAPTCHA validation (m)** field, enter the number of minutes that the user is allowed/blocked after completing the CAPTCHA validation. The minimum value is five minutes and the maximum is 30, the default is 15 minutes.
8. Click **ACCEPT** to save your changes.

Configuring Geo IP & Botnet Filter Policies

The **Geo IP & Botnet Filter > Policies** page is used to view, add, edit, and delete Geo IP and Botnet Filter access policies. Up to a total of 64 Geo IP and Botnet Filter access policies can be created.

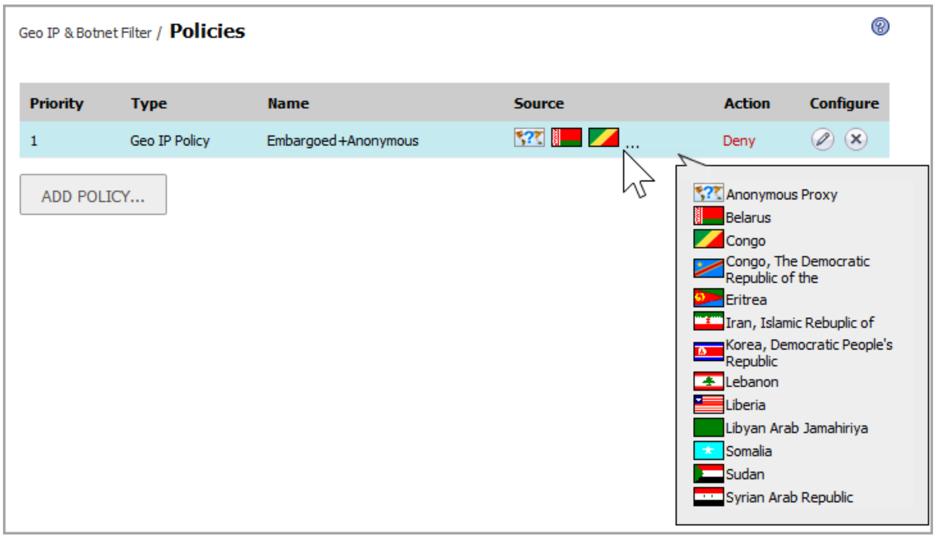
Geo IP & Botnet Filter > Policies Page



Geo IP & Botnet Filter / **Policies**

Priority	Type	Name	Source	Action	Configure
1	Botnet Policy	Block 66.249.79.77	66.249.79.77	Deny	✎ ⊗
2	Botnet Policy	Block 66.249.79.151	66.249.79.151	Deny	✎ ⊗
3	Botnet Policy	Whitelist teambeanie.com	143.95.251.86	Allow	✎ ⊗

ADD POLICY...



Geo IP & Botnet Filter / **Policies**

Priority	Type	Name	Source	Action	Configure
1	Geo IP Policy	Embargoed+Anonymous	...	Deny	✎ ⊗

ADD POLICY...

- Anonymous Proxy
- Belarus
- Congo
- Congo, The Democratic Republic of the
- Eritrea
- Iran, Islamic Rebuplic of
- Korea, Democratic People's Republic
- Lebanon
- Liberia
- Libyan Arab Jamahiriya
- Somalia
- Sudan
- Syrian Arab Republic

Each policy is automatically assigned a different priority with 1 being the highest priority. A policy's priority determines the order of enforcement.

- Botnet Filter policies have a higher priority than Geo IP policies. Geo IP policies are prioritized according to the time they were created with those created first having the higher priority.
- Botnet Filter policies defined for a single IP address have a higher priority than Botnet Filter policies defined for a subnet, and each type is then prioritized based on the time they were created with those created first having the higher priority.
- Custom created policies are enforced first, which means if an IP address is listed in the SonicWall Botnet Filter database, but the administrator defines an allow policy for this IP, then access from this IP is allowed.

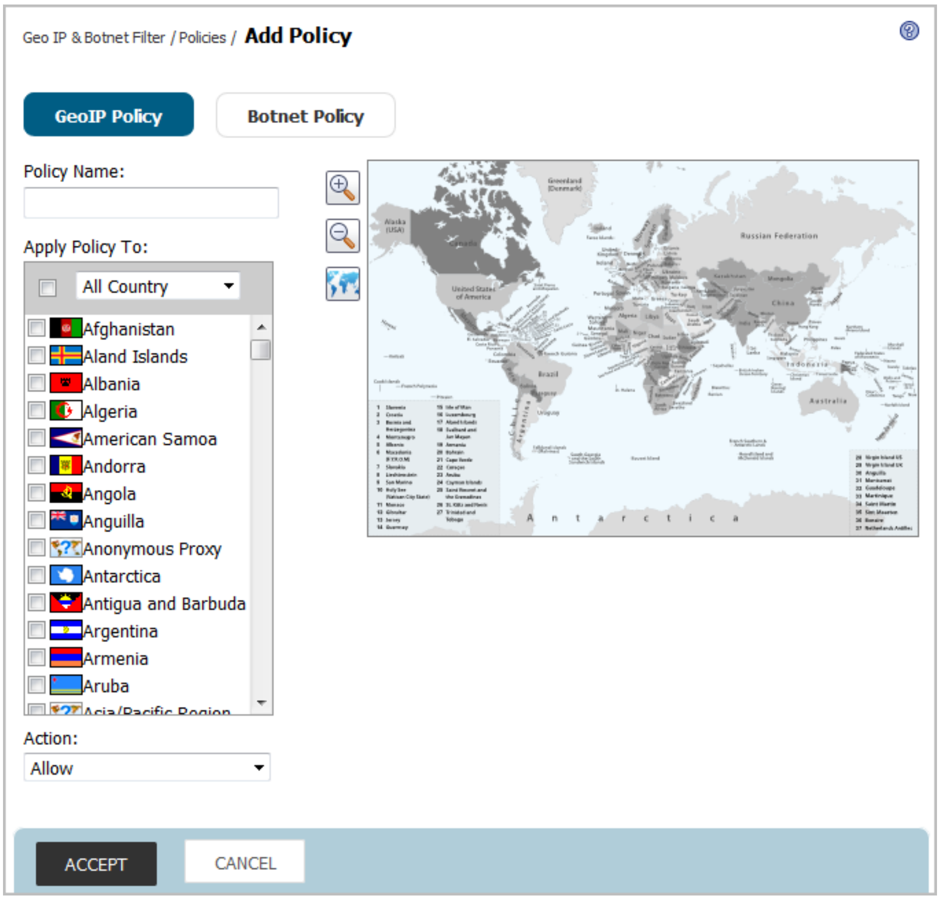
Topics:

Adding a Geo IP Policy

A Geo IP policy allows or denies traffic from specified countries.

To add a Geo IP policy:

1. Navigate to the **Geo IP & Botnet Filter > Policies** page.
2. Click the **GeoIP Policy** button.
3. On the **GeoIP Policy** page type a descriptive name into the **Policy Name** field.



Geo IP & Botnet Filter / Policies / **Add Policy**

Policy Name:

Apply Policy To: □ All Country

Action: Allow

4. In the **Apply Policy To** list, select the **Countries** you want to allow or deny.

   You can sort countries by continent by clicking the drop-down at the top of the list and selecting the desired continent or group of countries. This displays all the countries within that continent/group in the **Apply Policy To** list.

   To find a country faster, you can start typing the country name after clicking in the list. WAF does a context sensitive search for the name.

   You can also select countries directly from the map. The map displays selected countries in color, while the deselected countries display gray. Mouse over a country in the **Apply Policy To** list and the corresponding country blinks on the map.

   Use the Zoom In or Zoom Out buttons next to the map to zoom in or out on the map. If you do not wish to use the map, hide it by clicking the Hide Map button.

5. Select **Allow** or **Deny** from the **Action** drop-down list.
6. Click **ACCEPT** to save your changes.

Adding a Botnet Filter Policy

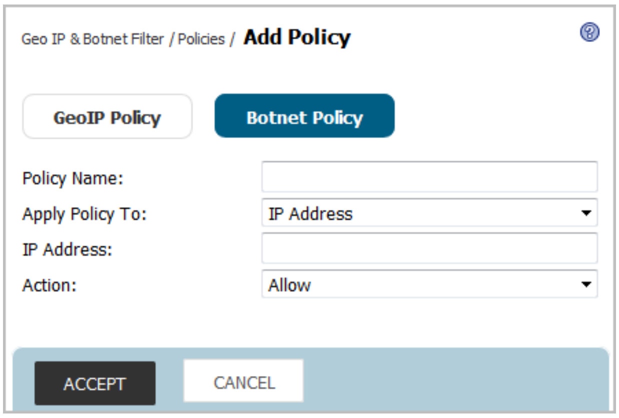
A Botnet Policy allows or denies access from a specified IPv4 IP address or IP address range. Up to 64 policies can be created.

To add a Botnet Filter policy:

1 Navigate to the **Geo IP & Botnet Filter > Policies** page.

2 Click the **Botnet Policy** button.

3 On the **Botnet Policy** page, type a descriptive name into the **Policy Name** field.



Geo IP & Botnet Filter / Policies / **Add Policy**

Policy Name:

Apply Policy To: IP Address

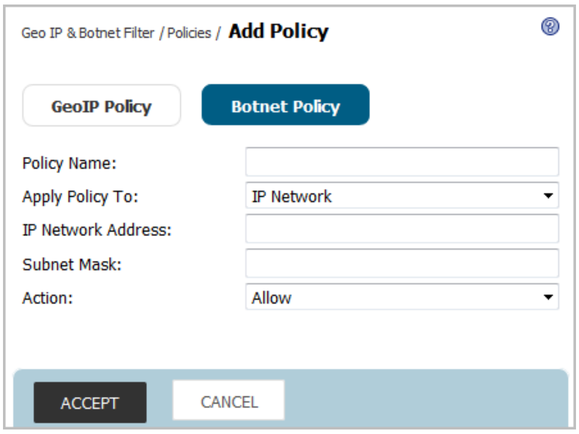
IP Address:

Action: Allow

4 In the **Apply Policy To** list, select **IP Address** or **IP Network**.

5 If you selected **IP Address** in Step 4, then type the desired address into the **IP Address** field.

6 If you selected **IP Network** in Step 4, the display changes.



Geo IP & Botnet Filter / Policies / **Add Policy**

Policy Name:

Apply Policy To: IP Network

IP Network Address:

Subnet Mask:

Action: Allow

a Type the desired network address into the **IP Network Address** field.

b Type the subnet mask into the **Subnet Mask** field. A subnet mask is a 32-bit number that separates the network part of an IP address from the host part. The network bits are all ‘1’s , while the host bits are all ‘0’s in the subnet mask. For example, 255.255.255.0 designates the first 24 bits of an IP address as the network part.

7 Select **Allow** or **Deny** from the **Action** drop-down list.

8 Click **ACCEPT** to save your changes.

Editing a Geo IP or Botnet Filter Policy

To edit a policy:

1. Navigate to the **Geo IP & Botnet Filter > Policies** page.
2. In the policies table, click the edit button in the **Configure** column for the policy you want to edit.
3. On the **Edit Policy** page, make the desired changes. The policy name cannot be edited, but you can edit the other fields.
4. Click **ACCEPT** to save your changes.

Deleting a Geo IP or Botnet Filter Policy

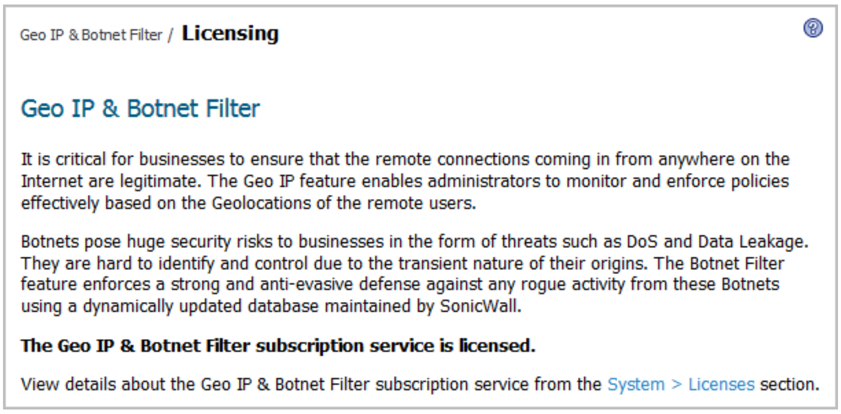
To delete a policy:

1. Navigate to the **Geo IP & Botnet Filter > Policies** page.
2. In the policies table, click the delete button in the **Configure** column for the policy you want to edit.
3. Click **OK** in the confirmation dialog.

Viewing Geo IP & Botnet Filter Licensing

The **Geo IP & Botnet Filter > Licensing** page displays a brief description of the Geo IP and Botnet Filter features and provides a link to the **System > Licenses** page.

Geo IP & Botnet Filter > Licensing Page



Geo IP & Botnet Filter / **Licensing**

Geo IP & Botnet Filter

It is critical for businesses to ensure that the remote connections coming in from anywhere on the Internet are legitimate. The Geo IP feature enables administrators to monitor and enforce policies effectively based on the Geolocations of the remote users.

Botnets pose huge security risks to businesses in the form of threats such as DoS and Data Leakage. They are hard to identify and control due to the transient nature of their origins. The Botnet Filter feature enforces a strong and anti-evasive defense against any rogue activity from these Botnets using a dynamically updated database maintained by SonicWall.

The Geo IP & Botnet Filter subscription service is licensed.

View details about the Geo IP & Botnet Filter subscription service from the System > Licenses section.

Geo IP & Botnet Filter is a subscription service that can be licensed from the **System > Licenses** page.

8

Capture ATP

Capture Advanced Threat Protection (Capture ATP) is a cloud-based batch-mode service that analyzes various types of content for malicious behavior. Supported content types include executables, archives (e.g., Zip), Adobe Portable Document Format (PDF), office documents, and more.

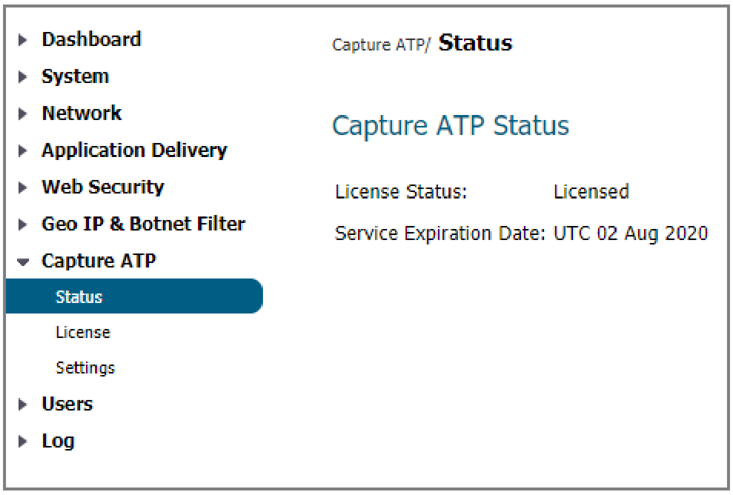
This section provides information and configuration tasks specific to the **Capture ATP** pages in the SonicWall Web Application Firewall management interface.

ⓘ | **NOTE:** Capture ATP must be licensed to activate Capture ATP monitoring and support.

Topics:

Viewing Capture ATP Status

The **Capture ATP > Status** page displays the License Status and the Service Expiration Date.



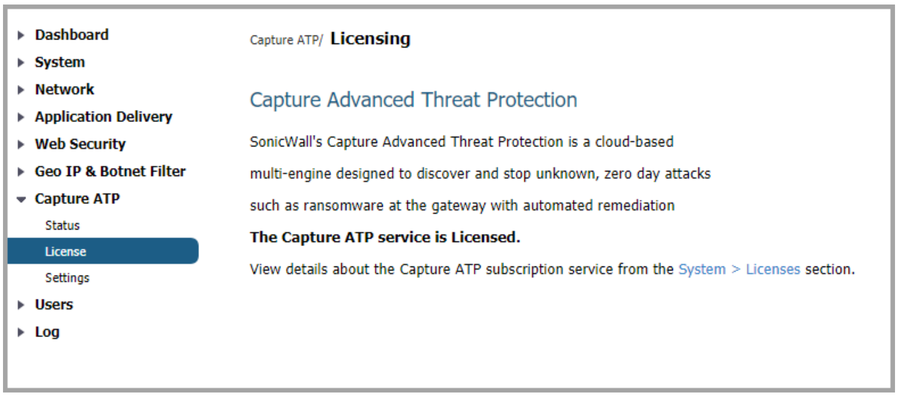
Capture ATP Status

License Status: Licensed

Service Expiration Date: UTC 02 Aug 2020

Viewing Capture ATP License

The **Capture ATP > License** page displays the license status and links to the **System > Licenses** page.



Capture Advanced Threat Protection

SonicWall's Capture Advanced Threat Protection is a cloud-based multi-engine designed to discover and stop unknown, zero day attacks such as ransomware at the gateway with automated remediation

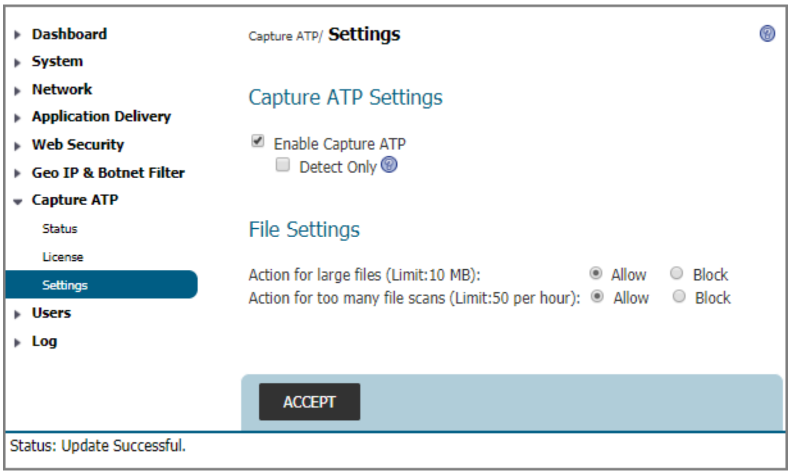
The Capture ATP service is Licensed.

View details about the Capture ATP subscription service from the System > Licenses section.

Click the **System > Licenses** to view details about the Capture ATP subscription service.

Configuring Capture ATP Settings

The **Capture ATP > Settings** page provides configuration options for Capture ATP Settings and File Settings.



Capture ATP Settings

☑ Enable Capture ATP

☐ Detect Only

File Settings

Action for large files (Limit:10 MB): ● Allow ○ Block

Action for too many file scans (Limit:50 per hour): ● Allow ○ Block

Status: Update Successful.

The **Capture ATP > Settings** page provides the **Capture ATP Settings** and **File Settings** sections. Under **Capture ATP Settings**, you find **Enable Capture ATP** and **Detect Only** options. **Under File Settings**, you find the **Action for large files (Limit: 10 MB)** and **Action for too many file scans (Limit: 50 per hour).**

To enable Capture ATP:

1. Navigate to **Capture ATP > Settings | Capture ATP Settings**.
2. Select the check box to **Enable Capture ATP**.
3. Optionally, select the check box for **Detect Only** to log Capture ATP.
4. Navigate to **Capture ATP > Settings | File Settings**.
5. Optionally, select the radio button for **Allow** to allow large files, or select **Block** to block large files.
6. Optionally, select the radio button for **Allow** to allow many file scans, or select **Block** to block many file scans.

Users Configuration

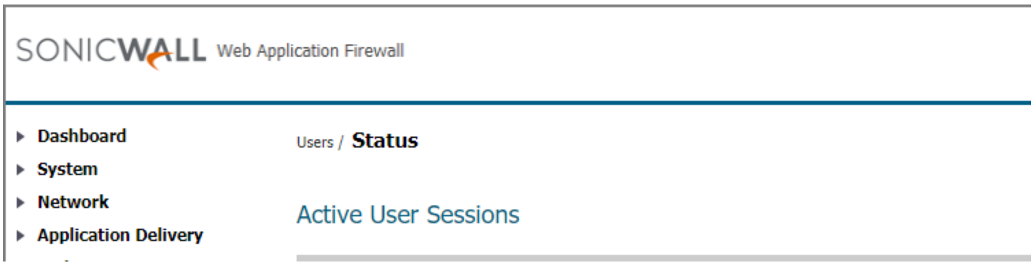
This section provides information and configuration tasks specific to the **Users** pages in the SonicWall Web Application Firewall management interface.

Topics:

Using the Users Status Page

The **Users > Status** page provides information about users and administrators who are currently accessing a web application protected by SonicWall WAF or are logged into the SonicWall WAF virtual appliance.

Users > Status Page



When **Streaming Updates** is set to **ON**, the **Users > Status** page content is automatically refreshed so that the page always displays current information. Toggle to **OFF** by clicking **ON**.

The **Active User Sessions** table displays the current users or administrators accessing protected web apps or the management interface of Web Application Firewall. Each entry displays the name of the user, the group to which the user belongs, the web app the user is accessing, the IP address of the user, the location of the user (if the Geo IP service is licensed and enabled), a time stamp indicating when the user logged in, the duration of the session, and the cumulative idle time during the session.

An administrator can terminate a user session and log the user out by clicking the disconnect user button in the **Logout** column of the user row.

The Active User Information table describes the information displayed in the **Active User Sessions** table on the page.

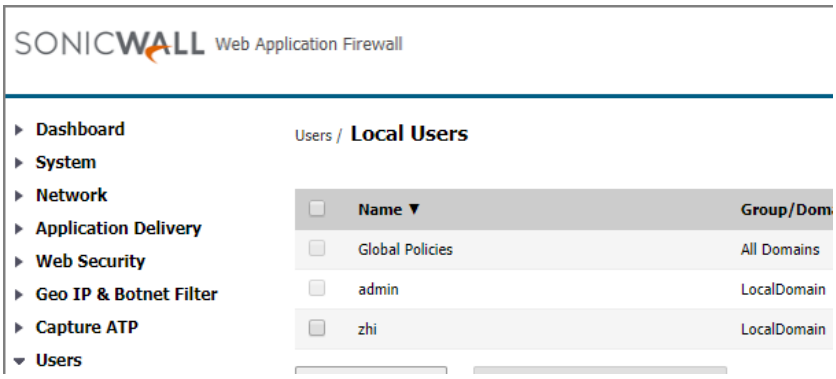
Active User Information

Column	Description
Name	A text string that indicates the ID of the user.
Group	The group to which the user belongs.
Web App	The name of the web application that the user is accessing. This displays “Administration” for an admin who is logged into the WAF web management interface.
IP Address	The source IP address of the user.
Location	The geographical location of the source IP for the user. This is only displayed when the Geo IP service is licensed and enabled.
Login Time	The time when the user first established connection with Web Application Firewall expressed as day, month, date, time (HH:MM:SS), and year.
Logged In	The amount of time since the user first established a connection with Web Application Firewall expressed as number of days and time (HH:MM:SS).
Idle Time	The amount of time the user has been in an inactive or idle state.
Logout	Displays the disconnect user button that enables the administrator to log the user out of Web Application Firewall.

Configuring Local Users

The **Users > Local Users** page allows you to add, edit, and delete local user accounts on the SonicWall WAF virtual appliance.

