



Web Application Firewall

Getting Started Guide

April 11, 2019

Copyright 2014-2019 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

Why Use a Web Application Firewall	4
The Qualys Advantage	5
Get Started	6
Create WAF Cluster	7
Explore Security Policies	10
Create application profiles	12
Web Server Pool Profile	12
Healthcheck Profile	13
SSL Certificate Profile	14
Custom Response Pages	15
HTTP Profile	16
Define Your Web Application	18
Configure WAF Appliance	21
Configure Your Web Environment	23
We're Now Monitoring Your Web Application!	24
Add Exceptions	25
Add Virtual Patches	27
Add Custom Rules	29
Upgrading WAF clusters	32
Schedule appliance auto-update	33
Upgrading specific WAF appliances	34
Contact Support	35

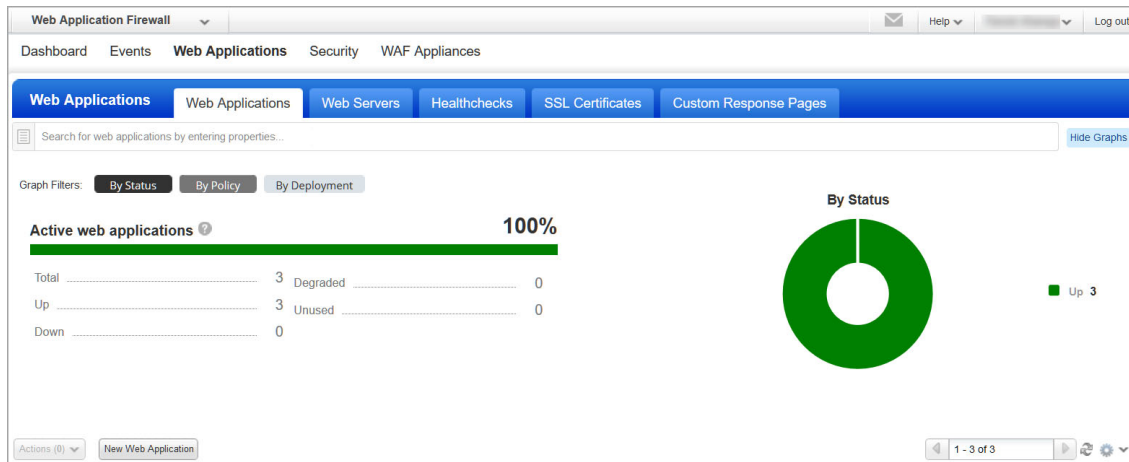
Why Use a Web Application Firewall

HTTP(S) is the foundation of data communication for the World Wide Web, and functions as a request-response protocol for communications. Mobile apps, cloud computing, API communications, Intranet applications and webmail are common tools we use every day. These applications are all communicating over HTTP(S).

Qualys provides applications that allow you to scan and identify vulnerabilities - Qualys Vulnerability Management (VM) and Qualys Web Application Scanning (WAS).

Experience shows that patching web site source code can take longer than expected, depending on the affected component, development resources, and how agile the company is in applying and validating software updates.

That's where Qualys Web Application Firewall (WAF) comes in. This is an immediate remediation tool that is able to protect your web applications against attacks and gives your development team time to fix important security issues.



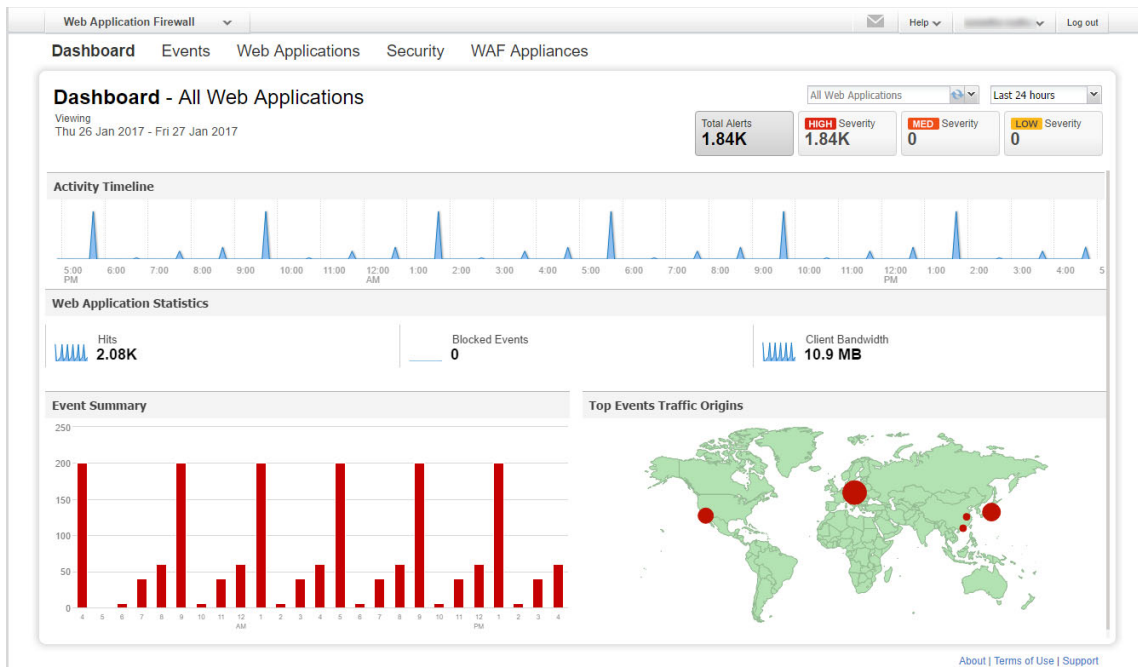
Using WAF users can deploy multiple firewall instances for their web applications. Each firewall consists of a virtual appliance that is configured to reverse proxy your HTTP(S) traffic. This appliance will be located in your virtualization platform (Amazon EC2, Microsoft Azure, Google Cloud, VMware or Hyper-V) on a server or docker (container), and will be instantiated from a Qualys image. We'll walk you through the steps in this user guide.

The Qualys Advantage

Qualys offers a powerful, next generation web application firewall that uses an always up to date security ruleset to secure your web applications. This modern firewall uses a cloud-based approach and provides a classic mode of operation and deployment.

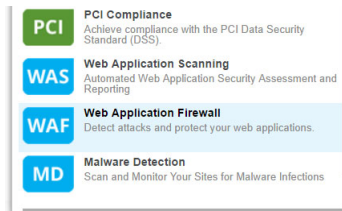
All security events are routed through the Qualys Cloud Platform. They are continuously monitored and analyzed by our security researchers in order to compute the best ruleset for blocking the latest attacks and zero-day vulnerabilities. Qualys WAF users set up security policies for their web applications based on rules to filter, monitor, block and report on events.

Qualys WAF makes it easy to understand the security of all your web applications at once. A concise visual dashboard summarizes the various events that have occurred, when they took place and where they came from. Easily get interactive insights into potential threats and find detailed information on each potential threat and how to address it.



