FortiWeb Cloud - User Guide

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FortiWeb Cloud User Guide

TABLE OF CONTENTS

Overview

FortiWeb Cloud is a SaaS cloud-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero day threats, and other application layer attacks.

Requiring no hardware or software FortiWeb Cloud colony of WAF gateways run in AWS, Azure, OCI, and Google Cloud regions allowing to scrub your application traffic within the same region your applications reside addressing performance, regulation concerns and keeping traffic cost to minimum.

To get started protecting your applications, refer to Onboarding applications on page 47.

What's new

24.2 released on April 4, 2024

Enhanced bandwidth Usage insights

Detailed bandwidth and data usage insights with our new Usage page. Offers clear understanding of overall bandwidth and data consumption. For more information, see Usage on page 87.

Review and release blocked IPs

You can now view the list of blocked IP addresses and release them from your blocklist as needed. This provides greater flexibility and control over your network security settings. For more information, see Review and release blocked IP addresses on page 191.

Region IP update

A new scrubbing center will be live on the date of the upcoming release. Please make sure to allow access to your applications from the IP addresses listed below.

- GCP me-west1 (Tel Aviv)
  - 34.165.140.173
  - 34.165.109.6
  - 34.165.80.144
  - 34.165.254.142
  - 34.165.184.29
  - 34.165.1.25

24.1 released on Feb 1, 2024

Support for FortiADC Threat Analytics

FortiWeb Cloud now supports the analysis of attack logs from FortiADC, utilizing its advanced AI-based threat analytics system to provide cross-platform visibility. For setup information, see Forwarding FortiADC attack logs to Threat Analytics on page 95.

Splunk Version 9 support

You can now export Traffic Logs directly to the latest version of Splunk. This allows seamless ingestion and mapping of security and audit data collected from FortiWeb Cloud. For more information, see FortiWeb Cloud and Splunk on page 228.

23.4 released on Nov 16, 2023

Consumption report

A new Consumption report is now available, detailing data/bandwidth consumption for each application. Enable in **Global > Settings**. For more information, see Settings on page 77.

Security Fabric Support for FortiGate 7.x

FortiWeb Cloud devices can now be integrated into the Security Fabric of any FortiGate running 7.0.0 or newer. For more information, see Fortinet Security Fabric on page 236.

Redesign rewriting requests to support multiple rules

Rewriting Requests has been redesigned to support multiple actions in single rewrite rule. For more information, see Rewriting Requests on page 180.

Support signature exceptions for JSON format

Attack Log has been enhanced to support Exceptions for JSON format requests. You can specify JSON element in the exception rules in Known Attacks and Information Leakage.

Add RST_STREAM Restriction

FortiWeb Cloud has been enhanced to provide better protection for the HTTP/2 Rapid Reset Attack. A new Request Limit has been added that allows limiting the number of RST_STREAM per session. Configure it in **Access Rules>Request Limits**. For more information, see Request Limits on page 144.

Sub-user and Admin (Legacy) migration

FortiWeb Cloud will cease to support Sub-user and Admin (Legacy) accounts starting from version 24.1, which is scheduled for release in January 2024. To ensure uninterrupted access, kindly migrate Sub-user and Admin (Legacy) to IAM user in advance. Failure to do so may result in the them losing access to FortiWeb Cloud. For more information, see Migrating to IAM user on page 70.

23.3.a released on Sept 7, 2023

Region IP update

An additional AWS scrubbing center has deployed in the following region. Please make sure to allow access to your application from the IP addresses listed below.

- AWS il-central-1: Israel (Tel Aviv)
  - 51.17.26.125
    2a05:d025:c86:1702:3be9:6a28:de24:3589
  - 51.16.192.242
    2a05:d025:c86:1702:4ddf:2b90:a945:ea28
  - 51.16.118.151
    2a05:d025:c86:1701:39b:f35d:2126:5c85
  - 51.16.198.214
    2a05:d025:c86:1701:1eb6:57b5:dfe6:4cfb

FortiCloud Organizations (OUs)

FortiWeb Cloud now supports FortiCloud Organization. This centralized account management service consolidates multiple FortiCloud accounts into a structured system of Organization/Organizational Units (OUs). For more information, see FortiCloud Organizational Units on page 70.

FortiFlex Contract Support

FortiWeb Cloud is introducing FortiFlex (formerly Flex-VM), a new contract management system that allows customers to buy points that can be directed to match their specific requirements for Application and Bandwidth, instead of being restricted to a limited array of contract choices. For more information, see FortiFlex on page 32.

FortiSIEM Support

You can now export your attack and audit logs to FortiSIEM. See Log Settings for more information.

Traffic log export to Azure Storage

You can now export your attack logs to Azure blob storage. See Log Settings for more information.

Allow WAF Cloud IP addresses

You now have the option to download a list of all IP addresses that you need to configure on the firewall. For more information, see Application management on page 65.

Custom Rules ordering

You can now adjust the order of custom rules. See Custom Rule on page 162 for more information.

23.3 released on July 6, 2023

Region IP update

A new scrubbing center will be live on the date of the upcoming release. Please make sure to allow access to your applications from the IP addresses listed below.

- GCP europe-west-8 (Milan)
  - 34.154.63.30
  - 34.154.60.54
  - 34.154.148.78
  - 34.154.84.52

Waiting Room

Control visitor traffic using a virtual holding space and queuing First-In/First-Out system.

See Waiting Room for more information.

Using FortiAnalyzer as syslog server

You now have the option to export logs to FortiAnalyzer to leverage its powerful log management, analytics, and reporting capabilities.

See Log Settings for more information.

Vulnerability Scan service available on Public Cloud Marketplace

Customers that subscribed via Public Cloud marketplace can now run vulnerability scans without having to purchase a separate license. They will be automatically billed via the existing subscription

See Vulnerability Scan for more information.

IAM user role management in FortiCloud

You can now directly assign roles to IAM users in FortiCloud, simplifying the process of managing user access and permissions

See Admin management for more information.

Cache clear for all pages or a single page

The Caching and Compression module now includes the capability to clear the cache for all pages or a single page.

See Caching and Compression for more information.

23.2 released on April 28, 2023

ML based API Protection - Schema and Threat Protection

A new protection layer called “Threat Protection” has been added to the ML based API Protection module. It learns parameter value patterns from API body requests and builds mathematical models to screen out abnormal requests that are deemed malicious. Additionally, you can now set individual API path schema protection rules to detect malformed API requests.

See ML Based API Protection for more information.

IP Protection – uploading an IP List in batch

In IP Protection, instead of configuring IPs one by one, you can now upload a CSV file with a list of IPs instead. See IP Protection for more information.

SOC Analyst Workflow - ServiceNow Integration

Incident Notifications now supports Service Now. You can configure FortiWeb Cloud to create an incident in ServiceNow when threat incidents occur. See Settings for more information.

Account permission control at the Application level moved to Admin Management

The account permission control at the application level was in Role Management. Now it’s moved to Admin Management. See Admin management for more information.

Log filtering enhancements

Attack log now displays logs from all applications, filtering for a specific application is not required. Additionally, filters have been enhanced with filter suggestions.

Application configuration clone

In previous versions, applying a configuration template to specific applications could be done in **Global > Templates**. However, now you can create a new template by cloning an existing application's configuration in **Global > Applications**.

RESTful API version upgraded to v2

FortiWeb Cloud now supports RESTful API v2. Currently v1 is still supported, but some URLs and formats have changed. We cannot guarantee that the RESTful API scripts in v1 format still work.

Please note that starting from the next version 23.2.a, v1 will be no longer supported.

23.1 released on February 24, 2023

SOC Analyst Workflow – Jira and Email Integration

You can now define various rules to automatically create a Jira ticket or send an email when certain Incidents occur. This can help SOC analysts assign an incident to someone else in the organization. See Settings for more information.

Update Details in Audit Logs

Audit logs now provide details on the configuration changes with before&after information.

Threat Analytics – Aggregation across multiple applications

Threat Analytics now aggregates events and finds patterns across multiple applications within the same account. This can help identify sophisticated attack campaigns that focus on multiple customer web assets.

Vulnerability scan bypassing FortiWeb Cloud

You can now bypass the FortiWeb Cloud protection when running a FortiWeb Cloud’s vulnerability scan. This can help to understand if the application is vulnerable, before implementing FortiWeb Cloud security. Enable the **Bypass WAF** option in **Vulnerability Scan**. See Vulnerability Scan for more information.

Validate HTTPS Origin Server Certificates

You can now upload SSL certificates to secure the connections between FortiWeb Cloud and your origin sever. See Origin Servers for more information.

URL rewriting based on protocol

When configuring the Rewriting Requests rule, you can now specify that the URL will be rewritten only if it's in HTTP or HTTPS request. See Rewriting Requests on page 180 for more information.

22.4.a released on December 15, 2022

CORS (Cross-Origin Resource Sharing) Protection

CORS (Cross-Origin Resource Sharing) is introduced to help protect users by controlling and restricting client browsers from accessing origins (domain, scheme, or port) other than the server itself.

For more information, see CORS protection on page 150.

Attack Log Changes

Attack logs tab now merged into Threat Analytics and display logs from all applications. Additionally, FortiWeb Cloud now collects and displays logs from WAF gateways as well.

Client Certificate Authentication

Configure client certificate authentication rules to verify users by their client certificate.

For more information, see Client Certificate Authentication in Endpoints.

CVE Widget/ FortiView CVE

Additional visibility to attacks trying to exploit known vulnerabilities is added in this version. New FortiView view by CVE and Threat Analytics CVE widget are added.

SSL/TLS Encryption Enhancements

- New SSL Encryption Level groups are added: In an effort to follow industry standards, new encryption groups added - Mozilla-Modern, Mozilla-Intermediate, and Mozilla Old.
- The existing "High or Medium" SSL Encryption Level groups will only be available for existing applications. It is recommended to switch them to the new groups.
- New SSL Encryption Level groups are now also available for Origin Servers to control the encryption levels from FortiWeb Cloud to the backend application.

ML Based API Protection data view enhancement

- ML based API Protection is enhanced to automatically update API endpoints when the application changes.
- UI is rearranged to provide easier visibility to API endpoints.
- PII specific data labels have been added.

22.4 released on November 06, 2022

Bug fix

We have fixed several bugs to deliver better performance.

Region IP update

IP addresses of the following scrubbing centers are being updated. Please make sure to allow access to your application from the IP addresses listed below.

- AWS eu-west-2: Europe (London)
  - 18.168.230.94
  - 2a05:d01c:64d:7001:1e54:38a8:2653:4d95
  - 18.130.48.8
  - 2a05:d01c:64d:7002:8a95:b846:2f49:ca5b

22.3.c released on October 6, 2022

Bug fix

We have fixed several bugs to deliver better performance.

Region IP update

IP addresses of the following scrubbing centers are being updated. Please make sure to allow access to your application from the IP addresses listed below.

- AWS sa-east-1: South America (Sao Paulo)
  - 18.229.224.63
  - 2600:1f1e:653:3201:6d62:b616:3070:869f

  - 15.229.95.152
  - 2600:1f1e:653:3202:cad1:1b69:28e2:ccea
- Azure East US2
  - 20.14.167.255
  - 20.65.95.32

22.3.b released on September 23, 2022

Region IP update

IP addresses of the following scrubbing centers are being updated. Please make sure to allow access to your application from the IP addresses listed below.

- AWS us-east-1: US East (N. Virginia)
  - 3.214.245.110
  - 2600:1f18:1492:1701:7c58:5331:25e3:3343
  - 3.225.188.145
  - 2600:1f18:1492:1702:b3ff:2b1d:d9a7:9e88
- New region on Azure: Canada Central
  - 20.63.56.203
  - 20.63.58.199
  - 20.48.236.10
  - 20.48.236.225

Threat Analytics Incident Tags

Administrators can now use predefined tags or create their own tags for Threat Analytics incidents. This helps in labeling incidents for future usage such as sorting, filtering and acknowledging incidents.

Allowlist FortiWeb Cloud IP Addresses

The following links include up to date FortiWeb Cloud IPs. For security best practice configure your web and network firewall to only accept traffic to your web applications from these IPs - https://www.fortiweb-cloud.com/ips-v4 and https://www.fortiweb-cloud.com/ips-v6.

22.3.a released on August 19, 2022

Threat Analytics integrated with FortiWeb

FortiWeb Cloud now integrates with FortiWeb appliances. Collect attack logs from all your FortiWeb platforms and leverage the power of threat analytics across your entire web assets.

Insights tab in Threat Analytics

The new Insights tab is added in Threat Analytics. It provides an additional layer of incident analysis and offers recommendations to improve your security posture. See Threat Analytics for more information.

Vulnerability Scan

A new Web Vulnerability Scan module is introduced. It helps identify OWASP Top 10 flaws in web applications. Get a comprehensive report with remediation recommendations to protect your web applications. See Vulnerability Scan for more information.

Cookie Exception

It's now supported to add exceptions based cookie name and value. This option is available in Signature Based Detection and Syntax Based Detection in Known Attacks, Information Leakage, and attack logs.

New subscription option on AWS

You can now subscribe FortiWeb Cloud on AWS with a yearly data plan.

22.2.b p2 released on July 27, 2022

Region IP updated

IP addresses of the following scrubbing centers on AWS are being updated. Please make sure to allow access to your application from the IP addresses listed below.

- AWS eu-central-1: Europe (Frankfurt)
  - 3.127.31.213
  - 2a05:d014:f3c:6c01:5e7a:1eba:64:30ce
  - 52.58.147.238
  - 2a05:d014:f3c:6c02:3b5d:afaa:1d4:b8f1

22.2.c released on June 29, 2022

Sensitivity level for signatures

Known Attacks now include Sensitivity Levels. You can now choose from four categories of attack signatures (L1 to L4) based on their sensitivity to false positives and their requirement for a higher security level. Every level adds additional signatures thus increasing security but also the possibility of blocking legitimate traffic.

Personally Identifiable Information

On Information Leakage page, you can now configure FortiWeb Cloud to identify personally identifiable information (PII)

Top Known Threats widget

A Top Known Threats widget is added to the Dashboard. It lists the top attacks triggered on your web assets by CVE.

New SOC Analyst role

A new SOC Analyst role is added to the Role management tab.

Region IP updated

IP addresses of scrubbing centers on Azure and Google Cloud are being updated and they will be in effect in the next release 22.3.a. Make sure to update your systems if you created rules limiting access to these IPs. Refer to Restricting direct traffic & allowing FortiWeb Cloud IP addresses for the updated IP addresses.

22.2.a p1 released on June 10, 2022

New scrubbing center clusters

Additional AWS WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.

- AWS ap-east-1 (Hongkong)
  - 18.166.240.188
  - 2406:da1e:b:ae01:31b6:202a:2bbc:79da
  - 18.167.155.174
  - 2406:da1e:b:ae02:f3f4:38fa:d7a2:311a
  - 16.163.110.210
  - 2406:da1e:b:ae01:b1ae:20d2:703f:a868
  - 18.167.190.240
  - 2406:da1e:b:ae01:841e:27d4:4642:5f7f
  - 16.163.212.249
  - 2406:da1e:b:ae02:5b3d:9808:f840:b303

22.2.a released on May 16, 2022

Machine Learning based API Protection

Machine Learning based API Discovery is now upgraded to Machine Learning based API Protection. FortiWeb Cloud can now block anomalies based on the schema it has automatically created and built for the application.

UI enhancements for Machine Learning based API Protection

A new API Collection tab is added with two views, Path List and API View. Path list provides an way to sift through all APIs and easily identify, parameters and schema action. The tree view has been removed.

Machine learning changes

- The API Discovery module is removed. The old configurations and the machine learning models are cleared.
- The configurations of the Anomaly Detection are not affected, but its machine learning models are cleared.

Traffic Summary

A new page named Traffic Summary is added under FortiView. View traffic statistics such as source IP addresses, URL, User Agent, Return Code, and Request Method.

Billing system update

Due to a metering issue, customers that have CDN enabled were only partially billed for their traffic. This issue is now fixed.

Region IP updated

IP addresses of scrubbing centers on AWS are being updated and they will be in effect in the next release 22.2.b. Make sure to update your systems if you created rules limiting access to these IPs. Refer to Restricting direct traffic & allowing FortiWeb Cloud IP addresses for the updated IP addresses.

Traffic log exporting

You can now use FortiWeb Cloud to log all access requests and export traffic log to an AWS S3 bucket. See Exporting traffic logs.

Threat Analytics widget on Dashboard

A Dashboard tab has been added to Threat Analytics.

22.1.c released on April 4, 2022

Threat Analytics

We're introducing a new service called Threat Analytics in this release. The service uses machine learning algorithms to identify attack patterns across your entire application assets and aggregate them into security incidents and assign severity. It helps separate real threats from informational alerts and false positives and help you focus on the threats that matter. See Threat Analytics for more information.

OWASP 2021 attack type

Attack types have been aligned to the OWASP Top 10. You will notice attack logs being tagged with new category names.

DNS status update

FortiWeb Cloud now updates your application's DNS status every two minutes on the first day when it's onboarded, then once an hour after that. An "Update" button had been added to allow to manually update the DNS status at any time.

22.1.b released on February 24, 2022

Blocking Known Engines

In addition to allowing known engines, you can now also set the action to block or bypass.

Domain filter type in Attack Logs

You can now filter the attack logs by domain names.

CC-attack detection

Bot Detection can now prevent against Challenge Collapsar (CC) attacks.

22.1.a released on January 9, 2022

New scrubbing center clusters

Additional AWS WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.

- AWS us-east-1 (N.Virginia)
  - 3.228.64.186
  - 2600:1f18:1492:1701:e54f:59c6:7114:2878
  - 3.231.16.50
  - 2600:1f18:1492:1702:e618:cb8e:f4b5:4ba4
- AWS eu-central-1 (Frankfurt)
  - 35.156.146.120
  - 2a05:d014:f3c:6c01:24c5:1d8d:b3be:2785
  - 35.158.251.28
  - 2a05:d014:f3c:6c02:2490:b345:e759:f43f

Chat bot integration

A new chatbot has been integrated to help address frequently asked questions.

Signature search

It is now possible to search for specific signatures in the Known Attacks and Information Leakage dictionaries. You can search by CVE, keywords, signature IDs and by attack category.

21.4.b released on December 5, 2021

Action required! Change your A record ASAP!

The IP addresses of FortiWeb Cloud have changed. If you are using a CNAME record to point your domains to FortiWeb Cloud you do not need to do anything.

However, if you are using an A record to point your domain to FortiWeb Cloud you need to change the IP address in your DNS A record as soon as possible, otherwise when your web application certificate expires it will fail to renew.

