# Citrix Web App and API Protection

## Contents

# Get started with CWAAP

May 28, 2021

Citrix Web Application and API Protection (CWAAP) is a comprehensive and easy-to-use cloud service that offers protection against security attacks.

The Citrix Web Application and API Protection (CWAAP) is a layered security solution that consists of a full-featured, always-on distributed denial of service (DDoS) defense, denial of service (DoS) protection, and a web application firewall (WAF).

CWAAP, is cloud service with 14 points of presence (PoPs) across the world, CWAAP offers a consistent security posture across all clouds and private data centers, with a low latency and application responsiveness.

Built on Citrix Web App Firewall and enhanced with volumetric DDoS protection and expanded machine learning capabilities, the service allows IT to:

- Define application and API-specific security to safeguard against the OWASP's top 10 and zero-day attacks.
- Apply one of the largest scrubbing networks to protect applications from large DDoS attacks.
- Reduce security configuration errors and simplify visibility and governance across multi-cloud environments.
- Configure rules and policies and adjust them as application security requirements change.
- Secure applications fast wherever they are deployed without more infrastructure or operational complexity.
- Scale in minutes with simple license upgrades.

The cloud-based solution keeps your applications safe as you migrate workloads from on-premises to cloud or among public clouds.

> **Note:**
>
> If you are an existing customer, you can sign into CWAAP.
>
> If you are a new user, you can request for a CWAAP trial or demo. Please contact your Citrix account manager, or see our Citrix Web App and API Protection product page.

## Benefits

Citrix Web App and API Protection service offers the following benefits to customers:

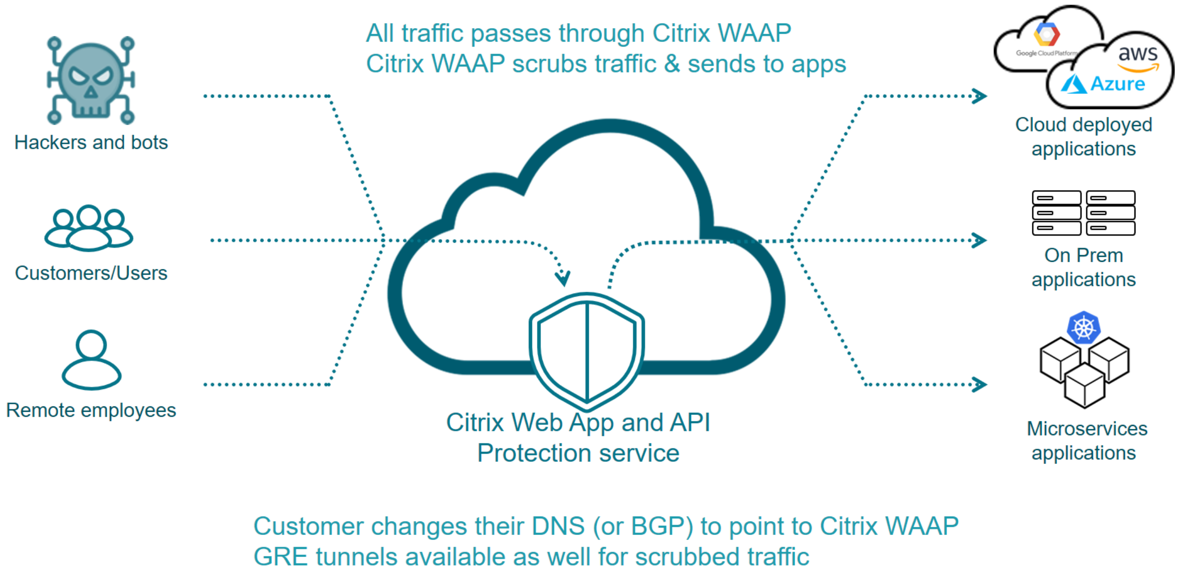
- Provides holistic, proven, and layered protection.
- Protects any application, anywhere.

- Enables protection fast and scale protection quickly and easily.
- Provides simple and predictable consumption model.
- Provides multi-cloud compliance and governance.

For more information, see CWAAP benefits

### How CWAAP works

Citrix Web App and API Protection is simple to deploy and easy to configure across multi-cloud environments—all from a single pane of glass. Protect any application, anywhere, with a holistic security approach that provides volumetric DDoS protection with the Citrix web application firewall solution.


Hackers and bots
Customers/Users
Remote employees
All traffic passes through Citrix WAAP
Citrix WAAP scrubs traffic & sends to apps
Citrix Web App and API Protection service
Google Cloud Platform
aws
Azure
Cloud deployed applications
On Prem applications
Microservices applications
Customer changes their DNS (or BGP) to point to Citrix WAAP
GRE tunnels available as well for scrubbed traffic

### CWAAP DDoS and WAF protection for web applications and APIs

CWAAP provides security protection against the following WAF and DDoS attacks.

#### CWAAP mitigates the following security attacks

- SQL injection
- Cross-site scripting (cross-site scripting)
- Cross-site request forgery (CSRF)
- Buffer overflow
- Form/hidden field manipulation

- Forceful browsing protection
- Cookie or session poisoning
- Command injection
- Error triggering sensitive information leak
- Insecure use of cryptography
- Server misconfiguration
- Back doors and debug options
- Rate-based policy enforcement
- Well-known platform vulnerabilities
- SOAP array attack protection
- Content rewrite and response control
- Authentication, authorization, and auditing (authentication, authorization, and auditing)
- Layer 4-7 services DoS and DDoS protection

### CWAAP mitigates attacks and protects your Web Server and Web Services

- Deep stream inspection; bi-directional analysis
- HTTP and HTML header and payload inspection
- Full HTML parsing; semantic extraction
- Session-aware and stateful
- HTTP Signature scanning
- Scan thousands of signatures
- Response side checks
- Protocol neutrality
- HTML form field protection:
- Drop-down list & radio button field conformance
- Form-field max-length enforcement
- Cookie protection – Signatures to prevent tampering; cookie encryption and proxying
- Legal URL enforcement – Web application content integrity
- Configurable back-end encryption
- Support for client-side certificates
- XML data protection:
- XML security: protects against XML denial of service (xDoS), XML SQL and
- `Xpath` injection and cross site scripting.
- XML message and schema validation, format checks, `WS-I` basic profile compliance, XML attachments check
- URL transformation

**CWAAP mitigates DDoS attacks from layer 3 through layer 7**

**Network Layer Attacks:**

- AKA - Layer3/Layer4 attacks
- High volume of bits/sec
- High volume of packets/sec
- Burst attacks
- Carpet bomb attacks

**Common attacks: UDP floods:**

- SYN floods
- NTP Amplification
- SSDP Amplification
- DNS Amplification
- Chargen Amplification
- SNMP Amplification
- Memcached Amplification

**Application Layer Attacks:**

- AKA - Layer 7 Attacks
- These attacks are typically more complex to generate and more complex to block
- Not necessarily high bandwidth
- GET floods, POST floods
- Slow and Low
- Session exhaustion
- CPU/Memory exhaustion
- Stealth
- Require more SOC analysis

## Understanding Citrix CWAAP and its features

CWAAP portal is a cloud-based analytics solution that enables you to monitor and troubleshoot security incidents. The solution provides personalized experience, greater automation, and real-time analytics that you can quickly act upon. Following are the features available on the CWAAP portal:

- Displays network sources and attacked protocols in an easy, informative way
- Shows real-time and historical information about security attacks.
- Empowers you to route and scrub traffic without any cumbersome interaction.
- Enables automated mitigation of traffic attacks.
- Provides insights for traffic statistics, including top talkers and top routes
- Shows D&A Alerts information including attacked origin server IP, type of attack, and traffic type.

CWAAP features are available under four categories, basic operations, system configuration, analytics, and events.

**Basic operations**. You can access CWAAP either using the API or GUI. Once you log on to the portal, you can access the Account Information module on the left pane to set up user accounts, manage existing accounts, manage user notifications. For more information, see CWAAP Basic Operation topic.

**System configuration**. You can access the Configuration module on the left pane for system configurations such WAF policies, network assets, and associate SSL certificates. For more information, see CWAAP System Configuration topic.

**Analytics**. The Analytics module enables you to monitor data related traffic scrubbed, traffic routed, traffic violations, and asset configuration. For more information, see CWAAP Analytics topic.

**Events**. Displays events triggered when CWAAP detects security attacks. When using different event logs generated by hosts, devices, applications, and databases, network traffic and its vulnerabilities, the CWAAP capability provides deep visibility and analytics to address the most demanding security requirements. For more information, see CWAAP Events topic.

For a quick demo, see Citrix Web App and API Protection demo.

## Basic operation

May 27, 2021

The following sections enable you understand the basic system operations that you can perform on CWAAP cloud service.

- Access management
- Notification management
- Audit logging

## CWAAP dashboard

June 28, 2021

The dashboard page provides a snapshot view of your traffic analyzed by CWAAP. You can specify the time window you want to view (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). Also, you can view this traffic in real-time by enabling the Real-Time Data flag on the top right corner of the chart.

The dashboard displays the following data points for your user account:

- Packets/Sec In – Total traffic directed to the SiteProtect NG Platform in Packets Per Second

- Aggregate in – Total traffic directed to the SiteProtect NG Platform in Mbps
- Mitigated Traffic – Total traffic that is being blocked by the SiteProtect NG Service
- Clean Traffic In – All the clean traffic sent to the customer origin server after removing any attack traffic.
- Egress Traffic – Total Response Traffic sent, via the SiteProtect NG service, to the end user in response to the clean traffic. (Applies to Proxy Only)

These data points are represented in a circular chart displaying the Maximum (outer ring), ninety-fifth Percentile (middle ring), Average (inner ring). This data is also displayed in a line chart which can be configured to display any or none of these data points by clicking the labels in the legend below the chart.

## Notification management

May 27, 2021

You can configure notifications on the CWAAP portal so that you can stay informed about various events via Email, Slack, or Webhook.

There are two notification types available on the CWAAP portal:

- **Account Level** - Allows you to configure Email, Slack, or Webhook notifications.
- **User Level** - Allows you to configure email notifications that can be sent to a specific email address for various types of events associated with your CWAAP account.

> **Note:**
>
> The account level notifications are typically used to send notifications to a SOC, NOC, or other distribution lists and also for sending emails to individuals.

### Configure account level notification

To configure account level notifications on the CWAAP portal:

1. Click your user name and select **Management** from the drop-down menu.
2. From the Account Management page, click **Notifications**, and then select **Configure**.
3. The **Configure Notifications** page is separated into **Email, Slack, and Webhooks** allowing you to customize the types of notifications you want to receive per notification type.

### Configure user level notification

To configure your personal User Level notification:

1. click your user name in the upper right-hand corner, and then select **Your Profile** from the drop-down menu.

Or

1. If you are still on the **Account Management -> Configure Notifications** section, click **edit your profile** link at the top of the screen.
2. The **Edit Profile** page has a section for **Email Notifications** similar to the **Account Level Configurations** section, where you can use the toggle On/Off buttons to enable or disable specific notifications are sent to your email address (that is listed at the top of the screen).
3. click **Save**.