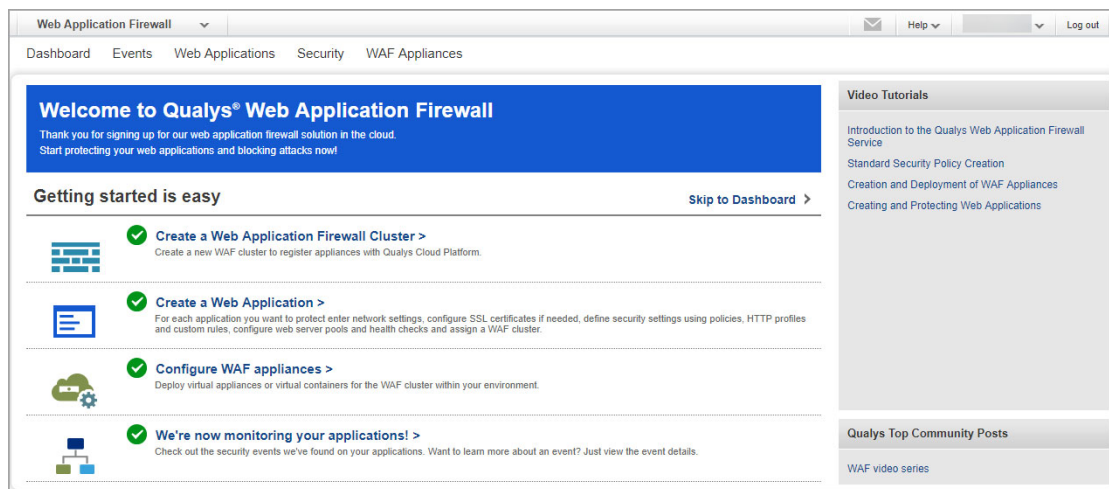
Get Started

Start protecting your web applications and blocking attacks now! We'll help you do this quickly.

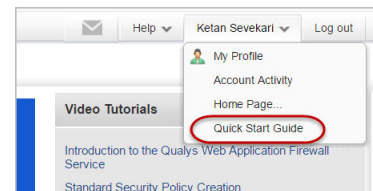


Log in to your Qualys account and choose WAF

You'll see our Quick Start Guide the first time you log in - just follow the steps to get started. You'll find tutorials and links to other helpful information.



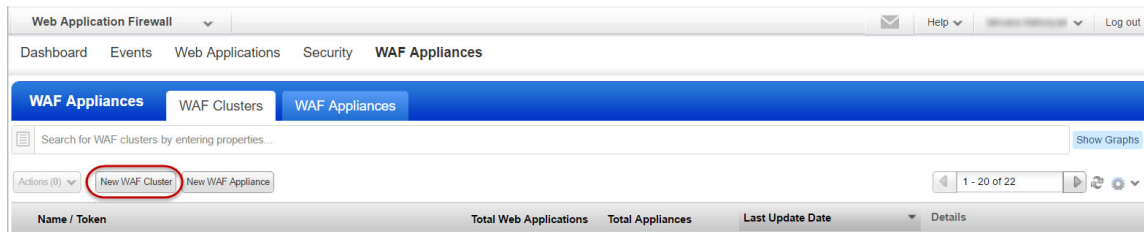
Tip Get back to the Quick Start Guide anytime - it's on the user name menu.



Create WAF Cluster

A WAF cluster is the pivot between the web application and the appliance it is being proxied through. It is a group of one or more WAF appliances (or proxy-set). A WAF Cluster can contain several appliances, but each will act as standalone, while processing the traffic exactly the same way across all the appliances that are registered with the named Cluster. A Web Application can be proxied over several clusters.

It's easy to create a WAF Cluster. Go to WAF Appliances > WAF Clusters and click the New WAF Cluster button.



Enter an arbitrary name. To help with cluster management you can add description and assign tags.

WAF Cluster Creation

Turn help tips. On | Off Launch help

Step 1 of 4

1 Cluster Details

2 Configuration

3 Automatic Updates

4 Review And Confirm

Configure basic information about your WAF cluster

A cluster might regroup several appliances. Several web applications might be linked to the same cluster. (*) REQUIRED FIELDS

Basic Information

Name*

My WAF Cluster

Description

2048 characters maximum.

Tags

Select tags to apply to the cluster

Region A

Select

Create

Remove All

7

For error responses you can choose to show the default WAF error page (404), or define a custom response or a redirection code (301 or 302) along with a location. Selecting Block will display the default WAF error page.

WAF Cluster Creation Turn help tips: On | Off Launch help

Step 2 of 4

- 1 Cluster Details ✓
- 2 Configuration ✓
- 3 Automatic Updates
- 4 Review And Confirm

Cluster Configuration

Error response (*) REQUIRED FIELDS

Whenever a request can't be routed to your origin server (a URL that is not configured) WAF returns an error page. By default an error page for HTTP status code 404 is returned. You can configure the error page to instead be a redirect to another URL for HTTP status code 301 or 302, or you can display a custom page.

Action* **Block**

X-Forwarded-For Trusted Proxies

Provide IP addresses of trusted proxies.

Trusted IPs

IP: Range: **Range** **Add**

1.2.3.5/23 **Remove**

1.2.3.5 **Remove**

Whenever a request is addressed to a nonexistent FQDN, you can choose to display the default WAF error page, a custom response page or you can redirect the request towards a specified location. This happens if a malicious user forges a request with a false host header or the host requested is missing in the alias configured for your web site.

You can provide the IP address/range/network of trusted origin proxies or load balancers configured in full-proxy mode. If the request is not from a trusted source the X-Forwarded-For header values are automatically discarded. If you do not provide IP addresses for trusted origin proxies or load balancers, then IP addresses as per RFC1918 are trusted.

You can schedule automatic updates for appliances registered to this cluster. See [Schedule appliance auto-update](#).

Once your cluster is created it shows up on the UI under the WAF Appliances > WAF Clusters tab. To view information about various cluster statuses and their meanings, click Help > Online Help and then on the Manage WAF clusters page, click **Tell me about cluster status**. The status  means the cluster does not have any WAF appliances assigned to it yet (we'll do this soon).

Web Application Firewall Help Log out

Dashboard Events Web Applications Security **WAF Appliances**

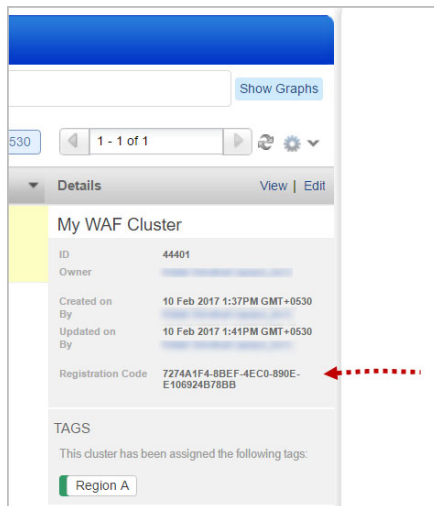
WAF Appliances WAF Clusters WAF Appliances

Search for WAF clusters by entering properties... **Show Graphs**

Actions (1) New WAF Cluster New WAF Appliance

Last synchronization date: 10 Feb 2017 1:43PM GMT+0530 1 - 1 of 1

Name / Token	Total Web Applications	Total Appliances	Last Update Date	Details
 My WAF Cluster Region A	0	0	10 Feb 2017 by Admin	My WAF Cluster ID: 44401 Owner: Admin Created on: 10 Feb 2017 1:37PM GMT+0530 By: Admin Updated on: 10 Feb 2017 1:41PM GMT+0530 By: Admin Registration Code: 7274A1F4-BBEF-4EC0-B90E-E10B34B78DB



Notice the Registration Code. You'll use this to register your WAF cluster when you configure a WAF appliance.

Explore Security Policies

The security policy you assign to your web application determines the WAF inspection criteria and sensitivity level - this impacts what violation we'll report for your web application and whether or not we'll flag the traffic as malicious.

Good to know

Only one security policy can be assigned to each web application.