Users > Local Users Page



□	Name ▼	Group/Dom
□	Global Policies	All Domains
□	admin	LocalDomain
□	zhi	LocalDomain

Topics:

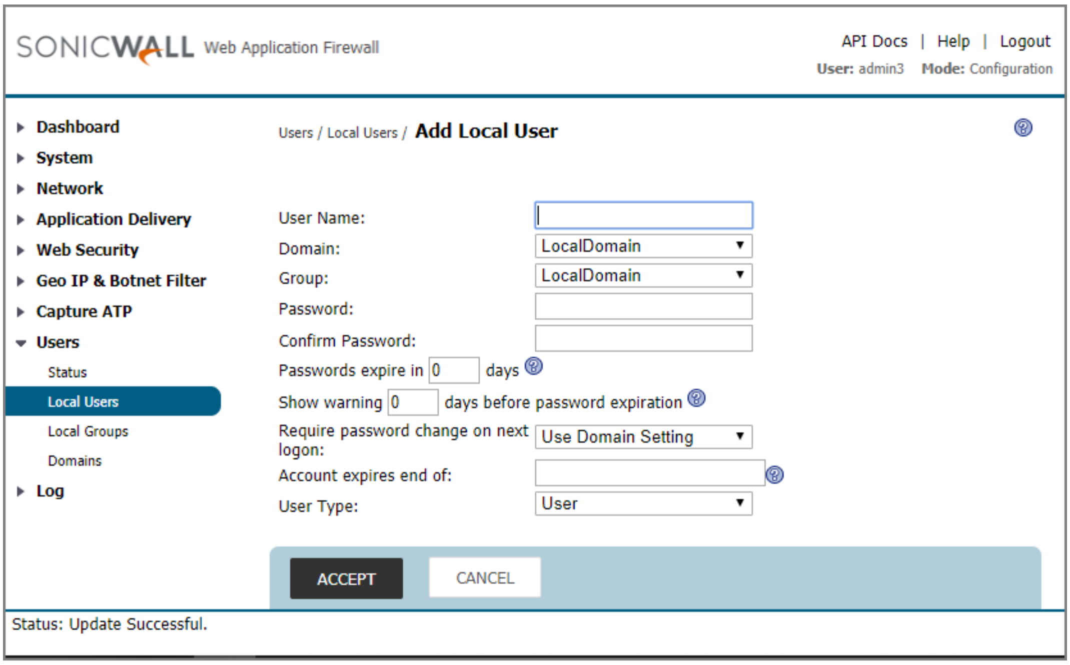
- Adding a Local User on page 151
- Removing a Local User on page 152
- Editing Local User Settings on page 152

Adding a Local User

To create a new local user:

1 Navigate to the **Users > Local Users** page.

2 Click the **ADD USER** button. The **Add Local User** page is displayed.



User: admin3 Mode: Configuration

Users / Local Users / Add Local User

User Name:

Domain: LocalDomain

Group: LocalDomain

Password:

Confirm Password:

Passwords expire in 0 days

Show warning 0 days before password expiration

Require password change on next logon: Use Domain Setting

Account expires end of:

User Type: User

Status: Update Successful.

3 Type the new user name into the **User Name** field. This is the login ID for the user.

4 Select the name of the domain to which the user belongs from the **Domain** drop-down list.

Domains can be added on the **Users > Domains** page.

5 Select the name of the group to which the user belongs in the **Group** drop-down list.

6 Type the user password into the **Password** field.

7 Retype the password in the **Confirm Password** field to verify the password.

> **NOTE:** When logging in, the user name is not case-sensitive, but the password and domain are case-sensitive.

8 Optionally, force a user in the Local User database to change their password at set intervals or the next time they login. To force a user to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field.

9 If you set a password expiration interval, type the number of days before expiration that users should receive notifications in the **Show warning *x* days before password expiration** field. Set it to **0** for no warning.

When configured and a password is expiring, a notification is displayed on the user’s login session page or on an administrator’s management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

10 Optionally, use **Require password change on next logon** to force a user to change their password the next time they log in by selecting **Use Domain Setting** or **Enabled**. Selecting **Use Domain Setting** uses the setting configured on the **Users > Domains** page.

11 With the **Account expires end of** setting, you can set an expiration date with a pull-down calendar. No setting indicates that the account never expires.

12 From the **User Type** drop-down list, select a user type option. The available user types are **User**, **Administrator**, or **Read-only Administrator**.

13 Click **ACCEPT** to save your changes.

Removing a Local User

To remove a local user:

1 Navigate to the **Users > Local Users** page.

2 Click the delete user button in the **Configure** column for the user you want to remove.

3 Click **OK** in the confirmation dialog.

Editing Local User Settings

You can create access policies and make changes to the settings for a Local User by clicking the edit button for that user in the table on the **Users > Local Users** page.

The table also has a row for **Global Policies**, which you can edit to create new global access policies or change existing ones. For information about configuring Global Policies, see Global Policy Configuration on page 183.

The **Edit Local User** page provides four screens. Click the buttons along the top to display the screen you want, then click **ACCEPT** after making changes on that screen.

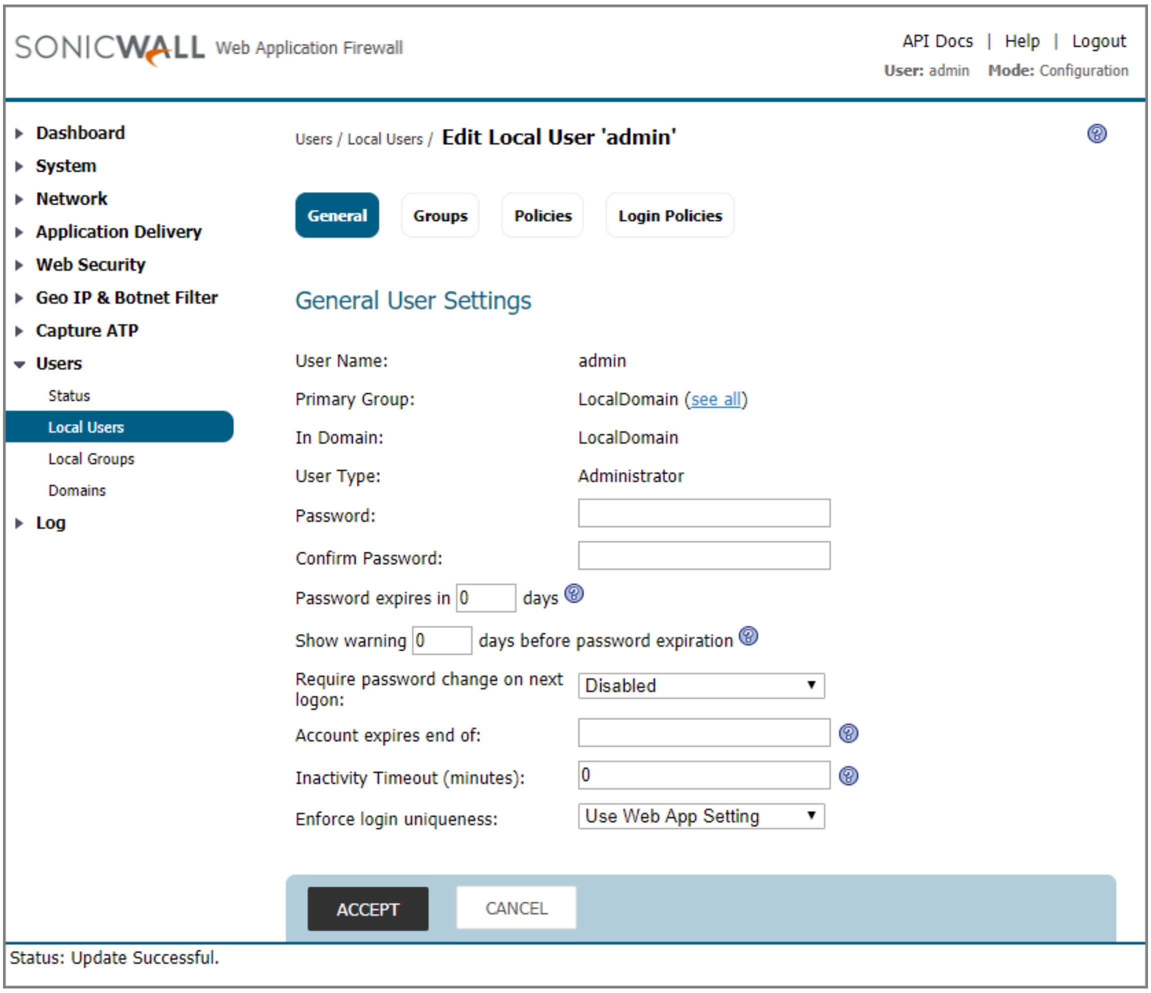
Topics:

- Editing General Settings for a Local User on page 152
- Editing Group Settings for a Local User on page 154
- Configuring Policies for a Local User on page 155
- Configuring Login Policies for a Local User on page 157

Editing General Settings for a Local User

The **General** screen of the **Edit Local User** page provides settings for the user type, password, account expiration, inactivity timeout, and for enforcing login uniqueness.

Edit Local User > General Screen



User: admin Mode: Configuration

Users / Local Users / Edit Local User 'admin'

General User Settings

User Name:	admin
Primary Group:	LocalDomain (see all)
In Domain:	LocalDomain
User Type:	Administrator
Password:	
Confirm Password:	
Password expires in 0 days	
Show warning 0 days before password expiration	
Require password change on next logon:	Disabled
Account expires end of:	
Inactivity Timeout (minutes):	0
Enforce login uniqueness:	Use Web App Setting

Status: Update Successful.

To edit General settings for an existing local user:

1 Navigate to the **Users > Local Users** page, then click the edit button in the **Configure** column for the user whose settings you want to edit.

2 In the **Edit Local User** page, click **General** to display the **General** screen. The **General** screen displays the following non-configurable fields: **User Name**, **Primary Group**, and **In Domain**. If these settings need to be modified, then remove the user as described in Removing a Local User on page 152 and add the user again.

3 To change the user type, select the type from the **User Type** drop-down list.

4 To change the user password, type the password in the **Password** field. Re-type it in the **Confirm Password** field.

5 To force a user to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field.

6 To change the password expiration notification setting, type the number of days before expiration that users should receive notifications in the **Show warning *x* days before password expiration** field. Set it to **0** for no warning.

When configured and a password is expiring, a notification is displayed on the user's login session page or on an administrator's management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

7 To change how a user is forced to change their password the next time they log in, set **Require password change on next logon** to **Use Domain Setting**, **Enabled**, or **Disabled**. Selecting **Use Domain Setting** uses the setting configured on the **Users > Domains** page.

8 To change the account expiration date, select a date from the pull-down calendar in the **Account expires end of** field. No setting indicates that the account never expires.

9 To change the number of inactive minutes before the user is logged out, type the number of minutes into the **Inactivity Timeout (minutes)** field. Set it to **0** to use the Group or Global timeout.

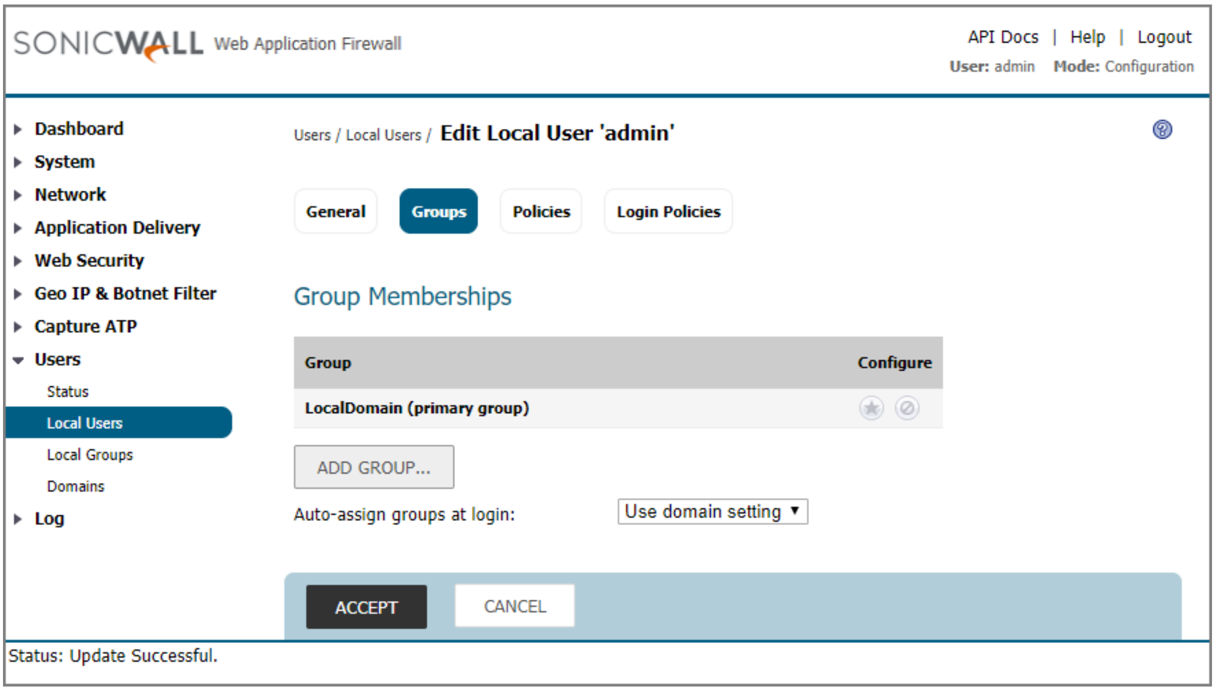
10 To change the login uniqueness requirement, select **Use Web App Setting**, **Enabled**, or **Disabled** from the **Enforce login uniqueness** drop-down list.

11 Click **ACCEPT** to save your changes.

Editing Group Settings for a Local User

The **Groups** screen of the **Edit Local User** page provides settings to add a group membership, configure a primary group, and control whether groups are automatically assigned at login.

Edit Local User > Groups Screen



Group	Configure
LocalDomain (primary group)	★ ⊘

Auto-assign groups at login: Use domain setting ▾

Status: Update Successful.

To edit Group settings for an existing local user:

1 Navigate to the **Users > Local Users** page, then click the edit button in the **Configure** column for the user whose settings you want to edit.

2 In the **Edit Local User** page, click **Groups** to display the **Groups** screen.

3 To set a group as the primary group for this user, click the **Set primary group** star button corresponding to the group you wish to set as the primary.

4 To add a group of which this user is a member, click **ADD GROUP**. The group must be already configured from **Users > Local Groups**. If no other groups are available to add, the button shows **All AVAILABLE GROUPS HAVE BEEN ADDED**.

5 Select the desired group from the drop-down list.

6 Click **ADD GROUP** to add the selected group to the **Group Memberships** list.

7 Select one of the following from the **Auto-assign groups at login** drop-down list:

- **Use domain setting** – Use the setting configured for the domain.
- **Enabled** – Enable automatic assignment of this user to the configured groups upon login.
- **Disabled** – Disable automatic assignment of this user to the configured groups upon login.

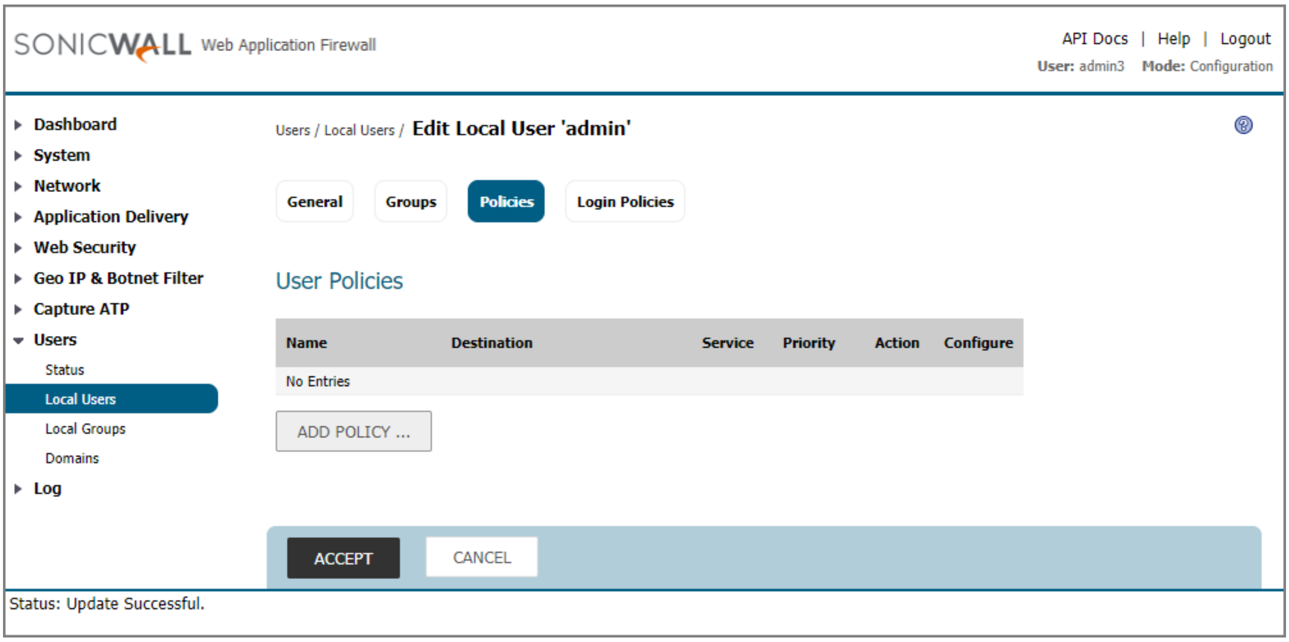
8 Click **ACCEPT** to save your changes.

Configuring Policies for a Local User

The **Policies** screen of the **Edit Local User** page provides a way to create access policies that control access to resources from user sessions.

User policies are the highest priority type of policy, and are enforced before group policies or global policies.

Edit Local User > Policies Screen



Name	Destination	Service	Priority	Action	Configure
No Entries					

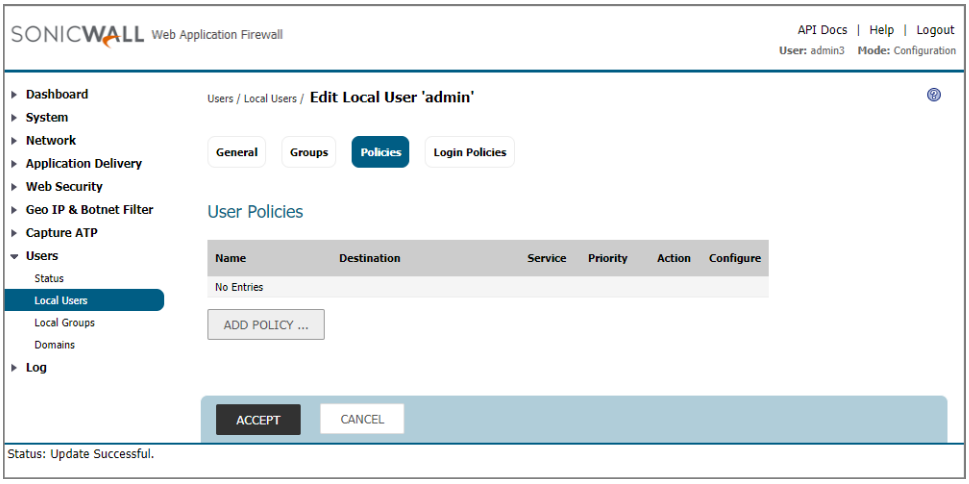
Status: Update Successful.

To add a policy for a local user:

1 Navigate to the **Users > Local Users** page, then click the edit button in the **Configure** column for the user whose settings you want to edit.

2 In the **Edit Local User** page, click **Policies** to display the **Policies** screen.

3 Click the **ADD POLICY** button. The **Add Policy** page is displayed.



Name	Destination	Service	Priority	Action	Configure
No Entries					

Status: Update Successful.

4 Select one of the following from the **Apply Policy To** drop-down list:

- **IP Address** – Select this if the policy applies to a specific host.
- **IP Network** – Select this if the policy applies to all IP addresses in a specific subnet.
- **All Addresses** – Select this if the policy applies to all addresses.
- **URL** – Select this if the policy applies to a specific web site or web application.

The displayed fields change depending on the selected value.

NOTE: Policies apply to the destination address(es) of the Web Application Firewall connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to Web Application Firewall through the policy engine.

5 Type a name for the policy in the **Policy Name** field.

6 If **Apply Policy To** is set to **IP Address**:

a Type the IP address of the host machine into the **IP Address** field.

b Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

7 If **Apply Policy To** is set to **IP Network**:

a Type the IP network address into the **IP Network Address** field.

b Type the network mask into the **Subnet Mask** field. For example, 255.255.255.0 designates the first 24 bits of an IP address as the network part.

c Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

8 If **Apply Policy To** is set to **All Addresses**, there are no unique fields to configure.

9 If **Apply Policy To** is set to **URL**, type the URL into the **URL** field. For example, “sonicwall.com”.

10 In the **Service** drop-down list, select one of **All Services**, **Web (HTTP)**, or **Secure Web (HTTPS)**.

11 In the **Status** drop-down list, select either **Allow** or **Deny** to either permit or deny Web Application Firewall connections for the specified service and host(s).

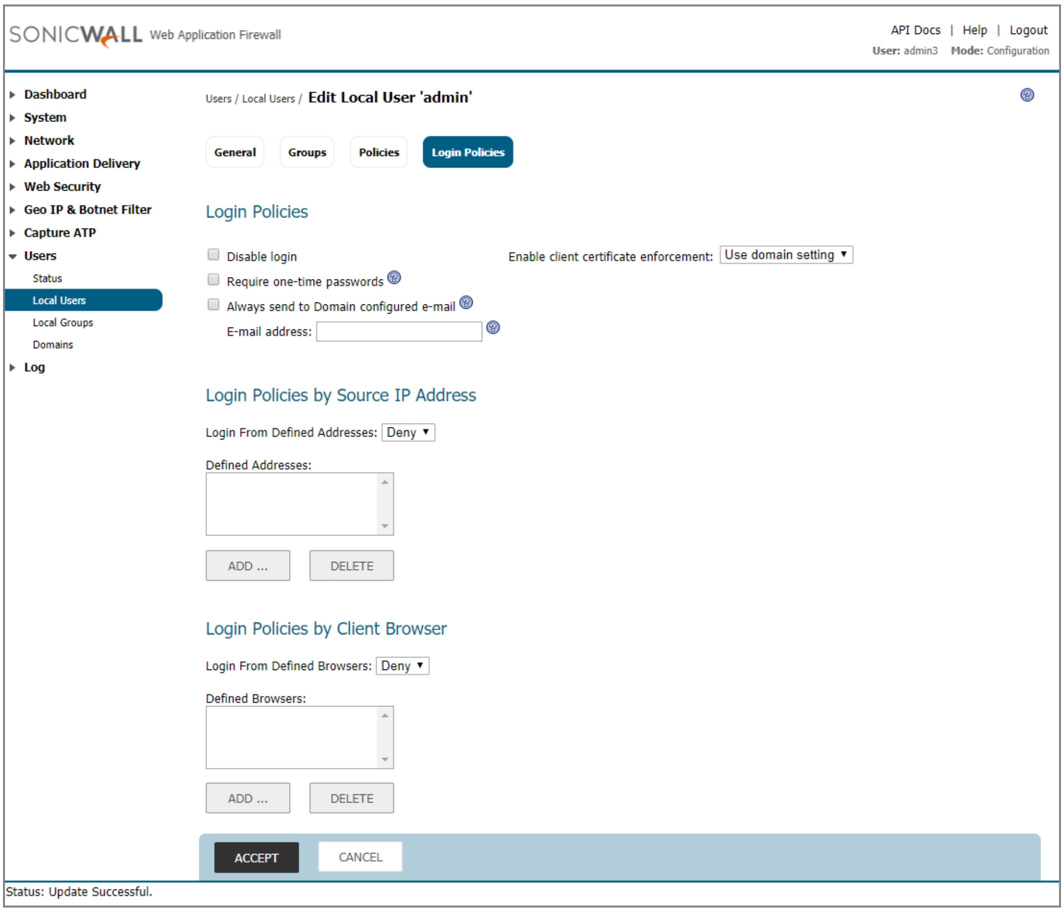
12 Click **ACCEPT** to save your changes.