### Notification types and methods

- **Email Addresses** - Provide a valid email address or provide multiple valid emails addresses separated by a comma.
- **Slack** - Enter the Slack Webhook URL and Slack Channel to receive notifications.
- **Webhooks** - To configure Webhook notifications, see the CWAAP Portal Notification Webhooks page.

Each notification method lists the various types of notifications that you receive when you enable the **On/Off toggle** button. Following is a list of different notification types you can enable for your account.

- **Messages from the SOC** - Notifications sent by the SOC.
- **D&A Alert (High)** - A notification sent when high alert is triggered. You receive one notification per alert.
- **D&A Alert (Medium)** - A notification sent when a medium alert is triggered. You receive one notification per alert.
- **D&A Alert (Low)** - A notification sent when low alert is triggered. You receive one notification per alert.
- **D&A Flow Up/Down** - A notification is sent when flow records are not received from one of your routers. You receive notification per router when flow is down, and notification per router when flow resumes.
- **Proxy Certificate Expiration** - A notification sent when one of your SSL certificates are expiring soon. You receive one notification per expiring SSL certificate.
- **Event Start** - A notification sent when mitigation begins. You receive one notification per attack.
- **Event End** - A notification sent when mitigation ends. You receive one notification per attack.

Once you have selected all of your desired Notification methods and types, click **Save** at the bottom of the screen.

## Access management

October 21, 2021

After you have logged into the portal, click **CWAAP** from the dashboard. Then, click &`lt`;`Your Name` &`gt`; from the upper-right corner of the page. Select **Management** from the drop-down menu.

**Note:** Only account administrators and CWAAP administrators can modify a user account.

### Create a user account

From the Account Management screen, select **Users** from the left navigation bar. The Users list page appears.

To add a new user:

1. Click **Add New User**.
2. In the **Add New User** page provide the contact information for the user (Email, First/Last Name, Job Title, Phone, Mobile).
3. Specify if the user must be designated as a global administrator. A global administrator is able to make updates to the Account (adding/deleting users, submitting/updating configurations).
4. You must assign a role (admin/read only) with permissions for the user with services which you have active.
5. Click **Save**. The user account is created in the portal and an email notification is sent.
6. You must click the account activation link in the notification email. The link directs you to the portal to create a password and login to the portal.

### Update an existing user account

From the Account Management page, select the user you want to update. A highlight of the user profile will be displayed on the right side of the screen. The profile identifies the user, the roles they have for each product, and a short list of the user's activity history. At the top of the profile, there are two action buttons (Send Email and Edit). The **Send Email** allows you to contact the user directly through the portal. To make updates to the user account information, you can use the edit option.

> **Note:**

> To log in to the portal, third party cookies **must** be enabled. Please instruct new users to disable third party cookies. It is necessary for users to enable cookies to access the portal.

### Enable a user account

From the Account Management screen, click **Users** from the left navigation bar. The user list displays. Select &lt;`User’ s Name`&gt; you want to update. A details message box appears on the right side of the screen. Select &lt;`Edit Icon`&gt; and update the status of the user by using the toggle switch to enable or disable. When you are done, click **Save**.

## Audit logging

May 27, 2021

Audit logging displays the log details of vulnerability attacks.

## System configuration

May 27, 2021

This section provides system-level information of the CWAAP functionalities. This includes a detailed explanation of system configurations for networking assets, policies, SSL certification, and Web Application Firewall (WAF).

- Asset configuration
- Policy configuration
- SSL certification
- WAF configuration

## WAF profile configuration

October 21, 2021

To access the WAF profile from the CWAAP GUI, you must access the Configuration module and click Policies. The `Policy Configuration` page shows the `WAF Profile` option. To configure a new WAF Profile, you must first set up a Proxy configuration. Once you have an active Proxy configuration:

- Click the **Configure a New Policy** button. A menu for ‘Choose Proxy for WAF Profile Configuration options’ will be displayed.

- Select one of the Proxy configurations by clicking the associated **Configure WAF Profile**. The WAF Policy Editor will be displayed.
- assigns the policy options you want to create for your profile. Details for the policies are shown in the tables below.
- Once you have provided all the policy information, click the submit button at the bottom right of the screen.

### Manage existing WAF configuration

From the WAF Profile page, click "Edit" next to the host name field of the configuration you want to update. The update configuration screen will be displayed. Here you can make any changes you want make and click **Save** to submit the updated configuration. From this screen, you can also **Delete** the configuration by selecting the "Delete" button at the top right of the screen.

### Enable WAF

Before you can create and configure your Web Application Firewall (WAF) Policies, you must first enable WAF for your account, and select the type of WAF Policy you want to configure.

From the **Edit Account** page, navigate down to the *Services* section. For WAF to be enabled for the account, the **Proxy** settings have to be **Enabled**. If they are Disabled, the options to configure and customize the basic WAF settings will be removed.

In the **WAF** drop-down menu, you can select either:

- Disabled
- Basic Application Security (Basic WAF)
- Advanced Application Security

Once you have selected the WAF type, the **WAF Signatures** default to 3, unless you select another option. You can opt to enable any other Proxy and WAF settings, but click the **Save** button when you are done.

### Access WAF profile

To access the Web Application Firewall (WAF) Profile, select **Configuration** from the left-hand navigation panel, and then click **Policies**, and then click **WAF Profile** tab.

If there are no WAF Policies configured, or you want to create a WAF Policy, you must first configure a Proxy. To find more details on how to configure a Proxy, please use the following help file `DNS Proxy Configuration`.

Once you have an active Proxy configuration:

1. Click the **Configure New Proxy** button.
2. Select one of the Proxy configurations by clicking the associated **Configure WAF Profile**.
3. Using the WAF Policy Editor, assign the policy options you want to create for your profile.
4. Once you have provided all the policy information, click the **Create Profile** button at the bottom right of the screen.

The WAF profile page has security checks available under three categories - Core, Advanced, and XML.

### Core security checks

The core security checks apply to any aspect of web security that either does not involve content or is equally applicable to all types of content.

The core security checks are as follows:

1. HTML SQL Injection. The CWAAP HTML SQL Injection check provides special defenses against injection of unauthorized SQL code that might break the security. If CWAAP detects unauthorized SQL code in a user request, it either transforms the request, to render the SQL code inactive, or blocks the request.

2. HTML cross-site scripting. The HTML Cross-Site Scripting (cross-site scripting) check examines both the headers and the POST bodies of user requests for possible cross-site scripting attacks. If it finds a cross-site script, it either modifies (transforms) the request to render the attack harmless, or blocks the request.

3. CSRF Settings. The Cross Site Request Forgery (CSRF) settings check each web form sent by a protected website to users with a unique and unpredictable FormID, and then examines the web forms returned by users to ensure that the supplied FormID is correct. This check protects against cross-site request forgery attacks. This check applies only to HTML requests that contain the web form, with or without data. It does not apply to XML requests.

4. Buffer overflow. The Buffer Overflow check detects if there is buffer overflow on the web server. If CWAAP detects a URL, cookies, or header are longer than the configured length, it blocks the request because it can cause a buffer overflow

### Advanced security checks

The advanced security checks examine web form data to prevent attackers from compromising your system by modifying the web forms on your websites or sending unexpected types and quantities of data to your website.

The advanced security checks are as follows:

1. Cookie consistency. The Cookie Consistency check examines cookies returned by users, to verify that they match the cookies that your website set for that user. If you modify a cookie, the

cookie is ripped from the request before it is forwarded to the web server. You can also configure the Cookie Consistency check to transform all of the server cookies that it processes, by encrypting the cookies, proxying the cookies, or adding flags to the cookies. The check applies to requests and responses.

2. Field consistency. The Form Field Consistency check examines the web forms returned by users of your website, and verifies that web forms were not modified inappropriately by the client. This check applies only to HTML requests that contain the web form, with or without data. It does not apply to XML requests.
3. Field format. The Field Formats check verifies the data that users send to your websites in web forms. It examines both the length and type of data to ensure that it is appropriate for the form field. If the Web App Firewall detects inappropriate web form data in a user request, it blocks the request.
4. Content type. Web servers add a Content-Type header with a `MIME`/`type` definition for each content type. Web servers serve many different types of content. For example, standard HTML of type `text`/`html` `MIME`. JPG images are assigned content types. A normal web server can serve different types of content, all defined in the Content Type header by type `MIME`/`type`.
5. HTTP RFC profile. Citrix Web App Firewall inspects the incoming traffic for HTTP RFC compliance and drops any request that has RFC violations by default. However, there are certain scenarios, where the appliance might have to bypass or block a non-RFC compliance request. In such cases, you can configure the appliance to bypass or block such requests at global or profile level.
6. Deny URL. The Deny URL check examines and blocks connections to URLs that hackers commonly access. This check contains a list of URLs that are common targets of hackers or malicious code and that rarely if ever appear in legitimate requests. You can also add URLs or URL patterns to the list. The Deny URL check prevents attacks against various security weaknesses known to exist in the web server software or on many websites.
7. POST body limit. Limits the request payload (in bytes) inspected by Web Application Firewall.

### XML security checks

The XML Protection checks examine requests for XML-based attacks of all types.

The XML security checks are as follows:

1. XML SQL Injection. The XML SQL injection check examines the user requests for possible XML SQL Injection attacks. If it finds injected SQL in XML payloads, it blocks the requests.
2. XML cross-site scripting. The XML Cross-Site Scripting check examines the user requests for possible cross-site scripting attacks in the XML payload. If it finds a possible cross-site scripting attack, it blocks the request.

3. XML format. The XML Format check examines the XML format of incoming requests and blocks those requests that are not well formed or that do not meet the criteria in the XML specification for properly formed XML documents.

4. XML SOAP fault. The XML SOAP fault check examines responses from your protected web services and filters out XML SOAP faults. The detection prevents leaking sensitive information to attackers.

5. Web service interoperability. The Web Services Interoperability (WS-I) check examines both requests and responses for WS-I standard, and blocks those requests and responses that are not in compliance with WS-I. The purpose of the WS-I check is to block requests that might not interact with other XML appropriately. An attacker can use inconsistencies in the interoperability to attack your XML application.

### To disable WAF policies

1. From the **Edit Account** page, select **Disabled** to clear your WAF.
    a) Turning the Proxy setting OFF will also disable WAF, but we do not recommend this method.
2. Click the **Save** button.
3. You will no longer be able to access the Web Application Firewall section of your account when attempting to access it.

### To disable a single WAF policy

1. Edit the WAF Policy.
2. Click **disable** in the **Proxy Policies** section.

### To re-enable WAF

1. From the **Edit Account** page, select either **Basic** or **Advanced Application Security** from the drop-down menu.
2. The **WAF Signatures** displays the default value of 3.
3. Click **Save**.
4. Navigate to the **Configuration** option on the left-hand navigation panel, select **Security**, and then **Web Application Firewall**.
5. Click **pencil** icon to edit the WAF policy.
6. Click **enable** (“lock” icon).
    a) All of your previously saved configurations will be applied.
7. Click **Save Changes**.