Choose from out-of-the box policy templates provided by Qualys with this release - Drupal, Joomla!, Wordpress, and OWA. Built-in Templates and System Policies are not modifiable.

☐ • Drupal	Template
☐ • Wordpress	Template
☐ • Joomla!	Template

Or start with a blank policy and customize the policy settings. You can create multiple policies and assign them to your various web applications (one to each web app).

Go to Security > Policies and click the New Policy button.

The screenshot shows the WAF interface with the 'Security' tab selected and the 'Policies' sub-tab active. A search bar is present at the top. Below it, an 'Actions (0)' dropdown menu is visible, with 'New Policy' highlighted by a red circle. A table lists the existing policies:

Name	Type	Last Update Date	Details
Custom security policy	Custom	13 Sep 2016 by Varvara Matosyan (mscu_vm)	Please select a record.
SUB SEC POLICY	Custom	27 Aug 2016 by balaji Gopal (mscu_bg)	

Our wizard will help you with the settings.

Application Security -

Configure a sensitivity rating (20 to 80) for the various detection categories. This impacts what inspection will be performed by filtering potentially noisy events.

Policy Controls - Set threat level thresholds (1 to 100) for logging and blocking. This impacts what events we will log and block.

Security Policy Creation Turn help tips: On | Off Launch help

Step 3 of 3

1 Policy Details ✓
2 Application Security ✓
3 Policy Controls ✓

Configure policy controls for your security policy

Threat Levels (*) REQUIRED FIELD

Set threat level thresholds (1 to 100) for logging and blocking. This impacts what events we will log and block. You must set the blocking level greater than or equal to the logging level so blocked events will always be logged. Still have questions? The threat level and severity values seen in events may guide you in tuning these values.

Thresholds

1 50 100

Logging: 25 Blocking: 75

Cancel Previous Finish

Create application profiles

Qualys WAF now allows you to create reusable profiles for settings which can be commonly used by multiple web applications. Reusable profiles can be created for Web server pools, healthcheck parameters, SSL certificates, and HTTP protocol filters.

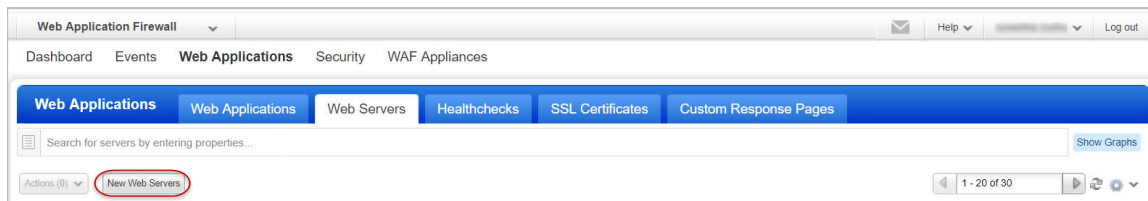
Good to know

For each web application in your account you'll assign 1 profile of each type, i.e. Web server pool, healthcheck, SSL certificate, and HTTP protocol filters.

Web Server Pool Profile

Don't have a dedicated load balancer? No worries, with newly introduced web server pools, Qualys WAF can now load balance traffic between multiple origin servers. Alternatively, if your web application resides on a docker (container), enable Docker platform to provide docker information. You can choose one web server pool per web application.

Go to Web Applications > Web Servers and click the New Web Servers button.



For docker support, specify the docker image ID. This will create a pool of all containers spawned from the docker image.

For Web servers, add one or more servers in the pool, having common port and protocol.

Step 2 of 3

1 Web Servers Details ✓
2 Configuration ✓
3 Review And Confirm

Web Servers configuration

Port* 443
Protocol HTTPS ON
Docker platform OFF

All servers must have a common port and a common protocol

Web Servers

Fill with your web servers' addresses and their weight

https:// Type address + Enter 1 Remove All
https://www.server1 (1) Remove
https://www.server2 (2) Remove
https://www.server3 (3) Remove

Load-balancing roundrobin

You can use weights for WAF to distribute the request load to various servers in the Web Server Pool. Simply add the weight (number) beside the server address. You can add weights to your existing pool as well. Default is 1. Maximum allowed value is 256.

Consider a pool consisting of four origin servers with the weights 1, 2, 3 and 3. The total weights assigned to all servers is 9. WAF distributes 1/9th of total load to sever 1, then 2/9th of total load to server 2, and so on.

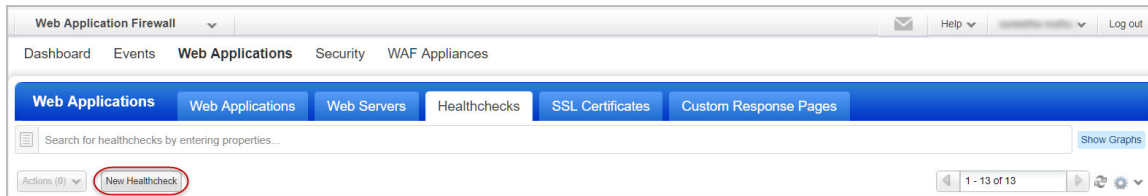
Then choose the load balancing method to determine which server receives the connection.

Healthcheck Profile

Create healthcheck profiles to monitor application's availability against your web servers (containers). You'll choose one healthcheck profile per Web Application. It will be executed against all the web servers listed in the server pool, or against all containers spawned from the docker image ID, according to a user-defined frequency. If one backend web server (container) fails the healthcheck after X attempts, it will be considered down and no request will be steered to it until the service is back. Meanwhile, the firewall will keep probing the backend.

Consequently, if all backend web servers (containers) fail the healthcheck, they will all be considered as down by the firewall, thus leading to application unavailability – meaning the WAF will stop forwarding the traffic on server-side. Instead, it will respond to the client with a user-defined HTTP response code. This “failure response code” is set within the Web Application itself, in the Application tab.

Go to Web Applications > Healthchecks and click the New Healthcheck button.



While creating a healthcheck profile, specify the preferred HTTP method to query the application, the URL path to be checked, and the response code returned for success. You can also specify the “up” and “down” intervals and occurrences to fix the frequency of the

probes, along with the amount of successes or failures before changing backend web server's status. Based on the healthcheck result, the server status is set to active or inactive.

Healthcheck Creation Turn help tips: On | Off Launch help ✕

Step 2 of 3

- 1 Healthcheck Details ✓
- 2 **Configuration** ✓
- 3 Review And Confirm

Healthcheck configuration

Transaction Details (*) REQUIRED FIELDS

Define the monitoring attributes for checking backend availability, i.e. the details of a periodic request meant to test the application on server-side : HTTP method, full path, and the successful response code that is expected in order to keep forwarding the traffic towards pool members.

Method*

Path

Expected response code*

Intervals and occurrences

Define the various metrics the healthcheck should follow on execution. For instance, set the interval of execution when the application is up (in seconds), the amount of failures before going down, or interval when the application is down (in seconds), and the amount of successes before going up.

Interval when up* Number of checks before down*

Interval when down* Number of checks before up*

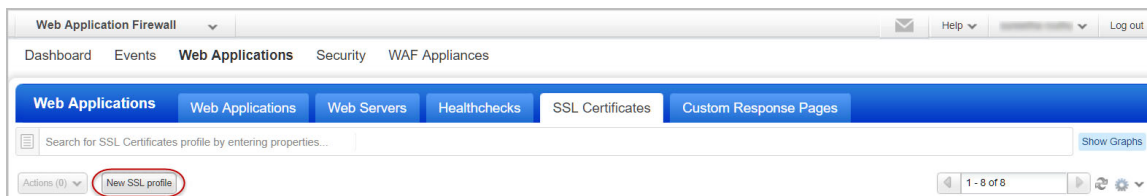
Healthcheck is performed on this path

The WAF appliances tab displays the healthcheck status for all servers covered by an appliance. This server healthcheck information is grouped by each web application that the appliance monitors.