After the configuration has been updated, the new policy is displayed on the **Edit Local User > Policies** screen. The policies are displayed in the policy list in the order of priority, from the highest priority policy to the lowest priority policy.

Configuring Login Policies for a Local User

The **Login Policies** screen of the **Edit Local User** page provides settings to create user login policies, including policies for specific source IP addresses and policies for specific client browsers. You can disable the user's login, require One Time Passwords, and specify client certificate enforcement. Login policies can allow or deny users with specific IP addresses permission to log into Web Application Firewall and access the protected web apps.

Edit Local User > Login Policies Screen



Edit Local User 'admin'

Login Policies

□ Disable login

□ Require one-time passwords

□ Always send to Domain configured e-mail

E-mail address:

Enable client certificate enforcement: Use domain setting

Login Policies by Source IP Address

Login From Defined Addresses: Deny

Defined Addresses:

Login Policies by Client Browser

Login From Defined Browsers: Deny

Defined Browsers:

Status: Update Successful.

To configure Login Policies for an existing local user:

1 Navigate to the **Users > Local Users** page, then click the edit button in the **Configure** column for the user whose settings you want to edit.

2 In the **Edit Local User** page, click **Login Policies** to display the **Login Policies** screen.

3 To block the user from logging into Web Application Firewall, select the **Disable login** check box.

4 Select one of the following from the **Enable client certificate enforcement** drop-down list:

- **Use domain setting** – Use the setting configured for the domain.

- **Enabled** – Require the use of client certificates for login. By selecting this option, you require the client to present a client certificate for strong mutual authentication. Two additional fields appear:
    - **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user's account name matches their client certificate.
    - **Verify partial DN in subject** - Use the following case-sensitive variables to configure a partial DN that matches the client certificate subject:
        - **%USERNAME%** – User name
        - **%USERDOMAIN%** – User's domain name
        - **%ADUSERNAME%** – User's name in Active Directory
        - **%WILDCARD%** – Wildcard variable
        - **%AD:mail%** – User's email address as configured in Active Directory
        - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft's Documentation of Active Directory user attributes link for more information.
- **Disabled** – Do not require the use of client certificates for login.

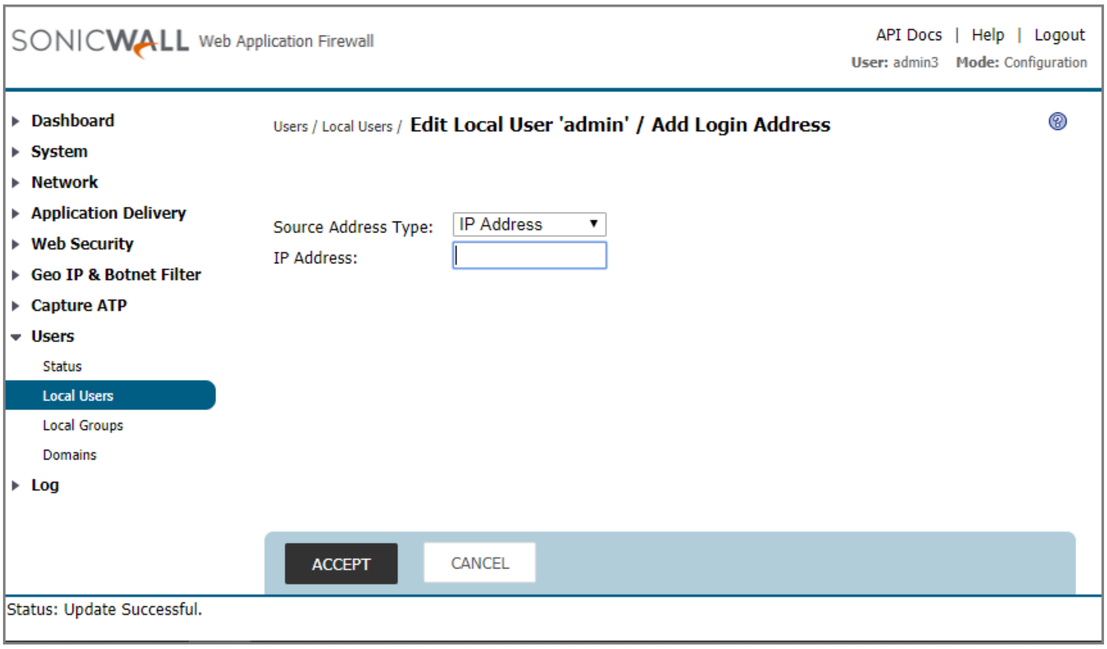
5 To require the use of one-time passwords for the specified user to log in to the appliance, select the **Require one-time passwords** check box. If the user's domain requires one-time passwords, then they will be required for the user even if this option is not selected.

For more information about one-time passwords, see How Does One Time Password Work? on page 9.

6 Select the **Always send to Domain configured e-mail** check box to always send the OTP code to the email address configured for the domain.

7 Enter the user's email address into the **E-mail address** field to override any address provided by the domain, unless the **Always send to Domain configured e-mail** option is selected. You can enter multiple email addresses separated by semicolons into this field.

8 Under **Login Policies by Source IP Address**, select an access policy (**Allow** or **Deny**) in the **Login From Defined Addresses** drop-down list and then click **ADD** under the list box to apply the login policy to a source IP address. The **Add Login Address** screen is displayed.



User: admin3 Mode: Configuration

Users / Local Users / Edit Local User 'admin' / Add Login Address

Source Address Type: IP Address
IP Address:

Status: Update Successful.

9 In the **Add Login Address** screen, select one of the following from the **Source Address Type** drop-down list:

- **IP Address** – Select this to use a specific IP address.
- **IP Network** – Select this to use all IP addresses in a specific subnet. If you select this option, the displayed fields change to show the **Network Address** and **Subnet Mask** fields.

10 If **Source Address Type** is set to **IP Address**:

a Type the IP address of the user's machine into the **IP Address** field.

11 If **Source Address Type** is set to **IP Network**:

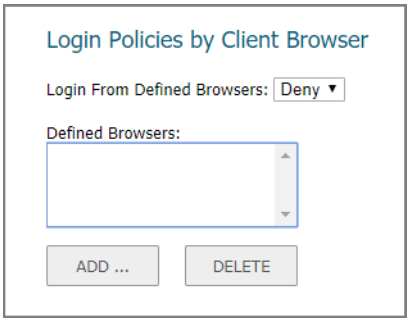
a Type the IP network address into the **IP Network Address** field.

b Type the network mask into the **Subnet Mask** field. For example, 255.255.255.0 designates the first 24 bits of an IP address as the network part.

12 Click **ACCEPT**. The address or network is displayed in the **Defined Addresses** list under **Login Policies by Source IP Address** on the **Edit Local User** page.

As an example, if you selected an IP network with 10.202.4.32 as the network address and 255.255.255.240 (28 bits) as the subnet mask value, the **Defined Addresses** list displays 10.202.4.32–10.202.4.47. In this case, 10.202.4.47 would be the broadcast address. Whatever login policy you selected is now applied to addresses in this range.

13 Under **Login Policies by Client Browser**, select an access policy (**Allow** or **Deny**) in the **Login From Defined Browsers** drop-down list and then click **ADD** under the list box to apply the login policy to a client browser. The **Add Login Browser** screen is displayed.



Login Policies by Client Browser

Login From Defined Browsers: Deny

Defined Browsers:

14 In the **Add Login Browser** screen, type a browser definition into the **Client Browser** field and then click **ACCEPT**. The browser name is displayed in the **Defined Browsers** list under **Login Policies by Client Browser** on the **Edit Local User** page.

Browsers are identified by user agent strings, such as “Mozilla/5.0 (Windows NT 6.1; Win64; rv:59.0) Gecko/20100101 Firefox/59.0”.

15 Click **ACCEPT** to save your changes. The new login policy is saved.

Configuring Local Groups

The **Users > Local Groups** page allows you to add and configure groups for granular control of user access by specifying a group name and domain.

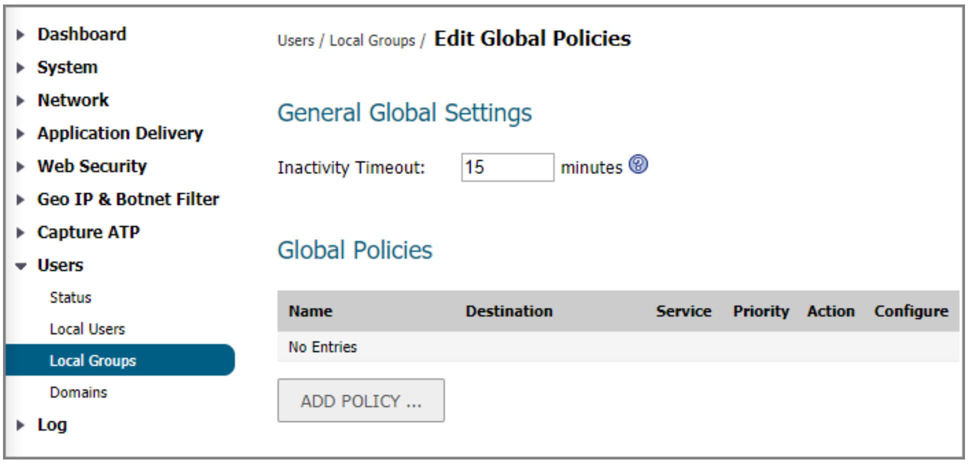
Note that a group is automatically created when you create a domain. You can create domains in the **Users > Domains** page. You can also create a group directly from the **Users** > **Local Groups** page.

Users can only belong to groups within a single domain.

The table on the **Users** > **Local Groups** page contains two automatically created entries:

- **Global Policies** - Contains access policies that apply to all nodes in the organization.
- **LocalDomain** - The LocalDomain group is automatically created to correspond to the default LocalDomain authentication domain. This is the default group to which local users are added, unless otherwise specified.

Users > Local Groups Page



Users / Local Groups / **Edit Global Policies**

General Global Settings

Inactivity Timeout: 15 minutes

Global Policies

Name	Destination	Service	Priority	Action	Configure
No Entries					

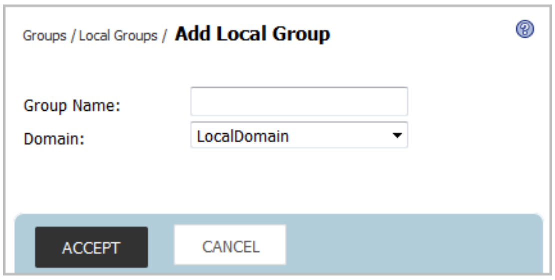
Topics:

- Adding a Local Group on page 160
- Deleting a Local Group on page 161
- Editing Local Group Settings on page 161

Adding a Local Group

To create a new local group:

1. Navigate to the **Users > Local Groups** page.
2. Click the **ADD GROUP** button. The **Add Local Group** page is displayed.



Groups / Local Groups / **Add Local Group**

Group Name:

Domain: LocalDomain

3. Type a descriptive name for the group into the **Group Name** field.
4. Select the appropriate domain from the **Domain** drop-down list. The domain is mapped to the group.
5. Click **ACCEPT** to save your changes. After the group has been added, the new group is added to the **Local Groups** page.

All of the configured groups are displayed in the **Users > Local Groups** page, listed in alphabetical order.

Deleting a Local Group

To delete a local group, click the delete button in the **Configure** column of the row for the group that you wish to remove in the Local Groups table on the **Users > Local Groups** page. The deleted group no longer appears in the list of defined groups.

> ⓘ **NOTE:** A group cannot be deleted if users have been added to the group or if the group is the default group created for an authentication domain. To delete a group that is the default group for an authentication domain, delete the corresponding domain (you cannot delete the group in the **Edit Group Settings** window). If the group is not the default group for an authentication domain, first delete all users in the group. Then you are able to delete the group on the **Users > Local Groups** page.

Editing Local Group Settings

You can create access policies and make changes to the settings for a Local Group by clicking the edit button for that group in the table on the **Users > Local Groups** page.

The table also has an entry for **Global Policies**, which you can edit to create new global access policies or change existing ones. For information about configuring Global Policies, see Global Policy Configuration on page 183.

The **Edit Local Group** page provides two screens. Click the buttons along the top to display the screen you want, then click **ACCEPT** after making changes on that screen.

Topics:

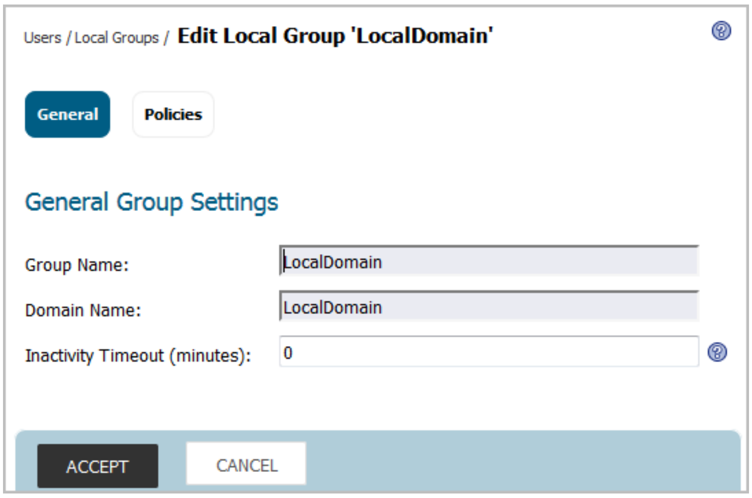
- Editing General Group Settings on page 161
- Adding Group Policies on page 162

Editing General Group Settings

The **General** screen provides a configuration option for a group's inactivity timeout value. The **General Group Settings** section displays the following non-configurable fields: **Group Name** and **Domain Name**.

To modify the general group settings:

1. Navigate to the **Users > Local Groups** page, then click the edit button in the **Configure** column for the group whose settings you want to edit.
2. In the **Edit Local Group** page, click **General** to display the **General** screen.



Users / Local Groups / Edit Local Group 'LocalDomain'

General Group Settings

Group Name: LocalDomain

Domain Name: LocalDomain

Inactivity Timeout (minutes): 0

3 In the **Inactivity Timeout (minutes)** field, type in the number of inactive minutes before a user is logged out.

The group timeout applies to all users in the group and overrides the Global timeout, but can be overridden by the User timeout. Set it to 0 to use the Global timeout.

4 Click **ACCEPT** to save your changes.

Adding Group Policies

With group access policies, all traffic is allowed by default. Additional allow and deny policies can be created by destination address or address range and by service type.

The most specific policy takes precedence over less specific policies. For example, a policy that applies to only one IP address has priority over a policy that applies to an IP network. If there are two policies that apply to a single IP address, then a policy for a specific service takes precedence over a policy that applies to all services.

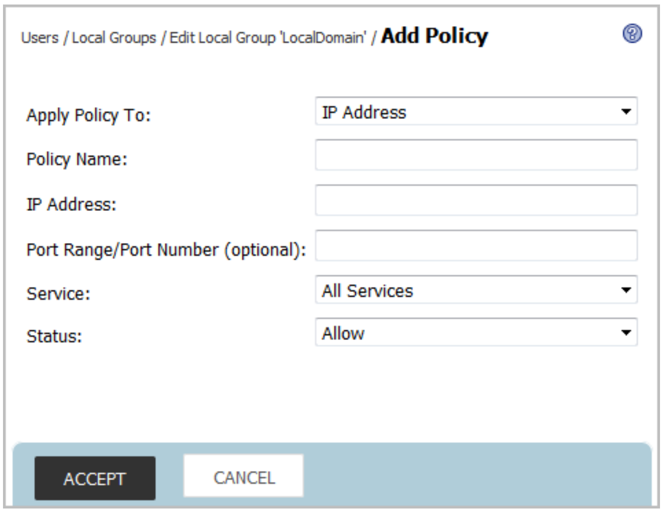
User policies take precedence over group policies and group policies take precedence over global policies, regardless of the policy definition. A user policy that allows access to all IP addresses takes precedence over a group policy that denies access to a single IP address.

To add a policy for a local group:

1 Navigate to the **Users > Local Groups** page, then click the edit button in the **Configure** column for the group whose settings you want to edit.

2 In the **Edit Local Group** page, click **Policies** to display the **Policies** screen.

3 Click the **ADD POLICY** button. The **Add Policy** page is displayed.


Users / Local Groups / Edit Local Group 'LocalDomain' / **Add Policy**

Apply Policy To: IP Address

Policy Name:

IP Address:

Port Range/Port Number (optional):

Service: All Services

Status: Allow

4 Select one of the following from the **Apply Policy To** drop-down list:

- **IP Address** – Select this if the policy applies to a specific host.
- **IP Network** – Select this if the policy applies to all IP addresses in a specific subnet.
- **All Addresses** – Select this if the policy applies to all addresses.
- **URL** – Select this if the policy applies to a specific web site or web application.

The displayed fields change depending on the selected value.

> **NOTE:** Policies apply to the destination address(es) of the Web Application Firewall connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to Web Application Firewall through the policy engine.

5 Type a name for the policy in the **Policy Name** field.

6 If **Apply Policy To** is set to **IP Address**:

   a Type the IP address of the host machine into the **IP Address** field.

   b Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

7 If **Apply Policy To** is set to **IP Network**:

   a Type the IP network address into the **IP Network Address** field.

   b Type the network mask into the **Subnet Mask** field. For example, 255.255.255.0 designates the first 24 bits of an IP address as the network part.

   c Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

8 If **Apply Policy To** is set to **All Addresses**, there are no unique fields to configure.

9 If **Apply Policy To** is set to **URL**, type the URL into the **URL** field. For example, “sonicwall.com”.

10 In the **Service** drop-down list, select one of **All Services**, **Web (HTTP)**, or **Secure Web (HTTPS)**.

11 In the **Status** drop-down list, select either **Allow** or **Deny** to either permit or deny Web Application Firewall connections for the specified service and host(s).

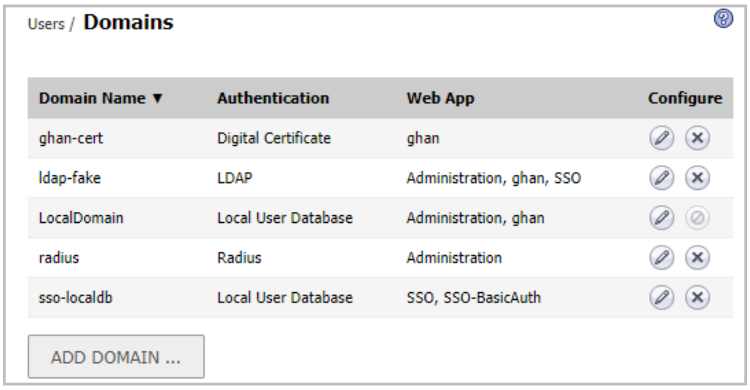
12 Click **ACCEPT** to save your changes.

After the configuration has been updated, the new policy is displayed on the **Edit Local Group > Policies** screen. The policies are displayed in the policy list in the order of priority, from the highest priority policy to the lowest priority policy.

Configuring Domains

The **Users > Domains** page allows you to add and configure domains. You can create multiple domains linked to different web apps and using different authentication methods. Domain choices are displayed in the login page for the user.

Users > Domains Page



Users / **Domains**

Domain Name ▼	Authentication	Web App	Configure
ghan-cert	Digital Certificate	ghan	✎ ⊗
ldap-fake	LDAP	Administration, ghan, SSO	✎ ⊗
LocalDomain	Local User Database	Administration, ghan	✎ ⊘
radius	Radius	Administration	✎ ⊗
sso-localdb	Local User Database	SSO, SSO-BasicAuth	✎ ⊗

The Domain Settings table summarizes the available options when adding a domain.

Domain Settings

Domain name	By default, the LocalDomain authentication domain is already defined. Its authentication type is the internal Local User Database. Domains can be added using other authentication types that use remote authentication servers. Domain names are case-sensitive when logging in.
Authentication	Available types include Local User Database, Active Directory, LDAP, NT Domain, RADIUS, and Digital Certificate.
Web App	You can link a web app to a domain when adding the domain. The web app is then available to all users in the domain.

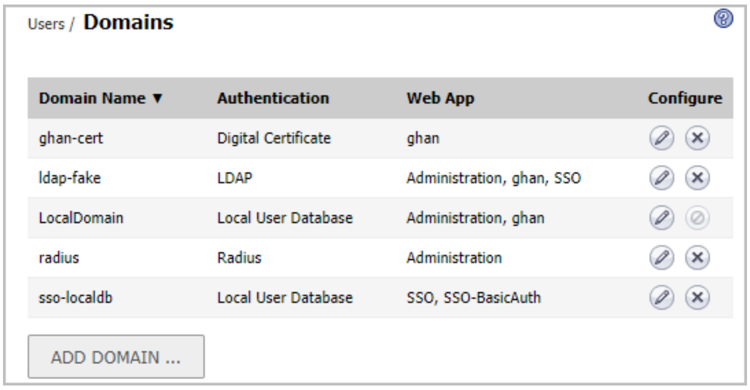
For Web Application Firewall administrator accounts, you can create a domain that provides administrator access for all users who log in to that domain. Either LDAP or Active Directory authentication is used for this type of domain.

Topics:

- Viewing the Domains Table on page 164
- Deleting a Domain on page 164
- Adding or Editing a Domain on page 165

Viewing the Domains Table

All of the configured domains are listed in the table in the **Users > Domains** page. The domains are listed in the order in which they were created. You can reverse the order by clicking the up/down arrow next to the **Domain Name** column heading.


Users / **Domains**

Domain Name ▼	Authentication	Web App	Configure
ghan-cert	Digital Certificate	ghan	✎ ⊗
ldap-fake	LDAP	Administration, ghan, SSO	✎ ⊗
LocalDomain	Local User Database	Administration, ghan	✎ ⊘
radius	Radius	Administration	✎ ⊗
sso-localdb	Local User Database	SSO, SSO-BasicAuth	✎ ⊗

Deleting a Domain

To delete a domain:

1. Navigate to **Users > Domains**.
2. In the table, click the delete button in the **Configure** column of the row for the domain that you wish to remove.
3. Click **OK** in the confirmation dialog box.