### Learning and relaxation

Given the sheer volume of traffic CWAAP examines, it is critical for our customers to understand the traffic patterns and types that they are experiencing. Enabling certain counter measures or features can actually be detrimental to a customer by creating false positives, which might require manual research and review. By enabling the CWAAP Learning feature, a complete traffic pattern can be analyzed, which then makes creating a Relaxation Rule that would prevent specific traffic patterns from being blocked painless and manageable.

Once the Learning behavior is actively monitoring traffic for the specified Protection Type, a comprehensive list of rules with its count appears. Once you have reviewed the list, if there are any entries that must not be blocked, or are not malicious, you can add them to the **Relaxation** section to prevent them from being blocked in the future.

## WAF core security protection

October 21, 2021

The core selection of the counter measures is the most commonly recommended and applied collection of counter measures to apply to your WAF policy.

| Counter measure Name | Description |
|---|---|
| HTML SQL Injection | The HTML SQL Injection Counter measure provides protection against the injection of unauthorized SQL code that might break security. SQL injection is a code injection technique that might destroy your database and is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via webpage input |

| Counter measure Name | Description |
|---|---|
| HTML XSS | Attackers can use cross-site scripting (Cross-Site Scripting) to send a malicious script to an unsuspecting user, where the user's browser has no way to know that the script should not be trusted, and will run the script. Once ran, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. |
| CSRF Settings | CSRF (Cross-Site Request Forgery) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. Some common examples include changing the email address on their account, changing a password, or even making a funds transfer. |
| Buffer Overflow | Buffer Overflow is one of the best-known forms of software (security) vulnerability. Buffer overflows can be used to corrupt the execution stack of a web application. "Sending carefully crafted input to a web application, an attacker can cause the web application to run arbitrary code – effectively taking over the machine." |

### HTML SQL Injection

When expanding the HTML SQL Injection counter measure, the following features and customization options will be available.

- Wildcard Characters - Enabled or Disabled
- Request containing the 4 fields - A drop-down menu providing various if/and/or statements to capture specific types of SQL content.
- Comment Handling - Indicates that all comments will be checked (enabled by default).
- Relaxation Rules - Relaxation rules can be manually created by clicking the Add button or directly added from the Learning section.
- The checkmark icon allows for the multi-selection of configured Relaxation Rules, which can then be removed in bulk.

- Learning - When set to On, traffic patterns are analyzed which can enhance the Relaxation Rules, or identify reoccurring threats.
- Alert Threshold - A configurable threshold (value) level that once reached (or exceeded), will begin to send alerts for the violations being triggered.

### HTML cross-site scripting

When expanding the HTML XSS Counter measure, the following features and customization options are available.

- Check Complete URLs - You can turn this feature On or Off to require the counter measure to check the full URL of the offending traffic.
- Relaxation Rules - Relaxation rules can be manually created by clicking the Add button or directly added from the Learning section.
- The checkmark icon allows for the multi-selection of configured Relaxation Rules, which can then be removed in bulk.
- Learning - When set to On, traffic patterns are analyzed which can enhance the Relaxation Rules, or identify reoccurring threats.
- Alert Threshold - A configurable threshold (value) level that once reached (or exceeded) begins to send alerts for the violations being triggered.

### CSRF Settings

When expanding the HTML cross-site scripting counter measure, the following features and customization options are available.

- Alert Threshold - A configurable threshold (value) level that once reached (or exceeded), will begin to send alerts for the violations being triggered.
- Relaxation Rules - Relaxation rules can be manually created by clicking the Add button or directly added from the Learning section.
- The checkmark icon allows for the multi-selection of configured Relaxation Rules, which can then be removed in bulk.
- Learning - When set to On, traffic patterns are analyzed which can enhance the Relaxation Rules, or identify reoccurring threats.

### Buffer Overflow

In contrast to the additional features and customization options of the HTML SQL Injection counter measure, the Buffer Overflow has a more simplistic configuration setup.

- Max URL Length - Configure the maximum URL length that can be allowed before triggering a violation.

- Max Cookie Length - Configure the maximum Cookie string length that can be allowed before triggering a violation.
- Max Header Length - Configure the maximum (raw) Header Length that can be allowed before triggering a violation.
- Alert Threshold - A configurable threshold (value) level that once reached (or exceeded), will begin to send alerts for the violations being triggered.

Each counter measure is slightly unique in the customization and configuration setup that can be set.

## WAF counter measures

October 22, 2021

The **Counter measures** section of the **WAF Profile** provides a collection of custom counter measures that can quickly and easily be applied to your policy.

Each counter measure has a quick access bar that allows you to select from three options to determine how your policy must implement the selected counter measure.

- None - The default setting for any new policy, which indicates the specified counter measure is not being implemented.
- Log - If a violation is detected, the action (traffic) is allowed, but the incident is logged and saved for review.
- Block and Log - If a violation is detected, the action (traffic) is denied, and the details of the incident is saved for review.

### Advanced counter measures

The advanced counter measures feature require more knowledge of your traffic patterns and configuration methods.

| counter measure name | Description |
|---|---|
| Cookie Consistency | The Cookie Consistency counter measures is designed to examine cookies that are returned, and then verify that they match the cookies that your website has configured. An attacker would normally modify a cookie to gain access to sensitive private information by posing as a previously authenticated user, or to cause a buffer overflow. |

| counter measure name | Description |
|---|---|
| Field Consistency | The Field Consistency counter measure is designed to prevent unauthorized changes to web forms and fields on a website. It can also be used to determine that the data a user provides adheres to any HTML restrictions set for length and type, and protecting any data that might be contained in hidden fields from being altered |
| Field Format | The Field Format counter measure is designed to examine the length and type of data being provided in a form field to ensure it adheres to accepted formats. If invalid values are submitted, the counter measure blocks the request. |
| Content Type | The Content Type counter measure is designed to inspect the Content-Type Header of a webserver. Common filtering rules apply to only one type of content (such as HTML), and are often ineffective when filtering different types of content. This counter measure allows you to customize the various Content Type to be filtered. |
| HTTP RFC Profile | The HTTP RFC Profile counter measure inspects the incoming traffic that might violate HTTP RFC compliance violations (commonly a “Parsing Error”). |
| Deny URL | The Deny URL counter measure inspects a list of common URLs used by hackers and malicious code that rarely appear in legitimate requests. |
| POST Body Limit | The POST Body Limit counter measure checks the size of a POST body request. The default value is set to 4 GB. |

### XML counter measures

The XML counter counter measures require more knowledge of your XML traffic patterns and configuration methods.

| counter measure Name | Description |
|---|---|
| XML SQL Injection | An XML SQL attack injects source code into a web application, often causing it to be interpreted and run as a valid SQL query, which is then able to perform a database operation with malicious intent. The XML SQL Injection countermeasure reviews XML payloads for inappropriate or injected SQL content. |
| XML XSS | The XML cross-site scripting (cross-site scripting) countermeasure is designed to prevent cross-site scripting In essence, this bot protection counter measure prevents scripts from accessing or modifying content on a server in which they are not natively located. |
| XML Format | The XML Format bot protection counter measure checks the XML format of incoming requests and blocks those requests that are not well-formed, or that do not meet specific pre-configured criteria for what a well-formed XML request must be. |
| XML SOAP Fault | The XML SOAP Fault counter measure is designed to check the responses from your protected web services and filters out XML SOAP faults. This counter measure can prevent the leak of sensitive information. |
| Web Service Interoperability | The Web Service Interoperability counter measure is designed to examine requests and responses against the WS-I standard, and then, block those requests and responses that do not adhere to the standard. |

# Bot configuration

October 21, 2021

Web and mobile applications are significant revenue drivers for business and most companies are under the threat of advanced cyberattacks, such as bots. A bot is a software program that automatically performs certain actions repeatedly at a much faster rate than a human. Bots can interact with webpages, submit forms, run actions, scan texts, or download content. They can access videos, post comments, and tweet on social media platforms. Some bots, known as chatbots, can hold basic conversations with human users.

With some bad bots performing malicious tasks, it is essential to manage bot traffic and protect your web applications from bot attacks.

The CWAAP bot management detects the incoming bot traffic and mitigate bot attacks to protect your web applications. The bot configuration helps identify bad bots and protect your application from security attacks. Beyond knowing when a bot is interacting with applications or networks, and knowing whether the bot is good or bad, the CWAAP Service platform informs users about the bot activity. The user can then decide on a bot action to apply (allow, block, log, delay, or deceive).

## Setting up CWAAP bot configuration

To begin the setup for CWAAP bot configuration, you must first have an asset, and a policy configured to the asset.

1. Select **Configuration** > **Policies**.
2. Select a policy and click **Edit** (pencil and paper).
3. Navigate to **Bot Profile** tab.

The CWAAP bot profile consists of bot protection techniques and bot signature configuration.

- Protection. List of bot protection techniques that you can configure as part of CWAAP bot configuration and associate bot actions to it.
- Signatures. A list of counter measures that protect your web application against bot attacks. Bot signatures help in identifying good and bad bots based on request parameters such as user-agent in the incoming request.

## Bot protection techniques

The CWAAP bot protection provides a list of bot techniques that you can configure and then enable or disable it for policy configuration.

Once you have configured your bot technique, you must first enable the technique for it to take effect on the policy.

Following are the list of bot protection techniques that CWAAP bot configuration supports:

- Allow list
- Block List
- Bot Trap
- Reputation
- Device Fingerprint
- Rate Limiting
- Transactions Processing System (TPS)
- CAPTCHA

### Allow list

A customized list of IP addresses, subnets, and policy expressions that can be bypassed as an allowed list for your bot policy.

> **Note:**
>
> You can configure up to 32 bindings as part of the allow list configuration in a bot profile.

Configure allow list by using the CWAAP GUI:

1. Click **Add**.
2. In the **Add to Allow List Bindings** page, set the following parameters:
    a) Active. Select to activate the protection technique.
    b) Type. Select type as Expression, IPv4, or Subnet.
    c) Value. Provide the associated Value, and then select the corresponding Response (or Action) to be carried out.
    d) Response. Select response as Log or None.
3. Click **Commit**.

### Block list

A customized list of IP addresses, subnets, and policy expressions that must be blocked from accessing your web applications. The configured traffic is blocked only when you enable the block list feature.

> **Note:**
>
> You can configure up to 32 bindings as part of the block list configuration in a bot profile.

Configure block list bot protection technique by using the CWAAP GUI:

1. Click **Add**.
2. In the **Add to Block List Bindings** page, set the following parameters:

   a) Active. Select to activate the protection technique.
   b) Type. Select type as Expression, IPv4, or Subnet.
   c) Value. Provide the associated Value, and then select the corresponding Response (or Action) to be carried out.
   d) Response. Select response as Action and log, log, or None.

3. Click **Commit**.

### Bot trap

The CWAAP bot trap protection technique randomly or periodically inserts a trap URL in the client response. You can also create a default trap URL and add URLs for that. The URL appears invisible and not accessible if the client is a human user. However, if the client is an automated bot, the URL is accessible and when accessed, the attacker is categorized as bot and any subsequent request from the bot is blocked. The trap technique is effective in blocking attacks from bots.