To update the A record:

1. Log in to FortiWeb Cloud.
2. Go to **Global > Applications**.
3. Find the application which uses the A record.
4. Click **Update Pending** in DNS Status column. You can find the new IP addresses in the pop-up window.
5. Go to your DNS service and find the A record, then pair your domain name with the new IP addresses.

This change applies only to A record. For restricting direct traffic and configuring the allowlist in a DDoS device, you can use the same IP addresses as before.

An easier way to look up Cloud WAF IP addresses

The **Regions** column in the applications tab has been populated with additional information. It displays the IP addresses of the Cloud WAF scrubbing centers assigned to your applications.

Caching added to dashboard widgets

Caching data has been added to the Throughput and Incoming Requests dashboard widgets.

Default action changed for GEO IP violations

The action taken for the GEO IP violations is changed from Deny&Alert to Period Block (600 seconds).

Minimum interval of Information Leakage logs

To avoid log flooding, the minimum interval of Information Leakage logs is set to 1 second.

21.4.a p3 released on November 12, 2021

New scrubbing center clusters

Additional AWS WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.

- AWS ap-south-1 (Mumbai)
  - 3.109.248.211
  - 2406:da1a:31:d501:fc19:5e59:9804:b392
  - 3.109.17.189
  - 2406:da1a:31:d502:2eaf:153f:91b3:7dc0
  - 3.108.0.134 (offline)
  - 2406:da1a:31:d501:4933:f303:c5b:4726 (offline)
- AWS us-east-2 (Ohio)
  - 3.131.242.28
  - 2600:1f16:160:aa01:4584:fec1:ab59:6bd4
  - 18.188.127.1
  - 2600:1f16:160:aa02:5629:28f1:196d:acbe
  - 3.132.52.4 (offline)
  - 2600:1f16:160:aa01:6d33:94aa:74c0:7cf0 (offline)

21.4.a released on October 8, 2021

- **URL Redirection enhancement**
  When redirecting clients to a new host or IP address in a “301 Permanently” response, you can now keep the URL path while executing redirection. For example, clients visiting "www.aaa.com/test.html" can be redirected to "www.bbb.com/test.html".
- **CDN enhancement**

CDN feature is enhanced to allow selecting a specific continent instead of caching globally. This can help address compliance requirements that mandate application traffic must be served from a specific continent.

- **New scrubbing centers**

  Additional AWS WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.

  - AWS ap-southeast-1 (Singapore)
    - 18.136.170.71
    - 2406:da18:ad1:1101:b6ad:34de:de05:5ef3
    - 13.214.45.126
    - 2406:da18:ad1:1102:9a1c:767e:1e67:4763
    - 13.250.74.198(Offline)
    - 2406:da18:ad1:1101:1fb2:25ab:77f1:42e4(Offline)
  - AWS ca-central-1 (Canada)
    - 3.97.158.98
    - 2600:1f11:8c:9101:eb3:39f1:1815:884e
    - 3.97.249.50
    - 2600:1f11:8c:9102:411d:63f2:e5b4:5209
    - 3.98.118.237(Offline)
    - 2600:1f11:8c:9101:62aa:927:70dd:acfa(Offline)
  - AWS us-west-1 (N.California)
    - 52.8.219.206
    - 2600:1f1c:b97:d801:ff83:8b03:7a29:5981
    - 52.9.219.121
    - 2600:1f1c:b97:d802:fe8f:1a5d:5d1:1c6b
    - 54.215.20.148(Offline)
    - 2600:1f1c:b97:d801:fd1b:8346:e92e:466b(Offline)
  - AWS us-west-2 (Oregon)
    - 35.160.55.58
    - 2600:1f14:b5a:da01:a32:4cac:f337:9c00
    - 44.241.247.81
    - 2600:1f14:b5a:da02:5a8e:d30:ff37:18a9
    - 52.37.161.224(Offline)
    - 2600:1f14:b5a:da01:c9ac:e531:128b:ae2c(Offline)

21.3.b patch2 released on September 24, 2021

Additional AWS WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.

- AWS eu-west-1 (Ireland)
  - 54.78.90.129
  - 2a05:d018:77c:d901:4f37:924f:6ea2:5952

  - 54.217.132.119
  - 2a05:d018:77c:d902:6605:9bef:2ca3:f220
  - 52.18.74.99 (offline)
  - 2a05:d018:77c:d901:550f:2833:9dbd:362c (offline)
- AWS eu-west-2 (London)
  - 18.134.173.119
  - 2a05:d01c:64d:7001:7f27:28fe:f43b:e55b
  - 52.56.112.105
  - 2a05:d01c:64d:7002:a0b0:a076:53b2:31e3
  - 35.178.16.146 (offline)
  - 2a05:d01c:64d:7001:b99d:28b6:db62:e2bd (offline)
- AWS eu-south-1 (Milan)
  - 15.161.215.247
  - 2a05:d01a:9f2:1701:4d5b:f1a8:d291:5a84
  - 15.161.76.114
  - 2a05:d01a:9f2:1702:8e71:e939:c954:1608
  - 15.160.42.32 (offline)
  - 2a05:d01a:9f2:1701:75ab:6622:8788:fdb2 (offline)

21.3.b released on September 3, 2021

- **Know Bots module**
  Known bad bots and known search engines configuration is moved from Threshold Based Detection to a new module named Known Bots. See Known Bots on page 155 for more information.
- **User Management enhancement**
  Tighter and stricter integration with FortiCloud is introduced. FortiCloud sub users and IAM users are automatically assigned certain permissions on FortiWeb Cloud. See Admin management.
- **SQL and XSS Syntax Based Detection Enhancements**
  Additional granularity is available for SQL and XSS Syntax Based Detection. You can specify the SQL injection types and XSS attack types to parse against. See Known Attacks for more information.
- **Alert notification upon certificate renewal failure**
  When FortiWeb Cloud fails to renew or retrieve a certificate, a notification message will be displayed on the Web UI. An alert email will be sent as well.
- **Block page layout enhancement**
  The layout of the "Server Unavailable Message" and "Attack Block Page" displayed to your application users is enhanced. Go to **Global > System Settings > Custom Block Pages** to view the updated pages.
- **Filter type changes in Custom Rule**
  The filter type "Security Rules" in Custom Rule is now renamed to Known Attacks. "Information Disclosure" and "Known Bad Bots" are no longer available when Known Attacks is chosen.
- **DNSSEC support on AWS**
  DNS Security Extensions (DNSSEC) has been enabled for CNAMEs associated with applications hosted on AWS to protect against DNS spoofing, cache poisoning, or other DNS-related man-in-the-middle attacks.

- **DevOps tools configuration file update**
  The configuration file for Ansible and Terraform is updated so that the API token is not exposed in yml file. See Using FortiWeb Cloud with DevOps tools.

21.3.a released on July 24, 2021

- **API Discovery (Beta)**
  Use Machine Learning Based API discovery to learn the REST API data structure from user traffic. By studying the samples, a Swagger file will be generated describing the data structure such as the URL pattern and schema of endpoint data. See ML Based API Protection for more information.
- **Bot Detection (Beta)**
  The AI-based machine learning bot detection model is introduced to complement the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected. See ML Based Bot Detection for more information.
- **Syntax based Cross Site Scripting detection**
  Syntax Based Cross Site Scripting detection is introduced in the Known Attacks module to detect the XSS injection attacks using a sophisticated, non-signature based module that analyzes HTML/JavaScript syntax. See Known Attacks for more information.
- **Caching and Compression enhancements**
  Additional granularity available for Caching and Compression. You can configure HTTP Method, Allow Return Code, Allow File Type, and Key Generation Factor to define the content to be cached. Resources cached on FortiWeb Cloud can now be purged. See Caching and Compression for more information.
- **DNS and HTTP challenges for Automatic Certificate**
  It's now allowed to select whether to use DNS or HTTP challenge to validate your ownership of the domains. See Endpoints for more information.
- **Wildcard in domain names**
  You can use wildcard to match multiple domains when onboarding an application. SeeEndpoints for more information.
- **HTTP only flag**
  You can configure the Endpoints settings to add "HTTP Only" flag to internal cookies, which prevents client-side scripts from accessing the cookie. SeeEndpoints for more information.
- **Server certificate verification for log exporting**
  FortiWeb Cloud by default enforces server certificate verification before it sends logs to the log server. See for more information.
- **Customizing HTTP Response Code**
  It's now allowed to change the HTTP Response Code of Attack Block Page in custom block message.

21.2.c released on June 11, 2021

- **Sensitive Data Masking**
  Sensitive Data Masking allows masking certain data types such as user names, passwords and other PII information that could appear in the packet payloads accompanying a log message. See Sensitive Data Masking on

page 111 for more information.

- **Parameter Validation**

  A new security module named Parameter Validation is introduced in this release. It validates parameter input such as whether they're required, maximum allowed length or whether they match pre-defined/customized patterns. See Parameter Validation on page 134 for more information.
- **New scrubbing center**

  A New scrubbing center has been deployed on Azure. Please allow access to your application from the IP addresses of these scrubbing centers.
  - Brazil South (São Paulo State)
    - 20.195.163.139
    - 20.197.225.122
    - 20.197.226.167 (Offline)
- **Origin Server Lock**

  Origin Server Lock protects your application from attackers that try to bypass FortiWeb Cloud security measures by pointing their onboarded application to your origin server. See Origin Server Lock on page 79 for more information.
- **Full support of HTTP/2**

  HTTP/2 was supported only in certain security modules previously. Now FortiWeb Cloud fully supports HTTP/2 across all security modules.
- **Customized SSL/TLS Encryption Level**

  You can customize the SSL/TLS Encryption Level by selecting the ciphers from the available ciphers list. See SSL/TLS on page 122 and Supported cipher suites & protocol versions for more information.
- **Alerts for soon to expire certificates**

  FortiWeb Cloud can now send an email alert when local certificates in Endpoints are about to expire.
- **Third Party IdP initiated SAML support**

  Third Party IdP initiated SAML is now supported allowing to automatically access FortiWeb Cloud admin interface using your organization's user credentials via a third party ID provider. See Managing External IdP roles in FortiCloud IAM on page 237 for more information.

21.2.b released on May 26, 2021

- It is now possible to enable sub categories and allow or deny specific bots in Threshold Based Detection's Known Bad Bots, replacing the exception rules. If you had known bad bots exception rules configured make sure you enable/disable the bad bots via the new interface.
- Syntax Based Detection exceptions are now based on attack types instead of signature IDs. Exceptions are configured separately from Signature Based Detection exceptions.

21.2.a released on May 1, 2021

- The number of allowed custom rules per application has been raised to 24.
- Additional granularity available for Credential based brute force protection. You can configure a target URL and occurrence period.

- Additional WAF clusters have deployed in the following existing regions. Please make sure to allow access to your application from the IP addresses listed below.
  - **AWS**
    - eu-central-1 (Frankfurt)
      - 18.192.64.32
      - 2a05:d014:f3c:6c01:99d0:8c50:ae51:99ac
      - 3.125.233.133
      - 2a05:d014:f3c:6c02:58:3e12:a98a:df9f
      - 3.64.105.7 (offline)
      - 2a05:d014:f3c:6c01:55bc:c559:8bb1:11e0 (offline)
    - sa-east-1 (Sao Paulo)
      - 54.207.227.252
      - 2600:1f1e:653:3201:eac8:161d:c0a:6915
      - 177.71.170.92
      - 2600:1f1e:653:3202:3615:6e2c:7b0c:85c9
      - 54.232.72.181 (offline)
      - 2600:1f1e:653:3201:d1a5:34ae:e023:be2d (offline)
  - **Azure**
    - West Europe
      - 20.86.129.248
      - 20.86.49.155
      - 20.86.49.12 (offline)

21.1.c released on March 1, 2021

The following enhancements are made in Rewriting Requests module:

- In addition to the connection's source IP, it's now possible to record the connection's source port in the `X-Forwarded-For:` header.
- The `X-Forwarded-Port:` header can be added to record the connection's original destination port.

See Rewriting Requests for more information.

21.1.b released on February 9, 2021

- It's now supported to redirect requests based on host names, for example, redirecting from example.com to www.example.com. See Rewriting Requests.
- You can now sign in FortiWeb Cloud as IAM users.
- New scrubbing centers have been deployed on the following regions on OCI. Please allow access to your application from the IP addresses of these scrubbing centers.

  - US West (Phoenix)
    - 158.101.43.252
    - 158.101.43.253
    - 129.146.233.205 (Offline)
  - Germany Central (Frankfurt)
    - 158.101.176.179
    - 193.122.55.66
    - 132.145.248.29 (Offline)

21.1.a released on January 11, 2021

- It is no longer required to have a port 80 HTTP service enabled to successfully generate automatic certificates. The limitation has been removed.
- Custom ports HTTP 9219 and HTTPS 8181 are now supported.
- You can now customize the following pages that FortiWeb Cloud displays to your users:
  - Attack Block Page
  - Server Unavailable Page
  - Captcha Enforcement Page

  The old Custom Block Page configurations will be discarded. You need to re-configure it through the new page. See Custom block pages.
- New scrubbing centers have been deployed on AWS and Azure. Please allow access to your application from the IP addresses of these scrubbing centers.

  East US2 on Azure
  - 20.69.235.177
  - 20.81.153.33
  - 20.81.153.78 (offline)

  Australia East on Azure
  - 20.70.160.47
  - 20.70.152.97
  - 20.70.152.115 (offline)

  Europe (Milan) on AWS
  - 15.161.173.116
  - 15.161.10.152
  - 15.161.24.119 (offline)
  - 2a05:d01a:9f2:1701:bd84:9314:f93:b2f
  - 2a05:d01a:9f2:1702:aca5:5d4d:1995:50d
  - 2a05:d01a:9f2:1701:3e5:91fb:2690:b114 (offline)

20.4.b released on November 23, 2020

- It is now possible to enable HSTS forcing clients to only use HTTPS with the application.
- When enabled, FortiWeb Cloud will use the Secure flag for its session management cookie only allowing its use over HTTPS.
- The logic in which FortiWeb Cloud retrieves automatic certificates has been optimized. Additionally, a new “Retrieve” button is added to allow manual retrieval of automatic certificates.

For more information on the new features, see Endpoints.

20.4.a released on November 10, 2020

- As the FortiWeb Cloud service is already protected against volumetric DDoS attacks, TCP flood prevention is removed in order to prevent conflicts.
- Configuration deployment is significantly improved to reduce service disruption.
- New scrubbing centers are deployed in eu-central-1: EU (Frankfurt) on AWS. See Restricting direct traffic & allowing FortiWeb Cloud IP addresses on page 53.

20.3.b released on September 16, 2020

- A new scrubbing center has been deployed on AWS - ap-south-1 : Asia Pacific (Mumbai). See FortiWeb Cloud scrubbing centers on AWS on page 54.
- API Key settings is no longer part of the Global Settings role, allowing to generate an API key for read-only defined roles as well.
- DNS status changes will now be recorded in the audit log.
- When a source violates the API Gateway rule, it is possible to automatically block the source IP for a period of 10 minutes.
- In addition to 443, 7443, and 8443, ports 8081 and 8014 can now be used for HTTPS service.
- Fabric Connectors is renamed to Cloud Connectors.

20.3.a released on August 10, 2020

- Optimizations on Reports:
  - Add a new query Applications Traffic Summary for report category.
  - Support adding or removing all applications once.
  - Activate or deactivate report generation for scheduled reports.
  - Weekly reports enabling is removed from Global Settings.
- A new trustlist module is added to allow trusting specific parameters. Once enabled security enforcement is bypassed for the specified parameters. See Global Trustlist.
- You can now define a separate Action per security module allowing, for example for some modules to only trigger an alert while others are set to block. Enabled when Advanced Configuration is enabled.

- The Filter option for Cloud Connector is optimized to show all available options for a selected fabric connector.
- A new Ansible template is released to allow configuring an endpoint’s certificate configuration. See Configuring FortiWeb Cloud with Ansible.
- FortiWeb Cloud now supports generating an API key for authentication. See API Key.
- Advanced Configuration is added in Global Settings. Once enabled a templates tab is introduced together with the ability to configure the Action interface for each security module.
- Six new predefined templates containing commonly used WAF security configuration for different known applications such as Drupal and WordPress are introduced in this release. See Templates
- FortiWeb Cloud will keep the data in your account for an additional week after you unsubscribe from FortiWeb Cloud.

20.2.d released on July 1, 2020

- Cloud Connectors is introduced to support origin servers with dynamically changing IP addresses. See Cloud Connectors on page 80.
- IPv6 is now supported for customers utilizing FortiWeb Cloud on AWS. You can enable IPv6 service in Endpoint, add origin servers with IPv6 addresses, or configure IPv6 addresses in IP Protection and Custom Rule.
- New report types added together with capability to schedule reports with granularity around application and report time frame.
- Support for DevOps tools including Jenkins, Ansible, and Terraform has been added. You can use them to automatically onboard or delete applications and change the IP list in IP Protection. Contact support to download the template.

20.2.c released on June 17, 2020

- Role Management is introduced to offer an easier way to manage access privileges and permissions specific to a job function. See Role management on page 77.
- Manually test in real-time the health status of a origin server. See Origin Servers on page 114.
- You can now insert Content-Security-Policy header to prevent certain types of attacks, including XSS and data injection attacks. See HTTP Header Security on page 140.

20.2.b released on May 29, 2020

- You can now configure **Allow Known Search Engines** in **Threshold Based Detection** to accept/deny the traffic from known search engines such as Google, Bing, and Yahoo, etc. This is enabled by default. See Threshold Based Detection on page 154.
- FortiWeb Cloud now supports onboarding applications running on non-standard ports. Certain limitations apply. See Traffic Type on page 119.
- A new scrubbing center has been deployed on AWS - sa-east-1 : South America. See FortiWeb Cloud scrubbing centers on AWS on page 54.
- A new protection mechanism is introduced for SQL Injection attacks called Syntax Based Detection. It uses a SQL parser to validate whether the pattern is real SQL language which helps identify true attacks while minimizing false

positives. See Known Attacks on page 128.

- Paging is optimized for Attack Logs and Audit Logs. A maximum of 10,000 attack/audit logs are displayed per each filter in Attack/Audit Logs.
- Audit logs now cover changes in automatic certificates status including: starting to apply, failed to apply, applied successfully, renewed successfully, and failed to renew.
- Additional health check statuses have been added to the audit log. The Server Status widget display is updated.

20.2.a released on April 27, 2020

- You can now define an **Allow Only** list in **IP Protection** to limit access to the application to specified IP addresses. See IP Protection on page 148.
- You can now send a customized block page to clients triggering WAF rules. See Endpoints on page 118.
- Forwarding attack and event logs to ElasticSearch is now supported. See Log Settings on page 105 and Audit logs on page 83.
- A new OWASP Top 10 widget together with a new FortiView OWASP Top 10 view have been added.