SSL Certificate Profile

Declare SSL materials used by your web applications on client-side.

Go to Web Applications > SSL Certificates and click the New SSL Profile button.



Provide a PFX (PKCS12) or a PEM file, or simply copy-paste the contents of the PEM certificate, private key, and passphrase directly into the UI.

SSL Certificates Profile Creation Turn help tips: On | Off Launch help X

Step 2 of 4

- 1 Basic Information ✓
- 2 **Certificate**
- 3 CA Certificate
- 4 Review And Confirm

Certificate and Private Key (*) REQUIRED FIELDS

Please import your certificate and private key.

Desired Method*

- Upload a PFX file
- Upload a PFX file
- Upload PEM files
- Copy/Paste PEM content

Please upload your PFX file.

Choose File No PFX file has been uploaded

Drop file here

WAF SSL Passphrase

The private key will be encrypted with the newly generated WAF SSL Passphrase. Copy-paste the 64 byte passphrase to your appliance “waf_ssl_passphrase” environment variable.

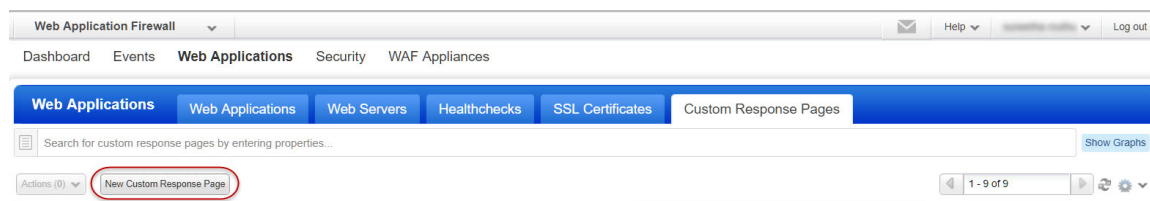
In the CA Certificate section, provide chained / intermediate certificate in PEM format.

See CLI Reference in [Virtual Firewall Appliance User Guide](#) for details.

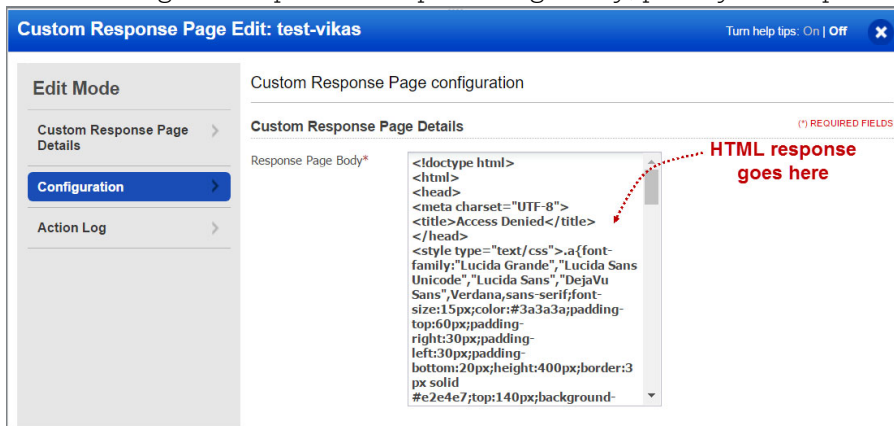
Custom Response Pages

Display a custom page instead of the default WAF error page, if your security policy blocks a particular section or a page on your web site or if a request cannot be routed to your origin server.

Go to Web Applications > Custom Response Pages and click the New Custom Response Page button.



In the Configuration panel's Response Page Body, paste your response in HTML format.

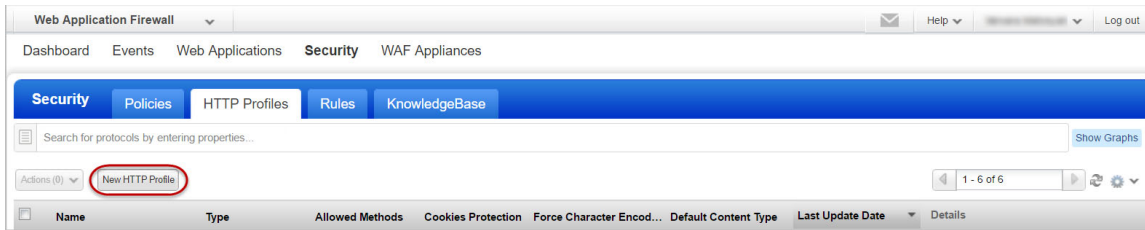


This custom response can now be reused for multiple web applications and appliance clusters. Simply select your custom response page in the web application wizard, and the WAF cluster wizard.

HTTP Profile

Set up an HTTP profile to filter protocol oriented attributes (methods, content-type, declarative security, and information leakage attributes). You can choose one HTTP profile per web application.

Go to Security > HTTP Profiles and click the New HTTP Profile button.



HTTP Protocol - Configure HTTP protocol analysis for the policy.

Web Services Protection
Enable XML/JSON parsing in HTTP profiles to validate that transmitted payload is XML/JSON compliant.

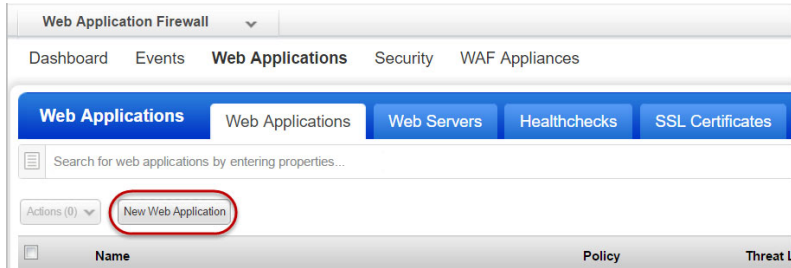
Information Leakage -
Choose options for server cloaking, sensitive header suppression.

Declarative Security -
Configure responses to cookies, content-type sniffing and browser cross-site scripting.