Configure bot trap protection technique by using the CWAAP GUI:

1. In the **Bot Trap** section, Click **Add**.
2. In the **Add Insertion URLs** page, set the following parameters:
   a) Active. Select to activate the specified URL Pattern.
   b) URL Pattern. Provide the URL Pattern (Insertion URL) for your top visited websites, or those frequently visited websites. If no URL is provided, and the bot protection techniquesmeasure is activate the technique and enable it for the policy. Also, a default trap URL is created for all URLs.
3. Click **Commit**.

### IP reputation

The CWAAP protection technique detects if the incoming bot traffic is from a malicious IP address. As part of the configuration, we set different malicious bot categories and associate a bot action to each of it.

Following are the IP reputation threat detection categories:

- Botnets
- DoS
- IP
- Mobile Threats
- Phishing
- Proxy
- Reputation

- Scanners
- Spam Sources

Each threat type can either be set to one of the following response types.

- Action and Log – Log the violation details, and take the configured Action type.
- Log – Capture and log any traffic matching the configurations, but take no Action.
- None – Take no action if a match occurs.

After setting the response type, you can configure any one of the following bot actions.

1. Drop
2. Mitigation
3. Redirect
4. Reset

### Device fingerprint

The CWAAP bot technique detects if the incoming bot traffic has the device fingerprint ID in the incoming request header and browser attributes of an incoming client bot traffic. The attributes are examined to determine whether the traffic is a Bot or a human. In this technique, the HTTP request header "User Agent" is the determining factor.

If the URL is already provided and it matches with the ADC list, then the domain name lookup occurs. If a matching domain name is identified, the traffic is considered good.

If, however, the domain name returned does not match what the ADC has, then the traffic is dropped and considered bad.

If a user agent search is completed and a match is found, then the traffic is dropped and designated bad.

Configure device fingerprint protection technique by using the CWAAP GUI:

1. In the **Device Fingerprint** section, set the following parameters.
   a) Response. Select a bot response.
      i. Action and Log – Log the violation details, and take the configured Action type.
      ii. Log. Capture and log any traffic matching the configurations, but take no Action.
      iii. None. Take no action if a match occurs.
   b) Action. You can configure any one of the following bot actions.
      i. Drop
      ii. Mitigation
      iii. Redirect
      iv. Reset

### Rate limiting

The CWAAP rate limiting protection technique examines the time frame in which a request is received from a Client IP Address, Session ID, or configured resource (incoming URL).

> **Note:**
>
> You can configure up to 32 bindings as part of the rate limiting configuration in a bot profile.

Configure rate limit bot protection technique by using the CWAAP GUI:

1. In the **Rate Limiting** section, Click **Add**.
2. In the **Add to Rate Limit Bindings** page, set the following parameters:
   a) Active: Select the Type from the drop-down menu.
   b) Type: Select a rate limit type:
      i. Source_IP – The Rate Limit will be determined by the client IP Address.
      ii. Session – The Rate Limit will be determined by the configured cookie name.
      iii. URL – The Rate Limit will be determined by the configured URL.
   c) URL: The Rate Limit will be determined by the configured URL.
   d) Rate: Configure the Rate value, which determines the number of requests allowed for a specified time Period
   e) Period: Configure the Period value for the selected Rate value in milliseconds (in multiples of 10)
   f) Response: Select the Response Type and if applicable, the associated Action type.
   g) Action: Select a bot action.
3. Click **Commit**.

### Bot Transactions Processing System (TPS)

The CWAAP Transaction Processing System (TPS) protection technique examines the number of requests and percentage increase in requests for a configured time interval to determine if the traffic is coming from a bot.

Configure Transaction Processing System (TPS) protection by using the CWAAP GUI:

1. In the **TPS Bindings** section, Click **Add**.
2. In the **Add to TPS Binding** page, set the following parameters:
   a) Type: Select the Type from the drop-down menu of either Host or Request URL.
   b) Fixed Threshold: Provide the Fixed Threshold value, which will determine the maximum number of requests allowed within a one second time interval.

   c) % Threshold: Provide the % Threshold value, which will determine the maximum percentage of requests increases allowable within a 30 minute time span.
   d) Response: Select the Response type from the drop-down menu.
      i. Action and Log – Log the violation details, and take the configured Action type.
      ii. Log – Capture and log any traffic matching the configurations, but take no Action.
      iii. None – Take no action if a match occurs.
   e) Action: Select a bot action.
3. Click **Commit**.

### CAPTCHA

CAPTCHA is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". CAPTCHA is designed to test if an incoming traffic is from a human user or an automated bot. CAPTCHA helps to block automated bots that cause security violations to web applications. In CWAAP, CAPTCHA uses the challenge-response module to identify if the incoming traffic is from a human user and not an automated bot.

> **Note:**
>
> Only one binding is allowed per URL. If a binding exists for a URL, and another binding is configured for the same URL, the previous binding information is removed. You can configure only up to 30 bindings per bot profile.

Configure CAPTCHA protection technique by using the CWAAP GUI:

1. In the CAPTCHA section, Click **Add**.
2. In the Add to CAPTCHA Bindings page, set the following parameters:
   a) Wait Time – Determines the duration until the client sends the CAPTCHA response. Allowable range is 10–60 (seconds).
   b) Grace Period – Determines the duration from when the current CAPTCHA response is sent, and a new challenge is not sent.
      i. Allowable range is 60–900 (seconds).
   c) Mute Period – Determines the duration to wait when an incorrect CAPTCHA response is received, and no additional requests from the client will be accepted.
      i. Allowable range is 60–900 (seconds).
   d) Request Length – Determines the size of the request body for the CAPTCHA challenge to be sent to the client. If the request body length exceeds the configured Request Length, the request is dropped.
      i. Allowable range is 10–30,000 (bytes).
   e) Retry Attempts – Determines the number of retry attempts that are allowed.
      i. Allowable range is 1–10.
   f) Select the Response and corresponding Action (if applicable).

3. Click **Commit**.

Click **Save** to apply the configuration to the policy.

## Policy configuration

October 21, 2021

Before you configure Web Application Firewall (WAF) policies, you must first create a WAF policy.

### Create a WAF policy

1. On the left-hand navigation panel, click Configuration.
2. Select Policies from the list of available features.
3. Click the Create Policy button.
4. Provide a Policy Name, and then ensure you select a WAF profile.
5. Select the checkmark to apply the WAF Profile to the policy.
    a) Optionally, you can enable the usage of the Semicolon Field Separator in URL Queries and Post form bodies, which simply indicate that a semicolon ( ; ) is separation multiple fields.
6. The counter measures section provides a list of common protection types and methods for users to select from. Expand each bot protection techniquesmeasure to configure the required values. Each bot protection techniquesmeasure can be set to one of the following statuses.
    a) Bypass / None – No action will be taken.
    b) Block – Once the threshold limit has been reached, the violating traffic will be blocked.
    c) Log – One or more requests or violations will not be blocked, but details will be logged for review.
    d) Block and Log – One or more requests are blocked and the details are stored.
7. Certain counter measures offer learning and relaxation rules.
    a) Relaxation Rules – You can manually enter the values that allow traffic matching the criteria through. If Learning was enabled, you can click + (plus) to an entry to apply it directly to the Relaxation Rules.
    b) Learning – Learning must be enabled for each bot protection techniquesmeasure before data can begin to be captured. Once traffic is actively being monitored, a list of blocked rules will be returned that you can review for accuracy.
8. To configure the Relaxation Rules, click Add, and then complete the fields that appear in the pop-up window.
9. **Click Commit**.
    a) Name – Provide a name for the configured Relaxation Rule.
    b) Enabled – Set to either ON or OFF.

   c) Is Name Regex – Set to either ON or OFF.
   d) URL – Provide the URL that is allowed.
   e) Location – Select from the drop-down menu either
      i. Cookie
      ii. Form Field,
      iii. Header.

10. Value Type – Select from the drop-down menu either
    1. Keyword
    1. Special String,
    1. Wildchar.
       a) Is Value Expression Regex – Set to either ON or OFF?
       b) Value Expression – Provide the value expression for the rule.
11. To enable Learning, select the ON/OFF option for your desired configuration.
12. Click **Save**.

### Configure responder policies

The **Responder Policies** section provides more flexibility to customers, but does require more detailed and in-depth knowledge of your traffic configurations to properly use and incorporate. When properly used however, the Responder Policies can inspect on any of the fields (values) and operands and then run a selected action.

1. From the Policy Configuration screen, select the Responder Policies tab.
2. Click the Start button to add a Responder Policy.
3. Provide a Name for the Policy.
4. Select the Action type from the drop-down menu.
   a) Drop
   b) Log
   c) Redirect To
   d) Respond With
5. The Response field will be determined by the Action you selected.
   a) Drop. Response is N/A as the traffic are dropped.
   b) Log. Response is N/A as the traffic are stored in your log file.
   c) Redirect To. Provide the URL to be redirected. The URL must start with a backslash (/).
   d) Respond With. Provide the text to display for the response.
6. Select the arrow next to the Matches section to configure exact specifications for your policy. Complete the following fields
   a) Field. Select the field type from the drop-down list of options.
   b) Operand. Select the operand type for the field from the drop-down menu.
   c) Value. Provide the value associated to the Field and Operand combination.

   d) To select more Match criteria, click the Plus icon.

7. To add more Responder Policies, click the Plus icon. Doing so increases the responder policy number in the upper left hand side of each configured policy. Also, if you are using multiple rules, all of the rules have to pass / match before the associated action can be taken.
8. Click **Save**.

### Network controls

The **Network Controls** section of the Policy allows for Geographical (GEO) blocking of traffic by country type. If however, you want to block an entire country, but allow a specific IP address through, you can configure the Network Controls to do so.
Click the Add button to indicate if an IP / CIDR address should be blocked or allowed. Click the **Commit** button when done.

The **Network Controls** section of the Policy allows for Geographical (GEO) blocking of traffic by country type. If however, you want to block a country but allow a specific IP address through, you can configure the Network Controls to do so.

1. From the Policy Configuration screen, select the Network Controls tab.
2. Click the Add button to configure an IP address that you want to either block, or allow through
3. Provide an IP Address, and then select Not Blocked (allow the IP Address through) or
   Blocked (prevent all traffic from the IP Address). Click the Commit button when finished
4. To select an entire country to block traffic from, click in the Blocked Countries drop-down menu. Select all of the countries that you want to block traffic from. Click out of the drop-down menu when you are finished making your selections
5. To allow list an IP Address from a blocked country, first select the Country to block, and then add the IP address from that country to allow through, and select the Not Blocked option. The allow list action happens before a block action is applied.
6. Click Save.

### Alert threshold

The **Alert Thresholds** section allows you to configure a threshold value, that once reached, will send alerts for the violations occurring for a configured rule.
To configure an Alert Threshold, click the **Add** button. Select the Dimension from the drop-down menu, and then configure the corresponding fields.

To further clarify, alerts will not be sent until the Occurrence count has been exceeded within the time frame specified. For example, if the occurrence rate was 3, and the timeframe was 60 seconds, alerts would not be sent until a fourth violation occurred within the 60-second timeframe.

A pop-up help window appears with an explanation of a selected Dimension from the drop-down menu.