After Web Application Firewall has been updated, the deleted domain is no longer displayed in the table.

ⓘ **NOTE:** The default **LocalDomain** domain cannot be deleted.

Adding or Editing a Domain

You can add a new domain or edit an existing one from the **Users > Domains** page. To add a domain, click the **ADD DOMAIN** button to display the Add Domain screen. To edit an existing domain, click the edit button in the **Configure** column of the row for the domain that you wish to configure.

The interface provides the same fields for both adding and editing a domain, but the **Authentication Type** and **Domain Name** fields cannot be changed when editing an existing domain.

ⓘ **NOTE:** After adding a new domain, user group settings for that domain are configured on the **Users > Local Groups** page. Refer to the Configuring Local Groups on page 159 for instructions on configuring groups.

The domain settings are quite different depending on the authentication type for the domain. See the following topics for instructions on adding domains for the various authentication types.

Topics:

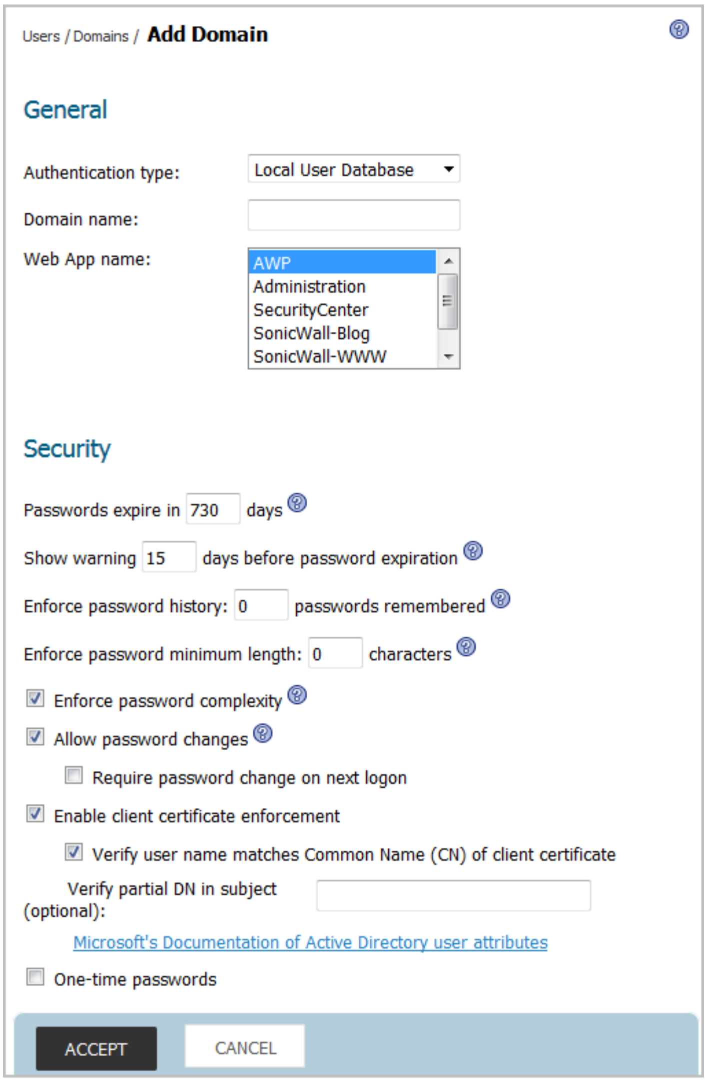
- Adding or Editing a Domain with Local User Authentication on page 165
- Adding or Editing a Domain with Active Directory Authentication on page 168
- Adding or Editing a Domain with LDAP Authentication on page 170
- Adding or Editing a Domain with NT Domain Authentication on page 174
- Adding or Editing a Domain with RADIUS Authentication on page 175
- Adding or Editing a Domain with Digital Certificates on page 178

Adding or Editing a Domain with Local User Authentication

To add or edit a domain for local database authentication:

1 Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 If adding the domain, select **Local User Database** from the **Authentication Type** drop-down list.



Users / Domains / **Add Domain**

General

Authentication type: Local User Database

Domain name:

Web App name: AWP, Administration, SecurityCenter, SonicWall-Blog, SonicWall-WWW

Security

Passwords expire in 730 days

Show warning 15 days before password expiration

Enforce password history: 0 passwords remembered

Enforce password minimum length: 0 characters

☑ Enforce password complexity

☑ Allow password changes

☐ Require password change on next logon

☑ Enable client certificate enforcement

☑ Verify user name matches Common Name (CN) of client certificate

Verify partial DN in subject (optional):

Microsoft's Documentation of Active Directory user attributes

☐ One-time passwords

3 If adding the domain, enter a descriptive name for the domain in the **Domain Name** field (maximum 24 characters). This is the domain name users select when logging in.

4 Select the name of the associated web application in the **Web App Name** field.

5 To force a user to change their password at set intervals, type the expiration interval in the **Passwords expire in *x* days** field. Set it to **0** for no expiration. The default is 730 days (two years).

> **NOTE:** If **Passwords expire in *x* days** is non-zero, the **Allow password changes** option should be enabled, or else the user may be locked out until an administrator updates the account.

6 Type the number of days before password expiration that users should receive notifications in the **Show warning *x* days before password expiration** field. Set it to **0** for no warning. The default is 15 days.

When configured and a password is expiring, a notification is displayed on the user's login session page or on an administrator's management console identifying the number of days before their password expires. Notifications also include a link to a screen where the password can be changed.

7 Enter the number of passwords that are tracked and cannot be reused for a user account into the **Enforce password history, *x* passwords remembered** field. The value specified must be between 0 and 10 passwords.

8 Enter a value between 1 and 14 characters into the **Enforce password minimum length** field. This is the minimum number of characters required for a user password.

9 Select the **Enforce password complexity** check box to require at least *three* of the four following parameters to be met when setting a password:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

10 Select the **Allow password changes** check box to allow users to change their own passwords after their account is set up. This setting does not affect administrator accounts. Full administrators can always change their password.

11 To force users logging into the domain to change their password the next time they log in, select the **Require password change on next logon** check box.

12 Select the **Enable client certificate enforcement** check box to require the use of client certificates for login. If set, this option requires the client to present a client certificate for strong mutual authentication.

ⓘ | **NOTE:** Client certificates cannot be used with the default LocalDomain domain.

Two additional fields appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that matches the client certificate subject:
  - **%USERNAME%** – User name
  - **%USERDOMAIN%** – User's domain name
  - **%ADUSERNAME%** – User's name in Active Directory
  - **%WILDCARD%** – Wildcard variable
  - **%AD:mail%** – User's email address as configured in Active Directory
  - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft's Documentation of Active Directory user attributes link for more information.

13 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.
  - If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, *abc.com*).

14 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page.

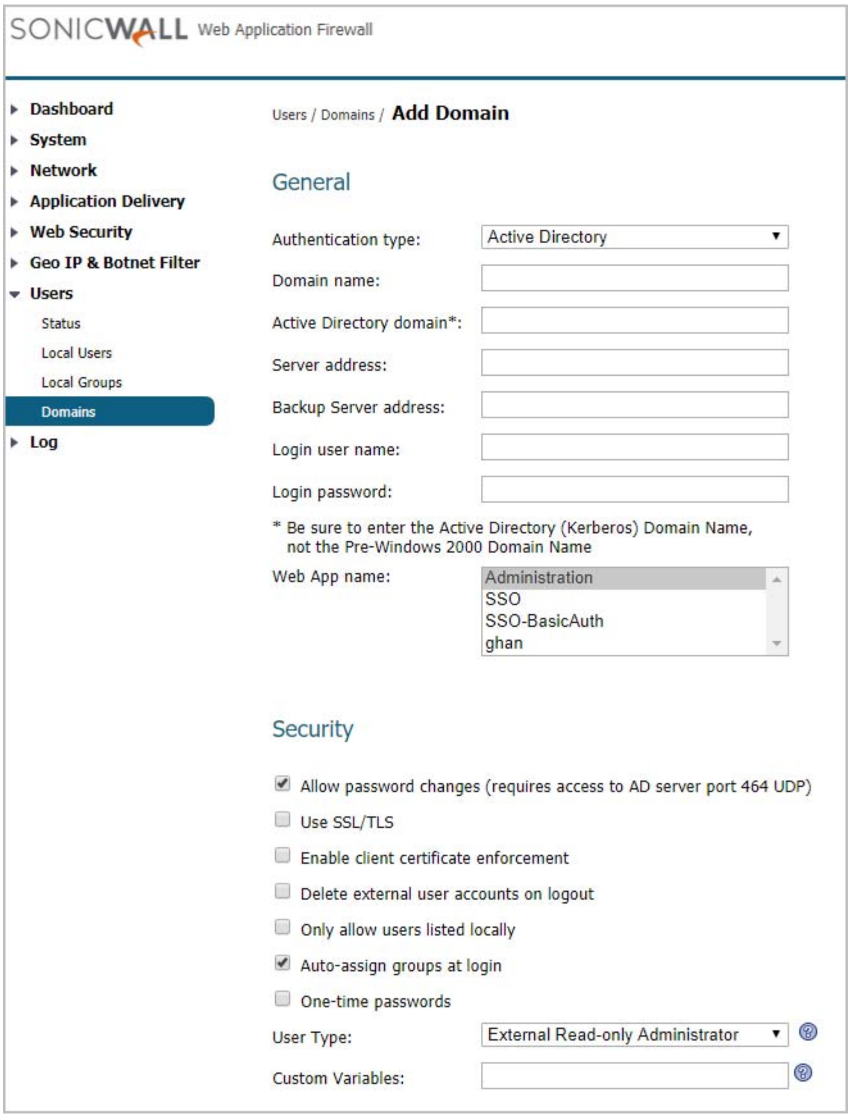
Adding or Editing a Domain with Active Directory Authentication

To add or edit a domain for Active Directory authentication:

1. Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.
2. If adding the domain, select **Active Directory** from the **Authentication Type** drop-down list.

> ⓘ **NOTE:** Of all types of authentication, Active Directory authentication is the most sensitive to clock skew, or variances in time between the Web Application Firewall virtual appliance and the Active Directory server against which it is authenticating. If you are unable to authenticate using Active Directory, configure Network Time Protocol on the **System > Time** page of the Web Application Firewall management interface and check that the Active Directory server has the correct time settings.

The Active Directory configuration fields are displayed.



General

Authentication type: Active Directory ▾

Domain name:

Active Directory domain*:

Server address:

Backup Server address:

Login user name:

Login password:

* Be sure to enter the Active Directory (Kerberos) Domain Name, not the Pre-Windows 2000 Domain Name

Web App name: Administration, SSO, SSO-BasicAuth, ghan

Security

☑ Allow password changes (requires access to AD server port 464 UDP)

□ Use SSL/TLS

□ Enable client certificate enforcement

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ Auto-assign groups at login

□ One-time passwords

User Type: External Read-only Administrator ▾

Custom Variables:

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log into Web Application Firewall. It can be the same value as the **Server address** field or the **Active Directory domain** field, depending on your network configuration.

4 Enter the Active Directory (Kerberos) domain name in the **Active Directory domain** field.

5 Enter the IP address or host and domain name of the Active Directory server in the **Server address** field.

6 Enter the IP address or host and domain name of the back up server in the **Backup Server address** field.

7 Enter the user name for the administrator account of the Active Directory server in the **Login user name** field.

8 Enter the password for the administrator account of the Active Directory server in the **Login password** field.

9 Select the name of the associated web application in the **Web App Name** field.

10 Select the **Allow password changes** check box to allow users to change their own passwords. This requires access to AD server port 464 UDP.

11 Select the **Use SSL/TLS** check box to allow SSL/TLS encryption to be used for Active Directory password exchanges.

12 Select the **Enable client certificate enforcement** check box to require the use of client certificates for login. If set, this option requires the client to present a client certificate for strong mutual authentication.

Two additional fields appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that matches the client certificate subject:
  - **%USERNAME%** – User name
  - **%USERDOMAIN%** – User's domain name
  - **%ADUSERNAME%** – User's name in Active Directory
  - **%WILDCARD%** – Wildcard variable
  - **%AD:mail%** – User's email address as configured in Active Directory
  - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft's Documentation of Active Directory user attributes link for more information.

13 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

14 Select **Only allow users listed locally** to allow only users with a local record in Active Directory to login.

15 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into Active Directory domains are automatically assigned in real time to Web Application Firewall groups based on their external AD group memberships. If a user's external group membership has changed, their WAF group membership automatically changes to match the external group membership.

16 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.

- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.

17 If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the Active Directory **AD e-mail attribute** drop-down list appears, in which you can select **mail**, **mobile**, **pager**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your AD server is configured to store email addresses using the "mail" attribute, select **mail**.
- **mobile** or **pager** - If your AD server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, but SMS addresses can.
- **userPrincipalName** - If your AD server is configured to store email addresses using the "userPrincipalName" attribute, select **userPrincipalName**.
- **custom** - If your AD server is configured to store email addresses using a custom attribute, select **custom**.
    - If you select **custom**, the **Custom attribute** field appears. Type the custom attribute that your AD server uses to store email addresses. If the specified attribute cannot be found for a user, the email address is taken from their individual policy settings.

18 If you selected **using domain name** in the **One-time passwords** drop-down list, an **E-mail domain** field appears. Type in the domain name where one-time password emails are sent (for example, abc.com).

19 Select the type of user from the **User Type** drop-down list. All users logging in through this domain are treated as this user type. The choices depend on user types defined already. Some possible choices are:

- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local WAF admin credentials. These users are presented with the admin login page.

  This option allows the SonicWall WAF administrator to configure a domain that allows WAF admin privileges to all users logging into that domain.

  SonicWall recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **External Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

20 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page.

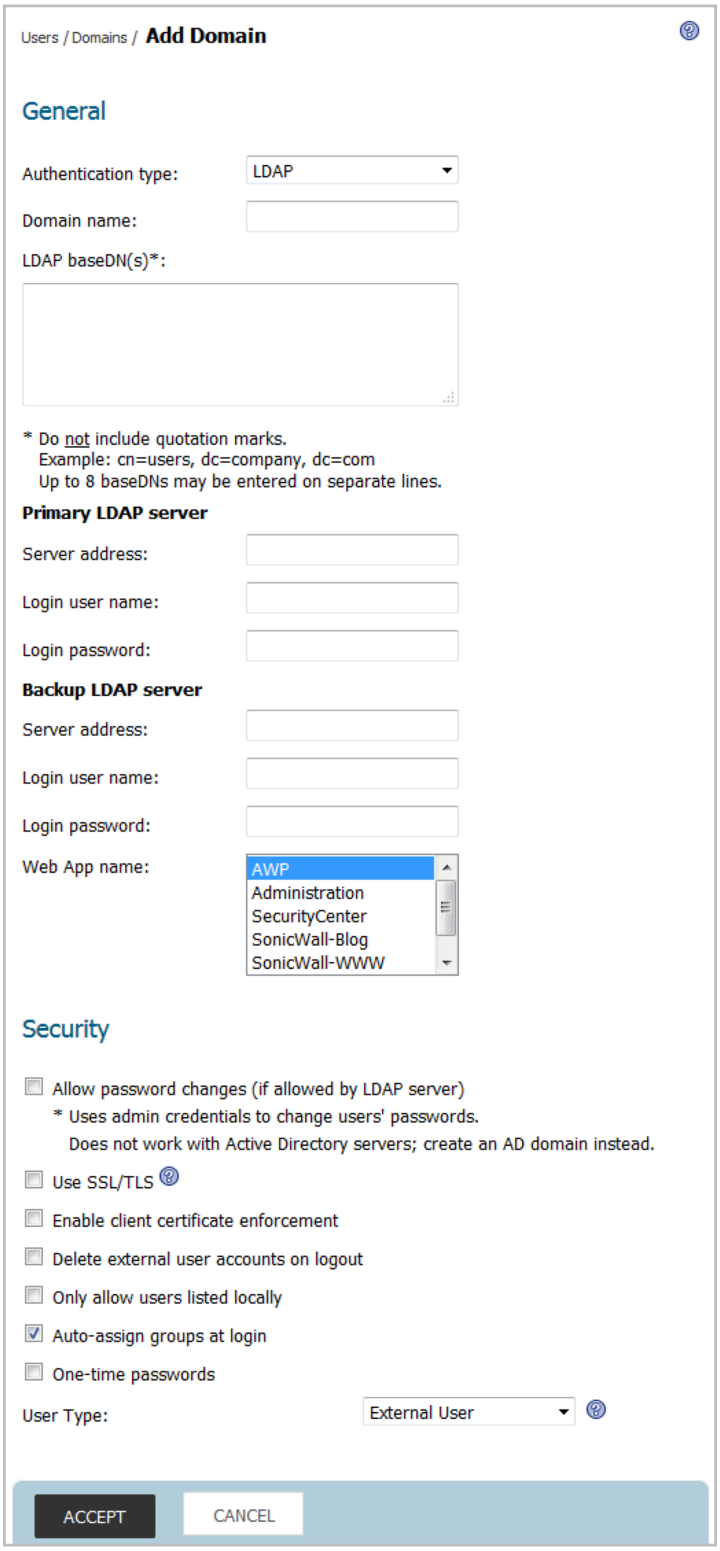
Adding or Editing a Domain with LDAP Authentication

To configure a domain with LDAP authentication:

1 Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 If adding the domain, select **LDAP** from the **Authentication Type** drop-down list.

The LDAP domain configuration fields are displayed.



Users / Domains / **Add Domain**

General

Authentication type: LDAP

Domain name:

LDAP baseDN(s)*:

* Do not include quotation marks.
Example: cn=users, dc=company, dc=com
Up to 8 baseDNs may be entered on separate lines.

Primary LDAP server

Server address:

Login user name:

Login password:

Backup LDAP server

Server address:

Login user name:

Login password:

Web App name: AWP, Administration, SecurityCenter, SonicWall-Blog, SonicWall-WWW

Security

□ Allow password changes (if allowed by LDAP server)
* Uses admin credentials to change users' passwords.
Does not work with Active Directory servers; create an AD domain instead.

□ Use SSL/TLS

□ Enable client certificate enforcement

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ Auto-assign groups at login

□ One-time passwords

User Type: External User

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log into Web Application Firewall. It can be the same value as the Primary LDAP **Server address** field.

4 Enter the search base for LDAP queries into the **LDAP baseDN** field. An example of a search base string is **CN=Users,DC=yourdomain,DC=com**.

> ⓘ **TIP:** It is possible for multiple OUs to be configured for a single domain by entering each OU on a separate line in the **LDAP baseDN** field. In addition, any sub-OUs are automatically included when parents are added to this field.

> ⓘ **NOTE:** Do not include quotes (“”) in the **LDAP BaseDN** field.

5 In the **Primary LDAP server** section, enter the IP address or domain name of the Primary LDAP server into the **Server Address** field.

6 Enter the common name and password of a user that has been delegated control of the primary server in the **Login Username** and **Login Password** fields. The user must belong to one of the LDAP baseDNs specified above, not to a lower level OU.

7 In the **Backup LDAP server** section, optionally enter the IP address or domain name of a backup LDAP server into the **Server Address** field.

8 Optionally enter the common name and password of a user that has been delegated control of the primary server in the **Login Username** and **Login Password** fields. The user must belong to one of the LDAP baseDNs specified above, not to a lower level OU.

9 Select the name of the associated web application in the **Web App Name** field.

10 Select the **Allow password changes (if allowed by LDAP server)** check box to allow users to change their own passwords. This option, if allowed by your LDAP server, enables users to change their LDAP password during a Web Application Firewall session.

11 Select the **Use SSL/TLS** check box to allow SSL/TLS encryption to be used for LDAP password exchanges. This option is disabled by default as not all LDAP servers are configured for SSL/TLS.

12 Select the **Enable client certificate enforcement** check box to require the use of client certificates for login. If set, this option requires the client to present a client certificate for strong mutual authentication.

Two additional fields appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user’s account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that matches the client certificate subject:
  - **%USERNAME%** – User name
  - **%USERDOMAIN%** – User’s domain name
  - **%ADUSERNAME%** – User’s name in Active Directory
  - **%WILDCARD%** – Wildcard variable
  - **%AD:mail%** – User’s email address as configured in Active Directory
  - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft’s Documentation of Active Directory user attributes link for more information.

13 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

14 Select **Only allow users listed locally** to allow only users with a local record in LDAP to login.

15 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into LDAP domains are automatically assigned in real time to Web Application Firewall groups based on their external LDAP group memberships. If a user's external group membership has changed, their WAF group membership automatically changes to match the external group membership.

16 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.

17 If you selected **if configured** or **required for all users** in the **One-time passwords** drop-down list, the **LDAP e-mail attribute** drop-down list appears, in which you can select **mail**, **mobile**, **pager**, **userPrincipalName**, or **custom**. These are defined as:

- **mail** - If your LDAP server is configured to store email addresses using the "mail" attribute, select **mail**.
- **mobile** or **pager** - If your LDAP server is configured to store mobile or pager numbers using either of these attributes, select mobile or pager, respectively. Raw numbers cannot be used, but SMS addresses can.
- **userPrincipalName** - If your LDAP server is configured to store email addresses using the "userPrincipalName" attribute, select **userPrincipalName**.
- **custom** - If your LDAP server is configured to store email addresses using a custom attribute, select **custom**.
  - If you select **custom**, the **Custom attribute** field appears. Type the custom attribute that your LDAP server uses to store email addresses. If the specified attribute cannot be found for a user, the email address is taken from their individual policy settings.

18 If you selected **using domain name** in the **One-time passwords** drop-down list, an **E-mail domain** field appears. Type in the domain name where one-time password emails are sent (for example, abc.com).

19 Select the type of user from the **User Type** drop-down list. All users logging in through this domain are treated as this user type. The choices depend on user types defined already. Some possible choices are:

- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local WAF admin credentials. These users are presented with the admin login page.

  This option allows the SonicWall WAF administrator to configure a domain that allows WAF admin privileges to all users logging into that domain.

  SonicWall recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **External Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

20 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page.

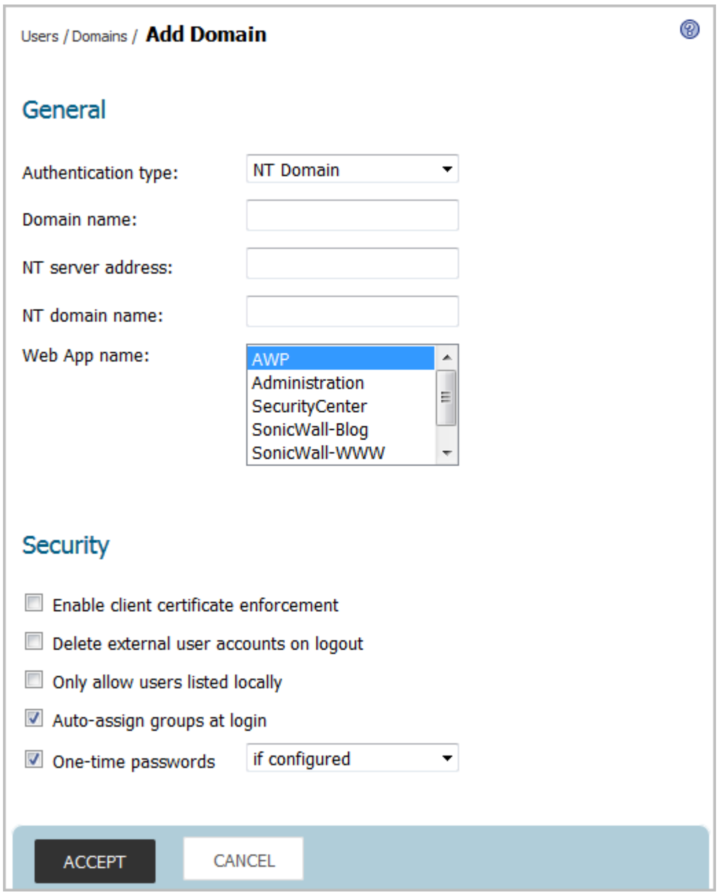
Adding or Editing a Domain with NT Domain Authentication

To configure a domain with NT Domain authentication:

1 Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 If adding the domain, select **NT Domain** from the **Authentication Type** drop-down list.