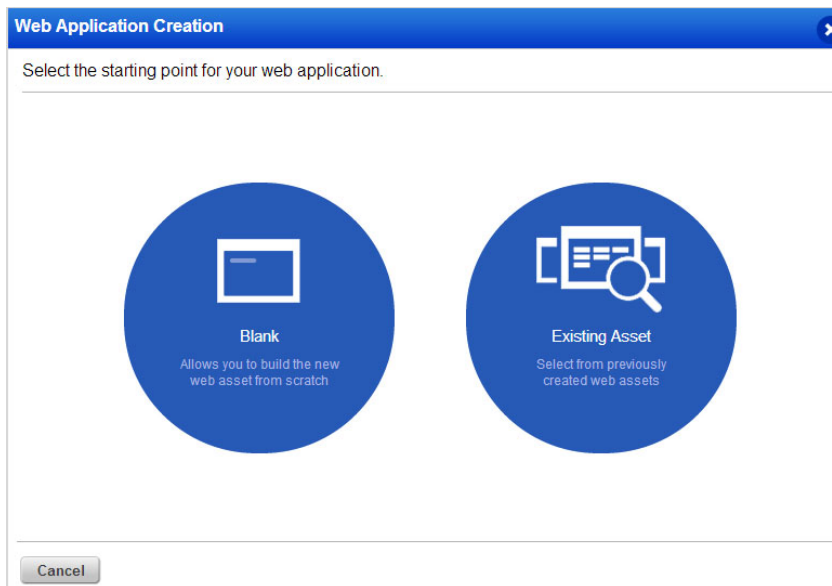
The screenshot shows the 'Profile Creation' wizard, specifically 'Step 2 of 6'. The left sidebar shows a progress list: 1 Profile Details (checked), 2 HTTP Protocol (active), 3 Web Services (checked), 4 Information Leakage (checked), 5 Declarative Security (checked), and 6 Review And Confirm. The main content area is titled 'Configure HTTP Protocol analysis for your HTTP profile'. It has three sections: 'Request Method' with options 'Allow All, Detect Violations' (selected) and 'Detect Invalid Methods', 'Detect TRACE, TRACK', and 'Deny All, But Explicitly Allow' (with a text input 'GET, POST'); 'Request Headers' with options 'Detect Invalid Headers', 'Detect Repeated Headers', and 'Detect Chunked Encoding'; and 'Request Content-Type'. At the bottom, there are 'Cancel' and 'Previous' buttons.

Define Your Web Application

Tell us about the web application you want to monitor.



Go to Web Applications and click the New Web Application button.



Choose Blank and we'll help you build the web asset from scratch.

Tip Is the web asset already in your subscription? Use Existing Asset to save time! (You'll just enter WAF settings.)

1) Asset Details Give your web asset a name, tell us the primary URL, add custom attributes if any, and assign tags (optional)

Tip Turn on help tips (in the title bar) and we'll show you useful tips as you hover over the various

2) Application Set secondary URLs, and then select the reusable profiles created for Web Server pool and SSL Certificate. You can create new profiles directly from this wizard.

Tip Optionally select a Healthcheck profile and set the failure response code.

Select the SSL profile, appropriate protocols, security levels, and ciphers. An SSL profile contains details about the required security certificate. List of available ciphers depends on the selected protocols and security levels. Default security filters are Strong, Good and default protocols are TLS1.1 and TLS1.2. Ciphers are used in the order in which they are displayed.

3) Security Select an action, and then select or create security policy and HTTP profiles. Selecting Block with Custom Response allows you to display a custom message to the user if your security policy blocks a particular section or a page on your web site. Select a custom response page that you have created.

Then add one or more custom rules to allow or block access to certain web application resources.

The screenshot shows the 'Web Application Creation' interface at Step 3 of 6, titled 'Configure policies for your web application'. On the left, a sidebar lists the steps: 1 Asset Details, 2 Application, 3 Security (current), 4 WAF Clusters, 5 Comments, and 6 Review And Confirm. The main area is divided into sections: 'Security Policy' (marked as a required field), 'Custom Rules', and 'HTTP Profile'. Under 'Security Policy', there's a dropdown for 'Action' set to 'Block with Custom Response', a dropdown for 'Custom Response Page' set to 'customPageOne', a dropdown for 'Policy' set to 'Standard Policy', and a dropdown for 'HTTP Profile' set to 'Standard Protocol'. Each dropdown has 'Edit' and 'Create' links. Below these is the 'Custom Rules' section, which includes a search bar and 'Add All' and 'Remove All' buttons. At the bottom, it states 'No custom rules selected'.

4) WAF clusters Select a cluster to deploy your web app in. A cluster contains one or more appliances (reverse-proxies).

It's possible for multiple WAF clusters to monitor the same web application.

The screenshot shows the 'Web Application Creation' interface at Step 4 of 5, titled 'Configure WAF clusters for your web application'. The sidebar on the left shows steps 1 through 6, with 'WAF Clusters' (Step 4) highlighted. The main area is titled 'Selected WAF Clusters' (marked as a required field) and includes a prompt: 'Please select WAF clusters to which your web application will be deployed'. Below this, there are two radio button options: 'My WAF Cluster' (selected) and 'Cluster'.

Once your web application is created it shows up on the UI under the Web Applications tab. To view information about various web application statuses and their meanings, click **Help > Online Help** and then on the Start monitoring your web applications page, click **Tell me about status**.

Configure WAF Appliance

You'll add a WAF virtual appliance and configure it for your WAF cluster within your environment (Amazon EC2, Microsoft Azure, Google Cloud, VMware or Microsoft Hyper-V) on a server or docker (container).

Good to know

A WAF cluster can be assigned as many WAF appliances as your subscription allows guaranteeing high availability and/or fault tolerance in your firewalling operations.

Tell me the steps

1) Add a new WAF Appliance for your WAF cluster. Just go to WAF Appliances > WAF Appliances, click New WAF Appliance, and we'll walk you through the steps.



2) Configure the WAF appliance for your environment. See our step by step instructions for VMware, Hyper-V, Amazon EC2, Microsoft Azure, Google Cloud in [Virtual Firewall Appliance User Guide](#), and Docker in [Virtual Firewall Container User Guide](#).

Once your appliance is registered it shows up on the UI under the WAF Appliances tab. To view information about various appliance statuses and their meanings, click Help > Online Help and then on the Manage WAF appliances page, click **Tell me about appliance status**.

Firewall rules / EC2 security groups

- Allow HTTP(S) traffic (TCP-80,443; or any other) to the WAF appliance from Internet.
- Allow SSH (TCP-22) to the WAF appliance from a trusted management network only.
- Allow minimum access to the origin web server(s): only the WAF appliance ip address should be granted access to web servers' production [ip:port]. Any direct access should be strictly limited to the administration network only.

Load balancer considerations

- Load balancers should be configured to hand off to WAF cluster nodes so we can appropriately configure redundancy within the infrastructure.
- The WAF appliance functions as a reverse proxy. It is important that any DNS configurations, firewall NAT or load balancer configurations are set to forward traffic towards the WAF appliance. It will then inspect incoming request, and based on your configuration, hand it off to the appropriate origin server.

Upgrading WAF appliances

We regularly release scanner appliance software to bring you our latest features and improvements. When software updates are available use the cluster Upgrade option to upgrade all Scanner Appliances registered to that cluster. You can now choose to auto-update the appliances registered with a cluster. See [Upgrading WAF clusters](#).

Configure Your Web Environment

Be sure to get traffic to your WAF appliance - configure load balancers and/or DNS as needed to direct traffic to your WAF cluster for inspection.

We recommend you check to be sure your WAF cluster has an active status. Go to WAF Appliances > WAF Clusters.

- Status ☐ means the cluster does not have any WAF appliances assigned to it.
- Status ☒ means the cluster has appliances registered, none are inactive, and the cluster protects at least one site.

Sample WAF Clusters list

Web Application Firewall

Help

Dashboard

Events

Web Applications

Security

WAF Appliances

WAF Appliances

WAF Clusters

WAF Appliances

Search for WAF clusters by entering properties...