The **Alert Threshold** section allows you to define a threshold that must be reached before Alerts are sent for violations that are relevant to your configured rules.
Alert Thresholds are set by Dimension, a KEY, and a designated Count or amount. The threshold alerts can be synced to SLACK, with a link provided directly to the alert page of the Portal, and being sent out in email format. The alert notifications will also be displayed on the UI Portal under the bell (notifications) icon.
It is important to note that Alert Thresholds are also set on the **WAF Profile** section, per bot protection techniquesmeasure.

1. From the Policy Configuration screen, select the Alert Thresholds tab.
2. Click Add.
3. Select the Dimension from the list of drop-down menu options. Each dimension selection provides a brief explanation at the top of the pop-out window.
    a) More fields are determined by the Dimension type you select.
4. Complete any additional fields that appear based on the Dimension type selected.
5. Select the number of Occurrences. This determines the threshold limit that must be reached for a violation to occur, and a notification to be sent.
6. The Timeframe by default stays at 60 seconds.
7. Click the Commit button when you are finished customizing the Application Security Threshold.
8. Click the Save button when you are done adding Alert Thresholds

#### Trusted sources

The **Trusted Sources** section helps to configure a list of IPs that can be reliably used for learning traffic data and generate recommendations for relaxation. If Trusted Sources are not configured, traffic from all the sources will be used for learning and not providing appropriate recommendations for relaxation.

1. Click **Add** to configure a new Trusted Source. Select whether the Trusted Source is going to be Enabled or not, and then provide the IP Address/CIDR. The Description field is an optional field that can be filled using free text.
2. Click Commit when you are done.
3. Click **Save**.

#### Assets

The **Assets** tab displays any asset that this policy is currently assigned to. If there are any associated assets, you can remove them which will cause each asset to undergo a provisioning process in which rules and configurations might be temporarily disabled.

If no Assets are associated with your policy, the Associated Assets drop-down menu displays "0 Selected". Select an Asset to associate with your policy.

To remove an associated Asset, hover over the drop-down menu and click the Minus button next to the Asset you want to remove, or, click in the drop-down menu and click a highlighted Asset to remove it.

### bot protection techniques measure

The **counter measures** section provides a list of common protection types and methods for users to select from.

1. Expand each bot protection techniquesmeasure to configure the required values. Each bot protection techniquesmeasure can be set to one of the following statuses.
    a) Bypass / None – No action is taken.
    b) Block – Once the threshold limit has been reached, the violating traffic are blocked.
    c) Log – One or more requests or violations are not blocked, but details are logged for review.
    d) Block and Log – One or more requests are blocked and the details are logged.
2. Certain counter measures offer Learning and Relaxation Rules.
    a) Relaxation Rules – You can manually enter the values that allow traffic matching the criteria through. If Learning was enabled, you can click the + (plus) Icon next to an entry to apply it directly to the Relaxation Rules.
    b) Learning – Learning must be enabled for each bot protection techniquesmeasure before data can begin to be captured. Once traffic is actively being monitored, a list of blocked rules will be returned that you can review for accuracy.
3. To configure the Relaxation Rules, click the Add button, and then complete the fields that appear in the pop-up window. Click Commit when finished.
    a) Name – Provide a name for the configured Relaxation Rule.
    b) Enabled – Set to either ON or OFF.
    c) Is Name Regex – Set to either ON or OFF.
    d) URL – Provide the URL that is allowed.
    e) Location – Select from the drop-down menu either
        i. Cookie
        ii. Form Field,
        iii. Header.
    f) Value Type – Select from the drop-down menu either
        i. Keyword
        ii. Special String,
        iii. Wildchar.

    g) Is Value Expression Regex – Set to either ON or OFF
    h) Value Expression – Provide the value expression for the rule.

4. To enabled Learning, select the OFF / ON option for your desired configuration.
5. Click **Save**.

### Signatures

The Signatures section allows you to designate specific, configurable rules to simplify the task of protecting your websites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, web server, website, XML-based web service, or other resource.

### Standard signatures

The Standard Signatures section displays a preconfigured set of literal and Perl Compatible Regular Expressions (PCRE) keywords and special strings used to protect against common web vulnerabilities. These configured signatures cannot be edited as they are our default configurations.

1. Select the Signatures tab, and then select the Standard Signatures option.
2. The Configured Signatures section displays any Signatures that have been selected or added to the WAF Profile Policy you are currently viewing or creating.
    a) For a new policy, this section is empty.
3. In the Signatures Pool section, you see the list of pre-configured signatures that we have created for you. You can use the arrows or page number options to view more signatures, or use the Filter option if you are looking for a specific signature.
    a) The filter option searches for your criteria across each field (ID, Category, Description, References), and return the results accordingly.
4. Click the View icon to see a simplified overview of the Signature Pool, or click the Add
   to Add the Signature Pool to your Configured Signatures section.
5. Click the Save button once you have added your desired signatures

### Custom signatures

The Custom Signatures section allows you to craft custom signatures to protect against attacks and vulnerabilities.

1. Select **Custom Signatures**.
2. Click **Add**.
3. Select the Action type for the signature.
    a) Block & Log
    b) Log
    c) None

4. Provide the category type for the signature.
5. Provide a description for the custom signature
6. Optionally, you can configure the Request Rules and/or the Response Rules.
    a) Request Rules inspect only on the request, and Response Rules inspect only on the response.
7. For the Request Rules, click the Start button, and then select the Area type from the drop-down menu. This determines the additional fields that you will be required to complete.
    a) You can click the Plus Icon to add another row or entry, or the Minus Icon to remove the selected row
8. For the Response Rules, click **Start**, and then select the Area type from the drop-down menu. This determines the additional fields that you will be required to complete.
    a) You can click the Plus Icon to add another row or entry, or the Minus Icon to remove the selected row.
9. To cancel the creation of Request or Response Rules, click **Allow X** next to Response Rules to remove them from your custom signature.
10. Click the Commit button when you are finished configuring your signature.
11. Click the Save button when you have finished configuring your WAF Profile Policy

#### Associate CWAAP profile to an asset

Once you have created your CWAAP profile, the next step is to apply it to an asset so that your configuration can go into effect.

1. From the Configuration section on the left-hand navigation menu, select Assets.
2. Select the Pencil Icon for the Asset that you want to add the policy to. If you do not have an Asset already created, please see our Guides on how to Create an Asset.
3. Select the Policies tab.
4. From the drop-down menu, select your newly created Policy name.
   a. If you do not see the policy name listed, please refresh and try again as the provisioning period can take a few minutes.
5. Click the Save button.

Once your CWAAP policy has been applied to a policy, please allow a few minutes for provisioning to occur.

### Edit a WAF policy

Once a Policy has been created, you can easily edit any of the existing configurations. However, changes to a Policy that has been associated to an Asset causes a provisioning period to occur which can have a temporary impact on your traffic configuration.

1. From the Configuration section on the left-hand navigation menu, select Policies.

2. Click the Pencil Icon next to the policy you want to edit.
3. Navigate through each of the Policy Configuration tabs to make changes, and click the Save button after making changes on any/all tabs.

### Delete a WAF policy

If you need to remove a CWAAP Policy from an Asset, there are several ways in which you can accomplish this.

> Note:
>
> 1. From the Configuration section on the left-hand navigation menu, select Policies.
> 2. Click the Pencil Icon next to the policy you want to delete.
> 3. Click Delete.

### Disassociate assets from a WAF policy

From the Policy, you can disassociate the Assets that the policy is assigned to, or disable the WAF Profile.

1. From the Configuration section on the left-hand navigation menu, select Policies.
2. Click **Pencil** Icon to edit the policy.
3. On the **WAF Profile** tab, clear the box under the "Apply WAF Profile to Policy?" section to Ignore. This disables the WAF profile.

OR

1. From the **Policy Configuration** screen, select the **Assets** tab.
2. Select the Minus Icon to remove the selected Asset.
3. Click **Save**.

#### Edit an asset

From the **Asset** section, you can edit a selected Asset and remove the Policy.

1. From the Configuration section on the left-hand navigation menu, select **Assets**.
2. Click the **Pencil** Icon next to the asset you want to edit.
3. Select **Policies** tab.
4. Hover over the drop-down menu and click **Minus** Icon to remove the associated Policy.
5. Click **Save**.

# Asset configuration

June 17, 2021

The following steps enable you to configure a proxy asset.

From the CWAAP NG Dashboard, select the Configuration option at the left side of the screen – A new set of options become available. Select **Proxy** from the list. The list of configured proxy services displays, if any exist.

## To configure a proxy asset

1. Click the Configure New Proxy button at the top right of the screen. The Configure New Proxy screen will be displayed.
2. Provide the Proxy Name – The host name that you must proxy.
3. Enter the front end Port and bind it to a corresponding back-end Origin Server, Port, and Protocol. Back-end Origin Servers can be an IP Address, CNAME, or host name and Multiple back-end Services per VIP.

> **Note:**
>
> Matching back-end ports load balance between the back-end services using a 'Least Connection' method.

1. Once you have entered all the host information, you must assign the Advanced Options for your Proxy configuration.
   a) LoadBalancer Balance Method: Indicate which option you want to use for load balancing. You have the following options for load balancing.
      i. Least Connection: Selects the service with the least number of active connections to ensure that the load of the active requests are balanced on the services.
      ii. Round Robin: Responds to DNS requests not only with a single potential IP address, but with one out of a list of potential IP addresses corresponding to several servers that host identical services. The list is cycled through in a "round-robin" style, selecting each address and moving onto the next for subsequent requests.
      iii. Least Response Time: Selects the service with the least number of active connections and the least average response time.
      iv. Least Bandwidth: Selects the service that is currently serving the least amount of traffic, measured in megabits per second (Mbps).
      v. Least Packets: Selects the service that has received the fewest packets in the last 14 seconds.
      vi. Least Request: Selects the service that has received the fewest requests in the last 14 seconds.

Lowest Response Time:

vii. URL Hash: The Citrix ADC generates a hash value of the HTTP URL present in the incoming request. If you select a service by the hash value as DOWN, the algorithm has a method to select another service from the list of active services. The NetScaler caches the hashed value of the URL, and when it receives subsequent requests that use the same URL, it forwards them to the same service. If the NetScaler cannot parse an incoming request, it uses the round robin method for load balancing instead of the URL hash method.

viii. Domain Hash: Uses the hashed value of the domain name in the HTTP request to select a service. The domain name is taken from either the incoming URL or the Host header of the HTTP request. If the domain name appears in both the URL and the Host header, the NetScaler gives preference to the URL.

ix. Destination IP Hash: Uses the hashed value of the destination IP address to select a server. You can mask the destination IP address to specify which part of it to use in the hash value calculation, so that requests that are from different networks but destined for the same subnet are all directed to the same server.

x. Source IP Hash: Uses the hashed value of the client IP address to select a service.

xi. Source IP & Destination Hash: Uses the hashed value of the source and destination IP addresses to select a service. This ensures that all packets flowing from a particular client to the same destination are directed to the same server.

xii. Source IP & Source Port Hash: Uses the hash value of the source IP (either IPv4 or IPv6) and source port to select a service. This ensures that all packets on a particular connection are directed to the same service.

b) LoadBalancer Persistence Type: Select the session persistence type for HTTPS requests. Select either Source IP or Cookie Insert.

c) X-Forwarded For Header: Enter the name of the header to use for forwarding HTTPS requests.