20.1.b released on March 21, 2020

- Parameter name is supported when creating a signature exception rule for Known Attacks, Information Leakage, and Threshold Based Detection.
- It's now supported to add URL and parameter exceptions in attack logs.

20.1.a released on February 29, 2020

- Three new modules supported for API PROTECTION.
  - **Mobile API Protection** module allows to protect your Mobile APIs from malicious attacks by verifying the mobile device authenticity. See Mobile API Protection on page 175.
  - **API Gateway module** allows to control and secure all access to you APIs. You can define API users, verify API keys, and perform access control, etc. See API Gateway on page 175.
  - **JSON Protection module** allows to verify JSON request limits and JSON request parameters to protect against API attacks. See JSON Protection on page 173.
- WAF configuration template is added for you to push WAF configurations to multiple applications. See Templates on page 67.
- Bot mitigation leverages various detection mechanisms to quickly filter out automated threats.
  - **Biometrics Based Detection**: FortiWeb Cloud can now verify whether a client is a bot by monitoring events such as mouse movement, keyboard, screen touch, and scroll, etc. See Biometrics Based Detection on page 153.
  - **Threshold Based Detection**: With predefined occurrence, time period, etc. of suspicious behaviors, FortiWeb Cloud judges whether the request comes from a human or a bot. See Threshold Based Detection on page 154.

  - **Bot Deception**: FortiWeb Cloud now provides a deception technique to identify bots. It inserts a hidden link into response pages. Clients that fetch the URL can accurately be classified as bots. See Bot Deception on page 156.
- XML Protection module is moved from Advanced Applications to API Protection. See XML Protection on page 174.
- User and Time Periods filters are added for Custom Rule. See Custom Rule on page 162.
- Three security modes are added in Cookie Security module. See Cookie Security on page 137.
- Applications page is optimized to accelerate the loading.
- With the Attack Log Alerts feature, FortiWeb Cloud now supports sending attack log alert emails based on threat level or customized alert email rule. See Log Settings on page 105.
- HTTP/2 communications can be protected when the traffic type is HTTPS. It's supported in Known Attacks, Information Leakage, and Cookie Security.
- FortiWeb Cloud now supports adding exceptions through Anomaly Detection logs.
- FortiWeb Cloud now supports Server Name Indication (SNI) configuration that identifies the certificate to use by domain. See Custom Certificate on page 121.

Contracts

There are three main types of FortiWeb Cloud Contracts.

- FortiWeb Cloud license purchased from your Fortinet reseller. The license allows you to protect certain number of applications and specifies the maximum bandwidth.
- FortiFlex on page 32 where you can buy points that can be directed to match their specific requirements for Application and Bandwidth, instead of being restricted to a limited array of contract choices.
- Public Cloud Marketplace subscriptions on page 33 that charges based on data sent to your app users with a pay-as-you-go model, rather than by the number of applications or amount of bandwidth.

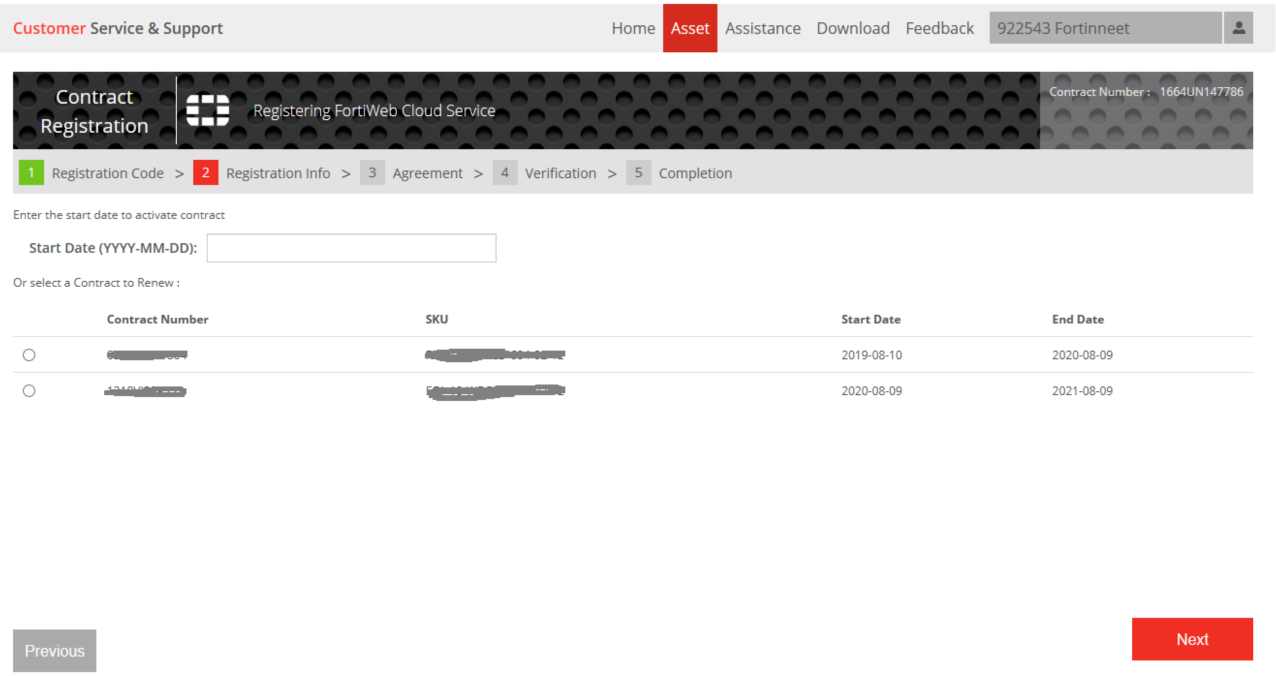
Regardless of the subscribing channel you choose, you can use FortiWeb Cloud to protect applications located on any cloud platform or in your own network. For example, even if you subscribed through AWS, you can use FortiWeb Cloud to protect applications located on Azure. The subscription channel only determines the billing places for your FortiWeb Cloud usage.

Licenses purchased from Fortinet

If you purchase FortiWeb Cloud service from Fortinet sales team, you will be charged for the Bandwidth contract and Applications contract, which respectively control how many applications you can add in your account and the maximum bandwidth.

1. Purchase FortiWeb Cloud contracts.
   There are separate licenses for applications and bandwidth, which respectively control how many applications you can add in your account and the maximum bandwidth. **Both licenses are required to activate the service contract.**
2. Create a FortiCloud account: https://support.fortinet.com/Login/CreateAccount.aspx.
   It can be used to log in to all the Fortinet products, including FortiWeb Cloud and Fortinet Support site. Skip this step if you already have one.
3. Log in to Fortinet Support site.
4. Click **Asset > Register/Activate**.
5. Enter the contract registration code that was emailed to you when you purchased the contract.
6. Select the **End User Type**. Click **Next**.

7. Enter the start date to activate the contract. The contract will automatically become active on the specified start date. You can also select an existing contract to extend its End Date. Click **Next**.



Customer Service & Support
Home
Asset
Assistance
Download
Feedback
922543 Fortinneet
Contract Registration
Registering FortiWeb Cloud Service
Contract Number : 1664UN147786
1 Registration Code > 2 Registration Info > 3 Agreement > 4 Verification > 5 Completion

Enter the start date to activate contract

Start Date (YYYY-MM-DD):

Or select a Contract to Renew :

	Contract Number	SKU	Start Date	End Date
○	[redacted]	[redacted]	2019-08-10	2020-08-09
○	[redacted]	[redacted]	2020-08-09	2021-08-09

8. Read *Fortinet Product Registration Agreement*. Check the box if you agree. Click **Next**.
9. A verification page is displayed. Check the box to acknowledge the activation of the contract. Please note the activation date cannot be changed once you confirm.
   Click **Confirm**.
10. Repeat the registration steps if you have multiple contracts.
11. Log in to FortiWeb Cloud with your FortiCloud account.
12. The contract information will be displayed in **Global > System Settings > Contracts**.

If you have previously subscribed from public cloud platforms, do remember to cancel the subscription if you switch to FortiWeb Cloud contracts.

FortiFlex

FortiWeb Cloud now supports FortiFlex (formerly Flex-VM), a new contract management system that allows customers to buy points that can be directed to match their specific requirements for Application and Bandwidth, instead of being restricted to a limited array of contract choices.

To use FortiFlex, you must have all of the following:

- A primary FortiCloud account or IAM user account.
- FortiFlex Program SKU (either Enterprise/prepaid or MSSP/postpaid) purchased from Fortinet's resellers and distributors.
- FortiFlex Point Pack SKU (only applicable to Enterprise/prepaid) purchased from Fortinet's resellers and distributors.

For more information, please see FortiFlex documentation on registration: https://docs.fortinet.com/document/flex-vm/latest/administration-guide/791307/registering-fortiflex.

To see your FortiFlex points and usage:

1. Log into FortiCloud.
2. Click on Services in the top navigation bar.
3. In the drop-down menu opened in step 2, look under **Assets & Accounts** and click on **FortiFlex**. This brings you to your FortiFlex dashboard.

Public Cloud Marketplace subscriptions

FortiWeb Cloud offers 14-day free trial on public cloud platforms. After the free trial, you can subscribe to FortiWeb Cloud or purchase service contracts from Fortinet to continue using it.

- Subscribing through AWS Marketplace.
- Subscribing through Azure Marketplace.
- Subscribing through Google Cloud Marketplace.

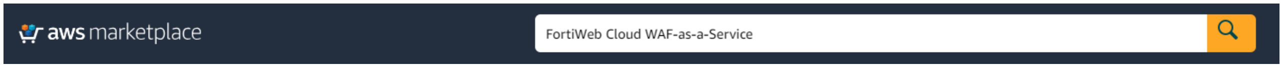
Regardless of the subscribing channel you choose, you can use FortiWeb Cloud to protect applications located on any cloud platform or in your own network. For example, even if you subscribed through AWS, you can use FortiWeb Cloud to protect applications located on Azure. The subscribing channel only determines the billing places for your FortiWeb Cloud usage.

Unsubscribing from FortiWeb Cloud on AWS, Azure, and Google Cloud

You can unsubscribe from FortiWeb Cloud anytime, while the data in your FortiWeb Cloud account will be kept for an additional week after you unsubscribe, which helps re-subscribe to FortiWeb Cloud seamlessly.

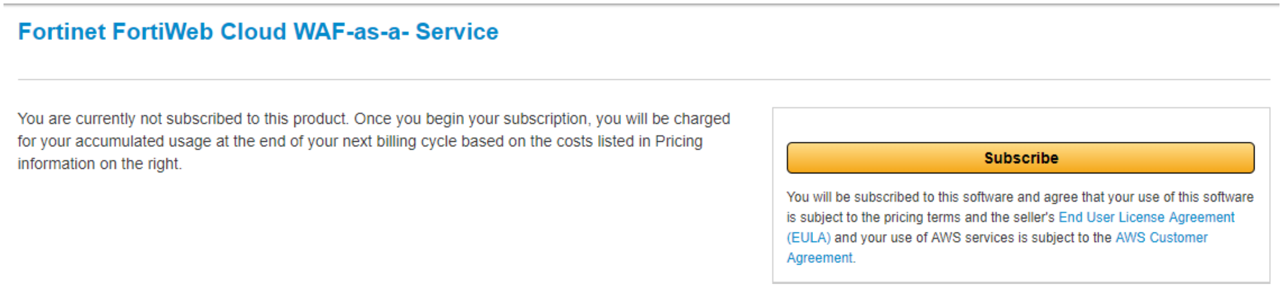
Subscribing on AWS Marketplace

Follow the steps below to subscribe FortiWeb Cloud on AWS and associate your AWS subscription with your FortiCloud account.

1. Log in to AWS. Search FortiWeb Cloud in AWS Marketplace or click here: AWS Marketplace


FortiWeb Cloud WAF-as-a-Service
2. On the **FortiWeb Cloud** page, carefully read the description under the **Subscribe** button. Click **Subscribe**. Wait for a few minutes for the subscription to be created.
Do not clear the browser's cookie once the subscription is created, otherwise Fortinet won't know you are a

subscribed user when you register or log in to FortiWeb Cloud in later steps.

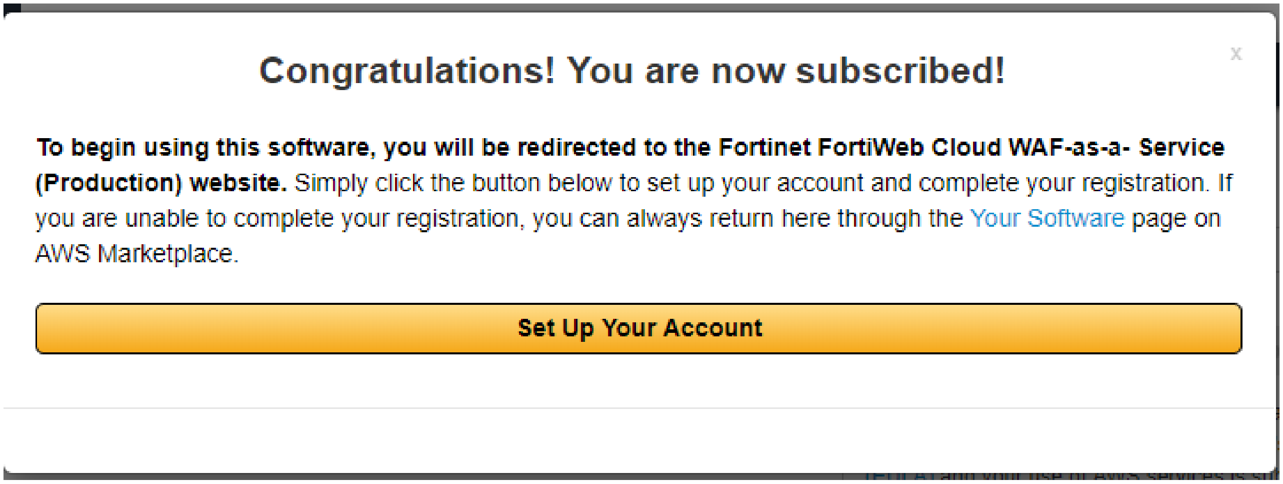


Fortinet FortiWeb Cloud WAF-as-a- Service

You are currently not subscribed to this product. Once you begin your subscription, you will be charged for your accumulated usage at the end of your next billing cycle based on the costs listed in Pricing information on the right.

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement.

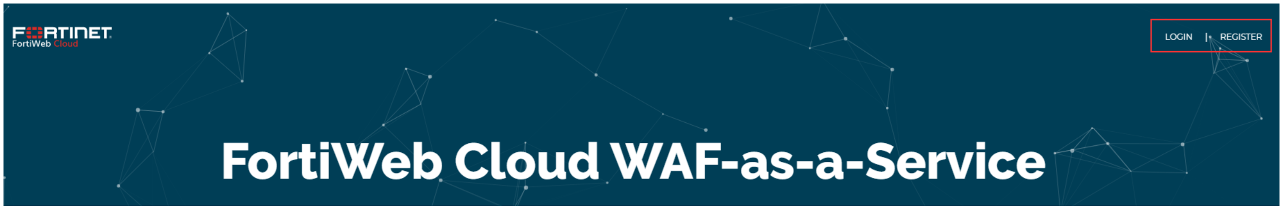
3. Click **Set Up Your Account.** You will be redirected to the FortiWeb Cloud landing page.



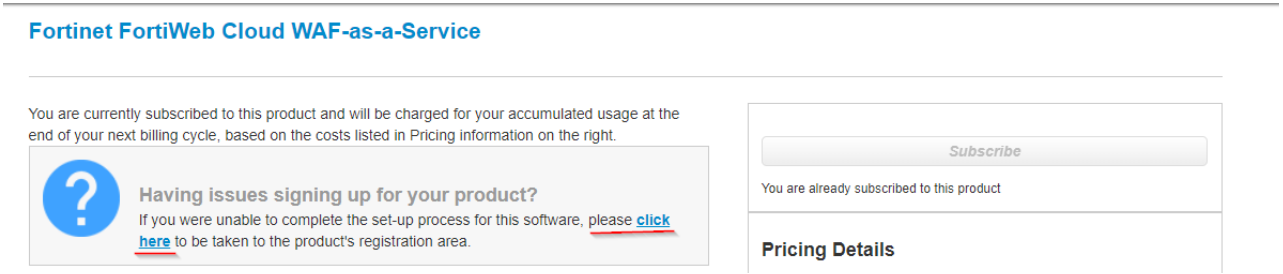
Congratulations! You are now subscribed!

To begin using this software, you will be redirected to the Fortinet FortiWeb Cloud WAF-as-a- Service (Production) website. Simply click the button below to set up your account and complete your registration. If you are unable to complete your registration, you can always return here through the Your Software page on AWS Marketplace.

4. Log in with an existing FortiCloud account, or register a new account. You can access all of your Fortinet Cloud services and the Fortinet Support site through FortiCloud account.
Your AWS subscription for FortiWeb Cloud will be automatically associated once you log in to your FortiCloud account.
Make sure you are using the same browser when subscribing FortiWeb Cloud and logging in to FortiCloud account.



If you accidentally cleared the cookie, return to AWS Marketplace and search FortiWeb Cloud WAF-as-a-Service. As shown in the following screenshot, there will be a Notice leading you to the registration process again.



Fortinet FortiWeb Cloud WAF-as-a-Service

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

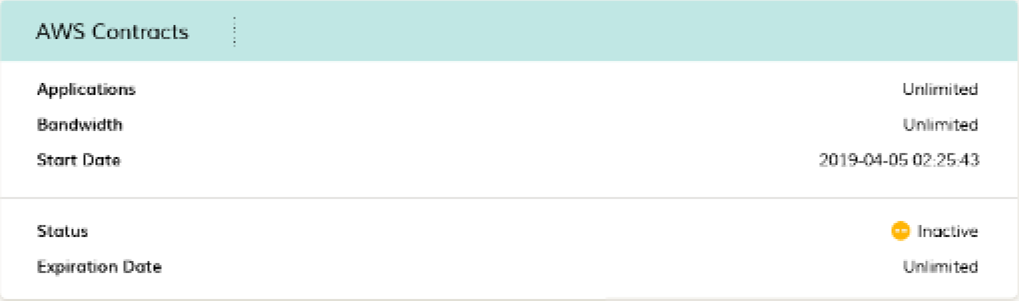
Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please click here to be taken to the product's registration area.

You are already subscribed to this product

Pricing Details

5. If you have successfully subscribed, there will be a **AWS contracts** column displaying in **Global > System Settings > Contracts**.