Sh

Actions (1)

New WAF Cluster

New WAF Appliance

Last synchronization date: 27 Jan 2017 1:36PM GMT-0800

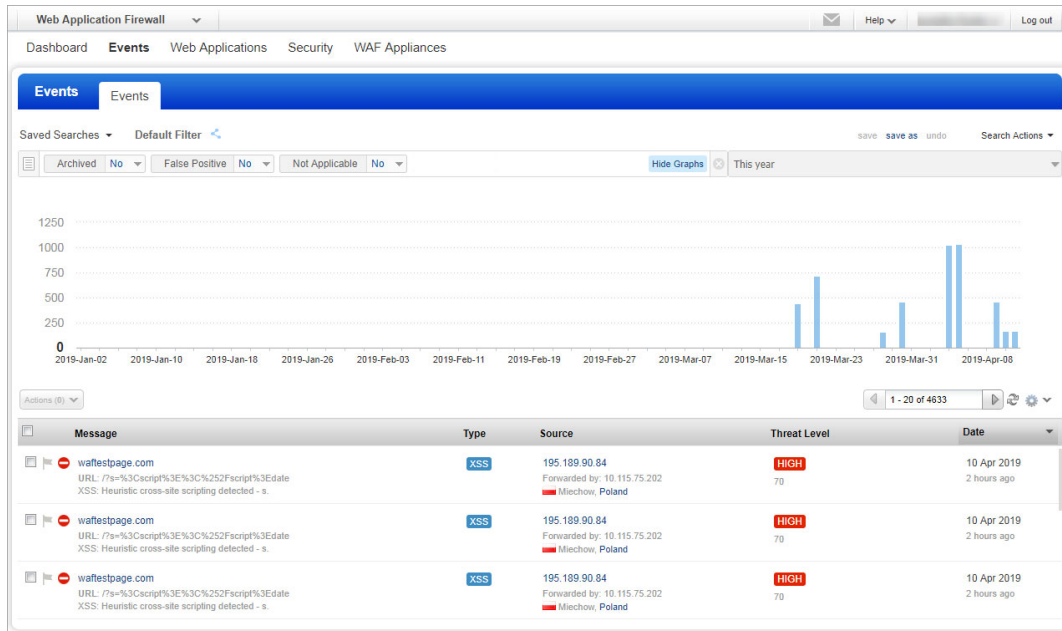
1 - 19 of 19

Name / Token	Total Web Applications	Total Appliances	Last Update Date	Details
☒ qwaf15.p04 ...	2	2	13 Jan 2017 by suncoastfirewall (qwaf15)	qwaf15.p04 ID 34402 Owner suncoastfirewall Created on 13 Jan 2017 8:03PM By suncoastfirewall Updated on 13 Jan 2017 8:03PM By suncoastfirewall Registration Token FCC10P04-7070-00XXXXXXXXXXXX

☒ qwaf13.p04 ...	1	1	13 Jan 2017 by suncoastfirewall (qwaf13)	
☐ WAFForm ...	—	—	11 Jan 2017 by System	
☒ qllog7.p04 ...	1	1	03 Jan 2017 by suncoastfirewall (qwaf13)	TAGS This cluster has not been assigned any tags
☐ qwaf7.p04 ...	—	—	07 Dec 2016 by suncoastfirewall (qwaf13)	APPLIANCES

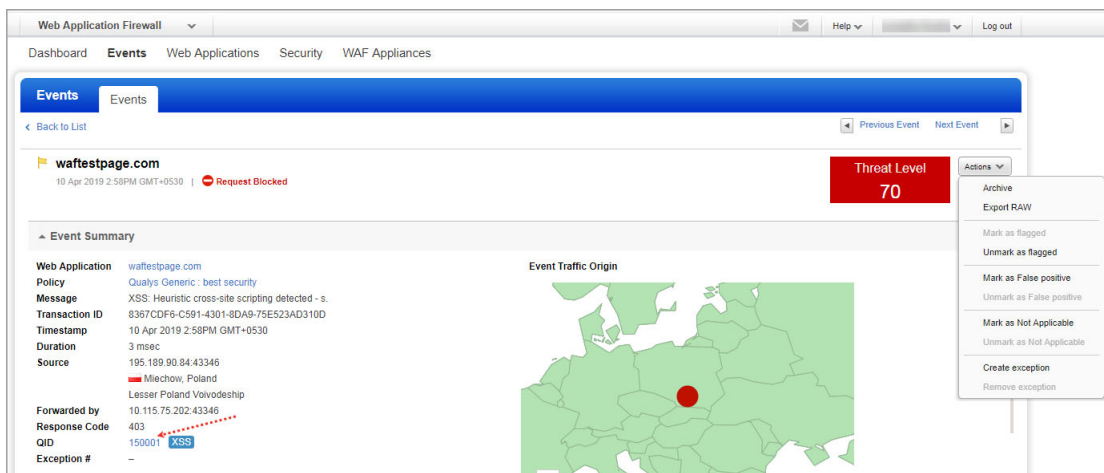
We're Now Monitoring Your Web Application!

Check out the security events (violations) we've found on your web application. To discover more about an event, double-click the event or click View in the Quick Actions.



You can view detailed information about each potential threat. Review the event details and take actions from the menu, i.e. mark the event as Flagged, False Positive, or Not Applicable.

Tip - Clicking on a QID will take you to Qualys comprehensive KnowledgeBase which provides additional information about each threat and how to address it.



Add Exceptions

Use Exceptions when you identify a false-positive or false-negative event. A false-positive is a legitimate request that has been unexpectedly blocked. A false-negative is a non-legitimate request that has been authorized while it shouldn't have.

With Qualys WAF you can flag an event as a false-positive. To do that, go to Events > Event List, select an event, click on the arrow and select “Mark as False positive”. Bear in mind this is a simple marker, it does not impact traffic processing behavior.

To create an exception, select an event, click on the arrow and select “Create exception” or select this option from the Actions menu when viewing an event.

Message	Type	Source	Threat Level	Date
waf-site6.eng.sjc01.qualys.com URL: / Web Service parsing error. Invalid char read in XML footer	Quick Actions View Archive Mark as flagged Unmark as flagged Mark as False positive Unmark as False positive Mark as Not Applicable Unmark as Not Applicable Create exception Remove exception	10.44.65.195	HIGH 100	02 Mar 2018 4:32AM GMT+0530
waf-site6.eng.sjc01.qualys.com URL: / SQLi: Condition escaping detected.			MED 60	02 Mar 2018 4:31AM GMT+0530
waf-site6.eng.sjc01.qualys.com URL: / SQLi: Condition escaping detected.			MED 60	02 Mar 2018 4:31AM GMT+0530
waf-site6.eng.sjc01.qualys.com URL: /?abdcfe={"deptno":{"site&q... XSS: Heuristic cross-site scripting detected - abdcfe.			HIGH 70	02 Mar 2018 3:51AM GMT+0530
waf-site6.eng.sjc01.qualys.com URL: /?abdcfe={"deptno":{"site&q... XSS: Heuristic cross-site scripting detected - abdcfe.			HIGH 70	02 Mar 2018 3:46AM GMT+0530
waf-site6.eng.sjc01.qualys.com URL: /?abdcfe={"deptno":{"site&q... XSS: Heuristic cross-site scripting detected - abdcfe.	XSS	10.44.65.195	HIGH 70	02 Mar 2018 3:46AM GMT+0530

Exceptions are created in the form of custom rules.

Rule Creation: Exception - Event 27A02C41-15F6-4056-9866-E75BE...

Turn help tips: On | Off Launch help

Step 1 of 4

1 Rule Details

2 Conditions

3 Actions

4 Review And Confirm

Configure basic information about your WAF rule

Several web applications might be linked to the same rule. (*) REQUIRED FIELD

Basic Information

Name*

Exception - Event 27A02C41-15F6-4056-9866-E75BE833716A

Description

2048 characters maximum.

Tags

Select tags to apply to the rule Select | Create | Remove All

(no tags selected)

Rule details and conditions for the custom rule are auto populated based on the event. By default, the action for an exception is Allow or Block (the opposite of the original event's action).