2. After completing the advanced options settings click **Save**.
3. Your new Proxy configuration is displayed.

## Manage existing asset configuration

From the **Proxy Assets** screen click the “Edit Icon” next to the host name field of the configuration you want to update. The update configuration screen will be displayed. Here you can make any changes you want make and click **Save** to submit the updated configuration. From this screen, you can also Delete the configuration by selecting the “Delete” button at the top right of the screen.

# SSL certification

June 17, 2021

To access SSL Certificates:

1. In the dashboard, select **Configuration -> Security -> SSL Certificates** on the left navigation bar.
2. The **SSL Certificates** page shows all the active SSL Certificates associated with your account.
3. To add a new SSL certificate, click **Add New Certificate**.
4. A prompt window appears allowing you to provide the SSL Certificate information:
   - Private Key – Upload or paste the Private Key information. Currently accepts either 2048 bit or 3072 bit RSA key in the PEM format.
   - Private Key Password (optional) – Provide the password associated with the Private Key
   - Public Certificate Chain – Detect, Upload, or Paste the Public Certificate. If you choose the Detect option, provide the publicly accessible HTTPS URL. Otherwise, upload or paste your public server certificate, followed by all intermediate certificates, in the PEM format.

## SSL requirements

The minimum requirements for CWAAP SSL certificates are RSA 2048 bit or 3072 keys. This is a requirement of the FIPS devices.

### Upload SSL certificate

To submit your SSL certification to the portal, you need the following information:

- Private Key
- Private Key Password
- Public Certificate Chain

You can upload your Private Key and your Public Certificate Chain. Also, you can also detect your Public Certificate Chain by providing the URL. You should also provide the Private Key Password, so the SSL certificate can be used.

### SSL certificates and components

There are four different ways to present SSL Certificates and their components:

1. **PEM**. Governed by RFCs, it's used preferentially by open-source software. It can have various extensions (.pem, key, .cer,.cert, more)

2. **PKCS#7 or P7B**. An open standard used by Java and supported by Windows. Does not contain private key details.
3. **PKCS#12 or PFX**. A Microsoft private standard that was later defined in an RFC that provides an enhanced security versus the plain-text PEM format. The format might contain the private key material. It's used preferentially by Windows systems, and are freely converted to the PEM format by using `openssl`.
4. **DER**. The parent format of PEM. It's useful to think of it as a binary version of the base64-encoded PEM file. Not routinely used by much outside of Windows.

> **Note:**
>
> Cirix highly recommends you to convert the `.pfx` files on your own machine using `OpenSSL` so you can store the private key.

Use the following `OpenSSL` commands to convert the SSL certificate in different formats on your own machine:

1. Convert DER to `PEM: openssl x509 -inform der -in certificate.cer -out certificate.pem`
2. Convert P7B to `PEM :: openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer`
3. Convert PFX to `PEM :: openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes`

Alternatively, you can use the free SSL converter available at SSL Shopper.

### Manage existing proxy configuration with SSL

From the **Proxy Assets** screen click the "Edit Icon" next to the host name field of the configuration you want to update. The update configuration screen displays. Here you can make any changes you want make and click **Save** to submit the updated configuration. From this screen, you can also **Delete** the configuration by selecting the "Delete" button at the top right of the screen.

### Validate your proxy configuration with SSL

To test your website using your own domain name `BEFORE DNS` propagation has completed, you can use your local computer's `HOSTS` file. Your computer uses the entries in your `HOSTS` file FIRST before it tries to use your IPS to look up the DNS information for your domain.
The `HOSTS` file is a special file on your workstation computer that stores the IP address and name information. You must check the file before DNS, so if you place an entry in this file it supersedes anything set in DNS. This feature is useful in testing websites as it allows you to control which IP your local computer visit regardless of the DNS configuration.

### Hosts file syntax

The format of the hosts file is simple. Each line has an IP address and a host name separated by one or more spaces. By default, hosts files typically contain entries for "localhost" and text describing the file usage. It is best not to change the description.

**Example:**

```
1.2.3.4 example.com
1.2.3.4 www.example.com
<!--NeedCopy-->
```

### Windows

1. From the Start drop-down list, search for "Notepad" (Win 8, 10) or navigate to: "All Programs -> Accessories -> Notepad" (Win XP, Vista, 7).
2. Right-click Notepad and select the **Run As Administrator** option.
3. In Notepad, click "Open" and select the file option. `C:\\Windows\\System32\\Drivers\\etc\\hosts`.
4. Edit the file and click **Save**.

### Linux

1. Open a terminal window.
2. Edit the file `/etc/hosts` as root with a text editor. Example: `sudo nano /etc/hosts`

### Testing your settings

1. Open a command prompt.
2. Type: `ping -c2 example.com`
3. The ping results show the IP address and confirm that it is responding.
4. Open the browser on the local computer where the host settings are available. The browser connects to the website.

> **Note:**
>
> When you are finished testing, remember to remove the custom lines that you added to your Hosts file.

# Analytics

May 27, 2021

The analytics page enables you to view the analytics details. Following are the options:

Attack Map – A real time geographical representation of scrubbed traffic.
Routed – Information related to your Routed Traffic.
Proxy – Information related to your Proxy Configuration.
WAF Violations – Information related to your WAF Profile.

## Attack map

This is a geographical representation of web attacks related to your network in real-time. The table shows the detected IP address, attack types, and source location. For information about the attacks related to your network, you can select a service type - Routed, Proxy, or WAF.

## Routed

The Routed page enables you to view your traffic by IP Address, Autonomous Systems Number, or TCP Flags by IP. For detailed information about the traffic, select one of the options from the left navigation bar.

- IP Address. Recently routed traffic by the attack target IP address.
- Autonomous Systems. Recent violations by the ASN.
- TCP Flags by IP. Recent violations by the attack Target IP address.

## Proxy

The Proxy page enables you to view your traffic by Domain, Geolocation, IP Address, URL Path, or User Agent.

- Domain - Recent traffic attack by the target domain.
- Geolocation - Recent violations by the attack source country.
- IP Targets - Recent violations by the attack target IP address.
- URL Path - Recent violations for the URL path.

## WAF violations

The **WAF Violations** section enables you to provide detailed information for your WAF mitigation profile. The following options are available to view your WAF violations details:

• Violation logs
• Violation types
• Domain targets
• Geolocation
• IP targets
• URL path

Select an option to view detailed traffic information and charts for your WAF profile. You can also export the information to your records.

### Violation logs

The **Violation Logs** screen displays the list of violations handled by your WAF profile. The default date range is the last day, however you can assign longer date range by selecting a value from the date range field. You can also export the Violation log by using the export option.
The Violation list shows a high-level description of the violation details. For more information, click the (+) icon for the violation you prefer to examine.

### Violation types

The WAF Violation Types page enables you to view all the recent violations by their Violation type. This page has a table and a graphical representation. You can select the date range to filter your search. You can also export the graph as an image or PDF and you can export the table as a csv or json file by using the export option.

## Alerts

May 27, 2021

The Alerts page displays a list of alerts that you have triggered. The alerts are displayed in a table highlighting the following features:

- Alert Type - Indicates the level of the attack (Low, Medium, High)
- Attack Type – Indicates the type of attack
- Destination – The destination IP
- Start Time – The time the alert was triggered
- End Time – The time the alert traffic was no longer a threat
- Duration – The time the alert was active
- Status – The status of the alert
- Report – A PDF containing a report on the Alert

### Traffic

The Traffic page displays a graph representation of the traffic for the monitored network.

## Routed

May 27, 2021

On the Routed page, you can view your traffic by IP Address, Autonomous Systems Number, TCP Flags by IP address. For more information, select an option from the left pane.

### IP address

The IP Address page displays all the recent Routed traffic by the attack source IP address. This page is categorized into four sections – a table representation and three graphical representations (Line, Pie, Bar charts). You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also view this information broken down into Aggregate In, Clean In, or Mitigated traffic. You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### Autonomous systems

The Autonomous Systems page displays all the recent traffic by the attack source ASN. This page has four sections – a table representation and three graphical representations (Line, Pie, Bar charts). You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also view this information broken down into Aggregate In, Clean In, or Mitigated traffic. You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### TCP flags by IP

The TCP Flags by IP page display all the recent TCP Flags for the attack source IP address. This page has four sections – a table representation and three graphical representations (Line, Pie, Bar charts). You can set the date range as 1 hr, 3 hr, 1 day, 7 day, 30 day, or 90 day. You can also view the details as Aggregate In, Clean In, or Mitigated traffic. You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

## Assets

June 28, 2021

The Assets feature display your network traffic by domain, geolocation, IP address, URL path, or user agent. For detailed information about your traffic, select an option from the left pane.

### Domain

The Domain page displays all the recent attack traffic by the attacks target domain. This page displays the data in a tabular and graphical format. You can set the date range as, 1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day and so forth. You can also export the graphical data as an image or PDF and you can export the table as a csv or json file.

### Geolocation

The Geolocation page displays all the recent violations by the attack source country. The page displays the data in a tabular and graphical format. You can set the date range as, 1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day and so forth. You can also export the graphical data as an image or PDF and you can export the table as a csv or json file.

### IP Address

The IP Address page displays all the recent violations by the Destination IP. This page is broken into two sections – a table representation and a graphical representation. You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export option buttons above the data.

### URL Path

The URL Path page displays all the recent violations for the URL path. This page is broken into two sections – a table representation and a graphical representation. You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### Manage asset configuration

From the Assets page, click **Edit** next to the host name field of the configuration you prefer to update. The update configuration screen will be displayed. Here you can make any changes you want make and click **Save** to submit the updated configuration.

### Validate your asset configuration

To test your website using your own domain name `BEFORE DNS` propagation has completed, you can use your local computer's `HOSTS` file. Your computer uses the entries in your `HOSTS` file first before it tries to use your ISP to look up the DNS information for your domain.
The `HOSTS` file is a special file on your workstation computer that stores IP address and name information. This file is checked before DNS, so if you place an entry in this file it supersedes anything set in DNS. This feature is useful in testing websites as it allows you to control which IP your local computer visits regardless of what is set in the DNS. The format of the `HOSTS` file is simple. Each line has an IP address and a host name separated by one or more spaces. By default, hosts files typically contain entries for the local host and some comment text describing the file and its use. It is best not to change any of these lines.

**Example:**

```
1.2.3.4 example.com
1.2.3.4 www.example.com
<!--NeedCopy-->
```

**Windows:**

1. From the **Start** menu, search for "Notepad" (Win 8, 10) or navigate to: `All Programs ->` Accessories -> Notepad (Win XP, Vista, 7)'.
2. Right-click Notepad and select `Run As Administrator`.
3. In Notepad, click "Open" and select the file - `C:\Windows\System32\Drivers\etc\hosts`.
4. Edit the file and save.