AWS Contracts

Applications	Unlimited
Bandwidth	Unlimited
Start Date	2019-04-05 02:25:43
Status	Inactive
Expiration Date	Unlimited

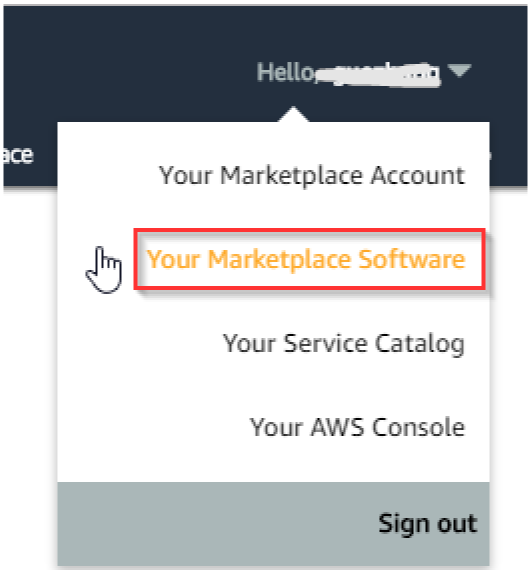
You will be charged based on an hourly rate of $0.03 per hour for every web application and a traffic usage rate of $0.4 per gigabyte (GB). The hourly rate metering will commence once you have onboarded an application on FortiWeb Cloud (regardless of its DNS status), while the traffic usage metering will begin when traffic is actively flowing through FortiWeb Cloud to your application.

Please note that even if you subscribed through AWS, you can use FortiWeb Cloud to protect applications located on any other cloud platform or in your own network. The subscribing channel only determines the billing places for your FortiWeb Cloud usage.

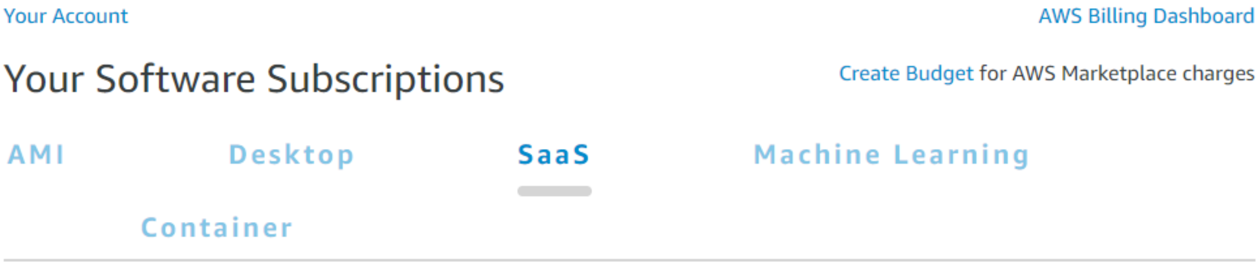
Unsubscribing from FortiWeb Cloud on AWS

You can unsubscribe from FortiWeb Cloud anytime, but keep in mind that the data in your FortiWeb Cloud account will be cleared in one week after you unsubscribe. It can't be restored even if you subscribe to FortiWeb Cloud again. Please make sure all DNS changes have been done so your web application does not experience service interruption.

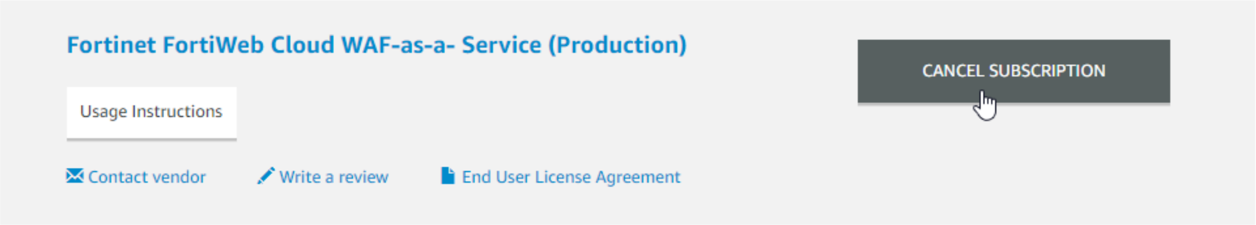
1. Log in to AWS. Click your account name at the top right corner, then select **Your Marketplace Software** in the drop-down list.



2. Select the **SaaS** tab.



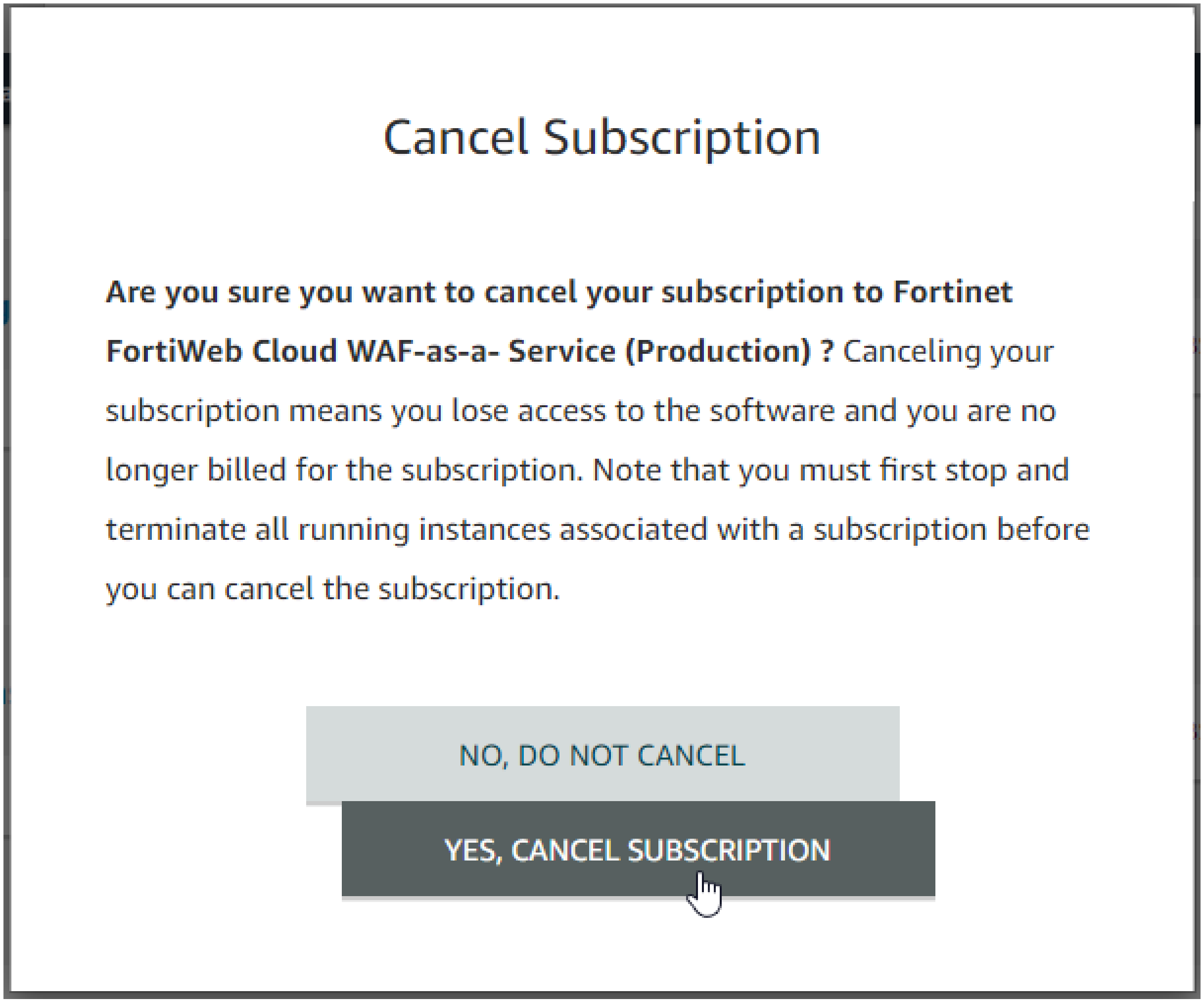
3. Find **FortiWeb Cloud**, then click **CANCEL SUBSCRIPTION**.



Fortinet FortiWeb Cloud WAF-as-a- Service (Production)
CANCEL SUBSCRIPTION
Usage Instructions
Contact vendor
Write a review
End User License Agreement

4. Click **YES, CANCEL SUBSCRIPTION**.
   FortiWeb Cloud will continue blocking threats for your application for one hour after you cancel subscription. After

an hour, all the data in your account will be cleared, and FortiWeb Cloud stops protecting your applications.



Cancel Subscription

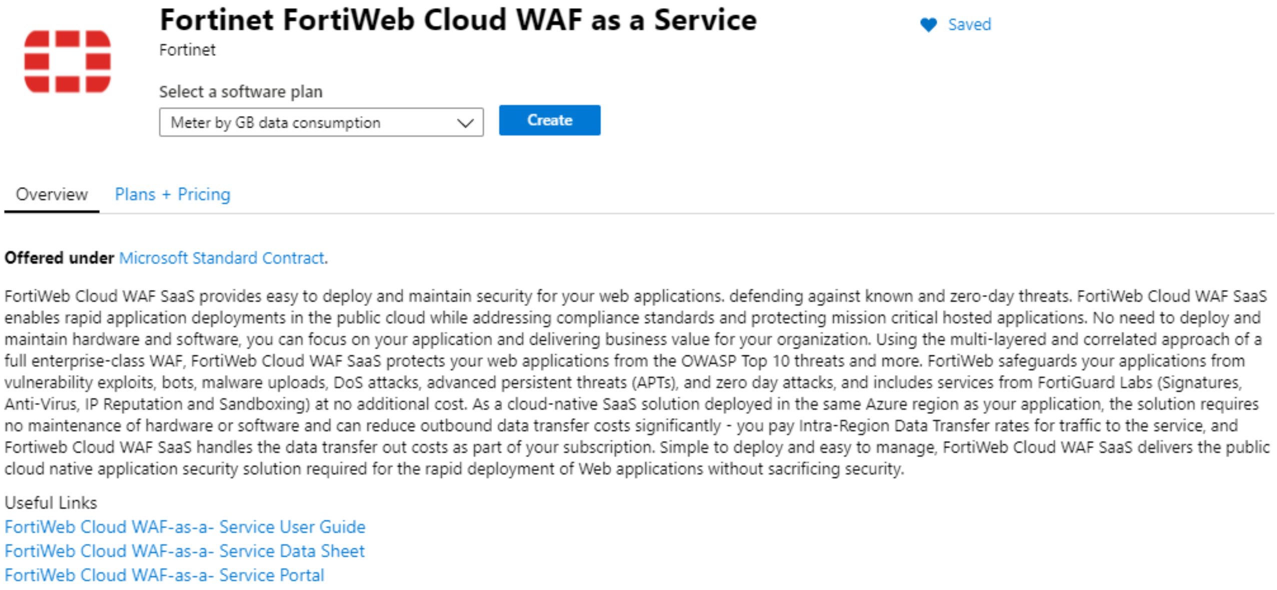
Are you sure you want to cancel your subscription to Fortinet FortiWeb Cloud WAF-as-a- Service (Production) ? Canceling your subscription means you lose access to the software and you are no longer billed for the subscription. Note that you must first stop and terminate all running instances associated with a subscription before you can cancel the subscription.

Subscribing on Azure Marketplace

Follow the steps below to subscribe FortiWeb Cloud on Azure and associate your Azure subscription with your FortiCloud account.

1. Log in to Azure. Search **FortiWeb Cloud WAF as a Service** in Azure Marketplace or click here: Azure Marketplace.

2. On **FortiWeb Cloud** page, click **Create**.



Fortinet FortiWeb Cloud WAF as a Service

Fortinet

Select a software plan

Meter by GB data consumption

Offered under Microsoft Standard Contract.

FortiWeb Cloud WAF SaaS provides easy to deploy and maintain security for your web applications. defending against known and zero-day threats. FortiWeb Cloud WAF SaaS enables rapid application deployments in the public cloud while addressing compliance standards and protecting mission critical hosted applications. No need to deploy and maintain hardware and software, you can focus on your application and delivering business value for your organization. Using the multi-layered and correlated approach of a full enterprise-class WAF, FortiWeb Cloud WAF SaaS protects your web applications from the OWASP Top 10 threats and more. FortiWeb safeguards your applications from vulnerability exploits, bots, malware uploads, DoS attacks, advanced persistent threats (APTs), and zero day attacks, and includes services from FortiGuard Labs (Signatures, Anti-Virus, IP Reputation and Sandboxing) at no additional cost. As a cloud-native SaaS solution deployed in the same Azure region as your application, the solution requires no maintenance of hardware or software and can reduce outbound data transfer costs significantly - you pay Intra-Region Data Transfer rates for traffic to the service, and Fortiweb Cloud WAF SaaS handles the data transfer out costs as part of your subscription. Simple to deploy and easy to manage, FortiWeb Cloud WAF SaaS delivers the public cloud native application security solution required for the rapid deployment of Web applications without sacrificing security.

Useful Links

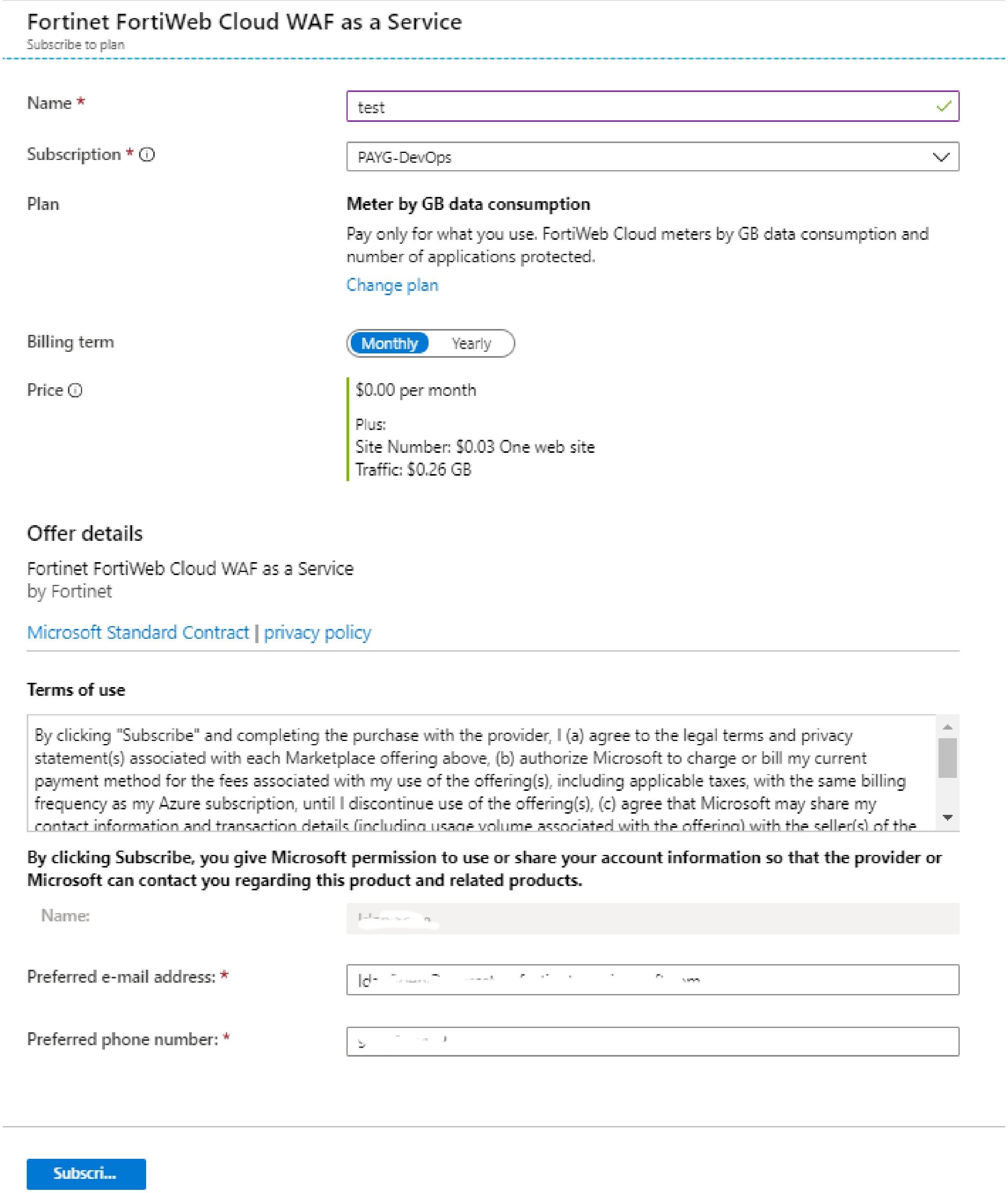
FortiWeb Cloud WAF-as-a- Service User Guide

FortiWeb Cloud WAF-as-a- Service Data Sheet

FortiWeb Cloud WAF-as-a- Service Portal

3. Enter a name for the subscription. Fill in the options on this page as desired, then click **Subscribe.** Wait for a few minutes for the subscription to be created.
   Do not clear the browser's cookie once the subscription is created, otherwise Fortinet won't know you are a

subscribed user when you register or log in to FortiWeb Cloud in later steps.



Fortinet FortiWeb Cloud WAF as a Service

Subscribe to plan

Name *	test ✓
Subscription * ⓘ	PAYG-DevOps
Plan	**Meter by GB data consumption** Pay only for what you use. FortiWeb Cloud meters by GB data consumption and number of applications protected. Change plan
Billing term	[✓ Monthly] Yearly
Price ⓘ	$0.00 per month Plus: Site Number: $0.03 One web site Traffic: $0.26 GB

Offer details

Fortinet FortiWeb Cloud WAF as a Service
by Fortinet

Microsoft Standard Contract | privacy policy

Terms of use

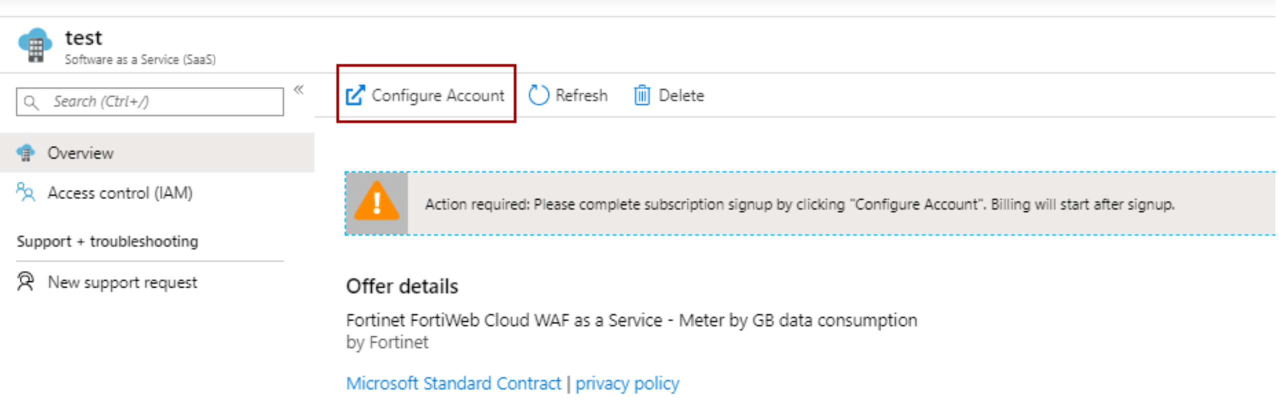
By clicking "Subscribe" and completing the purchase with the provider, I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), (c) agree that Microsoft may share my contact information and transaction details (including usage volume associated with the offering) with the seller(s) of the

By clicking Subscribe, you give Microsoft permission to use or share your account information so that the provider or Microsoft can contact you regarding this product and related products.