Rule Creation: Exception - Event 27A02C41-15F6-4056-9866-E75BE... Turn help tips: On | Off Launch help ✕

Step 2 of 4

- 1 Rule Details ✓
- 2 **Conditions** ✓
- 3 Actions
- 4 Review And Confirm

Rule conditions

Conditions (*) REQUIRED FIELDS

Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in four scopes: client, server, request and transaction. The help menu will assist you in learning the various keys available (use the up and down arrows in the textfield to display the complete list of available keys).

When **Add**

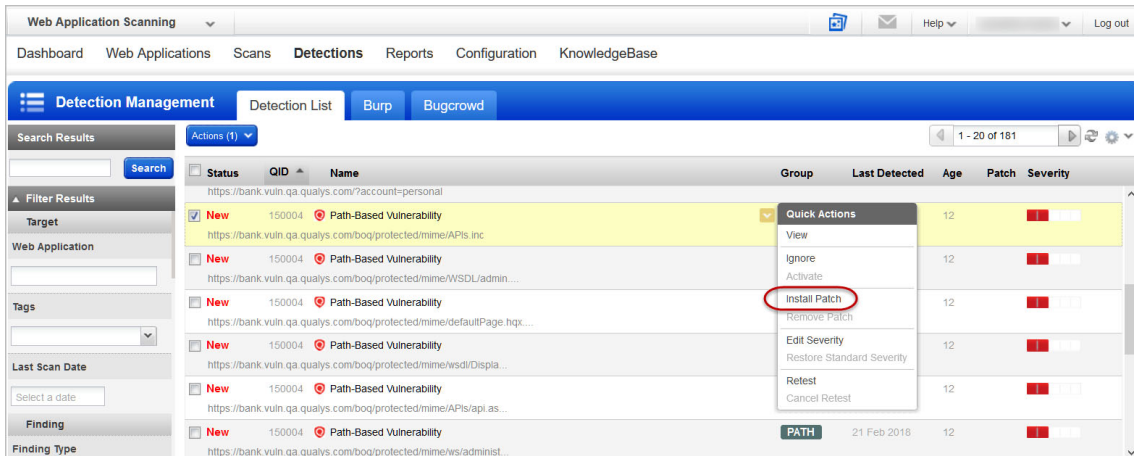
- 1 request_path EQUAL /
- 2 request_method EQUAL POST
- 3 request_body_parameter xml:/myheader DETECT qid/226022

Exceptions once created are linked to the web application. To view them, simply click View in the Quick Actions for a web application, and then click the Security pane.

Deleting an exception from WAF events list does not remove the associated WAF custom rule. You can use the custom rule in the future for similar web applications.

Add Virtual Patches

Use Virtual Patches upon vulnerability detection by the Web Application Scanning module. To do that, select the WAS module, go to Web Applications > Detections, click on the arrow and select “Install Patch”.



Virtual Patches are created in the form of custom rules.

The screenshot shows the 'Rule Creation: Virtual Patch (150004) - Path-Based Vulnerability' form. The 'Step 1 of 4' section is active, showing 'Rule Details'. The 'Basic Information' section contains a 'Name*' field with the value 'Virtual Patch (150004) - Path-Based Vulnerability (#204369)' highlighted by a red circle. Below it is a 'Description' field with a placeholder '2048 characters maximum.' and a 'Tags' section with a placeholder '(no tags selected)'. The 'Tags' section includes a 'Select' button, a 'Create' button, and a 'Remove All' button.

Rule details and conditions for the custom rule are auto populated based on the detection. By default, the action for a virtual patch is Block.

Rule Creation: Virtual Patch (150004) - Path-Based Vulnerability

Turn help tips: On | Off Launch help

Step 2 of 4

1 Rule Details ✓

2 Conditions ✓

3 Actions

4 Review And Confirm

Rule conditions

Conditions (*) REQUIRED FIELDS

Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in four scopes: client, server, request and transaction. The help menu will assist you in learning the various keys available (use the up and down arrows in the textfield to display the complete list of available keys).

When Add

1 request: path DETECT qid/150011

2 request: method EQUAL GET

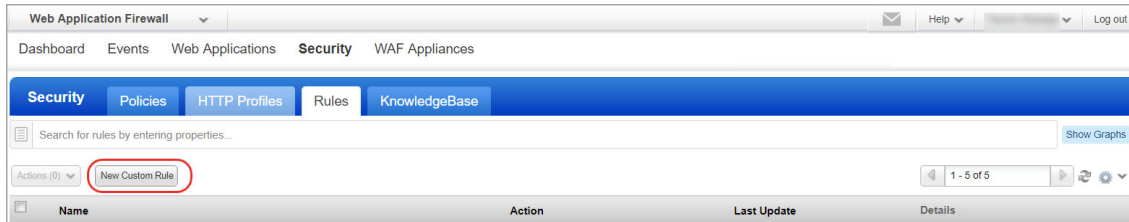
Virtual patches once created are linked to the web application. To view them, simply click View in the Quick Actions for a web application, and then click the Security pane.

Deleting a virtual patch from WAS detections list does not remove the associated WAF custom rule. You can use the custom rule in the future for similar web applications.

Add Custom Rules

Use Custom Rules to define static traffic workflow. Rules allow you to fully control HTTP transactions in order to adapt the security policy in effect for enterprise constraints. Custom rules replace previous Access Rules and Control Rules.

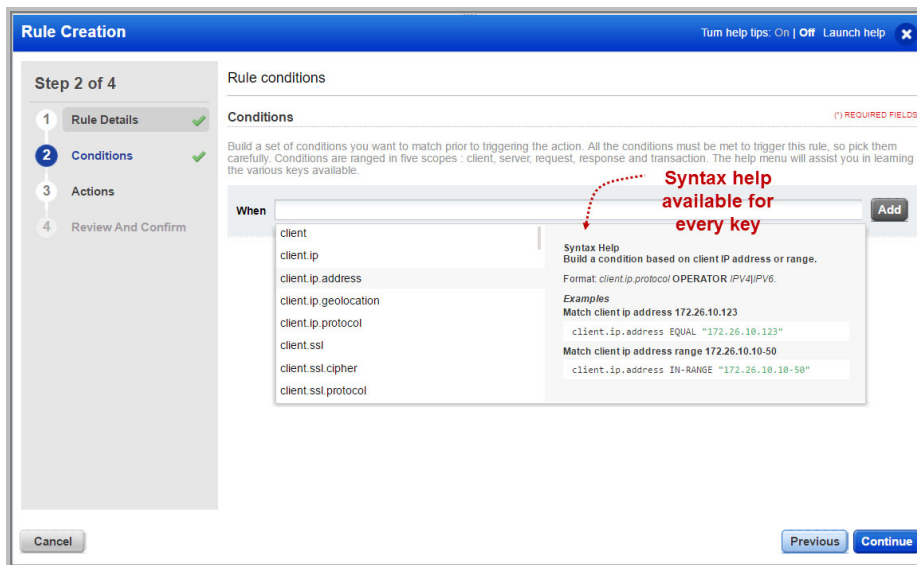
Go to Security > Rules and click the New Custom Rule button.



We have provided various keys to form conditions for a rule.

Want to see all the available keys? Simply place the cursor in the When field, and press the down arrow key on your keyboard to get a list of all available keys. Syntax help is available for every key.

How do I get started? Press the Down arrow to see the available keys.



How do I add a condition?

- Select a key like client.ip.address.
- Then select an operator. Refer to the WAF online help for information on the DETECT operator.

[Click here](#) for more information on using the MATCH operator.