The NT Domain configuration fields are displayed.



Users / Domains / **Add Domain**

General

Authentication type: NT Domain

Domain name:

NT server address:

NT domain name:

Web App name: AWP
Administration
SecurityCenter
SonicWall-Blog
SonicWall-WWW

Security

□ Enable client certificate enforcement

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ Auto-assign groups at login

☑ One-time passwords — if configured

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log into Web Application Firewall.

4 Type the IP address of the NT server into the **NT server address** field.

5 Type the NT domain name into the **NT domain name** field.

6 Select the name of the associated web application in the **Web App Name** field.

7 Select the **Enable client certificate enforcement** check box to require the use of client certificates for login. If set, this option requires the client to present a client certificate for strong mutual authentication.

Two additional fields appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user’s account name match their client certificate.

- **Verify partial DN in subject** - Use the following variables to configure a partial DN that matches the client certificate subject:
    - **%USERNAME%** – User name
    - **%USERDOMAIN%** – User’s domain name
    - **%ADUSERNAME%** – User’s name in Active Directory
    - **%WILDCARD%** – Wildcard variable
    - **%AD:mail%** – User’s email address as configured in Active Directory
    - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft’s Documentation of Active Directory user attributes link for more information.

8 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

9 Select **Only allow users listed locally** to allow only users with a local record to login.

10 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into NT domains are automatically assigned in real time to Web Application Firewall groups based on their external NT group memberships. If a user’s external group membership has changed, their WAF group membership automatically changes to match the external group membership.

11 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.
    - If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, *abc.com*).

12 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page.

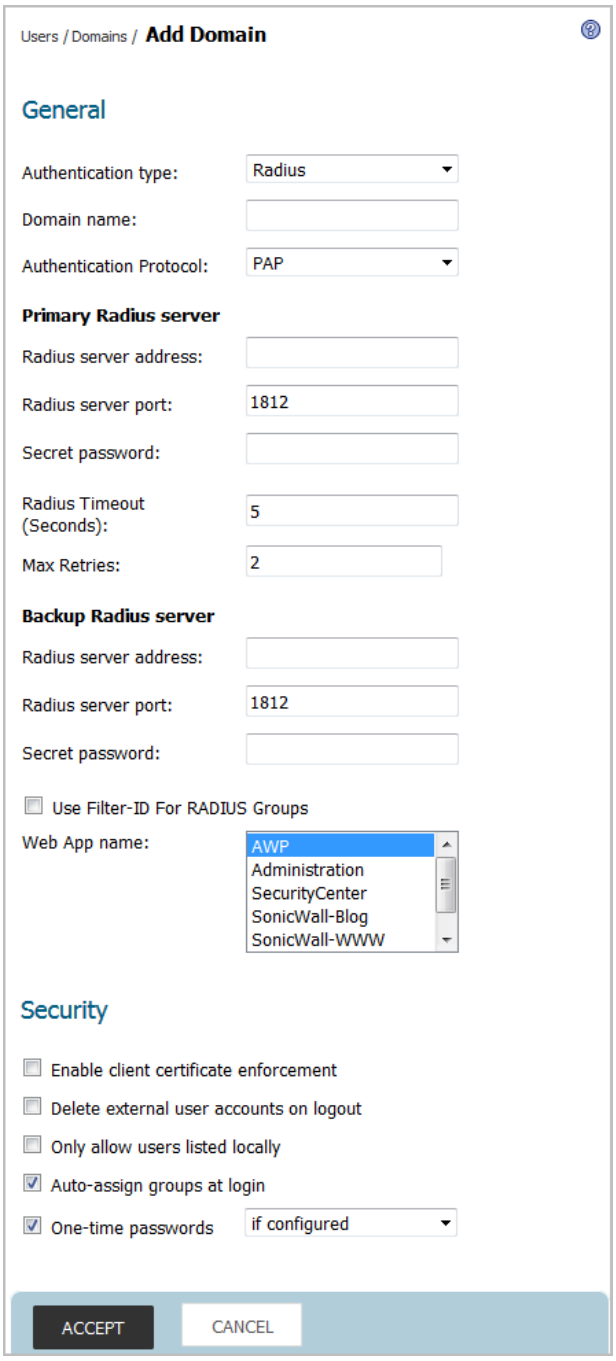
Adding or Editing a Domain with RADIUS Authentication

To configure a domain with RADIUS authentication:

1 Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 If adding the domain, select **Radius** from the **Authentication Type** drop-down list.

The Radius configuration fields are displayed.



Users / Domains / **Add Domain**

General

Authentication type:	Radius
Domain name:	
Authentication Protocol:	PAP

Primary Radius server

Radius server address:	
Radius server port:	1812
Secret password:	
Radius Timeout (Seconds):	5
Max Retries:	2

Backup Radius server

Radius server address:	
Radius server port:	1812
Secret password:	

□ Use Filter-ID For RADIUS Groups

Web App name: AWP, Administration, SecurityCenter, SonicWall-Blog, SonicWall-WWW

Security

□ Enable client certificate enforcement

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ Auto-assign groups at login

☑ One-time passwords — if configured

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log into Web Application Firewall.

4 Select the proper **Authentication Protocol** for your RADIUS server. Choose from **PAP**, **CHAP**, **MSCHAP**, or **MSCHAPV2**.

5 Under **Primary Radius server**, enter the IP address or domain name of the RADIUS server in the **Radius server address** field.

6 Enter the RADIUS server port in the **Radius server port** field.

7 If required by your RADIUS configuration, enter an authentication secret in the **Secret password** field.

8 Enter a number (in seconds) for RADIUS timeout in the **Radius Timeout (Seconds)** field.

9 Enter the maximum number of retries in the **Max Retries** field.

10 Under **Backup Radius Server**, enter the IP address or domain name of the backup RADIUS server in the **Radius server address** field.

11 Enter the backup RADIUS server port in the **Radius server port** field.

12 If required by the backup RADIUS server, enter an authentication secret for the backup RADIUS server in the **Secret password** field.

13 If using RADIUS for group-based access, select **Use Filter-ID for RADIUS Groups**.

14 Select the name of the associated web application in the **Web App Name** field.

15 If you selected the **Authentication Protocol** for your RADIUS server as **MSCHAP** or **MSCHAPV2**, you have the option to select **Allow password changes**. Note that if you enable password changes, you must also deploy the LAN Manager authentication.

16 Select the **Enable client certificate enforcement** check box to require the use of client certificates for login. If set, this option requires the client to present a client certificate for strong mutual authentication.

Two additional fields appear:

- **Verify user name matches Common Name (CN) of client certificate** - Select this check box to require that the user's account name match their client certificate.
- **Verify partial DN in subject** - Use the following variables to configure a partial DN that matches the client certificate subject:
  - **%USERNAME%** – User name
  - **%USERDOMAIN%** – User's domain name
  - **%ADUSERNAME%** – User's name in Active Directory
  - **%WILDCARD%** – Wildcard variable
  - **%AD:mail%** – User's email address as configured in Active Directory
  - **%AD:____%** – Any other Active Directory user attribute, such as **%AD:title%** or **%AD:cn%**. Click the Microsoft's Documentation of Active Directory user attributes link for more information.

17 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

18 Select **Only allow users listed locally** to allow only users with a local record in RADIUS to login.

19 Select **Auto-assign groups at login** to assign users to a group when they log in.

Users logging into RADIUS domains are automatically assigned in real time to SonicWall WAF groups based on their external RADIUS filter-IDs. If a user's external group membership has changed, their WAF membership automatically changes to match the external group membership.

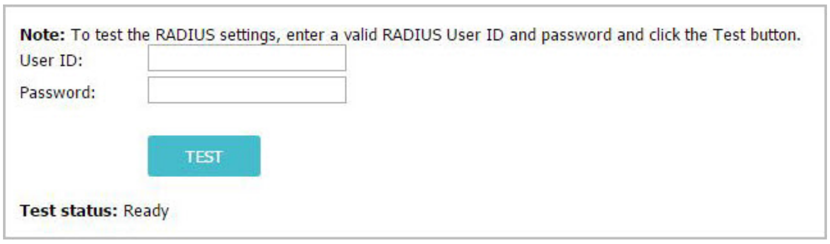
20 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.

- If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, *abc.com*).

21 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page.

22 Click **Configure** next to the RADIUS domain you added. The **Test** tab of the **Edit Domain** page displays.



Note: To test the RADIUS settings, enter a valid RADIUS User ID and password and click the Test button.

User ID:

Password:

Test status: Ready

23 Enter your RADIUS user ID in the **User ID** field and your RADIUS password in the **Password** field.

24 Click **TEST**. Web Application Firewall connects to your RADIUS server.

25 If you receive the message **Server not responding**, check your user ID and password and view the **General** section to verify your RADIUS settings. Try running the test again.

> **NOTE:** Web Application Firewall attempts to authenticate against the specified RADIUS server using PAP authentication. It is generally required that the RADIUS server be configured to accept RADIUS client connections from the Web Application Firewall virtual appliance. Typically, these connections appear to come from the Web Application Firewall virtual appliance X0 interface IP address. Refer to your RADIUS server documentation for configuration instructions.

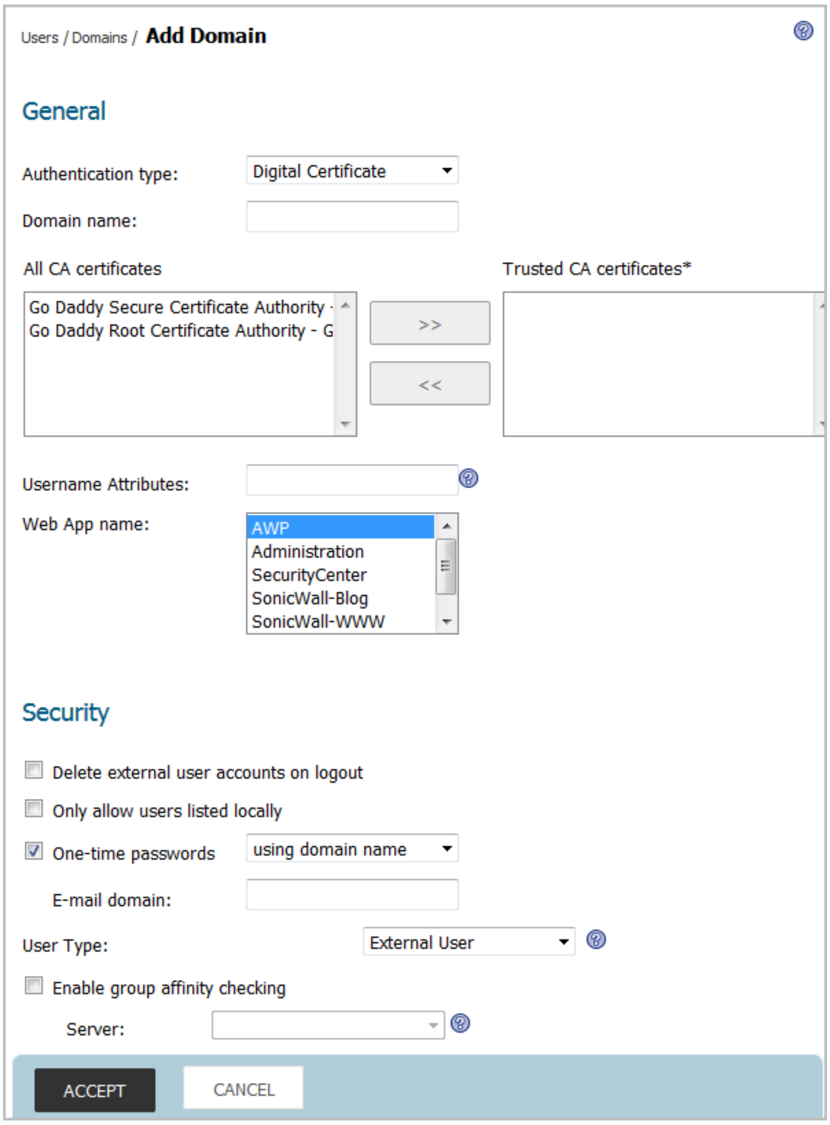
Adding or Editing a Domain with Digital Certificates

To add or edit a domain for digital certificate authentication:

1 Navigate to the **Users > Domains** page and click **ADD DOMAIN** or the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 If adding the domain, select **Digital Certificate** from the **Authentication Type** menu.

The Digital Certificate configuration fields are displayed.



Users / Domains / **Add Domain**

General

Authentication type: Digital Certificate

Domain name:

All CA certificates: Go Daddy Secure Certificate Authority -; Go Daddy Root Certificate Authority - G

Trusted CA certificates*

Username Attributes:

Web App name: AWP (selected), Administration, SecurityCenter, SonicWall-Blog, SonicWall-WWW

Security

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ One-time passwords: using domain name

E-mail domain:

User Type: External User

□ Enable group affinity checking

Server:

3 If adding the domain, enter a descriptive name for the authentication domain in the **Domain name** field. This is the domain name users select in order to log into Web Application Firewall.

4 Select one or more certificates from the **All CA certificates** list to be added to the **Trusted CA certificates** list. The **All CA certificates** list displays all available certificates for Web Application Firewall that were imported in **System > Certificates**.

5 Enter the attribute to be used for Single Sign-On in the **Username Attributes** field. Enter **CN** to use the common name attribute of the client certificate as the login username.

6 Select the name of the associated web application in the **Web App Name** field.

7 Select **Delete external user accounts on logout** to delete users who are not logged into a domain account after they log out.

8 Select **Only allow users listed locally** to allow only users with a local record to login.

9 Select the **One-time passwords** check box to enable the One Time Password feature. A drop-down list appears, in which you can select **if configured**, **required for all users**, or **using domain name**. These are defined as:

- **if configured** - Only users who have a One Time Password email address configured must use the One Time Password feature.
- **required for all users** - All users must use the One Time Password feature. Users who do not have a One Time Password email address configured are not allowed to log in.
- **using domain name** - Users in the domain must use the One Time Password feature. One Time Password emails for all users in the domain are sent to *username@domain.com*.
    - If you select **using domain name**, an **E-mail domain** field appears following the drop-down list. Type in the domain name where one-time password emails are sent (for example, *abc.com*).

10 Select the type of user from the **User Type** drop-down list. All users logging in through this domain are treated as this user type. The choices depend on user types defined already. Some possible choices are:

- **External User** – Users logging into this domain are treated as normal users without administrative privileges.
- **External Administrator** – Users logging into this domain are treated as administrators, with local WAF admin credentials. These users are presented with the admin login page.

  This option allows the SonicWall WAF administrator to configure a domain that allows WAF admin privileges to all users logging into that domain.

  SonicWall recommends adding filters that allow administrative access only to those users who are in the correct group. You can do so by editing the domain on the **Users > Local Groups** page.
- **External Read-only Administrator** – Users logging into this domain are treated as read-only administrators and can view all information and settings, but cannot apply any changes to the configuration. These users are presented with the admin login page.

11 The **Enable group affinity checking** setting and **Server** can be set after importing the client certificate, to authorize the certificate.

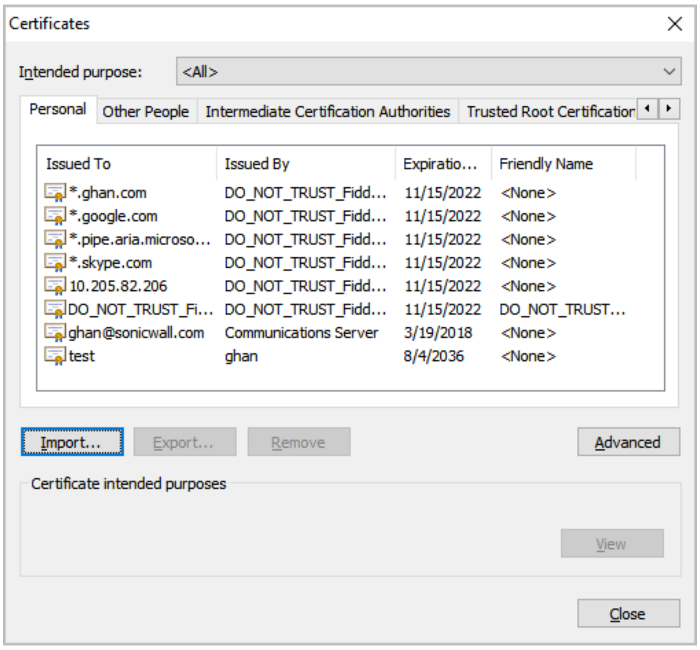
12 Click **ACCEPT** to save your changes. The domain is added to the table on the **Users > Domains** page. Next, you need to import the client certificate to your web browser.

Proceed to Importing the Client Certificate on page 181.

Importing the Client Certificate

To import the client certificate:

1 Navigate to the **Certificate** details on your web browser's settings.



Certificates

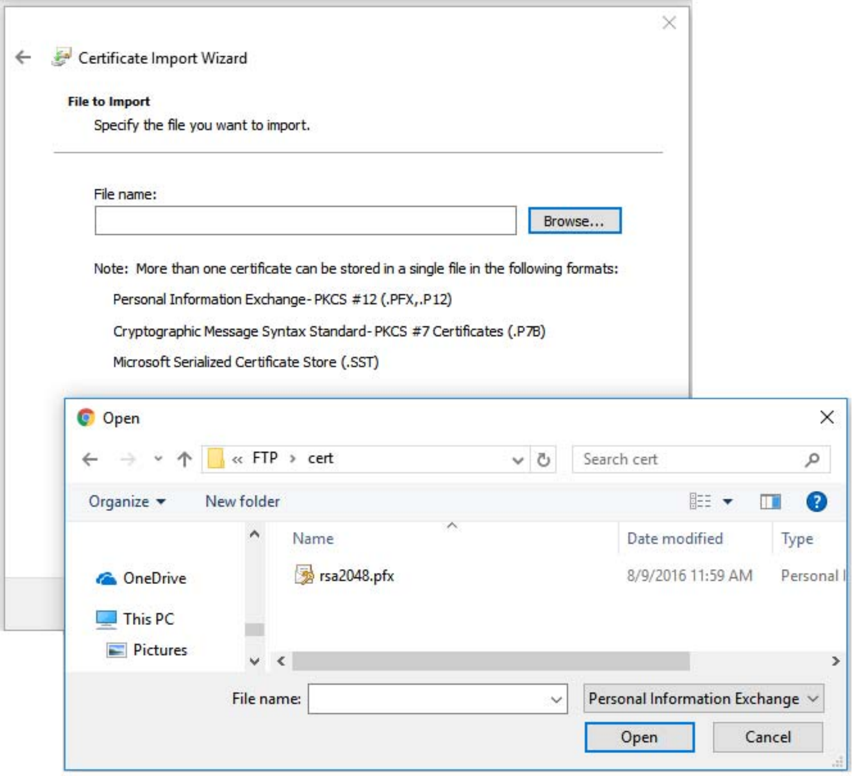
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
*.ghan.com	DO_NOT_TRUST_Fidd...	11/15/2022	<None>
*.google.com	DO_NOT_TRUST_Fidd...	11/15/2022	<None>
*.pipe.aria.microso...	DO_NOT_TRUST_Fidd...	11/15/2022	<None>
*.skype.com	DO_NOT_TRUST_Fidd...	11/15/2022	<None>
10.205.82.206	DO_NOT_TRUST_Fidd...	11/15/2022	<None>
DO_NOT_TRUST_Fi...	DO_NOT_TRUST_Fidd...	11/15/2022	DO_NOT_TRUST...
ghan@sonicwall.com	Communications Server	3/19/2018	<None>
test	ghan	8/4/2036	<None>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

2 Click **Import**.

3 Select the client certificate to import and follow the certificate import guide in the browser settings.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Open

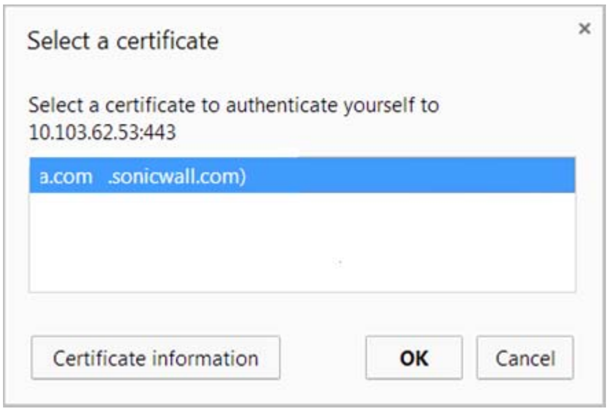
« FTP › cert

Name	Date modified	Type
rsa2048.pfx	8/9/2016 11:59 AM	Personal I

File name:

Personal Information Exchange

4 When the client accesses the web app, the browser asks the user to select a certificate to proceed. The user should enable the option to remember the certificate choice so the selection popup is not displayed the next time.



The authentication completes if the CA of the client certificate is on the Trusted CA certificates list. If the client certificate is not on the Trusted CA certificates list, Web Application Firewall blocks access and displays an error message.

5 Proceed to Enabling Group Affinity Checking on page 182.

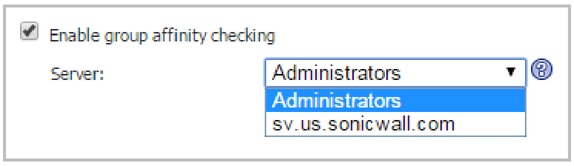
Enabling Group Affinity Checking

To enable group affinity checking:

1 Navigate to the **Users > Domains** page and click the edit button in the **Configure** column of the row for the domain that you wish to edit. The **Add Domain** or **Edit Domain** page is displayed.

2 Select the **Enable group affinity checking** check box.

3 Select one of the available domains from the **Server** drop-down list.



☑ Enable group affinity checking

Server: Administrators

4 Click **ACCEPT** to save your changes. A group affinity check is performed against an LDAP or Active Directory server.

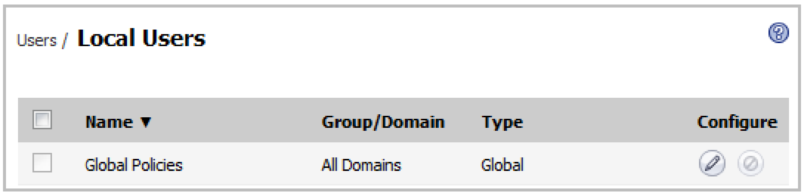
> **NOTE:** Only Active Directory or LDAP servers and domains are supported.