Name:	[redacted]
Preferred e-mail address: *	[redacted]
Preferred phone number: *	[redacted]

4. Select **Software as a Service (SaaS)** from Azure portal, find the FortiWeb Cloud subscription you just created. Click its name.

5. Click **Configure Account**. You will be directed to the landing page of FortiWeb Cloud where you can register or log in.



Action required: Please complete subscription signup by clicking "Configure Account". Billing will start after signup.

Offer details

Fortinet FortiWeb Cloud WAF as a Service - Meter by GB data consumption
by Fortinet

Microsoft Standard Contract | privacy policy

6. Log in with an existing FortiCloud account, or register a new account. You can access all of your Fortinet Cloud services and the Fortinet Support site through FortiCloud account.
   Your Azure subscription for FortiWeb Cloud will be automatically associated once you log in to your FortiCloud account.
   Make sure you are using the same browser when subscribing FortiWeb Cloud and logging in to FortiCloud account.

7. Log in to FortiWeb Cloud. Verify if the **Azure contracts** column displays in **Global > System Settings > Contracts**. If not, return to Azure Marketplace and search FortiWeb Cloud WAF-as-a-Service. There will be a notice leading you to the registration process again.

You will be charged based on an hourly rate of $0.03 per hour for every web application and a traffic usage rate of $0.4 per gigabyte (GB). The hourly rate metering will commence once you have onboarded an application on FortiWeb Cloud (regardless of its DNS status), while the traffic usage metering will begin when traffic is actively flowing through FortiWeb Cloud to your application.

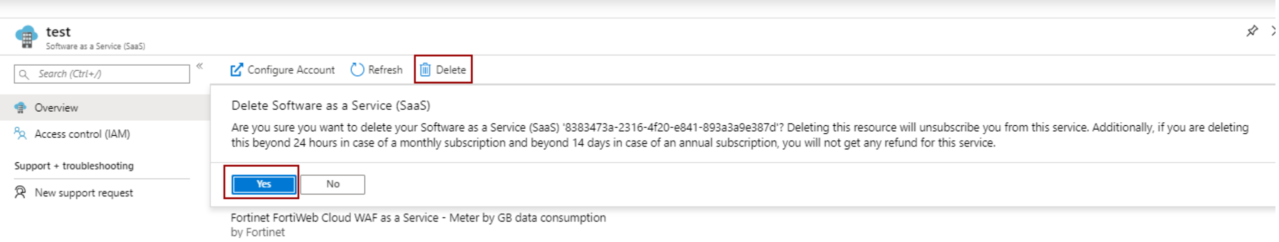
Please note that even if you subscribed through Azure, you can use FortiWeb Cloud to protect applications located on any other cloud platform or in your own network. The subscribing channel only determines the billing places for your FortiWeb Cloud usage.

Unsubscribing from FortiWeb Cloud on Azure

You can unsubscribe from FortiWeb Cloud anytime, but keep in mind that the data in your FortiWeb Cloud account will be cleared in one week after you unsubscribe. It can't be restored even if you subscribe to FortiWeb Cloud again. Please make sure all DNS changes have been done so your web application does not experience service interruption.

1. Log in to Azure. Select **Software as a Service (SaaS)** from Azure portal.
2. Find the FortiWeb Cloud subscription you want to cancel. Click its name.

3. Click **Delete**, then click **Yes** to confirm canceling the service.



Delete Software as a Service (SaaS)

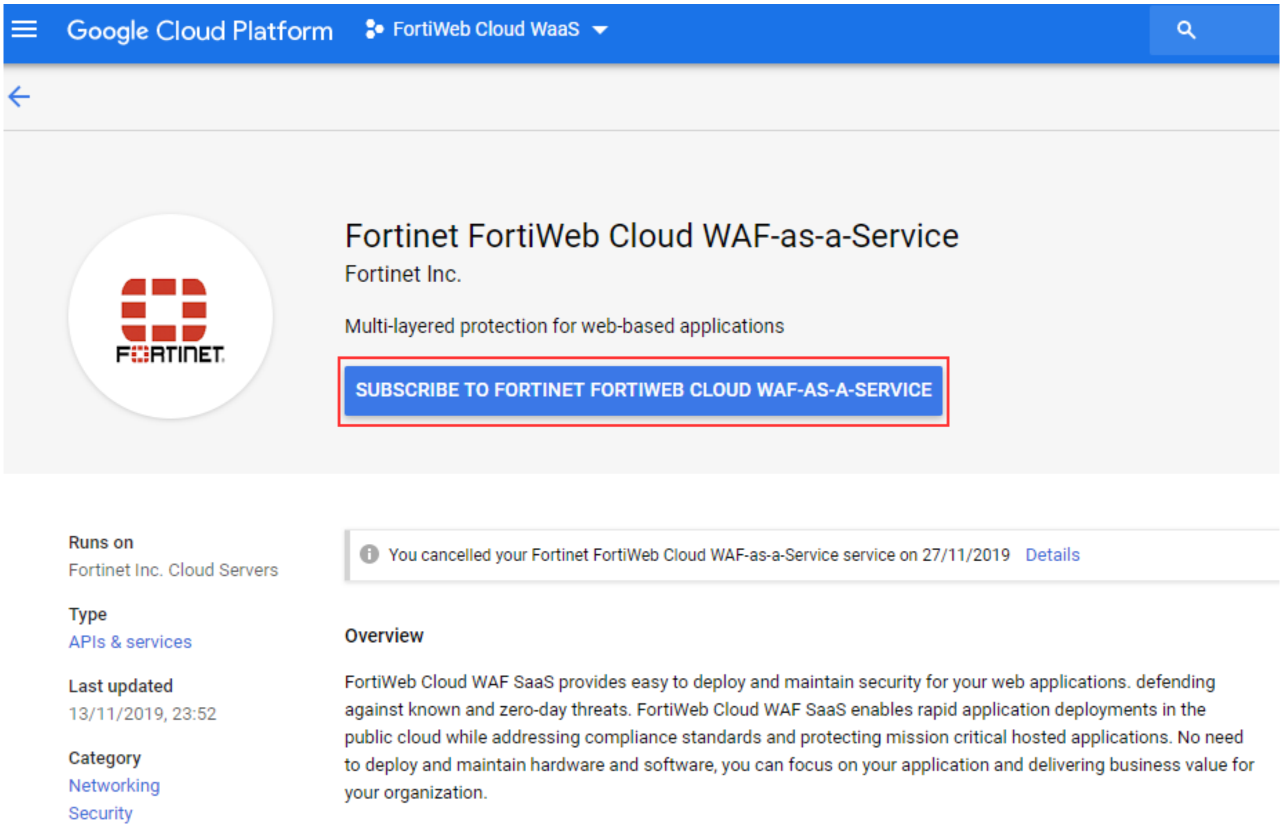
Are you sure you want to delete your Software as a Service (SaaS) '8383473a-2316-4f20-e841-893a3a9e387d'? Deleting this resource will unsubscribe you from this service. Additionally, if you are deleting this beyond 24 hours in case of a monthly subscription and beyond 14 days in case of an annual subscription, you will not get any refund for this service.

Fortinet FortiWeb Cloud WAF as a Service - Meter by GB data consumption
by Fortinet

Subscribing on Google Cloud Marketplace

Follow the steps below to subscribe FortiWeb Cloud on Google Cloud and associate your Google Cloud subscription with your FortiCloud account.

1. Log in to Google Cloud. Search **FortiWeb Cloud WAF as a Service** in Google Cloud Marketplace or click here: Google Cloud Marketplace.
.
2. Click **SUBSCRIBE TO FORTINET FORTIWEB CLOUD WAF-AS-A-SERVICE**.



Fortinet FortiWeb Cloud WAF-as-a-Service
Fortinet Inc.
Multi-layered protection for web-based applications

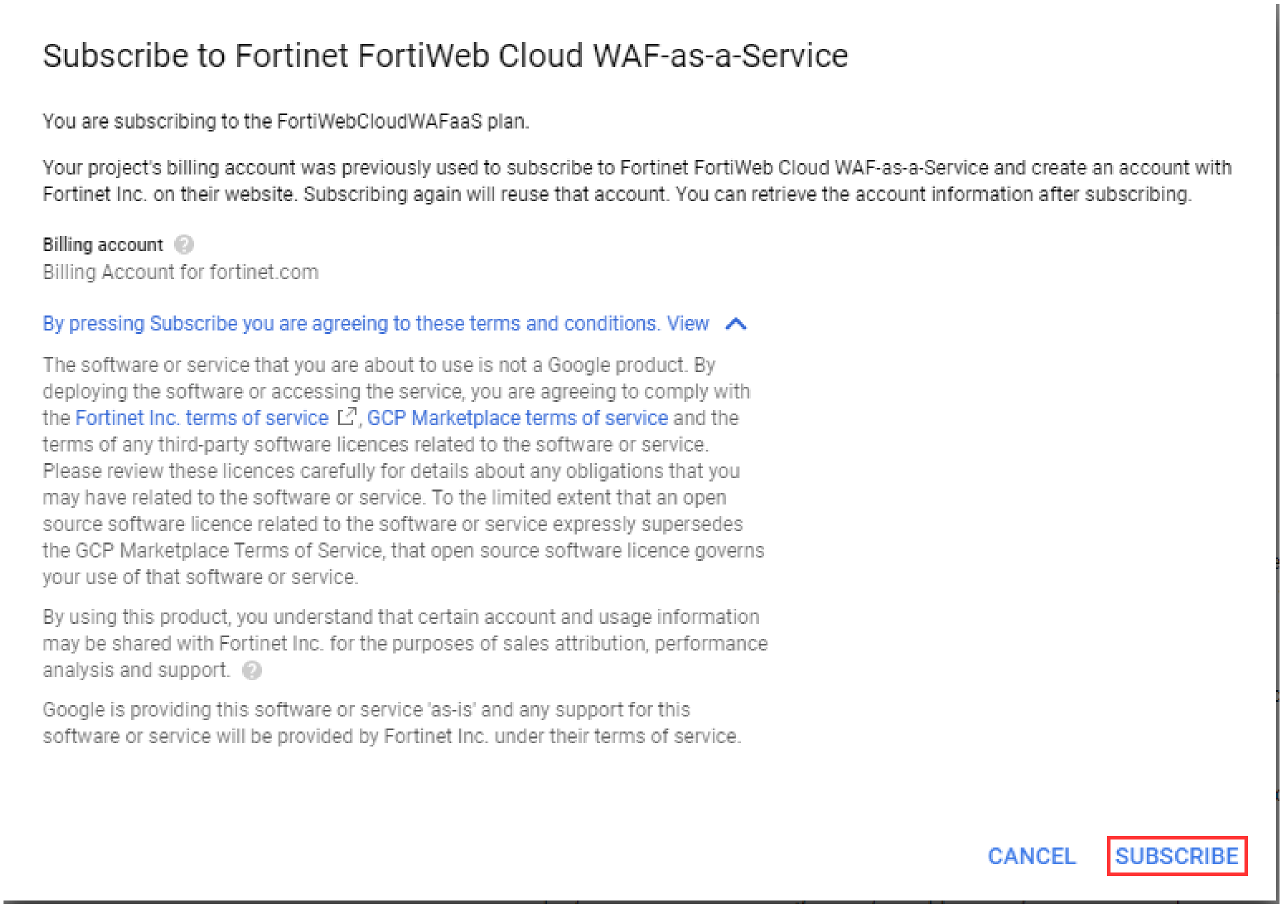
Runs on
Fortinet Inc. Cloud Servers
Type
APIs & services
Last updated
13/11/2019, 23:52
Category
Networking
Security

You cancelled your Fortinet FortiWeb Cloud WAF-as-a-Service service on 27/11/2019

Overview

FortiWeb Cloud WAF SaaS provides easy to deploy and maintain security for your web applications. defending against known and zero-day threats. FortiWeb Cloud WAF SaaS enables rapid application deployments in the public cloud while addressing compliance standards and protecting mission critical hosted applications. No need to deploy and maintain hardware and software, you can focus on your application and delivering business value for your organization.

3. Click **SUBSCRIBE**.



Subscribe to Fortinet FortiWeb Cloud WAF-as-a-Service

You are subscribing to the FortiWebCloudWAFaaS plan.

Your project's billing account was previously used to subscribe to Fortinet FortiWeb Cloud WAF-as-a-Service and create an account with Fortinet Inc. on their website. Subscribing again will reuse that account. You can retrieve the account information after subscribing.

Billing account ?
Billing Account for fortinet.com

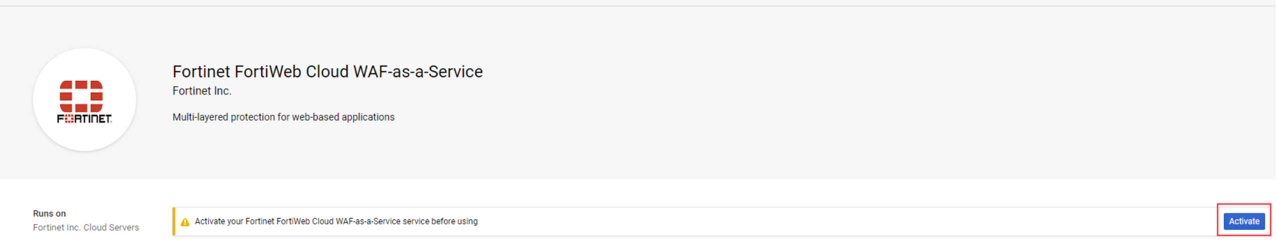
By pressing Subscribe you are agreeing to these terms and conditions. View ^

The software or service that you are about to use is not a Google product. By deploying the software or accessing the service, you are agreeing to comply with the Fortinet Inc. terms of service, GCP Marketplace terms of service and the terms of any third-party software licences related to the software or service. Please review these licences carefully for details about any obligations that you may have related to the software or service. To the limited extent that an open source software licence related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software licence governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with Fortinet Inc. for the purposes of sales attribution, performance analysis and support. ?

Google is providing this software or service 'as-is' and any support for this software or service will be provided by Fortinet Inc. under their terms of service.

4. Click **Activate**.



Fortinet FortiWeb Cloud WAF-as-a-Service
Fortinet Inc.

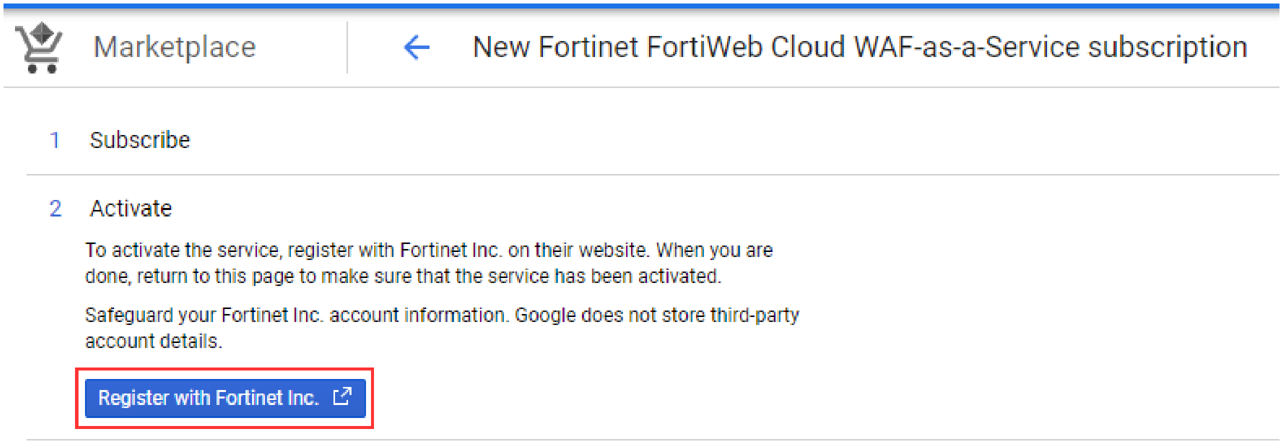
Multi-layered protection for web-based applications

Runs on
Fortinet Inc. Cloud Servers

Activate your Fortinet FortiWeb Cloud WAF-as-a-Service service before using

5. Click **Register with Fortinet Inc.** You will be directed to the landing page of FortiWeb Cloud where you can register or log in.
Do not clear the browser's cookie once the subscription is activated, otherwise Fortinet won't know you are a

subscribed user when you register or log in to FortiWeb Cloud in later steps.



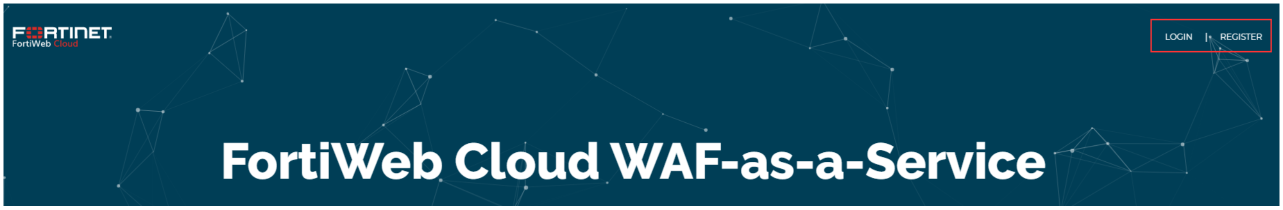
Marketplace
New Fortinet FortiWeb Cloud WAF-as-a-Service subscription
1 Subscribe
2 Activate

To activate the service, register with Fortinet Inc. on their website. When you are done, return to this page to make sure that the service has been activated.

Safeguard your Fortinet Inc. account information. Google does not store third-party account details.

Register with Fortinet Inc.