Rule Creation Turn help tips: On | Off Launch help

Step 2 of 4

- 1 Rule Details ✓
- 2 **Conditions** ✓
- 3 Actions
- 4 Review And Confirm

Rule conditions

Conditions (*) REQUIRED FIELDS

Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in five scopes : client, server, request, response and transaction. The help menu will assist you in learning the various keys available.

When

EQUAL
 NOTEQUAL
 MATCH
 NOTMATCH

Syntax Help
 Build a condition based on client IP address or range.
 Format: client.ip.protocol OPERATOR IPV4|IPV6
Examples
 Match client ip address 172.26.10.123
 client.ip.address EQUAL "172.26.10.123"
 Match client ip address range 172.26.10.10-50
 client.ip.address IN-RANGE "172.26.10.10-50"

- Enter a value for your condition in double quotes. In this case we've entered an IP address.

Rule Creation Turn help tips: On | Off Launch help

Step 2 of 4

- 1 Rule Details ✓
- 2 **Conditions** ✓
- 3 Actions
- 4 Review And Confirm

Rule conditions

Conditions (*) REQUIRED FIELDS

Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in five scopes : client, server, request, response and transaction. The help menu will assist you in learning the various keys available.

When

- Press Enter to add your condition. It will look like this.

Rule Creation Turn help tips: On | Off Launch help

Step 2 of 4

- 1 Rule Details ✓
- 2 **Conditions** ✓
- 3 Actions
- 4 Review And Confirm

Rule conditions

Conditions (*) REQUIRED FIELDS

Build a set of conditions you want to match prior to triggering the action. All the conditions must be met to trigger this rule, so pick them carefully. Conditions are ranged in five scopes : client, server, request, response and transaction. The help menu will assist you in learning the various keys available.

When

1 client ip address EQUAL 172.26.10.123

- Click the Add button to add another condition to your rule.
- Complete the steps to add conditions as needed.

We've added 3 conditions for our rule.

Here's the conditions:

```
client.ip.address EQUAL "172.26.10.123"
client.tcp.port EQUAL "45678"
transaction.day EQUAL "Sunday"
```

How does this rule work? The rule gets executed only when all conditions are met. Otherwise, the rule gets ignored.

In the actions panel of the wizard, you tell us what action to take when events match the conditions in the rule.

Once created, assign one or more rules to your web application from within the web application wizard. Rules are executed in the order defined in web application settings.

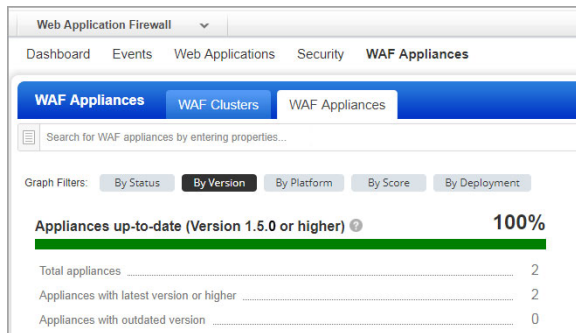
Good to know

Rules are parsed from top to bottom, in the order defined in web application settings. Custom rules support regular expressions with PCRE. Character escaping is possible with the backslash (\).

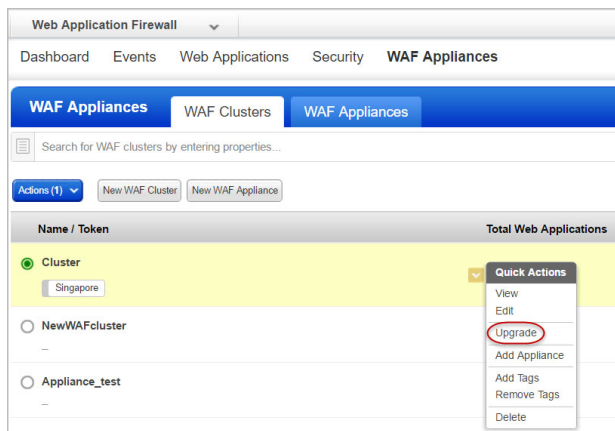
Upgrading WAF clusters

Our service regularly releases scanner appliance software to bring you our latest features and improvements. When software updates are available use the cluster Upgrade option to upgrade all Scanner Appliances registered to that cluster.

The WAF Scanner Appliances by Version graph tells you whether there's software updates available for your Scanner Appliances. You will see the number of appliances running the latest or outdated versions.



To upgrade a WAF cluster, go to WAF Appliances > WAF cluster, and then click Upgrade in the Quick Actions menu of the cluster that you want to upgrade.



Note: The Upgrade option is not available until the time you have chosen to freeze auto-updates. See [Schedule appliance auto-update](#).

You get a confirmation message displaying the number of appliances registered to the cluster. Click Confirm to upgrade.

To verify successful upgrade, check the WAF Scanner Appliances by Version graph. The number of appliances you have upgraded should get added to the number of Appliances with latest version or higher.

Schedule appliance auto-update

You can choose when the appliances registered with a cluster get auto-updated. Select days of the week and the start time. By default, auto-update is enabled for all days of the week.

You can choose to freeze auto-updates until a specific date. Auto-updates are stopped up to the end date and then resumed.

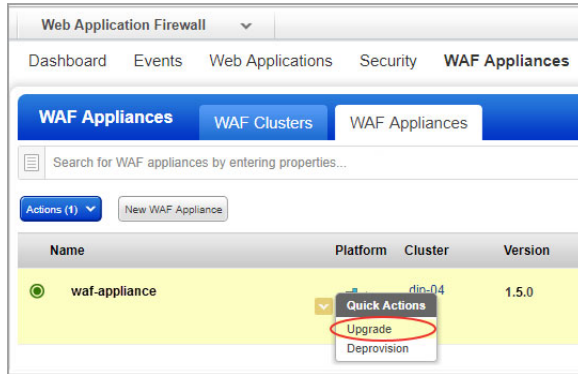
Simply go to WAF Appliances > WAF Cluster, create a new cluster or edit an existing cluster, and then click Automatic Updates.

The screenshot shows the 'WAF Cluster Creation' interface, specifically 'Step 3 of 4: Automatic Updates'. The left sidebar lists four steps: 1. Cluster Details (checked), 2. Configuration (checked), 3. Automatic Updates (active), and 4. Review And Confirm. The main content area is titled 'Schedule Appliance Updates' and includes a sub-header 'Appliance scheduled update configuration' with a red note '(*) REQUIRED FIELDS'. Below this, a description states: 'Choose when the appliances registered with this cluster get auto-updated. Appliances will be updated one by one.' The 'Enable' section has a toggle switch set to 'ON'. The 'Days' section shows checkboxes for all days of the week (Monday through Sunday), all of which are checked. The 'Start time*' is set to '12AM' via a dropdown menu. The 'Time Zone*' is set to '(GMT 05:30) India Standard Time (IST Asia/Colombo)' via a dropdown menu. The 'Freeze period' section includes a description: 'Freeze auto-updates until a specific date. Updates will be enabled again by the end of the day in the timezone that you have chosen above.' and an 'End date' field with a calendar icon.

In the clusters table, hovering over the  icon in the Last Update column shows the time when the next scheduled update is planned.

Upgrading specific WAF appliances

You can upgrade specific WAF appliances manually. It is recommended not to upgrade a WAF appliance if the associated cluster is in freeze period. See [Schedule appliance auto-update](#).



To upgrade a specific appliance, go to WAF Appliances > WAF Appliances, and then select **Upgrade** from the Quick Actions menu of the appliance.

Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.