10

Global Policy Configuration

This section provides information and configuration tasks specific to configuring global policies and settings in SonicWall Web Application Firewall. Global policies and settings are configured from the **Local Users** or **Local Groups** page by editing the **Global Policies** entry that appears at the top of the tables on both pages.

Global Policies Entry in Local Users Page



Users / **Local Users**

□	Name ▼	Group/Domain	Type	Configure
□	Global Policies	All Domains	Global	

For more information about policies, see How are Policies Created and Used in WAF? on page 9.

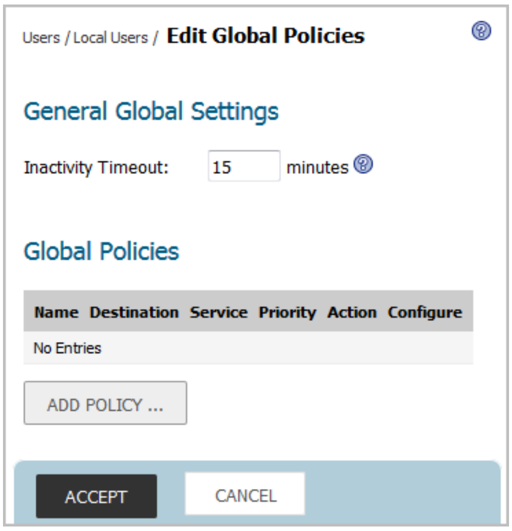
Topics:

- Editing Global Settings on page 183
- Adding a Global Policy on page 184

Editing Global Settings

To edit global settings:

1 Navigate to the **Users > Local Users** or **Users > Local Groups** page, then click the edit icon in the **Configure** column of the **Global Policies** entry. The **Edit Global Policies** page is displayed.



Users / Local Users / **Edit Global Policies**

General Global Settings

Inactivity Timeout: 15 minutes

Global Policies

Name	Destination	Service	Priority	Action	Configure
No Entries					

2 In the **Inactivity Timeout (minutes)** field, type in the number of inactive minutes before a user is logged out. The number should be greater than zero. This is the default setting for all users, but can be overridden by User or Group settings.

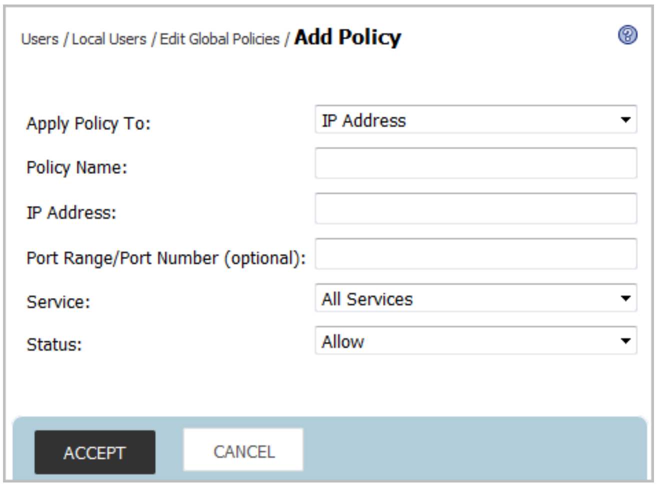
3 Click **ACCEPT** to save your changes.

Adding a Global Policy

To add a global policy:

1 Navigate to the **Users > Local Users** or **Users > Local Groups** page, then click the edit button in the **Configure** column of the **Global Policies** entry. The **Edit Global Policies** page is displayed.

2 In the **Global Policies** section, click **ADD POLICY**. The **Add Policy** page is displayed.



Users / Local Users / Edit Global Policies / **Add Policy**

Apply Policy To:	IP Address
Policy Name:	
IP Address:	
Port Range/Port Number (optional):	
Service:	All Services
Status:	Allow

3 Select one of the following from the **Apply Policy To** drop-down list:

- **IP Address** – Select this if the policy applies to a specific host.
- **IP Network** – Select this if the policy applies to all IP addresses in a specific subnet.
- **All Addresses** – Select this if the policy applies to all addresses.
- **URL** – Select this if the policy applies to a specific web site or web application.

The displayed fields change depending on the selected value.

> **NOTE:** Policies apply to the destination address(es) of the Web Application Firewall connection, not the source address. You cannot permit or block a specific IP address on the Internet from authenticating to Web Application Firewall through the policy engine.

4 Type a name for the policy in the **Policy Name** field.

5 If **Apply Policy To** is set to **IP Address**:

a Type the IP address of the host machine into the **IP Address** field.

b Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

6 If **Apply Policy To** is set to **IP Network**:

a Type the IP network address into the **IP Network Address** field.

b Type the network mask into the **Subnet Mask** field. For example, 255.255.255.0 designates the first 24 bits of an IP address as the network part.

c Optionally enter a port range (80-443) or a single port number into the **Port Range/Port Number** field.

7 If **Apply Policy To** is set to **All Addresses**, there are no unique fields to configure.

8 If **Apply Policy To** is set to **URL**, type the URL into the **URL** field. For example, “sonicwall.com”.

9 In the **Service** drop-down list, select one of **All Services**, **Web (HTTP)**, or **Secure Web (HTTPS)**.

10 In the **Status** drop-down list, select either **Allow** or **Deny** to either permit or deny Web Application Firewall connections for the specified service and host(s).

11 Click **ACCEPT** to save your changes.

After the configuration has been updated, the new policy is displayed on the **Edit Global Policies** page. The global policies are displayed in the policy list in the **Edit Global Policies** page in the order of priority, from the highest priority policy to the lowest priority policy.

ⓘ | **NOTE:** User and group access policies take precedence over global policies.

11

Log Access and Configuration

This section provides information and configuration tasks specific to the **Log** pages in the SonicWall Web Application Firewall management interface.

Topics:

Viewing the Log Files

The **Log > View** page provides three separate screens for the different types of logs maintained by Web Application Firewall:

- **Event Log** – Logs events such as authentication and user sessions.
- **Audit Log** – Logs configuration, system, and management transactions.
- **Access Log** – Logs access to web applications protected by Web Application Firewall.

Filtering, basic search, and advanced search using queries are supported on all three screens. The filtering and query fields change depending on the screen, but the functionality works in the same way on all screens.

All screens on the **Log > View** page provide the **EXPORT LOG**, **CLEAR LOG**, and **E-MAIL LOG** buttons.

The log table size is specified on the **System > Administration** page in the **Default Table Size** field. After the log file reaches the log size limit, the log entry is cleared and optionally emailed to the Web Application Firewall administrator.

Topics:

About the Log > View Buttons

The **Log > View** page provides options that allow the administrator to clear, email, or export log files for external viewing or processing.

Log Rendering Options

Button	Action
EXPORT LOG	Exports the current log contents to a text-based file.
CLEAR LOG	Clears the current log contents.
E-MAIL LOG	Emails the current log contents to the address specified in the **Log > Settings** screen.

Viewing the Event Log

The **Event Log** screen of the **Log > View** page displays event log messages in a sortable, searchable table. Each log entry contains the date and time of the event, plus other details and a brief message describing the event.

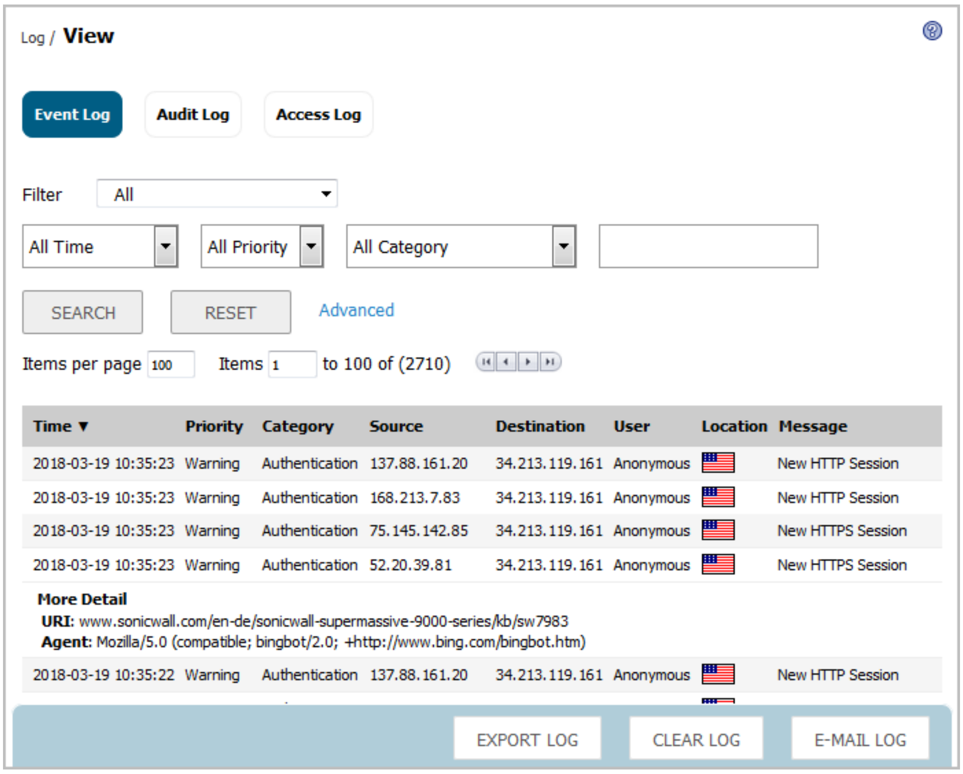
You can sort the table by clicking on any of the column headings. Click again to toggle the sort order.

The Event Log Columns table describes the event log table in more detail.

Event Log Columns

Column	Description
Time	The time stamp displays the date and time of log events in the format *YY/MM/DD/HH/MM/SS* (Year/Month/Day/Hour/Minute/Second). Hours are displayed in 24-hour clock format. The date and time are based on the local time of the Web Application Firewall virtual appliance, which is configured in the **System > Time** page. Click the **Time** heading to toggle the order of the log messages on the page by oldest or newest.
Priority	The level of severity associated with the event. Severity levels can be **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Information**, and **Debug**.
Category	The category of the event message. Categories include **Authentication**, **Access**, **GMS**, **System**, **Web Application Firewall**, **Geo IP & Botnet Filter**, **Reverse Proxy**, and **Capture ATP**.
Source	The source IP address of the system that generated the traffic or request which caused the log event. The source IP address cannot be displayed for certain events, such as system errors.
Destination	The name or IP address of the destination server or service associated with the event. For example, if a user accessed an intranet web site protected by Web Application Firewall, the corresponding log entry would display the IP address or Fully Qualified Domain Name (FQDN) of the web site accessed. If the event is not related to a backend server, the destination shows the IP address ofWAF.
User	The name of the user who was logged into Web Application Firewall when the message was generated.
Location	The geographical location of the source IP for each event log message. This is only displayed if the Geo IP & Botnet Filter service is licensed and enabled.
Message	The text of the log message.

Log > View > Event Log Screen



Filter: All

All Time | All Priority | All Category

Items per page 100 Items 1 to 100 of (2710)

Time ▼	Priority	Category	Source	Destination	User	Location	Message
2018-03-19 10:35:23	Warning	Authentication	137.88.161.20	34.213.119.161	Anonymous	🇺🇸	New HTTP Session
2018-03-19 10:35:23	Warning	Authentication	168.213.7.83	34.213.119.161	Anonymous	🇺🇸	New HTTP Session
2018-03-19 10:35:23	Warning	Authentication	75.145.142.85	34.213.119.161	Anonymous	🇺🇸	New HTTPS Session
2018-03-19 10:35:23	Warning	Authentication	52.20.39.81	34.213.119.161	Anonymous	🇺🇸	New HTTPS Session
More Detail **URI:** www.sonicwall.com/en-de/sonicwall-supermassive-9000-series/kb/sw7983 **Agent:** Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)							
2018-03-19 10:35:22	Warning	Authentication	137.88.161.20	34.213.119.161	Anonymous	🇺🇸	New HTTP Session

Topics:

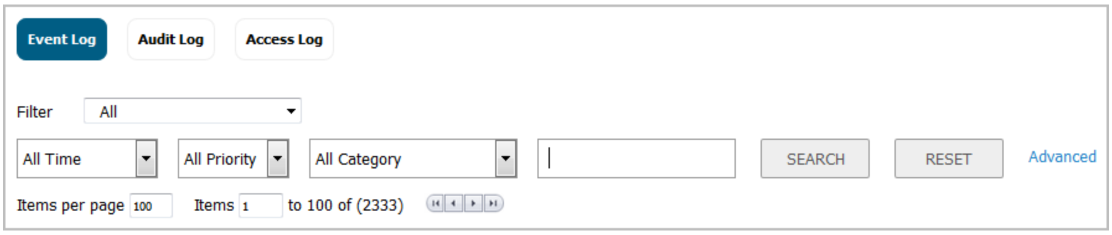
- Event Log Filtering and Basic Search on page 188
- Event Log Advanced Search on page 189

Event Log Filtering and Basic Search

The **Event Log** screen provides easy pagination for viewing large numbers of log messages. You can navigate these log messages by using the display options at the top of the page, including filter, search, and pagination controls.

To filter and search the Event Log:

1 Navigate to the **Event Log** screen of the **Log > View** page.



Filter: All

All Time | All Priority | All Category

Items per page 100 Items 1 to 100 of (2333)

The basic filter and search options are displayed at the top of the screen.

2 In the **Filter** drop-down list, choose a *Standard* or a *Custom* (saved) filter for a quick search without setting the other fields. Available *Standard* filters for **Event Log** are **All**, **Access**, **Web Application Firewall**, and **Geo Ip & Botnet Filter**.

Your selection in the **Filter** field is also displayed in the **Category** field. The table changes to display only those log messages matching the selected category.

3 To filter log messages by time, select the desired time period from the first drop-down list at the left under the **Filter** field. It displays **All Time** by default. Other options are **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 12 months**.

The table changes to display only those log messages matching the selected time period.

4 To filter log messages by priority, select the desired priority level from the second drop-down list from the left under the **Filter** field. It displays **All Priority** by default. Other options are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info**, and **Debug**.

The table changes to display only those log messages matching the selected priority.

5 To filter log messages by category, select the desired category from the third drop-down list from the left under the **Filter** field. It displays **All Category** by default. Other options are **Authentication, Access**, **GMS**, **System**, **Web Application Firewall**, **Geo IP & Botnet Filter**, **Reverse Proxy,** and **Capture ATP**.

The table changes to display only those log messages matching the selected category.

6 To search the log for a specific string or value, type the alphanumeric search pattern into the blank field to the left of the **SEARCH** button, and then click **SEARCH**.

The table changes to display only those log messages that contain a match for the search text.

7 To reset the listing of log messages to their default sequence after filtering or searching the log, click the **RESET** button.

8 To change the number of entries displayed per page, type the desired number into the **Items per page** field and press the **Enter** key. The default is 100.

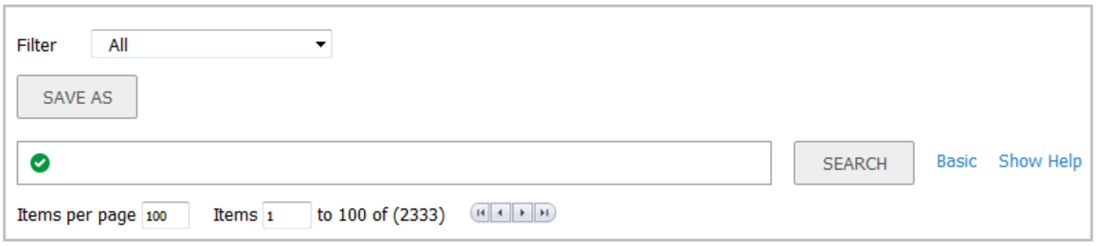
9 Use the arrow buttons to change the display to the first, previous, next, or last page of log messages.

Event Log Advanced Search

To perform an advanced search using queries on the Event Log screen:

1 Navigate to the **Event Log** screen of the **Log > View** page.

2 Click the **Advanced** link. The display changes, and the **Advanced** link changes to **Basic**, allowing you to display the basic search options again.


Filter: All

Items per page 100 Items 1 to 100 of (2333)

3 Click the **Show Help** link to display details about using advanced search. The usage is summarized here:

- A query consists of a ***field***, an ***operator***, and a ***value***. All words are case-insensitive.
- In a simple query, valid operators are colon (**:**), greater than (**>**), and less than (**<**).
- In a complex query you can combine simple queries with the logical operators **AND**, **OR**, and parentheses for grouping '**()**'.

Query Examples

Query	Description
Category:Access	Find all logs that contain Access in their Category. In this query Category is the field, ‘:’ is the operator, and “Access” is the value.
Time<2d or (Priority:warning and Category:System)	Find logs that are recorded within 2 days or that contain “warning” in their Priority and contain “System” in their Category.

- Supported fields include: **Time**, **Priority**, **Category**, **Source**, **Destination**, **User**, **Message**, **Location**, and **Text**.

  Location can be used only when the **Geo Ip & Botnet Filter** service is enabled.

  Text means all characters in one log message on one line in the **Log > View** page.

4 When your query is ready, click the **SEARCH** button.

5 To save the filter, click the **SAVE AS** button. In the popup dialog, type in a descriptive name for the search filter and click **OK**. The saved filter is added to the **Filter** drop-down list under *Custom*.

Viewing the Audit Log

The **Audit Log** screen of the **Log > View** page displays audit log messages in a sortable, searchable table. Each log entry contains the date and time of the event, plus other details.

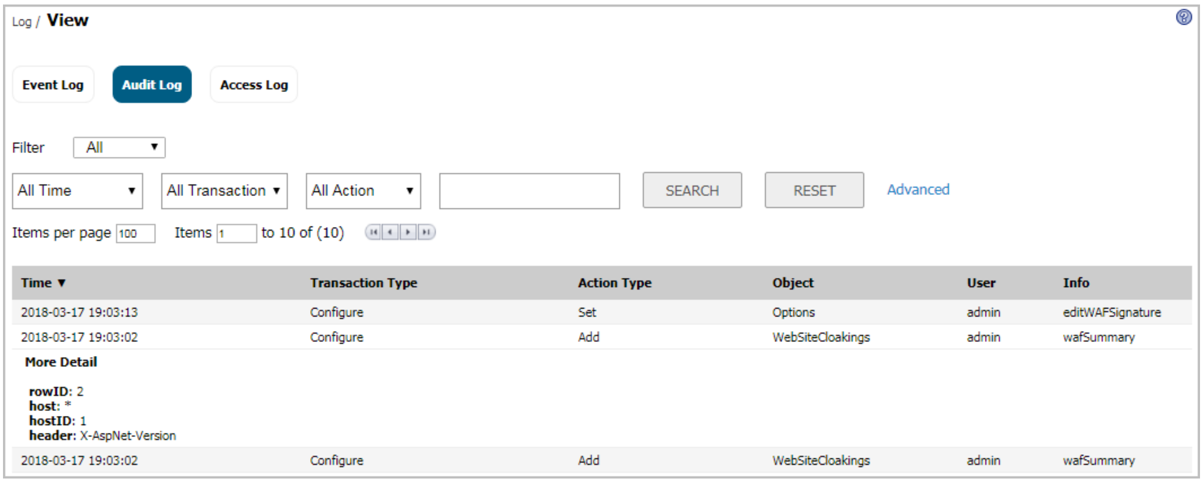
You can sort the table by clicking on any of the column headings. Click again to toggle the sort order.

The Audit Log Columns table describes the audit log table in more detail.

Audit Log Columns

Column	Description
Time	The time stamp displays the date and time of log events in the format *YY/MM/DD/HH/MM/SS* (Year/Month/Day/Hour/Minute/Second). Hours are displayed in 24-hour clock format. The date and time are based on the local time of the Web Application Firewall virtual appliance, which is configured in the **System > Time** page.
Transaction Type	The type of transaction associated with the log entry. Transaction types can be **Configure**, **System**, and **Management**.
Action Type	The action type associated with the log entry. Action types include **Add**, **Delete**, **Set**, **Login**, **Reboot**, and **Management**.
Object	The object on which the action is performed, usually a database table or configuration file.
User	The name of the user who was logged into Web Application Firewall when the message was generated.
Info	Detailed information about the operation, usually the name of the CGI on which page the operation is performed.

Log > View > Audit Log Screen



Log / **View**

Filter: All

All Time | All Transaction | All Action | SEARCH | RESET | Advanced

Items per page 100 Items 1 to 10 of (10)

Time ▼	Transaction Type	Action Type	Object	User	Info
2018-03-17 19:03:13	Configure	Set	Options	admin	editWAFSignature
2018-03-17 19:03:02	Configure	Add	WebSiteCloakings	admin	wafSummary
More Detail **rowID:** 2 **host:** * **hostID:** 1 **header:** X-AspNet-Version					
2018-03-17 19:03:02	Configure	Add	WebSiteCloakings	admin	wafSummary

Topics:

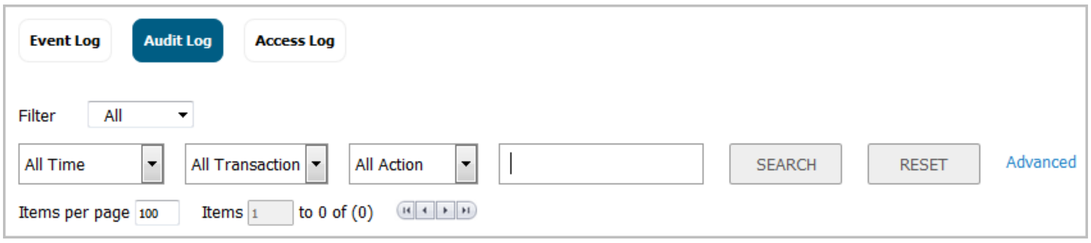
- Audit Log Filtering and Basic Search on page 191
- Audit Log Advanced Search on page 192

Audit Log Filtering and Basic Search

The **Audit Log** screen provides easy pagination for viewing large numbers of log messages. You can navigate these log messages by using the display options at the top of the page, including filter, search, and pagination controls.

To filter and search the Audit Log:

1 Navigate to the **Audit Log** screen of the **Log > View** page.



Filter: All

All Time | All Transaction | All Action | SEARCH | RESET | Advanced

Items per page 100 Items 1 to 0 of (0)

The basic filter and search options are displayed at the top of the screen.

2 In the **Filter** drop-down list, choose a *Standard* or a *Custom* (saved) filter for a quick search without setting the other fields.

The table changes to display only those log messages matching the selected option.

3 To filter log messages by time, select the desired time period from the first drop-down list at the left under the **Filter** field. It displays **All Time** by default. Other options are **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 12 months**.

The table changes to display only those log messages matching the selected time period.

4 To filter events by transaction type, select the desired transaction type from the second drop-down list from the left under the **Filter** field. It displays **All Transaction** by default. Other options are **Configure**, **System**, and **Management**.

The table changes to display only those log messages matching the selected transaction type.