**Linux:**

1. Open a terminal window.
2. Edit the file `/etc/hosts` as root with a text editor. Example: `sudo nano /etc/hosts`.

**Validate your Settings:**

1. Open a command prompt.
2. Type: `ping -c2 example.com`
3. The ping results show the IP address and confirm that it is responding.
4. Open your browser on the local computer where the host settings have been configured. The browser
   is now connected to the website.

> **Note:**
>
> When you are finished testing, remember to remove the custom lines that you added to your Hosts file.

## WAF

October 21, 2021

The WAF section gives violation details for your mitigation profile. The following options enable you to view your WAF violation details:

- Violation Logs
- Violation Types
- Domain Targets
- Geolocation
- IP Targets
- URL Path

Select an option to view traffic details and graphical representation for your WAF profile. You can also export the details for your records.

### Violation logs

The Violation Logs page displays all the violations handled by a WAF profile. The default date range is the last day, however, you can select a date to display one of the range options (Today, Yesterday, Last 7 Days, Last 30 Days, This Month, Last Month, Custom Range). You can also export the Violation log by using the export option.

The Violation list is compiled in a table showing the high-level description of a violation (Action, Date/-Time, Source IP, and Reason). To view more information, click (+) for the violation you want to examine further.

### Violation types

The WAF Violation Types page displays all the recent violations by their Violation type. This page has two sections – a table and a graph. You can set the date range from the following options (1 hr, 3 hr, 1day, 7day, 30day, 90day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options

The table view lists all the violation types sorted by the number of requests for each respective request.

## Access violation logs

The CWAAP violation logs display a comprehensive overview of violations in direct contrast to bot protection techniques that have been implemented to log or block specific requests that were captured for your account.

To access the violation Logs, using the left-hand navigation menu, select Analytics, then WAF, Logs, and then violation Logs from the drop-down list.

Following are the violation log menus available in the drop-down list.

### Application

The Applications drop-down menu allows for the selection of a custom configured asset (or all Assets) for your account. By default, the All Assets (Combined) application will be selected.

### Date range menu

The Date Range filter provides two methods of customizing the data that is displayed on the WAF Dashboard.

### Custom date range

Clicking on the displayed date range selection will open the pop-out calendar window, which allows you to select a beginning and end date, as well as selecting a custom time range as well.
Clicking the calendar icon allows you to quickly navigate through months, as well as years to select the beginning and end dates. Additionally, you can manually type in the desired date instead of using the calendar option.
The maximum number of days in the past that can be captured is ninety (90) days from the current date.
Click the green checkmark icon once you have selected your custom time frame to view the results

### Quick select date range

Instead of creating a custom time frame for your dashboard results, you can use one of the preconfigured quick select date range options. By default, the Dashboard will display the results for the previous seven days (7D).

- 1H - Displays the result details for the previous hour.
- 3H - Displays the result details for the previous three hours.
- 12H - Displays the result details for the previous twelve hours.
- 1D - Displays the result details for the previous calendar day.

- 7D - Displays the result details for the previous seven calendar days (week).
- 30D - Displays the result details for the previous thirty days (calendar month).

#### Field and text

The Field and Enter Text options enable custom search filters to be created to display your Violation Log details.

The Field drop-down menu has the following criteria options:

- All
- Source IP
- Timestamp
- Host
- Country
- User-Agent
- City
- Action
- Reason
- Domain
- URI
- Transaction ID
- Event ID
- Site
- Signature

> Note:
>
> - The URI and User-Agent fields are case-sensitive.
> - The maximum search number of characters allowed in the Search field is 90

### Export violation logs

The Violation Logs that are currently displayed on the screen (which includes any configured filters) can be exported in either a:

1. CSV file
2. JSON output

Clicking on either of the download options will display a greyed-out cloud icon as the file is compiled. Once the cloud icon becomes clickable, the file will begin to download

#### Violation log details

The Violation Log Details table displays a comprehensive overview of the violation that was captured, with hyperlinked content that will navigate you to the Enrichment section, for additional details.

| Action type | Response type |
|---|---|
| Action | Displays the action taken for the violation. Either Logged or Blocked |
| Timestamp | Displays the timestamp (as UTC) in which the violation was captured |
| Application | The Application name impacted by the violation. |
| Source IP | The specific Source IP belonging to the application that was impacted by the violation |
| Country | The country in which the traffic was originating from that triggered the violation. |
| Reason | A brief explanation about the violation, as well as what type of violation was triggered. |

#### Additional Features

A brief explanation about the violation, as well as what type of violation was triggered.

#### View Details

The View Details feature displays a more detailed overview of the violation details. Clicking on the Policy hyperlink will redirect you to the Configuration - Policies section of your account.

The double paper icon is a copy + paste option, as doing a manual copy and paste of the details may not work as the details may be truncated on the page.

#### Add IP Filter

Selecting the Add IP Filter button will add the selected IP address to the Blocklist for the account. On the pop-out window, the IP / CIDR address will be listed (which can be edited), as well as an indicator for Blocked (selected by default), or Not Blocked.
Once you click Save, the IP address filter will be added to your policy (which can be found in the View Details section).

**Create Relaxation Rule**

Selecting the Create Relaxation Rule will add the selected violation log entry to the allowed list for the account. The Violation Reason will determine the possible configuration settings for the Relaxation Rule.

Once you click the Save button, the Relaxation Rule will be added to your configured policy (which can be found in the View Details section

### Domain targets

The Domain Targets page displays all the recent violations by the attacks target domain. This page has two sections – a table representation and a graphical representation. You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### Geolocation

The Geolocation page displays all the recent violations by the attack source country. This page has two sections – a table representation and a graphical representation. You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### IP targets

The IP Targets page displays the recent violations by the attack Target IP address. The page has two sections – a table and a graph. You can set the date range from the following options (1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day). You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

### URL path

The URL Path page displays all the recent violations for the URL path having the most blocked or logged violations. This page has two sections – a table and a graph. You can set a date from the following options - 1 hr, 3 hr, 1 day, 7 day, 30 day, 90 day. You can also export the graph as an image or PDF and you can export the table as a csv or json file by selecting the export options.

## Enrichment

June 17, 2021

The CWAAP WAF enrichment section displays an enhanced overview for a selected destination IP address, Source IP address, or country.

The Enrichment details provided include:

- IP Intelligence Results
- Violation Logs - Graphical Data
- Violation Type - Graphical Data
- Violation Log Details

## Field and Search Options

To display results for a specific field type, use the **Select Field** drop-down menu and select one of the following.

- Destination IP
- Source IP
- Country

In the **Search** field, provide either IP address or the desired Country to return results for

## Date Range Filter

The Date Range filter provides two methods of customizing the data that is displayed on the WAF Dashboard.

### Custom Date Range

The displayed date range selection field opens the pop-out calendar window, which allows you to select a beginning and end date, and selecting a custom time range as well.

Clicking the calendar icon allows you to quickly navigate through months, and years to select the beginning and end dates. Also, you can manually type in the desired date instead of using the calendar option.
The maximum number of days in the past that can be captured is 90 (90) days from the current date.
Click the green checkmark icon once you have selected your custom time frame to view the results

### Quick Select Date Range

Instead of creating a custom time frame for your dashboard results, you can use one of the preconfigured quick select date range options. By default, the Dashboard displays the results for the previous seven days (7D).

- 1H - Displays the result details for the previous hour.

- 3H - Displays the result details for the previous three hours.
- 12H - Displays the result details for the previous 12 hours.
- 1D - Displays the result details for the previous calendar day.
- 7D - Displays the result details for the previous seven calendar days (week).
- 30D - Displays the result details for the previous 30 days (calendar month).

### IP Intelligence Results

The **IP Intelligence Results** section displays an overview of the selected IP Address details. The IP Intelligence details are powered by the CWAAP IPR (IP Reputation) Service.

### Violation Logs

The **Violation Logs** section displays a graphical representation of the last six days and the number of violations that occurred per day.

### Violation Type

The **Violation Type** section displays a graphical representation of the offending violation types and the total number of violations that occurred in correlation to the Violation Log timeframe.

### Violation Logs Details

The Violation Log Details table displays a comprehensive overview of the violation that was captured for the selected IP Address or Country for the date range identified in the Violation Logs graph.

### Additional Features

Each Violation Log entry in the table has more features that can be utilized to further enhance the usage of the Violation Log details.

#### View Details

The View Details feature displays a more detailed overview of the violation details. Clicking the Policy URL will redirect you to the Policy Configuration page for the policy that generated the violation log.

The blue "i" icon shows the full path details that might be condensed on the **Violation Log Details** screen due to length restrictions.

The double paper icon is a copy + paste option, as doing a manual copy and paste of the details might not work as the details might be truncated on the page.

Click the **Show Raw Headers** icon to view all of the Raw Headers.

### IP Filter

Selecting the **Add IP Filter** button will add the selected IP address to the Blocked list for the account. On the pop-out window, the IP / CIDR address is listed (which can be edited), as well as an indicator for Blocked (selected by default), or Not Blocked.
Once you click **Save**, the IP address filter will be added to your policy (which can be found in the View Details section).

### Relaxation Rule

Selecting the Create Relaxation Rule adds the selected violation log entry to the allowed list for the account. The Violation Reason will determine the possible configuration settings for the Relaxation Rule.
Once you click the **Save** button, the Relaxation Rule is added to your configured policy (which can be found in the **View Details** section.

# Responder policy logs

June 17, 2021

The **Responder Policy Logs** section displays an overview of Response Policies that have been configured and triggered.

## Access to responder policy logs

To access the CWAAP responder policy logs, use the left-hand navigation menu and select **Analytics**, then WAF, Logs, and then Responder Policy Logs.

### Responder policy logs filtering

The Responder Policy Logs filter option has a drop-down menu that allows you to select any configured Asset or VIP for your account. By default, the All Assets (Combined) is selected.

### Export responder policy logs

The Responder Policy Logs displayed on the screen can be exported into either a .PDF file, or in a JSON file.

### Date range configuration

The Responder Policy Log has various default time range configurations, and the option to create a custom time range to retrieve the Responder Policy Logs.

- Today
- Yesterday
- Last 7 Days
- Last 30 Days
- This Month
- Last Month
- Custom Range

The Custom Range can be up to ninety (90) days in the past.

### Responder policy log details

The Responder Policy Log Details table provides an overview of the policy by displaying the following details.
Each field has a sort option that sorts the results either in ascending or descending order (either alphabetical or numerical depending on the column details).

| Name | Description |
|---|---|
| Responder Action | Displays the Action taken. Either Log or Block. |
| Source IP | Displays the IP Address where the traffic originated. |
| Destination IP | Displays the IP Address of the intended destination. |
| Port | Displays the port number. |
| Method | Buffer Overflow is one of the best-known forms of software (security) vulnerability. Buffer overflows can be used to corrupt the execution stack of a web application. “Sending carefully crafted input to a web application, an attacker can cause the web application to run arbitrary code – effectively taking over the machine.” |
| Method | Displays the Method type (GET, POST, and so forth) |
| Host | Displays the IP Address of the configured host. |

| Name | Description |
|---|---|
| URI | |
| Site | |
| Date/Time | Displays the time in which the incident occurred (in UTC). |

# Violation logs

October 21, 2021

The **CWAAP Violation Logs** section displays a comprehensive overview of violations in direct contrast to counter measures that have been implemented to log or block specific requests that were captured for your account.