6. Log in with an existing FortiCloud account, or register a new account. You can access all of your Fortinet Cloud services and the Fortinet Support site through FortiCloud account.
   Your Google Cloud subscription for FortiWeb Cloud will be automatically associated once you log in to your FortiCloud account.
   Make sure you are using the same browser when subscribing FortiWeb Cloud and logging in to FortiCloud account.



7. Log in to FortiWeb Cloud, verify if the **Google Cloud contacts** column displays in **Global > Contacts**. If not, return to Google Cloud Marketplace and search FortiWeb Cloud WAF-as-a-Service. There will be a notice leading you to the registration process again.

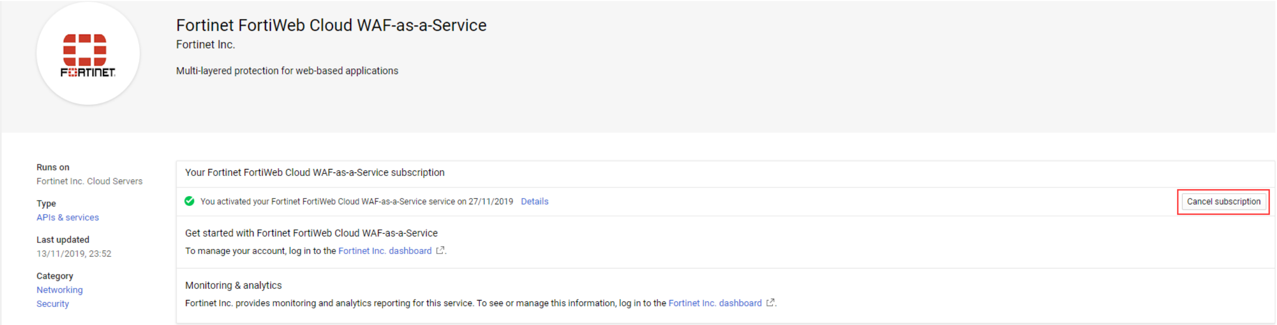
You will be charged based on an hourly rate of $0.03 per hour for every web application and a traffic usage rate of $0.4 per gigabyte (GB). The hourly rate metering will commence once you have onboarded an application on FortiWeb Cloud (regardless of its DNS status), while the traffic usage metering will begin when traffic is actively flowing through FortiWeb Cloud to your application.

Please note that even if you subscribed through Google Cloud, you can use FortiWeb Cloud to protect applications located on any other cloud platform or in your own network. The subscribing channel only determines the billing places for your FortiWeb Cloud usage.

Unsubscribing from FortiWeb Cloud on Google Cloud

You can unsubscribe from FortiWeb Cloud anytime, but keep in mind that the data in your FortiWeb Cloud account will be cleared in one week after you unsubscribe. It can't be restored even if you subscribe to FortiWeb Cloud again. Please make sure to replace CNAME with the right IP address in the DNS record so your web application does not experience service interruption.

1. Log in to Google Cloud. Search **FortiWeb Cloud WAF as a Service** in Google Cloud Marketplace.
2. Click **Cancel Subscription**.



Fortinet FortiWeb Cloud WAF-as-a-Service
Fortinet Inc.
Multi-layered protection for web-based applications

Runs on
Fortinet Inc. Cloud Servers
Type
APIs & services
Last updated
13/11/2019, 23:52
Category
Networking
Security

Your Fortinet FortiWeb Cloud WAF-as-a-Service subscription

✓ You activated your Fortinet FortiWeb Cloud WAF-as-a-Service service on 27/11/2019 Details

Get started with Fortinet FortiWeb Cloud WAF-as-a-Service
To manage your account, log in to the Fortinet Inc. dashboard.

Monitoring & analytics
Fortinet Inc. provides monitoring and analytics reporting for this service. To see or manage this information, log in to the Fortinet Inc. dashboard.

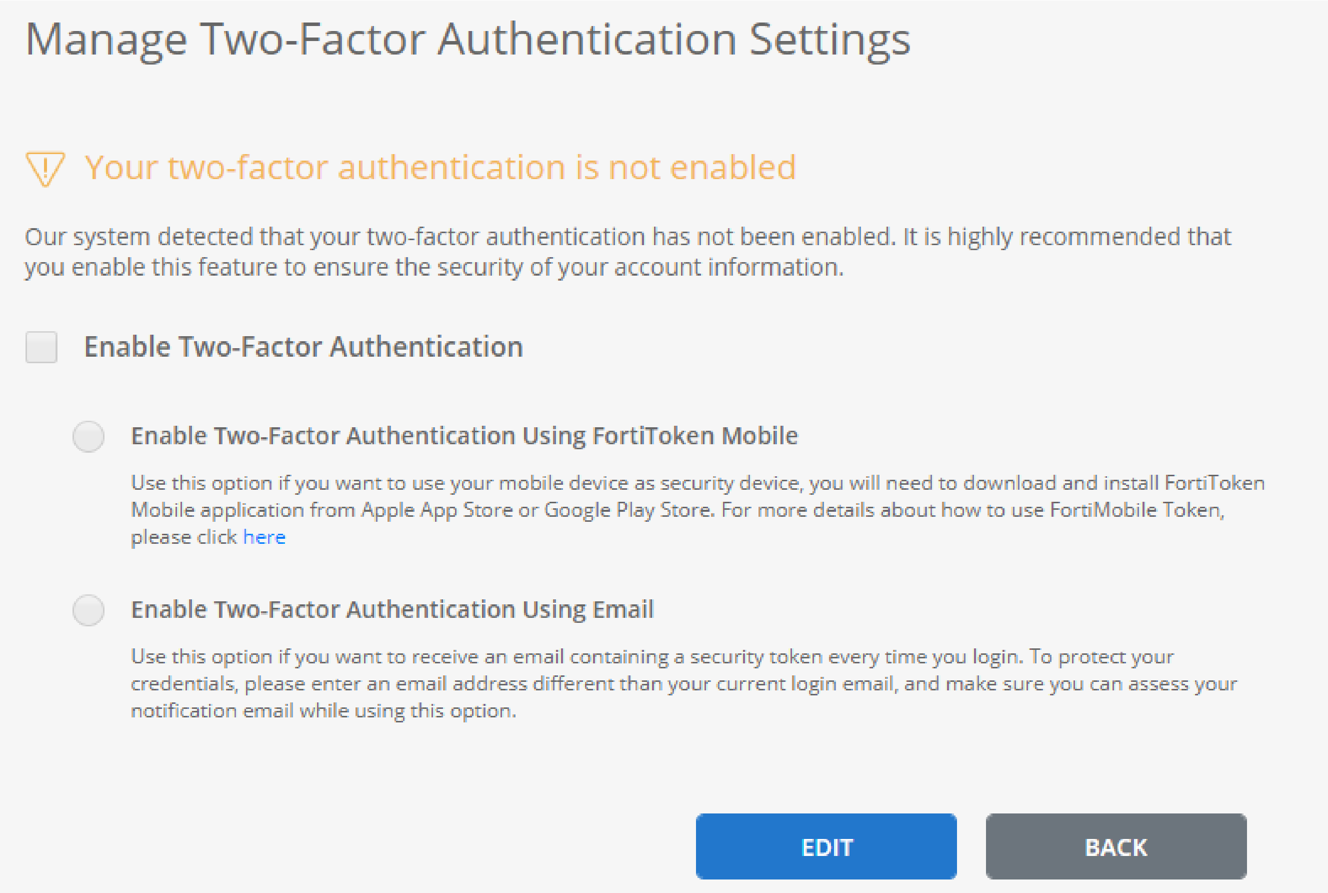
Subscribing on OCI Marketplace

Subscription via the OCI marketplace is not currently supported. To deploy on OCI, please see Licenses purchased from Fortinet.

Two-Factor Authentication

You can enable **Two-Factor Authentication** offered by FortiCloud for free. Your FortiCloud account will be secured by an additional security token sent through email or the FortiToken Mobile application: https://support.fortinet.com/Credentials/Account/TwoFASettings.aspx.

For more information, please see FortiCloud documentation for Two-Factor Authentication (2FA): https://docs.fortinet.com/document/forticloud/latest/identity-access-management-iam/729949/two-factor-authentication-2fa



Manage Two-Factor Authentication Settings

Your two-factor authentication is not enabled

Our system detected that your two-factor authentication has not been enabled. It is highly recommended that you enable this feature to ensure the security of your account information.

□ Enable Two-Factor Authentication

○ Enable Two-Factor Authentication Using FortiToken Mobile

Use this option if you want to use your mobile device as security device, you will need to download and install FortiToken Mobile application from Apple App Store or Google Play Store. For more details about how to use FortiMobile Token, please click here

○ Enable Two-Factor Authentication Using Email

Use this option if you want to receive an email containing a security token every time you login. To protect your credentials, please enter an email address different than your current login email, and make sure you can assess your notification email while using this option.

Getting started

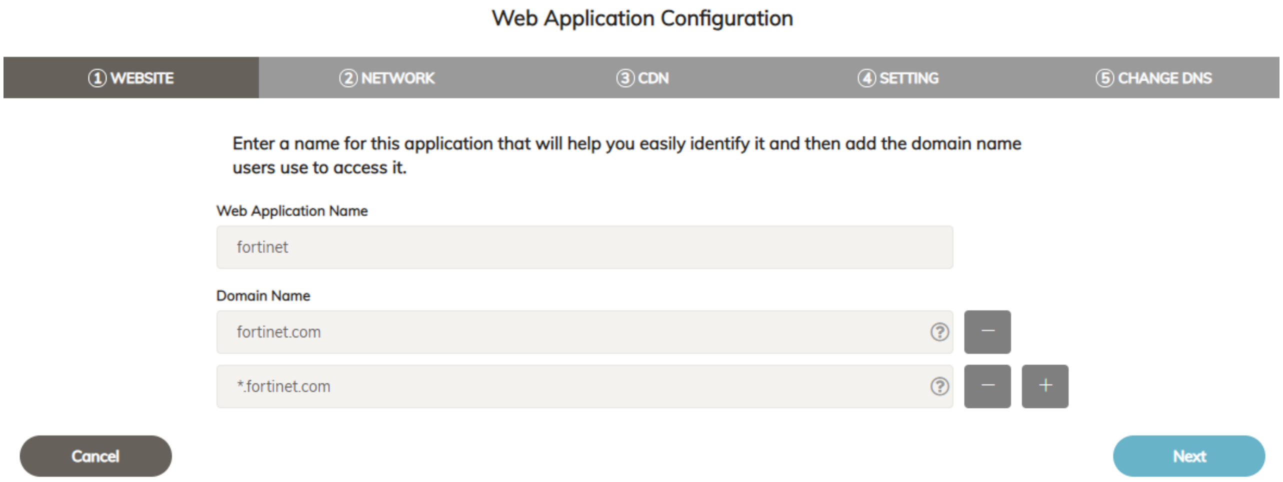
This section introduces how to onboard your applications and the basic setups of the network.

- Onboarding applications
- Example: Changing DNS records on AWS Route 53
- Changing IP addresses of origin servers
- Restricting direct traffic & allowing FortiWeb Cloud IP addresses
- How does FortiWeb Cloud choose regions?
- CDN
- Understanding block mode and action

Onboarding applications

Configure FortiWeb Cloud to protect your web applications by following these steps.
To onboard applications by DevOps tools, see Using FortiWeb Cloud with DevOps tools on page 193.

1. Go to www.fortiweb-cloud.com and log in with your FortiCloud account credentials.
2. Click **ADD APPLICATION** near the top right corner of the page. The ADD APPLICATION Wizard will open. You can return to this page by navigating to **Global>Applications**.
3. **Web Application Configuration**



Enter a name for this application that will help you easily identify it and then add the domain name users use to access it.

Web Application Name: fortinet

Domain Name: fortinet.com

*.fortinet.com

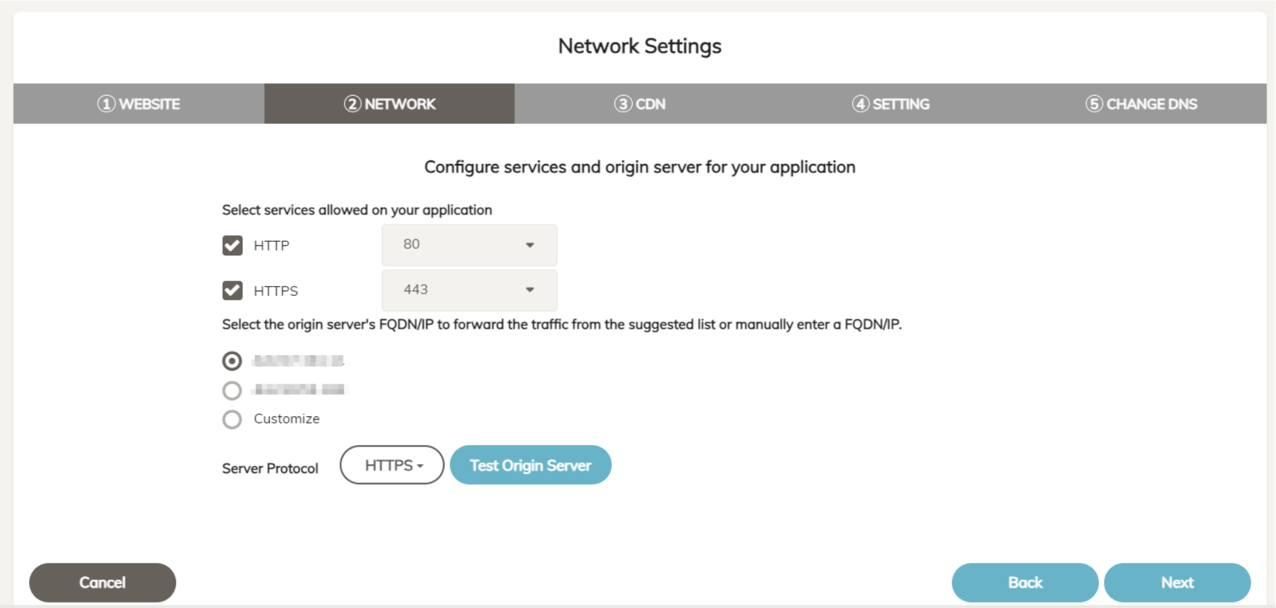
   a. Web Application Name: Enter a name for this application that will make it easy for you to identify within the FortiWeb Cloud UI.
   b. Domain Name: You can add up to 10 domains. They should belong to the same root domain, such as www.example.com and mail.example.com.

      Note: Once the application is onboarded, you cannot change the first domain in the list. Therefore, it is strongly recommended to enter the root domain as the initial domain, for example, example.com or www.example.com.
   c. Wildcard entries are allowed for all domains in the list except the first one. Ensure that domain name entries don't overlap; for instance, you can't add both "www.example.com" and "*.example.com" together.

      Wildcards only match strings at the same domain level; for example, "a.example.com" matches "*.example.com," but "a.a.example.com" does not.

      You can later go to **Network > Endpoints** to change or add domains.

4. **Network Settings**



Network Settings

① WEBSITE ② NETWORK ③ CDN ④ SETTING ⑤ CHANGE DNS

Configure services and origin server for your application

Select services allowed on your application

☑ HTTP 80

☑ HTTPS 443

Select the origin server's FQDN/IP to forward the traffic from the suggested list or manually enter a FQDN/IP.

● [redacted]

○ [redacted]

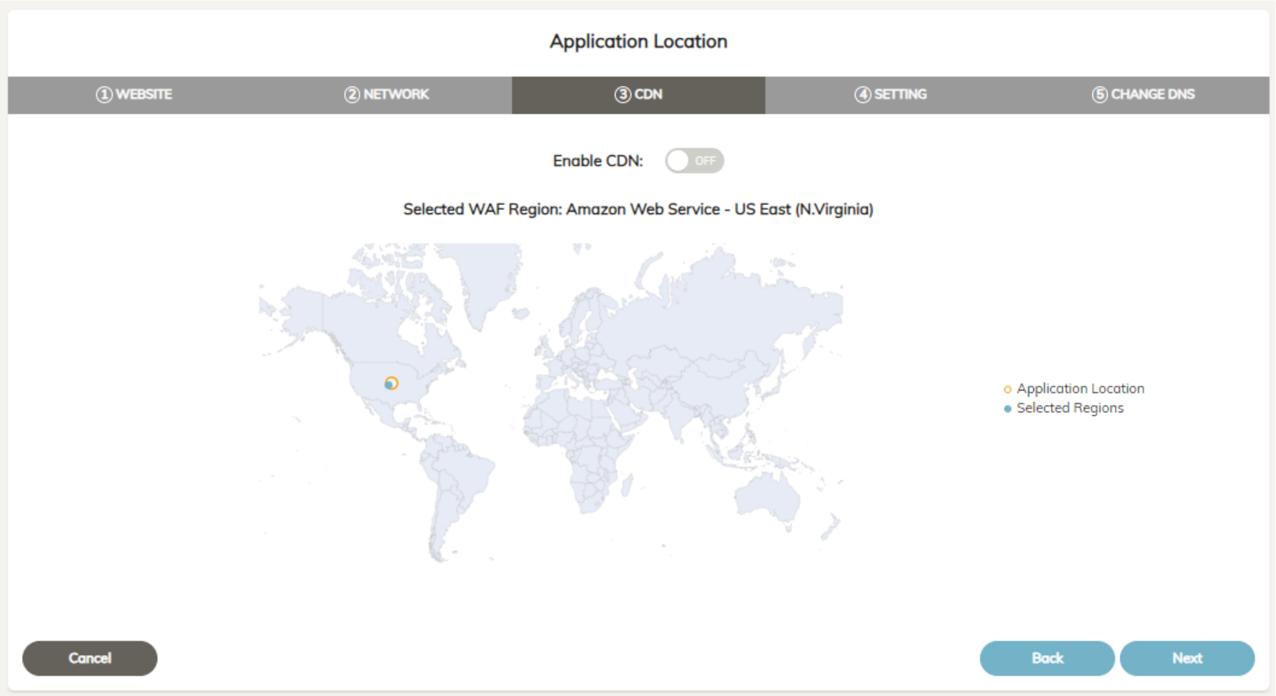
○ Customize

Server Protocol HTTPS ▾ Test Origin Server

Cancel Back Next

   a. Select the services allowed on your application and their corresponding ports. FortiWeb Cloud listen for HTTP and/or HTTPS traffic on the selected ports to allow only legitimate traffic to pass through. If the port number you want to use is not in the drop-down list, please contact Fortinet Support or your sales engineer to customize the port number. Please note that not all non-standard ports can be used.
   b. Select the IP address/FQDN for your web application. FortiWeb Cloud will direct traffic to the specified IP address.
      FortiWeb Cloud automatically fetches and displays available IP addresses and/or FQDNs associated with your entered domain, using port 443 as the default. FortiWeb Cloud keeps this information up to date.
      You can also choose **Customize** to enter a different IP address/FQDN and port number.
      If there are multiple origin servers hosting your web application, you can add them later in **Network > Origin Servers**.
   c. Under **Server Protocol**, you can configure the connection between FortiWeb Cloud and the origin server. If you want to redirect HTTP traffic to HTTPS, ensure that you have selected HTTPS.
   d. Click **Test Origin Server** to ensure that FortiWeb Cloud can connect to the origin server. By default, FortiWeb Cloud sends request to the URL path "/" to test responsiveness of the server, then populates the response code received from the server in the **Response Code** field of the load balancing rule in **Network > Origin Servers**.