5 To filter events by action type, select the desired action type from the third drop-down list from the left under the **Filter** field. It displays **All Action** by default. Other options are **Add, Delete**, **Set**, **Login**, **Reboot**, and **Management**.

The table changes to display only those log messages matching the selected action type.

6 To search the log for a specific string or value, type the alphanumeric search pattern into the blank field to the left of the **SEARCH** button, and then click **SEARCH**.

The table changes to display only those log messages that contain a match for the search text.

7 To reset the listing of log messages to their default sequence after filtering or searching the log, click the **RESET** button.

8 To change the number of log messages displayed per page, type the desired number into the **Items per page** field and press the **Enter** key. The default is 100.

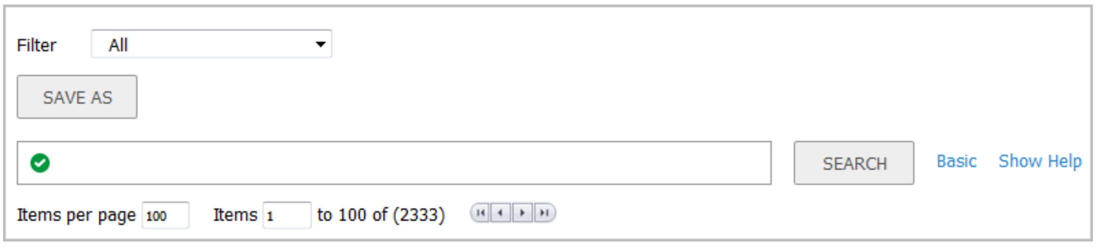
9 Use the arrow buttons to change the display to the first, previous, next, or last page of log messages.

Audit Log Advanced Search

To perform an advanced search using queries on the Audit Log screen:

1 Navigate to the **Audit Log** screen of the **Log > View** page.

2 Click the **Advanced** link. The display changes, and the **Advanced** link changes to **Basic**, allowing you to display the basic search options again.


Filter: All

Items per page: 100 Items: 1 to 100 of (2333)

3 Click the **Show Help** link to display details about using advanced search. The usage is summarized here:

- A query consists of a ***field***, an ***operator***, and a ***value***. All words are case-insensitive.
- In a simple query, valid operators are colon (**:**), greater than (**>**), and less than (**<**).
- In a complex query you can combine simple queries with the logical operators **AND**, **OR**, and parentheses for grouping '**()**'.

Query Examples

Query	Description
TransactionType:Configure	Find all logs that contain "Configure" in their TransactionType. In this query TransactionType is the field, ':' is the operator, and "Configure" is the value.
Time<2d or (TransactionType:Configure and ActionType:Add)	Find logs that are recorded within 2 days or that contain "Configure" in their TransactionType field and contain "Add" in their ActionType field.

- Supported fields include: **Time**, **TransactionType**, **ActionType**, **Object**, **User**, **Info**, and **Text**.

  Text means all characters in one log message on one line in the **Log > View** page.

4 When your query is ready, click the **SEARCH** button.

5 To save the filter, click the **SAVE AS** button. In the popup dialog, type in a descriptive name for the search filter and click **OK**. The saved filter is added to the **Filter** drop-down list under *Custom*.

Viewing the Access Log

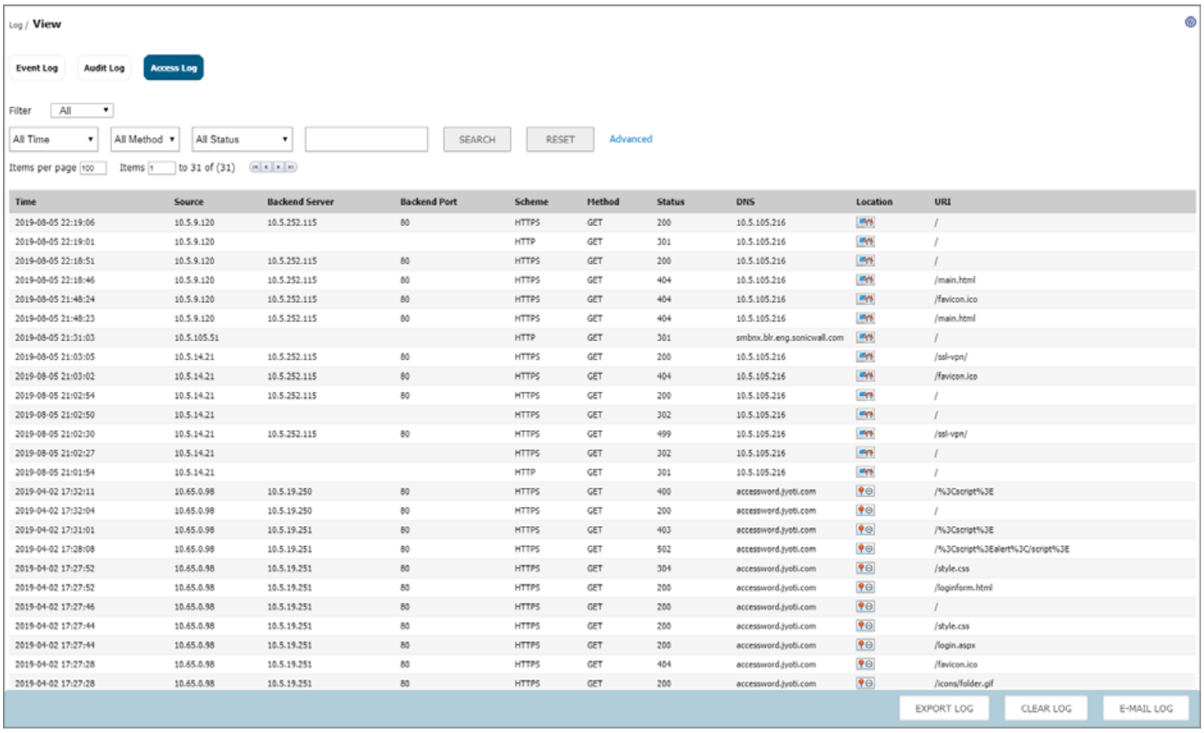
The **Access Log** screen of the **Log > View** page displays access log messages in a searchable table. Each log entry contains the date and time of the event, plus other details.

The Access Log Columns table describes the Access Log table in more detail.

Access Log Columns

Column	Description
Time	The time stamp displays the date and time of access events in the format *YY/MM/DD/HH/MM/SS* (Year/Month/Day/Hour/Minute/Second). Hours are displayed in 24-hour clock format. The date and time are based on the local time of the Web Application Firewall virtual appliance, which is configured in the **System > Time** page.
Source	The source IP address of the remote user.
Backend Server	The service IP address of the backend server.
Backend Port	The port number of the backend server.
Scheme	HTTP or HTTPS.
Method	The HTTP method used in the access.
Status	The status code of the response.
DNS	The virtual host domain name of the accessed web app.
Location	The geographical location of the source IP for each access log message. This is only displayed if the Geo IP & Botnet Filter service is licensed and enabled.
URI	The URI that was accessed.

Log > View > Access Log Screen



Filter All

All Time · All Method · All Status

Items per page 100 Items 1 to 31 of (31)

Time	Source	Backend Server	Backend Port	Scheme	Method	Status	DNS	Location	URI
2019-08-05 22:19:06	10.5.9.120	10.5.252.115	80	HTTPS	GET	200	10.5.105.216		/
2019-08-05 22:19:01	10.5.9.120			HTTP	GET	301	10.5.105.216		/
2019-08-05 22:18:51	10.5.9.120	10.5.252.115	80	HTTPS	GET	200	10.5.105.216		/
2019-08-05 22:18:46	10.5.9.120	10.5.252.115	80	HTTPS	GET	404	10.5.105.216		/main.html
2019-08-05 21:48:24	10.5.9.120	10.5.252.115	80	HTTPS	GET	404	10.5.105.216		/favicon.ico
2019-08-05 21:48:23	10.5.9.120	10.5.252.115	80	HTTPS	GET	404	10.5.105.216		/main.html
2019-08-05 21:31:03	10.5.105.51			HTTP	GET	301	smbnx.blr.eng.sonicwall.com		/
2019-08-05 21:03:05	10.5.14.21	10.5.252.115	80	HTTPS	GET	200	10.5.105.216		/ssl-vpn/
2019-08-05 21:03:02	10.5.14.21	10.5.252.115	80	HTTPS	GET	404	10.5.105.216		/favicon.ico
2019-08-05 21:02:54	10.5.14.21	10.5.252.115	80	HTTPS	GET	200	10.5.105.216		/
2019-08-05 21:02:50	10.5.14.21			HTTPS	GET	302	10.5.105.216		/
2019-08-05 21:02:30	10.5.14.21	10.5.252.115	80	HTTPS	GET	499	10.5.105.216		/ssl-vpn/
2019-08-05 21:02:27	10.5.14.21			HTTPS	GET	302	10.5.105.216		/
2019-08-05 21:01:54	10.5.14.21			HTTP	GET	301	10.5.105.216		/
2019-04-02 17:32:11	10.65.0.98	10.5.19.250	80	HTTPS	GET	400	accessword.jyoti.com		/%3Cscript%3E
2019-04-02 17:32:04	10.65.0.98	10.5.19.250	80	HTTPS	GET	200	accessword.jyoti.com		/
2019-04-02 17:31:01	10.65.0.98	10.5.19.251	80	HTTPS	GET	403	accessword.jyoti.com		/%3Cscript%3E
2019-04-02 17:28:08	10.65.0.98	10.5.19.251	80	HTTPS	GET	502	accessword.jyoti.com		/%3Cscript%3Ealert%3C/script%3E
2019-04-02 17:27:52	10.65.0.98	10.5.19.251	80	HTTPS	GET	304	accessword.jyoti.com		/style.css
2019-04-02 17:27:52	10.65.0.98	10.5.19.251	80	HTTPS	GET	200	accessword.jyoti.com		/loginform.html
2019-04-02 17:27:46	10.65.0.98	10.5.19.251	80	HTTPS	GET	200	accessword.jyoti.com		/
2019-04-02 17:27:44	10.65.0.98	10.5.19.251	80	HTTPS	GET	200	accessword.jyoti.com		/style.css
2019-04-02 17:27:44	10.65.0.98	10.5.19.251	80	HTTPS	GET	200	accessword.jyoti.com		/login.aspx
2019-04-02 17:27:28	10.65.0.98	10.5.19.251	80	HTTPS	GET	404	accessword.jyoti.com		/favicon.ico
2019-04-02 17:27:28	10.65.0.98	10.5.19.251	80	HTTPS	GET	200	accessword.jyoti.com		/icons/folder.gif

Topics:

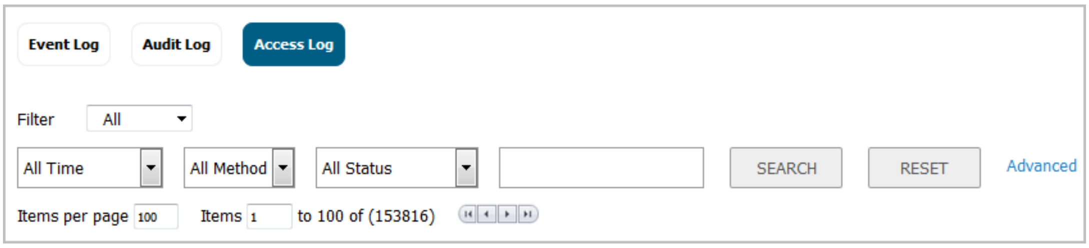
- Access Log Filtering and Basic Search on page 194
- Access Log Advanced Search on page 195

Access Log Filtering and Basic Search

The **Access Log** screen provides easy pagination for viewing large numbers of log messages. You can navigate these log messages by using the display options at the top of the page, including filter, search, and pagination controls.

To filter and search the Access Log:

1 Navigate to the **Access Log** screen of the **Log > View** page.



Filter All

All Time · All Method · All Status

Items per page 100 Items 1 to 100 of (153816)

The basic filter and search options are displayed at the top of the screen.

2 In the **Filter** drop-down list, choose a *Standard* or a *Custom* (saved) filter for a quick search without setting the other fields.

The table changes to display only those log messages matching the selected option.

3 To filter log messages by time, select the desired time period from the first drop-down list at the left under the **Filter** field. It displays **All Time** by default. Other options are **Last 24 hours**, **Last 7 days**, **Last 30 days**, **Last 12 months**.

The table changes to display only those log messages matching the selected time period.

4 To filter events by HTTP method type, select the desired method type from the second drop-down list from the left under the **Filter** field. It displays **All Method** by default. Other options are **HEAD**, **GET**, **POST**, **OPTIONS**, **PUT**, **DELETE**, **TRACE**, and **CONNECT**.

The table changes to display only those log messages matching the selected method type.

5 To filter events by status, select the desired action type from the third drop-down list from the left under the **Filter** field. It displays **All Status** by default. Other options are **Information(1xx), Success(2xx)**, **Redirect(3xx)**, **Bad Request(4xx)**, and **Server Error(5xx)**.

The table changes to display only those log messages matching the selected status.

6 To search the log for a specific string or value, type the alphanumeric search pattern into the blank field to the left of the **SEARCH** button, and then click **SEARCH**.

The table changes to display only those log messages that contain a match for the search text.

7 To reset the listing of log messages to their default sequence after filtering or searching the log, click the **RESET** button.

8 To change the number of log messages displayed per page, type the desired number into the **Items per page** field and press the **Enter** key. The default is 100.

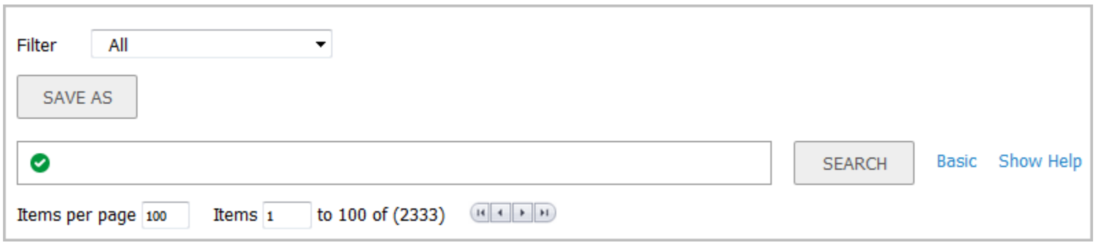
9 Use the arrow buttons to change the display to the first, previous, next, or last page of log messages.

Access Log Advanced Search

To perform an advanced search using queries on the Access Log screen:

1 Navigate to the **Access Log** screen of the **Log > View** page.

2 Click the **Advanced** link. The display changes, and the **Advanced** link changes to **Basic**, allowing you to display the basic search options again.


Filter All

Items per page 100 Items 1 to 100 of (2333)

3 Click the **Show Help** link to display details about using advanced search. The usage is summarized here:

- A query consists of a ***field***, an ***operator***, and a ***value***. All words are case-insensitive.
- In a simple query, valid operators are colon (**:**), greater than (**>**), and less than (**<**).
- In a complex query you can combine simple queries with the logical operators **AND**, **OR**, and parentheses for grouping ‘**()**’.

Query Examples

Query	Description
Status:403	Find all logs that contain “403” in their Status field. In this query, Status is the field, ‘:’ is the operator, and “403” is the value.
Time<2d or (Source:37. and Method:POST)	Find logs that are recorded within 2 days or that contain “37.” in their Source field and contain “POST” in their Method field.

- Supported fields include: **Time**, **Source**, **User**, **Text**, **Status**, **Referer**, **Agent**, **Received**, **Sent**, **Method**, **ServiceAddress**, **Host**, **URI**, **Scheme**, **Protocol**, **Args**, **ServerName**, **ServerAddress**, and **RequestTime**.

  Text means all characters in one log message on one line in the **Log > View** page.

4 When your query is ready, click the **SEARCH** button.

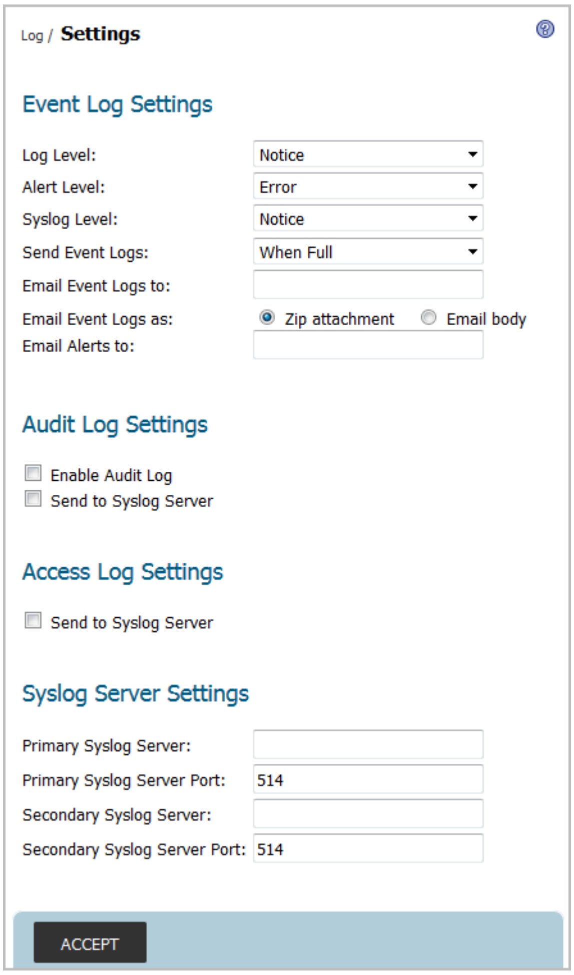
5 To save the filter, click the **SAVE AS** button. In the popup dialog, type in a descriptive name for the search filter and click **OK**. The saved filter is added to the **Filter** drop-down list under *Custom*.

Configuring Log Settings

The **Log > Settings** page provides options for the log, alert, and syslog levels, email settings, and settings for Audit Log, Access Log, and syslog servers.

Syslog is an industry-standard logging protocol that records system and networking activity. The syslog messages are sent in WELF (WebTrends Enhanced Log Format), so most standard firewalls and networking reporting products can accept and interpret the log files. The syslog service transmits syslog messages to external syslog server(s) listening on UDP port 514.

Log > Settings Page



Log / **Settings**

Event Log Settings

Log Level:	Notice
Alert Level:	Error
Syslog Level:	Notice
Send Event Logs:	When Full
Email Event Logs to:	
Email Event Logs as:	● Zip attachment ○ Email body
Email Alerts to:	

Audit Log Settings

☐ Enable Audit Log
☐ Send to Syslog Server

Access Log Settings

☐ Send to Syslog Server

Syslog Server Settings

Primary Syslog Server:	
Primary Syslog Server Port:	514
Secondary Syslog Server:	
Secondary Syslog Server Port:	514

Topics:

- Configuring Event Log Settings on page 197
- Configuring Audit Log Settings on page 198
- Configuring Access Log Settings on page 198
- Configuring Syslog Server Settings on page 199

Configuring Event Log Settings

To configure Event Log Settings options:

1 Navigate to the **Log > Settings** page.

2 In the **Event Log Settings** section, use the **Log Level**, **Alert Level**, and **Syslog Level** drop-down lists to select the severity level of log messages that are identified as log (event log), alert, or syslog messages.

Log levels are organized from most to least critical. If a level is selected for a specific logging service, then that log level and higher level events are logged. For example, if the ***Error*** level is selected for the **Log Level**, then all Emergency, Alert, Critical, and Error events are stored in the event log file.

3 Designate when log files are cleared and emailed to an administrator in the **Send Event Logs** field. If the option **When Full** is selected, the event log is emailed when it reaches the maximum file size of 200MB. The log file is then cleared.

If **Daily** is selected, select the hour at which to email the event log.

If **Weekly** is selected, select the day of the week and the hour.

If **Daily** or **Weekly** are chosen, the log file is still sent if the log file is full before the end of the period. In the **Log > View** page, you can click **CLEAR LOG** to delete the current event log. The event log is not emailed in this case.

4 To receive event log files through email, enter your full email address (username@domain.com) in the **Email Event Logs to** field. The event log file is emailed to the specified email address before the event log is cleared. If this field is left blank, log files are not emailed.

5 For **Email Event Logs as**, select **Zip attachment** to send the log as a zip file attached to the email, or select **Email body** to put the log content into the body of the email.

6 To receive alert messages through email, enter your full email address (username@domain.com) or an email pager address in the **Email Alerts to** field. An email is sent to the email address specified if an alert event occurs. If this field is left blank, alert messages are not emailed.

> ⓘ **NOTE:** Define the type of events that will generate alert messages on the **Log > Categories** page.

7 Click **ACCEPT** to save your changes.

Configuring Audit Log Settings

To configure Audit Log Settings options:

1 Navigate to the **Log > Settings** page.

2 In the **Audit Log Settings** section, select the **Enable Audit Log** check box to enable the logging of audit events.

3 Select the **Send to Syslog Server** check box to send the Audit Log contents to the configured syslog server when the log file size reaches 200MB.

4 Click **ACCEPT** to save your changes.

Configuring Access Log Settings

To configure Access Log Settings options:

1 Navigate to the **Log > Settings** page.

2 In the **Access Log Settings** section, select the **Send to Syslog Server** check box to send the Access Log contents to the configured syslog server when the log file size reaches 200MB.

3 Click **ACCEPT** to save your changes.

Configuring Syslog Server Settings

To configure Syslog Server Settings options:

1. Navigate to the **Log > Settings** page.
2. In the **Syslog Server Settings** section, enter the IP address or fully qualified domain name (FQDN) of your syslog server in the **Primary Syslog Server** field. Leave this field blank if you do not require syslog logging.
3. In the **Primary Syslog Server Port** field, accept the default port of 514 or enter a custom port number.
4. If you have a backup or second syslog server, enter the server's IP address or domain name in the **Secondary Syslog Server** field.
5. In the **Secondary Syslog Server Port** field, accept the default port of 514 or enter a custom port number.
6. Click **ACCEPT** to save your changes.

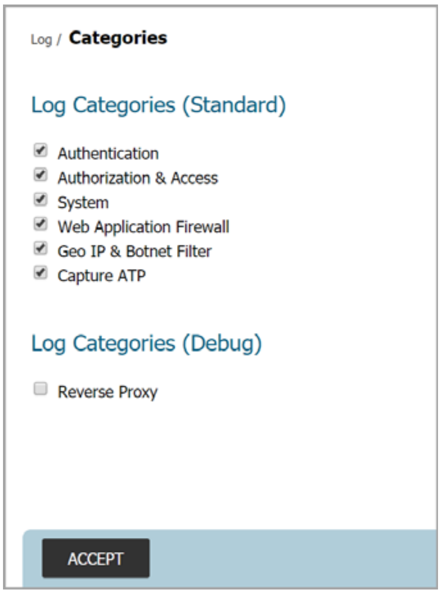
Configuring Log Categories

The **Log > Categories** page provides options to enable or disable logging for the following categories:

- Authentication
- Authorization & Access
- System
- Web Application Firewall
- Geo IP & Botnet Filter
- Reverse Proxy
- Capture ATP

Controlling the enabled categories can be particularly helpful when used to filter the log during the debug process.