## Accessing the CWAAP violation logs

To access the Violation Logs, using the left-hand navigation menu, select **Analytics**, then WAF, Logs, and then Violation Logs from the drop-down list.

## Applications

The **Applications** drop-down menu allows for the selection of a custom configured asset (or all Assets) for your account. By default, the All Assets (Combined) application is selected.

## Date range

The Date Range filter provides two methods of customizing the data that is displayed on the WAF Dashboard.

### Custom date range

Clicking the displayed date range selection opens the pop-out calendar window, which allows you to select a beginning and end date, and selecting a custom time range as well.
Clicking the calendar icon allows you to quickly navigate through months, as well as years to select the beginning and end dates. Also, you can manually type in the desired date instead of using the calendar option.

The maximum number of days in the past that can be captured is 90 (90) days from the current date. Click the green checkmark icon once you have selected your custom time frame to view the results.

#### Quick select date range

Instead of creating a custom time frame for your dashboard results, you can use one of the pre-configured quick select date range options. By default, the Dashboard displays the results for the previous seven days (7D).

- 1H - Displays the result details for the previous hour.
- 3H - Displays the result details for the previous three hours.
- 12H - Displays the result details for the previous 12 hours.
- 1D - Displays the result details for the previous calendar day.
- 7D - Displays the result details for the previous seven calendar days (week).
- 30D - Displays the result details for the previous 30 days (calendar month).

### Field and text

The Field and Enter Text options enable custom search filters to be created to display your Violation Log details.

The field drop-down menu has the following criteria options.

- All
- Source IP
- Timestamp
- Host
- Country
- User-Agent
- City
- Action
- Reason
- Domain
- URI
- Transaction ID
- Event ID
- Site
- Signature

> **Note:**

> - The URI and User-Agent fields are case-sensitive.
> - The maximum search number of characters allowed in the Search field is 90.

### Export options

The Violation Logs that are currently displayed on the screen (which includes any configured filters) can be exported in either a:

1. CSV file
2. JSON output

Clicking either of the download options display a grayed-out cloud icon as the file is compiled. Once the cloud icon becomes clickable, the file begins to download

### Violation log details

The Violation Log Details table displays a comprehensive overview of the violation that was captured, with hyperlinked content that will navigate you to the **Enrichment** section, for more details.

| Action Type | Response Type |
|---|---|
| Action | Displays the action taken for the violation. Either Logged or Blocked. |
| Timestamp | Displays the timestamp (as UTC) in which the violation was captured. |
| Application | The Application name impacted by the violation. |
| Source IP | The specific Source IP belonging to the application that was impacted by the violation. |
| Country | The country in which the traffic was originating from that triggered the violation. |
| Reason | A brief explanation about the violation, and what type of violation was triggered. |

### More features

Each Violation Log entry in the table has more features that can be selected.

#### View details

The View Details feature displays a more detailed overview of the violation details. Clicking the Policy hyperlink will redirect you to the Configuration - Policies section of your account.

The blue “ i “ icon shows the full path details that might be condensed on the **Violation Log Details** screen due to length restrictions.

The double paper icon is a copy + paste option, as doing a manual copy and paste of the details might not work as the details might be truncated on the page.

### IP filter

Selecting the **Add IP Filter** button adds the selected IP address to the Blocked list for the account. On the pop-out window, the IP / CIDR address is listed (which can be edited), and an indicator for Blocked (selected by default), or Not Blocked.
Once you click **Save**, the IP address filter is added to your policy (which can be found in the View Details section).

### Relaxation rule

Selecting the Create Relaxation Rule adds the selected violation log entry to the allowed (or listed) list for the account. The Violation Reason will determine the possible configuration settings for the Relaxation Rule.
Once you click the **Save** button, the Relaxation Rule is added to your configured policy (which can be found in the **View Details** section.

## Bot

October 19, 2021

The bot analytics gives insights about bot attacks and its violations occuring in your web applications. The bot analytics details you about the bot dashboard details and bot logging details.

## Bot dashboard

October 21, 2021

The bot analytics dashboard provides graphical insights to bot analytics and violation details. You can access the Bot Dashboard on the CWAAP portal to view the bot analytics.

The dashboard displays the details based on the application that you select from the drop-down list. When you select an application, the bot analytics such as violation type, IP address, URL path, or Geolocation are displayed in graphical format. You can selecta analytics type to navigate the log section.

## Applications

The Applications menu allows you to select a configured asset (or all assets) for your account that has CWAAP Bot enabled. By default, the "All Assets (Combined)" application is selected.

If a selected application has no violation details, the section does not display any graphical data.

## Date range filter

The Date Range filter provides two methods for customizing the data to display on the CWAAP Bot dashboard.

### Custom date range

The data range picker icon enables you to select a start and end date or select a custom time range.

The calendar icon allows you to quickly navigate through months, as well as years to select the beginning and end dates. You can also manually enter a date.

> **Note:**
>
> The maximum number of days in the past that can be captured is ninety (90) days from the current date.

### Quick Select Date Range

Instead of creating a custom time frame for your dashboard results, you can use one of the preconfigured quick select date range options. By default, the dashboard displays results for the last seven days (7D).

1H - Displays the result details for the previous hour.
3H - Displays the result details for the previous three hours.
12H - Displays the result details for the previous twelve hours.
1D - Displays the result details for the previous calendar day.
7D - Displays the result details for the previous seven calendar days (week).
30D - Displays the result details for the previous thirty days (calendar month).

Each of the field types displayed in each section is a clickable link that enables you to navigate to the Violation Logs section of the CWAAP portal.

Additionally, each of the results per insight chart is sorted in descending order based upon the number of requests.

### Violation types

The Violation Types section displays an insight chart of bot Violations that are captured by bot protection techniquesmeasure type and the total number of requests received for each bot violation type.

The Violation Type chart allows you to hover over a colored section to display the violation type and request count.

### Domain target

The Domain Target section displays the IP Address for the domain(s) that were impacted by the captured violations, as well as the total number of requests that were captured.

### IP targets

The IP Targets section highlights the specific IP addressess that are impacted, within the targeted Domain(s) for the captured violations. Also it displays the total number of requests that each IP address receives.

### URL path

The URL Path section displays various URLs that are targeted and the total number of requests for each URL path. The blue "i" icon next to a URL displays the full URL path name.

### Geolocation

The Geolocation section displays the geographical region of the bot violation and also the number of requests that are captured.

## Bot logging

October 21, 2021

The CWAAP Bot Logs section displays an overview of counter measures and associated violations that have been configured and triggered. The log type identifies an entry as either a "Violation" or as "Info."

> **Note:**
>
> The CWAAP bot configurations do not trigger a violation log entry, as they are not technically violations. However, these events are included in the "Requests" count on the bot dashboard.

Following is a list of bot protection techniques and its associated log entry.

| Bot technique | log |
|---|---|
| BOT_Allowlist | "Allow list" |
| BOT_CAPTCHA | Wait time: "Captcha max wait time", Invalid Captcha: "Invalid Captcha Submission. |
| BOT_TRAP_URL | Trap URL: "Trap URL Request" |
| BOT_DEVICE_FINGERPRINT | Bot Log: "Device Fingerprint Bot Request" |
| BOT_STATIC_SIGNATURE | "Bot signature matched" - Type: GOOD (Action: LOG) |

To view the CWAAP analytics, select **Analytics** from the left-hand navigation menu, select **BOT**, and then select **Logs**.

## Bot log filter

The CWAAP bot logs filter option has a drop-down menu that allows you to select any configured Asset for your account. By default, the All Assets (Combined) is selected.

### Log types

The **Log Type dropdown** menu allows you to select either:

- All
- Info
- Violation

### Field and text

The **Field search** menu allows you to select a specific Field or Value type to display the CWAAP results for.

- All
- Source IP
- Destination IP

- Host
- URI
- counter measure
- Action
- Reason
- Domain
- Profile
- Node
- Transaction ID
- Timestamp
- Country
- City

After selecting the field type, you can provide the matching search criteria in the **Enter Text** field to further narrow down your search results.

### Bot log export

The CWAAP bot logs displayed on the screen can be exported into either to a PDF or a JSON format.

### Bot log violation

The results displayed in the **Bot Violation Logs** section capturex details to identify the violation, protection technique and bot action applied for the violation.

Each entry captures the action that was taken (due to bot protection techniques configuration), the impacted policy, the offending Source IP address, the originating country for the offending IP, and the reason for the bot protection techniques to occur.
Clicking Application, Source IP, or Country links take you to the Enrichment details page, that displays the detailed description for each these parameters.

For example, clicking the Source IP address link displays the IP Intelligence Results enrichment page, and provides identifying information that is associated with the offending IP address.

## Events

October 21, 2021

1. Select **Services** from the top navigation options, and then click **Mitigation Events**. A list of all Mitigation Events for the account is displayed with the following details:

  - Account
  - Start Date and Time
  - End Date and Time
  - Duration
  - Prefixes
  - Status
  - Chart

2. To view the details of a Mitigation event, click the chart icon.

3. Under the **Associated Mitigations** section, click the green arrow under the **More Details** section to view Traffic details.

4. The **Dropped Traffic** details display the type of bot protection techniquesmeasure using during the mitigation, and how what percentage of traffic was dropped due to that bot protection techniquesmeasure being implemented.

   - The total percentage of traffic dropped will equal 100% to denote the end of the Mitigation Event.

## FAQ

June 15, 2021

This section provides question and answers related to CWAAP functionalities.

1. What is Citrix CWAAP?

   Citrix CWAAP is a cloud service compatible from anywhere for applications to be hosted. Citrix WAF solution integrated with DDoS mitigation service, the combination provides a comprehensive, layered protection stack that proactively prevents bot-based volumetric attacks, and threats that target the application layer, such as SQL, cross-site scripting, CSRF, session hijacking, data exfiltration and zero-day vulnerabilities.

2. What does Web Application Firewall do in the CWAAP service?

   Citrix Web App Firewall monitors, filters, or blocks inbound and outbound web application traffic that has security attacks.

3. What does CWAAP DDoS protect?

   CWAAP DDoS protection is a DDoS mitigation service. CWAAP scrubs malicious Internet traffic, allowing clean, legitimate traffic to flow to your infrastructure.

4. What is a distributed denial-of-service (DDoS) attack?

A distributed denial-of-service (DDoS) attack is when multiple entities are operating together to attack one target. DDoS attackers often use the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities to control numerous devices using command and control software.

5. What is the goal of a DDoS attack?

   To exhaust network bandwidth, server resources, or applications in such a way that legitimate users cannot access a site. The purpose for such attacks, however, can vary widely.

6. What are the common Web Application Firewalls (wAF) techniques of Layer 7 attacks?

   - Cross-site scripting (cross-site scripting) is an injection attack in which an attacker injects malicious script into a web application.
   - Cross-site request forgeries (CSRF) trick end users into running state-change actions on a web app with which they are authenticated. Such attacks can instigate actions such as transferring funds or changing email addresses.
   - SQL injections are well-known exploits in which an SQL data is inserted into the query response from a client.

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States