5. **Application Location**



Enable CDN: OFF

Selected WAF Region: Amazon Web Service - US East (N.Virginia)

In this step, FortiWeb Cloud automatically selects a scrubbing center for your application according to the following conditions:

- FortiWeb Cloud checks whether your application server is deployed on AWS, Azure, and Google Cloud, then assigns a corresponding scrubbing center on the same cloud platform as your application server.
- If your application server is deployed elsewhere, FortiWeb Cloud by default assigns a scrubbing center on AWS.

See How does FortiWeb Cloud choose regions? on page 62 for more information.

After onboarding, you can switch the chosen scrubbing center within **Global > Applications**. However, you cannot select a scrubbing center from a different cloud platform. For instance, if your application server is on AWS, you cannot pick scrubbing centers deployed on Azure.

a. **CDN**

   If you enable CDN, the data on your origin servers can be cached in FortiWeb Cloud scrubbing centers distributed around the world. When users visit your application, they can be directed to the nearest scrubbing center and rendered with the requested data.

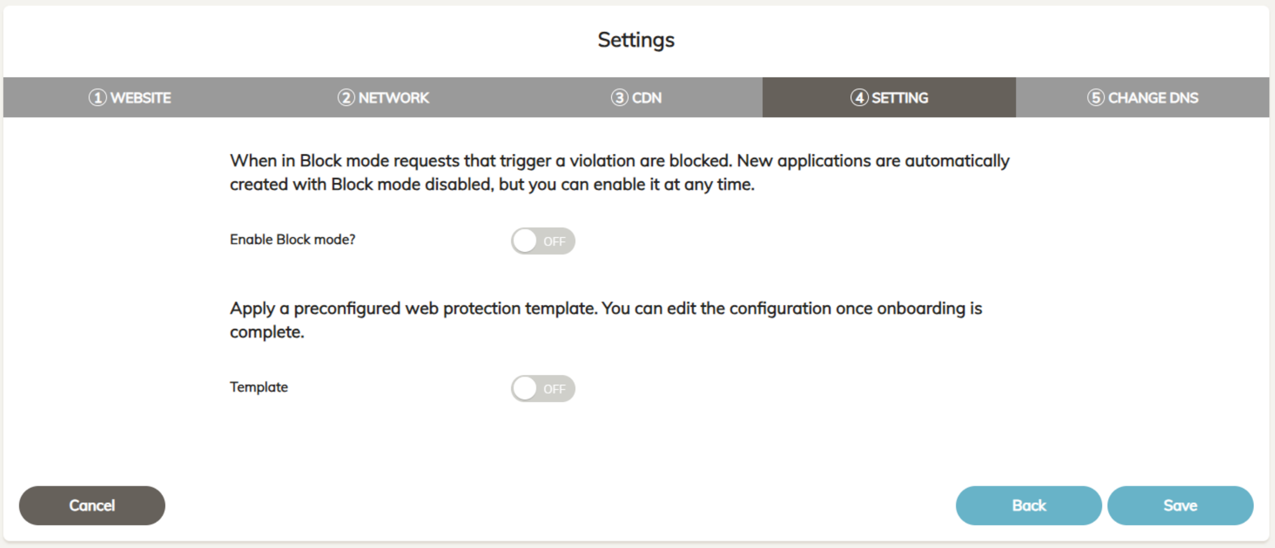
   With CDN enabled, you will be asked to select a specific continent or Global, which means your data will be cached on the scrubbing centers within a specific continent or around the world. Selecting a continent may reduce your traffic expense as data transfer is restricted within a continent rather than globally. For the impact on traffic expense when CDN is enabled, see CDN on page 62 for more information.

   By default, CDN is not enabled. This keeps your traffic bill to a minimum. Moreover, keeping traffic within the same region can help address compliance concerns.

   However, if user experience is your top concern, we recommend enabling CDN.

   If you can't decide now, you can revisit this option in **Global > Applications** after this application is onboarded.

6. **Settings**



Settings

When in Block mode requests that trigger a violation are blocked. New applications are automatically created with Block mode disabled, but you can enable it at any time.

Enable Block mode? OFF

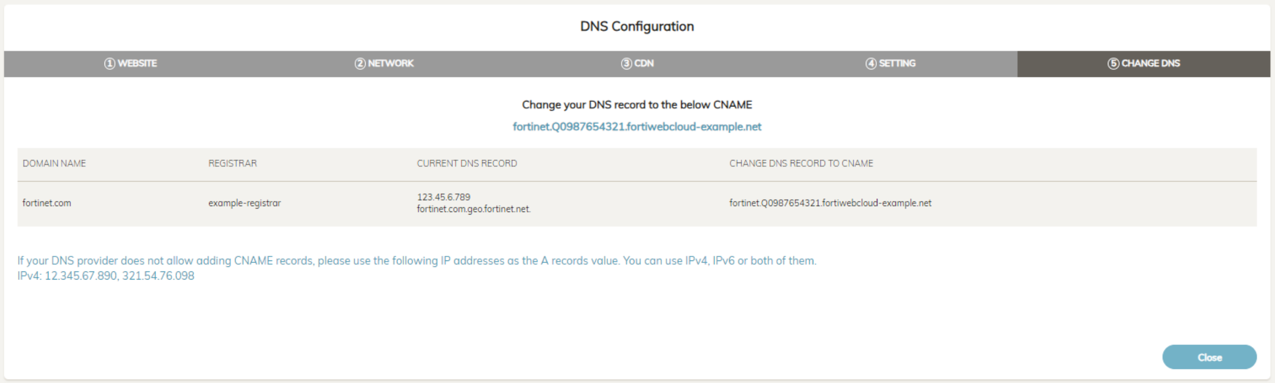
Apply a preconfigured web protection template. You can edit the configuration once onboarding is complete.

Template OFF

Configure Block mode and Template.

a. When **Block mode** is enabled, FortiWeb Cloud blocks requests if they trigger a violation. It's recommended to leave it disabled at the first week. During this period you can observe the attack logs and fine-tune the web protection configurations.
   You can later enable the Block Mode in **Dashboard** when you are confident that the traffic flow is stable and the legitimate traffic is not falsely blocked as attacks.
b. Enable **Template** if you would like to inherit WAF (Web Application Firewall) configurations from a template. You can edit the configuration after onboarding. See Templates on page 67 for more information. Leave this option unchecked if you prefer to fully customize your configuration from scratch.

7. **DNS configuration**



DNS Configuration

Change your DNS record to the below CNAME
fortinet.Q0987654321.fortiwebcloud-example.net

DOMAIN NAME	REGISTRAR	CURRENT DNS RECORD	CHANGE DNS RECORD TO CNAME
fortinet.com	example-registrar	123.45.6.789 fortinet.com.geo.fortinet.net.	fortinet.Q0987654321.fortiwebcloud-example.net

If your DNS provider does not allow adding CNAME records, please use the following IP addresses as the A records value. You can use IPv4, IPv6 or both of them.
IPv4: 12.345.67.890, 321.54.76.098

Go to your DNS provider, update your DNS record, and create a new record for the Automatic Certificate challenge as recommended. This ensures that traffic to your application can be correctly directed to FortiWeb Cloud.

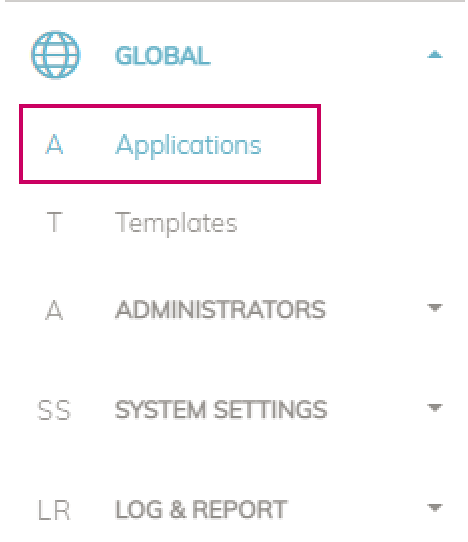
If there are multiple DNS records corresponding to the domain name, make sure to change all the records using the provided CNAME. Otherwise, users may encounter error when visiting your application. If the traffic to your application server should be first forwarded to a Content Distribution Service such as AWS CloudFront, before flowing to FortiWeb Cloud for threat detection, refer to Using FortiWeb Cloud behind a Content Distribution Service on page 218.
Please note that FortiWeb Cloud cannot get the DNS status if you use CloudFront, so the DNS status will always be

"Unknown" whether or not you have added the DNS record. Here we provide an example to show how to change the DNS record: Example: Changing DNS records on AWS Route 53

Note: You cannot directly access your website with the provided CNAME if you have not added the CNAME record in your DNS server. If you want to test it before changing the DNS record, follow steps below.

1. Run `ping` or `nslookup` command to get the IP address of CNAME.
2. Modify the HOST file of Windows or Linux by adding for example `www.<domain_name>.com` for the IP you get in Step a.
3. Access the domain name with the browser to test it.

8. To access the application you just onboarded, navigate to **Global > Applications** and click the name of the application.

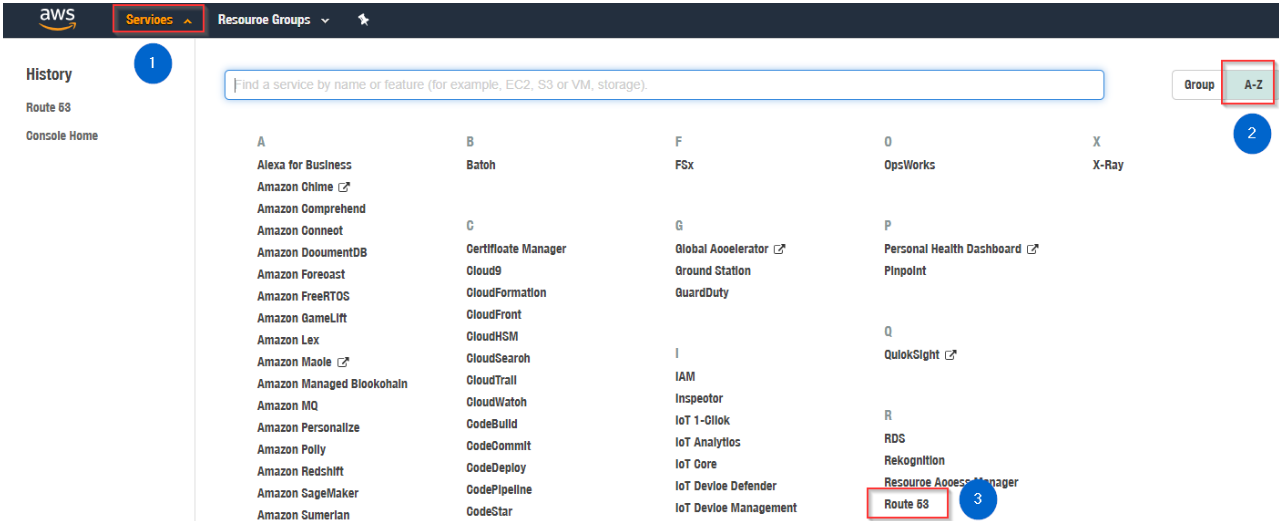


9. The application security modules will appear in the navigation pane. FortiWeb Cloud automatically assigns a security policy with the most basic web protection rules enabled. You can select additional protection rules using the **Modules** tab. See How to add or remove a module on page 127.

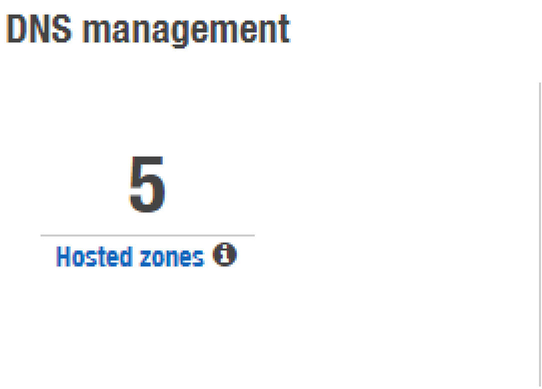
Example: Changing DNS records on AWS Route 53

To illustrate how to change DNS records using the CNAME provided by FortiWeb Cloud, here we suppose you are using AWS Route 53 as your DNS provider.

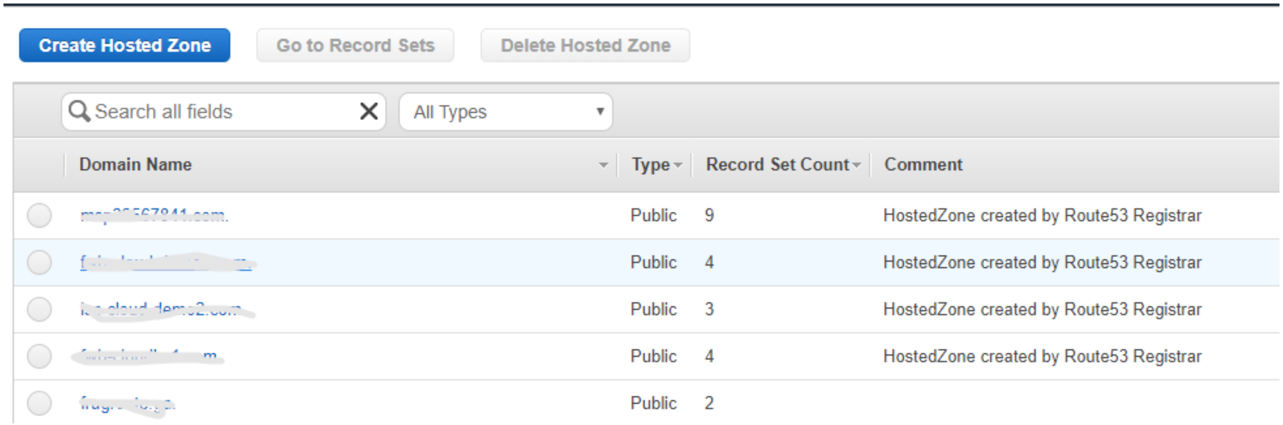
1. Log in to AWS. Select **Route 53**.



2. Click **Host zones** under **DNS management**.



3. Select the domain name of your application.

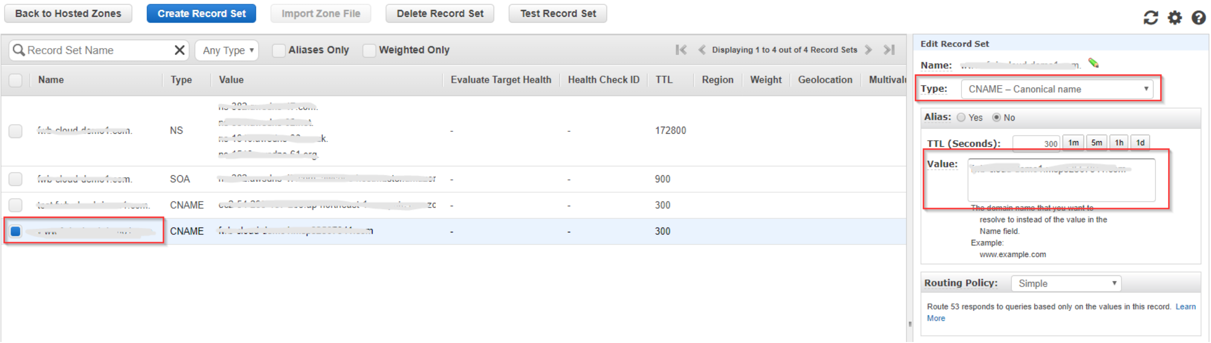


	Domain Name	Type	Record Set Count	Comment
○	[redacted]	Public	9	HostedZone created by Route53 Registrar
○	[redacted]	Public	4	HostedZone created by Route53 Registrar
○	[redacted]	Public	3	HostedZone created by Route53 Registrar
○	[redacted]	Public	4	HostedZone created by Route53 Registrar
○	[redacted]	Public	2	

4. Check the box before the domain name starting with "www.". The **Edit Record Set** pane will appear at the right side.

a. Select **CNAME - Canonical name** for the **Type**.

b. Delete the IP address(es) in the **Value** field, then paste the CNAME provided by FortiWeb Cloud.



Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region	Weight	Geolocation	Multivalu
[redacted]	NS	[redacted]	-	-	172800				
[redacted]	SOA	[redacted]	-	-	900				
[redacted]	CNAME	[redacted]	-	-	300				
[redacted]	CNAME	[redacted]	-	-	300				

Name: [redacted]

Type: CNAME – Canonical name

Alias: ○ Yes ● No

TTL (Seconds): 300

Value: [redacted]

The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

Changing IP addresses of origin servers

After the DNS records are changed, when users visit your application, the traffic is directed to FortiWeb Cloud instead of your back-end servers. Users will not be aware of the IP addresses of your back-end servers, but the IP addresses may exist in historical DNS lookups that were archived before you activated FortiWeb Cloud service. This could allow an attacker to bypass FortiWeb Cloud and attack your network infrastructure directly.

Therefore, it's recommended to change the IP addresses of your origin servers. Once they are changed, remember to update the IP address in **Network > Servers** so that FortiWeb Cloud can correctly forward traffic to the new address.

Restricting direct traffic & allowing FortiWeb Cloud IP addresses

Restricting direct traffic

Once you complete setting up FortiWeb Cloud, configure your application servers to only accept traffic from FortiWeb Cloud IP addresses.

- If CDN is enabled, make sure to accept traffic from **all the IP addresses listed in the following tables, including the service management IPs and the scrubbing centers' IPs**.
- If CDN is not enabled, configure to accept traffic from **the service management IPs and the scrubbing center assigned to your application server**.

However, it's recommended to accept traffic from all the following IP addresses, so that you don't need to go back and accept more IP addresses if you change the CDN status from disabled to enabled.