Log > Categories Page



Log / **Categories**

Log Categories (Standard)

☑ Authentication
☑ Authorization & Access
☑ System
☑ Web Application Firewall
☑ Geo IP & Botnet Filter
☑ Capture ATP

Log Categories (Debug)

□ Reverse Proxy

To enable or disable the log categories:

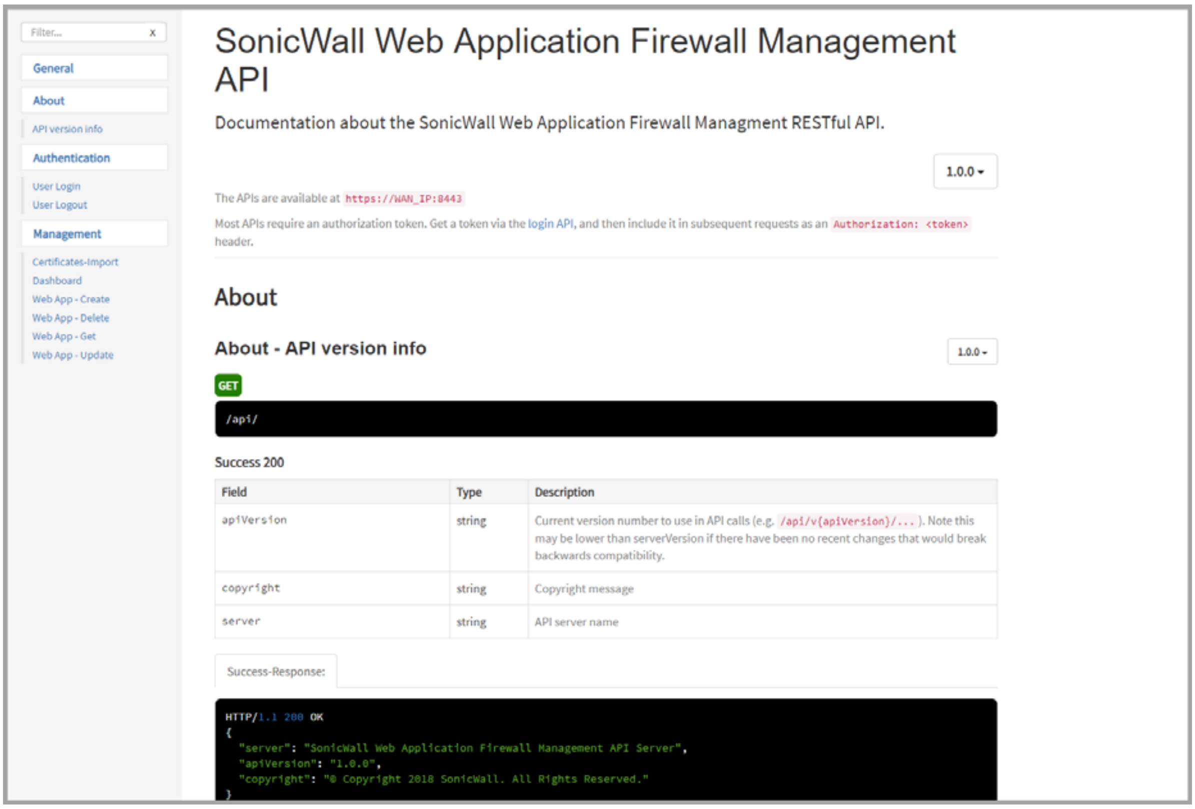
1. Navigate to the **Log > Categories** page.
2. For each of the following categories, select the check box to enable it or clear the check box to disable it:
    - **Authentication**
    - **Authorization & Access**
    - **System**
    - **Web Application Firewall**
    - **Geo IP & Botnet Filter**
    - **Capture ATP**
    - **Reverse Proxy**

      Reverse Proxy is generally only enabled for debugging purposes.
3. Click **ACCEPT** to save your changes.

12

Management API

This section provides information and configuration tasks specific to the SonicWall Web Application Firewall (WAF) Management API interface.



SonicWall Web Application Firewall Management API

Documentation about the SonicWall Web Application Firewall Managment RESTful API.

The APIs are available at `https://WAN_IP:8443`

Most APIs require an authorization token. Get a token via the login API, and then include it in subsequent requests as an `Authorization: <token>` header.

About

About - API version info

```
/api/
```

Success 200

Field	Type	Description
apiVersion	string	Current version number to use in API calls (e.g. `/api/v{apiVersion}/...`). Note this may be lower than serverVersion if there have been no recent changes that would break backwards compatibility.
copyright	string	Copyright message
server	string	API server name

Success-Response:

```
HTTP/1.1 200 OK
{
  "server": "SonicWall Web Application Firewall Management API Server",
  "apiVersion": "1.0.0",
  "copyright": "© Copyright 2018 SonicWall. All Rights Reserved."
}
```

The WAF Management RESTful API provides the following basic functionality options:

- Login – To get the API key
- Logout
- Get statistics – Includes traffic, threat, and web app statistics
- Create new Web App settings
- Update Web App settings
- Delete Web App settings

The API key is a security key used to authenticate with the API server. Administrators can use the Login API with admin credentials to get the API Key.

Refer to the *SonicWall Web Application Firewall Management API* document for details from your WAF web management interface. The *SonicWall Web Application Firewall Management API* document includes the following topics:

- **General** - This section provides a link to WAF Management APIs and login tokens.
- **About** - This section provides API Version information.
- **Authentication** - This section provides User Login and User Logout information.
- **Management** - This section provides information about importing certificates, the management dashboard, web app configurations.

Accessing the WAF Management API Documentation

You can access the WAF Management API documentation from the WAF Dashboard or from any web browser.

Topics:

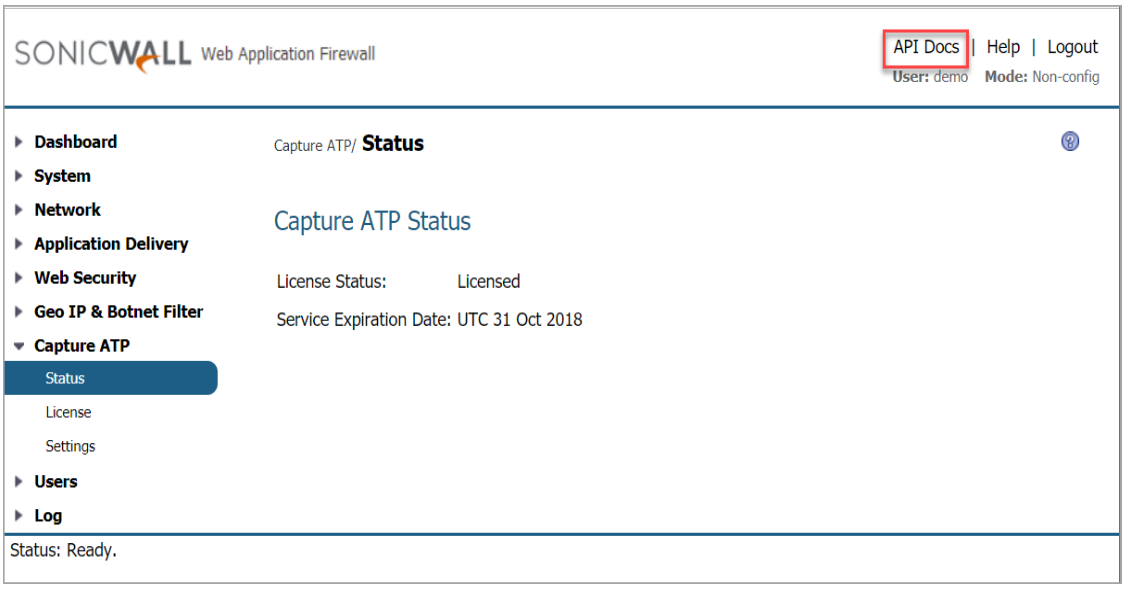
- Accessing the WAF Management API Document Using the Dashboard on page 202
- Accessing the WAF Management API Documentation Using a Web Browser on page 203

Accessing the WAF Management API Document Using the Dashboard

To Access the WAF Management API documentation from the Dashboard:

1 Enter your credentials to login to the WAF Dashboard.

2 Click the **API Docs** link at the top of the screen.



Capture ATP Status

License Status: Licensed

Service Expiration Date: UTC 31 Oct 2018

Status: Ready.

Accessing the WAF Management API Documentation Using a Web Browser

To Access the WAF Management API documentation from a web browser:

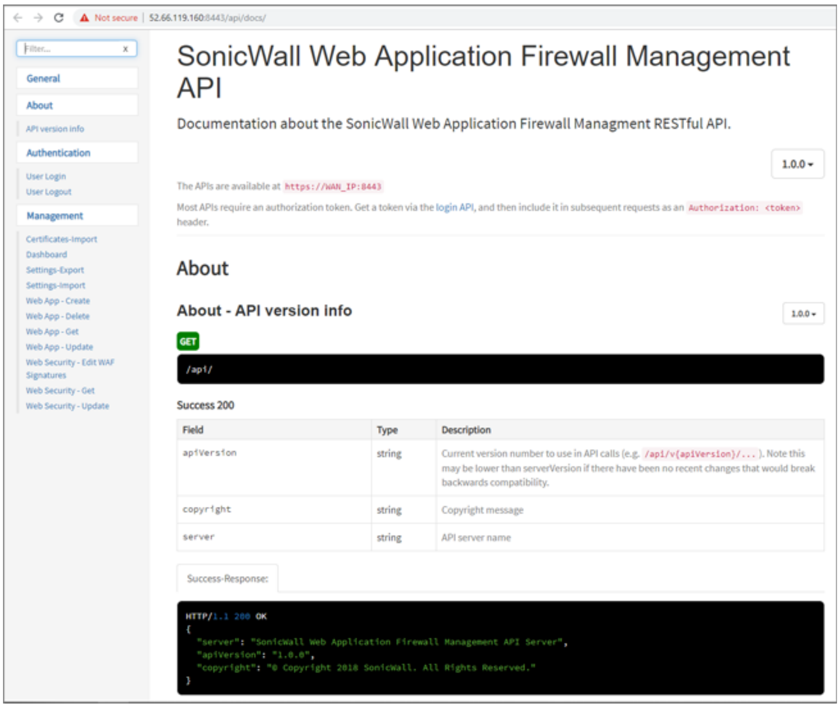
1. Launch a web browser and enter the URL for the WAF Management API:

   `https://<Your WAF IP>:8443/api/docs/`.

   For example, if your WAF IP address is https://wafdemo.eng.sonicwall.com, the WAF Management API address would be:

   `https://wafdemo.eng.sonicwall.com:8443/api/docs/.`

   An interface similar to the following appears when you access the API documents:



SonicWall Web Application Firewall Management API

Documentation about the SonicWall Web Application Firewall Managment RESTful API.

The APIs are available at `https://WAN_IP:8443`

Most APIs require an authorization token. Get a token via the login API, and then include it in subsequent requests as an `Authorization: <token>` header.

About

About - API version info

```
/api/
```

Success 200

Field	Type	Description
apiVersion	string	Current version number to use in API calls (e.g. `/api/v{apiVersion}/...`). Note this may be lower than serverVersion if there have been no recent changes that would break backwards compatibility.
copyright	string	Copyright message
server	string	API server name

```
HTTP/1.1 200 OK
{
  "server": "SonicWall Web Application Firewall Management API Server",
  "apiVersion": "1.0.0",
  "copyright": "© Copyright 2018 SonicWall. All Rights Reserved."
}
```

How to Use the Swagger Interface:

The RESTful APIs are a set of JSON objects that define their naming, order, and contents. By standardizing the API, each of its component can be displayed in a stylized, interactive framework. Within that framework, you can learn about a a specific API and try it.

1. Authenticate Yourself by navigating to `https://<Your WAF IP>:8443/api/docs/` where Your WAF IP needs to be replaced with the host IP address of your WAF configuration.
2. The operation POST/authenticate/user authenticates user access to WAF. This API call consumes the body parameters via the request header and produces the response via the response header.
3. Swagger responds with the cURL command and becomes your API script. It also provides the Request URL, Response Body, Response Code, and Response Headers for your requests as shown in the following example.
4. Use the WAF API HTTP protocol to define create, read, update, and delete resources.

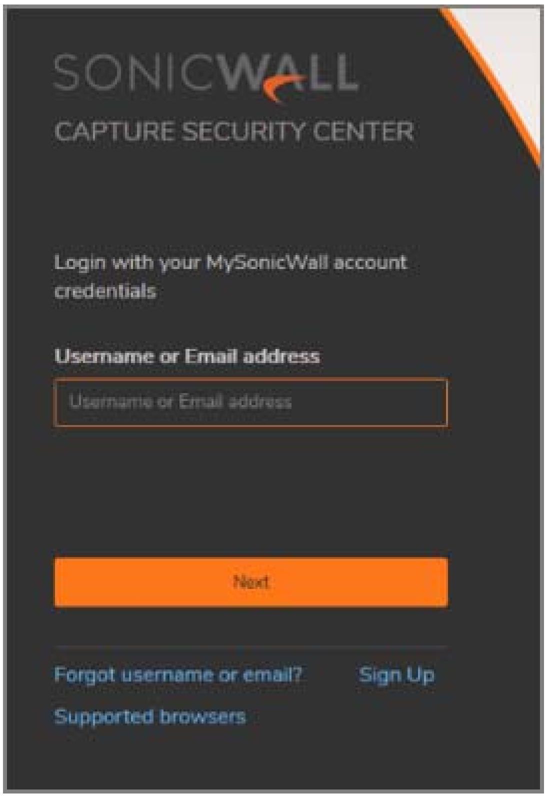
Supported HTTP request methods

HTTP method	Description
GET	Retrieves the specified resource or collection of resources. GET is a read-only operation that does not alter appliance state or configuration. A GET operation should not contain a request-body.
POST	Submits data to be processed by the specified resource or collection of resources. In most cases, WAF APIs uses the POST verb to create and add a resource to a collection of resources (for example, add a new MAC address-object to collection of objects).
PUT	Updates the specified resource. The data included in the PUT request-body replaces the previous configuration.
DELETE	Deletes the specified resource or collection of resources.

Getting Token to Make Calls to WASC API

How to make a WASC API call:

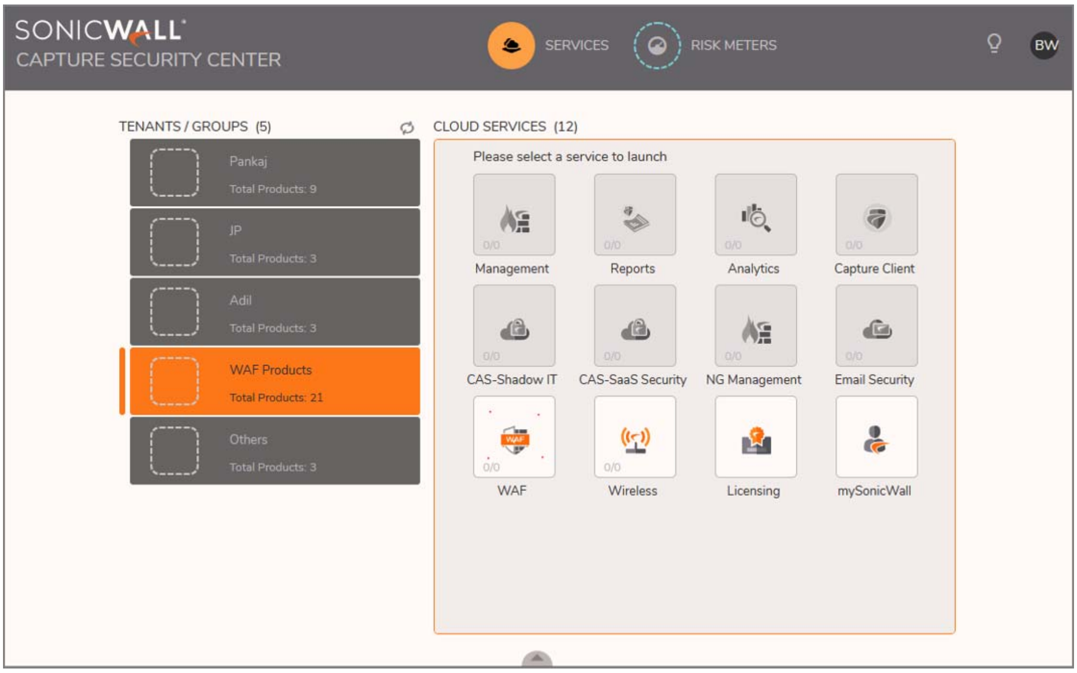
1 Open your browser and go to **CAPTURE SECURITY CENTER.**



SONICWALL
CAPTURE SECURITY CENTER
Login with your MySonicWall account credentials
Username or Email address
Username or Email address
Next
Forgot username or email?
Sign Up
Supported browsers

2 Log in to CSC.

3 Go to **SERVICES | TENANT/GROUPS > WAF Products**.



Pankaj
Total Products: 9

JP
Total Products: 3

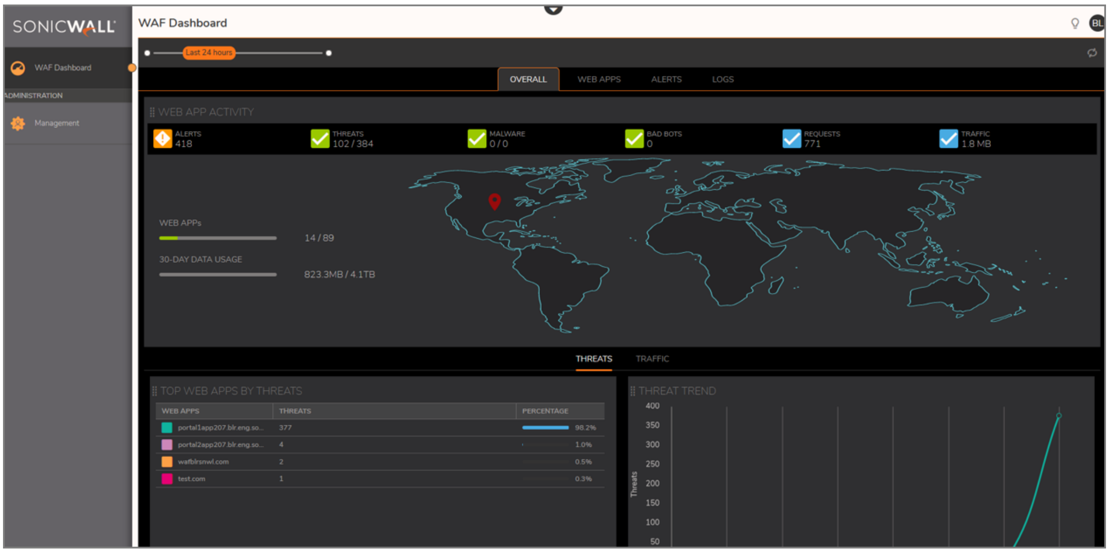
Adil
Total Products: 3

WAF Products
Total Products: 21

Others
Total Products: 3

The WASC Dashboard is displayed.

4 Open developer tools **(Shortcut Key F12)** and select the **Network** tab.



ALERTS 418
THREATS 102 / 384
MALWARE 0 / 0
BAD BOTS 0
REQUESTS 771
TRAFFIC 1.8 MB

WEB APPs 14 / 89
30-DAY DATA USAGE 823.3MB / 4.1TB

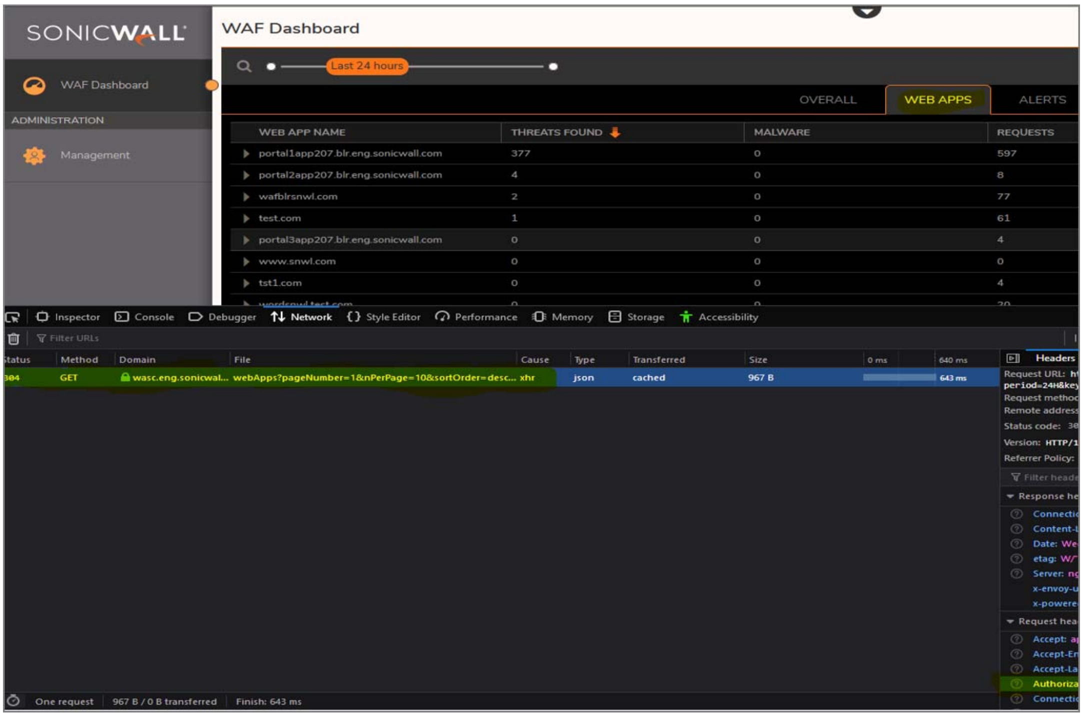
TOP WEB APPS BY THREATS

WEB APPS	THREATS	PERCENTAGE
portal1app207.blr.eng.so...	377	98.2%
portal2app207.blr.eng.so...	4	1.0%
wafblrsnwl.com	2	0.5%
test.com	1	0.3%

5 Navigate to the **WEB APPS** tab of the WASC Dashboard.

6 In the developer tools, select the latest **GET** request made to **WEB APPS** tab.

7 Under **Headers > Request headers**, look for the **Authorization** header.



WAF Dashboard

WEB APP NAME	THREATS FOUND	MALWARE	REQUESTS
portal1app207.blr.eng.sonicwall.com	377	0	597
portal2app207.blr.eng.sonicwall.com	4	0	8
wafblrsnwl.com	2	0	77
test.com	1	0	61
portal3app207.blr.eng.sonicwall.com	0	0	4
www.snwl.com	0	0	0
tst1.com	0	0	4
wordsnwl.test.com	0	0	20

Status	Method	Domain	File	Cause	Type	Transferred	Size	0 ms	640 ms
304	GET	wasc.eng.sonicwal...	webApps?pageNumber=1&nPerPage=10&sortOrder=desc...	xhr	json	cached	967 B		643 ms

Request URL: ht
period=24H&key
Request method
Remote address
Status code: 30
Version: HTTP/1
Referrer Policy:

One request | 967 B / 0 B transferred | Finish: 643 ms

8 Use the value of the **Authorization** request header value as the token for making API calls to WASC API.

13

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 WAF Administration Guide
Updated - August 2019
Software Version - 3.0
232-005047-00 RevA

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.

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