To know which scrubbing centers are assigned to your application, see How does FortiWeb Cloud choose regions? on page 62

Allowing FortiWeb Cloud IP addresses

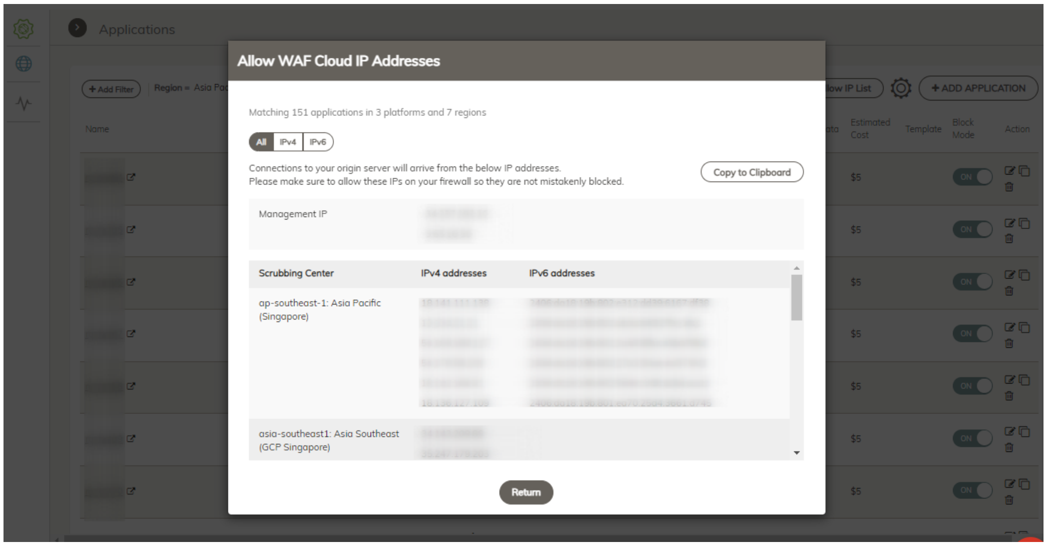
If you have deployed a DDoS device or system in your environment, it's most likely that FortiWeb Cloud's behavior will be detected as DDoS attacks, because all the requests arriving at your application server have FortiWeb Cloud's IP addresses as their source IP addresses.

To avoid this, highly recommend you to **add FortiWeb Cloud IP addresses to the allowlist of your DDoS device or system**.

The IP addresses labeled offline in the following tables are backup IP addresses, which can be used when the other IP addresses fail to work.

View the IP addresses of your region in **Global > Applications** by clicking the **Allow IP List** button. A window will pop up displaying all Cloud Waf IPs that need to be added to the firewall.

You can also filter for Platform, Name, and Domain Name by clicking **Add Filter** before clicking **Allow IP List**.



Allow WAF Cloud IP Addresses

Matching 151 applications in 3 platforms and 7 regions

Connections to your origin server will arrive from the below IP addresses.
Please make sure to allow these IPs on your firewall so they are not mistakenly blocked.

Management IP	[redacted]

Scrubbing Center	IPv4 addresses	IPv6 addresses
ap-southeast-1: Asia Pacific (Singapore)	[redacted]	[redacted]
asia-southeast1: Asia Southeast (GCP Singapore)	[redacted]	

We have provided two web pages listing all of the IPv4 and IPv6 addresses of the FortiWeb Cloud scrubbing centers: https://www.fortiweb-cloud.com/ips-v4 and https://www.fortiweb-cloud.com/ips-v6. These URLs can be referenced on a FortiGate as a "Threat Feed" which is dynamically kept up-to-date by the firewall, and can be referenced in security policy.

FortiWeb Cloud service management IP

The IP addresses of FortiWeb Cloud's services interacting with your application server	3.123.68.65 3.226.2.163

FortiWeb Cloud scrubbing centers on AWS

Scrubbing centers	IPv4 addresses	IPv6 addresses
ap-east-1: Asia Pacific (Hong Kong)	18.166.240.188 18.167.155.174	2406:da1e:b:ae01:31b6:202a:2bbc:79da 2406:da1e:b:ae02:f3f4:38fa:d7a2:311a

	16.163.110.210 18.167.190.240 16.163.212.249 18.166.175.52 18.162.227.141	2406:da1e:b:ae01:b1ae:20d2:703f:a868 2406:da1e:b:ae01:841e:27d4:4642:5f7f 2406:da1e:b:ae02:5b3d:9808:f840:b303 2406:da1e:b:ae01:b528:d77c:b017:a202 2406:da1e:b:ae02:52f5:30d5:fc8f:9e90
ap-southeast-1: Asia Pacific (Singapore)	54.179.22.186 18.140.21.233 18.136.170.71 13.214.45.126 52.77.123.220 13.215.241.201 13.251.178.146 52.220.49.161 13.228.126.80	2406:da18:ad1:1101:da8c:5ad5:b55e:5f54 2406:da18:ad1:1102:4019:44c9:e3ab:b2f6 2406:da18:ad1:1101:b6ad:34de:de05:5ef3 2406:da18:ad1:1102:9a1c:767e:1e67:4763 2406:da18:ad1:1101:f6f4:fec3:429b:cf21 2406:da18:ad1:1102:bcae:7ecd:6d98:a06 2406:da18:ad1:1101:5dbb:604b:b5b6:b092 2406:da18:ad1:1101:7215:137a:bfff:f7 2406:da18:ad1:1102:2df2:b6fb:c048:dcac
ap-southeast-2: Asia Pacific (Sydney)	13.236.106.64 13.237.77.127 13.237.159.2 54.79.207.53 13.54.172.164 13.210.41.167 54.252.85.192 54.153.144.173 52.62.180.47	2406:da1c:607:e201:df9c:6ba:4f89:6fd9 2406:da1c:607:e202:a298:e79a:d84b:cabc 2406:da1c:607:e201:dbc1:8ad8:624d:f906 2406:da1c:607:e202:30fe:b581:362b:e8b2 2406:da1c:607:e201:b8e0:4de5:dcdf:209c 2406:da1c:607:e202:9969:3b23:e201:e814 2406:da1c:607:e201:6e34:9ff2:ecb:c8eb 2406:da1c:607:e201:c0e7:f44c:7012:266a 2406:da1c:607:e202:1f5c:8b63:fbf2:28ea
ap-south-1: Asia Pacific (Mumbai)	15.207.198.87 15.206.52.49 3.109.248.211 3.109.17.189 13.234.208.160 3.108.143.49 43.204.40.78 13.235.108.225 13.232.35.27	2406:da1a:31:d501:50e1:400b:5699:2427 2406:da1a:31:d502:c14e:dcc9:5307:e359 2406:da1a:31:d501:fc19:5e59:9804:b392 2406:da1a:31:d502:2eaf:153f:91b3:7dc0 2406:da1a:31:d501:8064:5da4:4a3:5458 2406:da1a:31:d502:f7cf:30d8:60f3:ba2b 2406:da1a:31:d501:a644:652c:8e74:fa57 2406:da1a:31:d501:1972:5dbb:6a15:8486 2406:da1a:31:d502:bf3a:f0ac:d480:ed98
ca-central-1: Canada (Central)	52.60.112.90 99.79.174.29 3.97.158.98 3.97.249.50 3.99.18.71 99.79.119.81 99.79.85.123 15.223.11.8	2600:1f11:8c:9101:250e:bf5a:6646:e527 2600:1f11:8c:9102:abb2:7f29:6f98:ea53 2600:1f11:8c:9101:eb3:39f1:1815:884e 2600:1f11:8c:9102:411d:63f2:e5b4:5209 2600:1f11:8c:9101:d917:6c:8f07:f193 2600:1f11:8c:9102:729e:b7b1:34c:1e53 2600:1f11:8c:9101:86ea:d6ff:c7f0:ad44 2600:1f11:8c:9101:be54:e939:1483:fce6

	3.99.0.8	2600:1f11:8c:9102:974e:4977:6617:28a
eu-central-1: Europe (Frankfurt)	3.121.49.99 3.120.253.91 18.192.229.245 18.192.220.216 18.192.64.32 3.125.233.133 35.156.146.120 35.158.251.28 3.69.183.166 3.69.202.9 18.184.56.149 3.72.137.154 3.127.31.213 52.58.147.238 18.198.141.132 3.76.87.93 3.64.17.229 35.156.103.46 18.153.249.55 18.153.247.125	2a05:d014:f3c:6c01:cf53:8a1:630:517e 2a05:d014:f3c:6c02:30e:dcf4:4b91:8e01 2a05:d014:f3c:6c01:8571:cefb:8d43:6d3c 2a05:d014:f3c:6c02:2712:69b4:cf65:e99e 2a05:d014:f3c:6c01:99d0:8c50:ae51:99ac 2a05:d014:f3c:6c02:58:3e12:a98a:df9f 2a05:d014:f3c:6c01:24c5:1d8d:b3be:2785 2a05:d014:f3c:6c02:2490:b345:e759:f43f 2a05:d014:f3c:6c01:e799:dd65:59c7:d4b7 2a05:d014:f3c:6c02:af21:546d:5054:a7e3 2a05:d014:f3c:6c01:ae76:adc3:661d:29dc 2a05:d014:f3c:6c02:9041:85c2:24f5:592f 2a05:d014:f3c:6c01:5e7a:1eba:64:30ce 2a05:d014:f3c:6c02:3b5d:afaa:1d4:b8f1 2a05:d014:f3c:6c01:4508:b102:6ece:86cf 2a05:d014:f3c:6c02:f2cd:f562:1b85:dd7e 2a05:d014:f3c:6c01:a132:73e8:5b25:904d 2a05:d014:f3c:6c02:d36d:b5c3:b578:42de 2a05:d014:f3c:6c01:3d9f:78e9:cfe6:8fb8 2a05:d014:f3c:6c02:362:f81c:4417:a46a
eu-west-1: Europe (Ireland)	54.72.157.51 52.214.147.155 54.78.90.129 54.217.132.119 34.253.16.245 54.78.225.214 52.31.156.114 3.250.247.85 34.241.85.225 52.50.196.213 18.200.105.101	2a05:d018:77c:d901:e1bc:f536:85bb:5caa 2a05:d018:77c:d902:f60f:e089:c3ca:3743 2a05:d018:77c:d901:4f37:924f:6ea2:5952 2a05:d018:77c:d902:6605:9bef:2ca3:f220 2a05:d018:77c:d901:67a0:bb76:3597:b7f7 2a05:d018:77c:d902:a9ce:15bb:562f:7549 2a05:d018:77c:d901:7254:99fb:fee0:91c7 2a05:d018:77c:d901:12e0:4d59:ac0d:cceb 2a05:d018:77c:d902:608:4e5c:54c2:d4e2 2a05:d018:77c:d901:1509:1b4a:e9a1:8ce7 2a05:d018:77c:d902:4573:afbf:daf7:730a
eu-west-2: Europe (London)	18.130.214.145 3.9.251.147 18.134.173.119 52.56.112.105 3.11.174.119 3.11.12.196 3.11.216.166 18.168.230.94	2a05:d01c:64d:7001:5b0c:f5e1:f737:b883 2a05:d01c:64d:7002:e25b:55e:1564:21fd 2a05:d01c:64d:7001:7f27:28fe:f43b:e55b 2a05:d01c:64d:7002:a0b0:a076:53b2:31e3 2a05:d01c:64d:7001:dfb8:aa3d:3848:f26b 2a05:d01c:64d:7002:c77f:a8c8:7655:1cd1 2a05:d01c:64d:7001:d15a:3e1b:337f:92d7 2a05:d01c:64d:7001:1e54:38a8:2653:4d95

	18.130.48.8	2a05:d01c:64d:7002:8a95:b846:2f49:ca5b
	18.170.8.138	2a05:d01c:64d:7001:641e:9663:739a:33ca
	18.168.188.14	2a05:d01c:64d:7002:e585:8452:6fea:c326
eu-west-3: Europe (Paris)	35.181.28.236	2a05:d012:c22:9a01:77e0:8f18:fb7e:fb1e
	52.47.112.113	2a05:d012:c22:9a02:fa49:295e:27d5:1821
	13.36.206.34	2a05:d012:c22:9a01:d23a:98af:1e6c:c9fb
	15.188.2.107	2a05:d012:c22:9a02:fc4a:2226:47cd:66f5
	35.181.84.20	2a05:d012:c22:9a01:6fbc:eb92:7eb5:fa4a
	13.36.245.25	2a05:d012:c22:9a02:a1ca:7e27:28f7:bbba
	35.181.130.113	2a05:d012:c22:9a01:f7c8:b42:a1d9:1c5e
	13.36.99.148	2a05:d012:c22:9a01:85ed:d68a:483:26c7
	35.180.221.56	2a05:d012:c22:9a02:daa8:f4b8:3356:98e6
	13.39.124.108	2a05:d012:c22:9a01:335f:ba6:f76:df50
	13.36.113.40	2a05:d012:c22:9a02:b26d:7261:bc18:48c8
eu-south-1: Europe (Milan)	15.161.173.116	2a05:d01a:9f2:1701:bd84:9314:f93:b2f
	15.161.10.152	2a05:d01a:9f2:1702:aca5:5d4d:1995:50d
	15.161.215.247	2a05:d01a:9f2:1701:4d5b:f1a8:d291:5a84
	15.161.76.114	2a05:d01a:9f2:1702:8e71:e939:c954:1608
	18.102.20.169	2a05:d01a:9f2:1701:eb19:dfb0:2ba0:9782
	18.102.26.204	2a05:d01a:9f2:1702:306c:6cac:b6f3:d03e
	35.152.36.51	2a05:d01a:9f2:1701:9734:6666:5d:40ec
	15.161.83.238	2a05:d01a:9f2:1701:53ba:32e9:7ef2:198f
	18.102.19.162	2a05:d01a:9f2:1702:dead:f4ac:dc23:9d6e
	18.102.146.236	2a05:d01a:9f2:1701:b077:f47d:2a5c:96f2
	15.160.64.40	2a05:d01a:9f2:1702:8ba8:740e:184a:260e
Il-central-1: AWS Israel (Tel Aviv)	51.16.118.151	2a05:d025:c86:1701:39b:f35d:2126:5c85
	51.17.26.125	2a05:d025:c86:1702:3be9:6a28:de24:3589
	51.16.198.214	2a05:d025:c86:1701:1eb6:57b5:dfe6:4cfb
	51.16.192.242	2a05:d025:c86:1702:4ddf:2b90:a945:ea28
	51.16.117.96	2a05:d025:c86:1701:ed95:3527:e666:1dc9
	51.17.163.97	2a05:d025:c86:1702:ca77:80c5:56ba:45dd
us-east-1: US East (N. Virginia)	3.226.118.124	2600:1f18:1492:1701:5ebe:2322:bb2e:1c87
	3.210.115.14	2600:1f18:1492:1702:af7a:a957:dd53:be07
	54.144.250.206	2600:1f18:1492:1701:b42b:c8b6:9d9b:5752
	23.21.42.132	2600:1f18:1492:1702:eebf:68e3:7e83:a9a6
	34.233.191.126	2600:1f18:1492:1701:6910:cfcf:2f0a:9102
	54.198.165.25	2600:1f18:1492:1702:d556:77ec:34ad:4cbb
	3.228.64.186	2600:1f18:1492:1701:e54f:59c6:7114:2878
	3.231.16.50	2600:1f18:1492:1702:e618:cb8e:f4b5:4ba4
	54.156.35.181	2600:1f18:1492:1701:c65b:f5d9:784d:d3d6

	52.22.134.181	2600:1f18:1492:1702:7e65:574b:1013:7209
	3.224.233.117	2600:1f18:1492:1701:c800:b061:afc1:5a2a
	174.129.221.93	2600:1f18:1492:1702:aa32:a7b0:116f:1b69
	3.214.245.110	2600:1f18:1492:1701:7c58:5331:25e3:3343
	3.225.188.145	2600:1f18:1492:1702:b3ff:2b1d:d9a7:9e88
	18.214.30.87	2600:1f18:1492:1701:6451:e2d7:11bc:da4d
	34.206.129.226	2600:1f18:1492:1702:9f57:b34f:ef00:726
	100.25.206.91	2600:1f18:1492:1701:7906:404b:ba59:dff3
	52.44.217.91	2600:1f18:1492:1702:524:eda4:749f:26d6
	54.205.81.107	2600:1f18:1492:1701:a59a:4a1b:5e1a:f223
	54.86.225.255	2600:1f18:1492:1702:a3ca:e551:92ce:e11
us-east-2: US East (Ohio)	3.19.24.89	2600:1f16:160:aa01:f753:ce95:4466:884f
	3.13.39.239	2600:1f16:160:aa02:d842:2cf8:964c:b004
	3.131.242.28	2600:1f16:160:aa01:4584:fec1:ab59:6bd4
	18.188.127.1	2600:1f16:160:aa02:5629:28f1:196d:acbe
	3.139.50.156	2600:1f16:160:aa01:8769:8d0b:d2de:28d4
	18.189.50.81	2600:1f16:160:aa02:2752:5869:d2af:3811
	52.15.38.41	2600:1f16:160:aa01:4b21:e5ce:3c8e:c368
	3.129.83.41	2600:1f16:160:aa01:ad18:2fce:479f:a78f
	3.13.53.24	2600:1f16:160:aa02:3a6:c48:a903:de9
	18.224.115.39	2600:1f16:160:aa01:1749:9160:1c6a:5e9f
	3.134.201.211	2600:1f16:160:aa02:b510:7929:d3e6:12e6
us-west-1: US West (N. California)	13.56.33.144	2600:1f1c:b97:d801:6efe:3295:e11a:e6b
	52.52.208.2	2600:1f1c:b97:d802:d788:18f9:b8e3:a981
	52.8.219.206	2600:1f1c:b97:d801:ff83:8b03:7a29:5981
	52.9.219.121	2600:1f1c:b97:d802:fe8f:1a5d:5d1:1c6b
	54.193.111.235	2600:1f1c:b97:d801:e6c4:34b2:d9cb:4147
	52.9.188.134	2600:1f1c:b97:d802:d073:2d49:432:2aa6
	52.9.57.162	2600:1f1c:b97:d801:e507:2d99:87b1:b666
	184.169.166.201	2600:1f1c:b97:d801:8fb0:a6dd:1f2a:54db
	54.176.39.164	2600:1f1c:b97:d802:43f8:ddcc:da5e:b21e
us-west-2: US West (Oregon)	54.70.126.22	2600:1f14:b5a:da01:d056:d959:eb59:49e2
	54.186.80.150	2600:1f14:b5a:da02:88c1:8365:8baf:677
	35.160.55.58	2600:1f14:b5a:da01:a32:4cac:f337:9c00
	44.241.247.81	2600:1f14:b5a:da02:5a8e:d30:ff37:18a9
	35.85.67.11	2600:1f14:b5a:da01:ab8a:9684:cd53:598d
	35.155.214.19	2600:1f14:b5a:da02:fdfa:2560:ae51:20ee
	44.227.236.231	2600:1f14:b5a:da01:df9a:f157:a04a:b1a1
	18.224.115.39	2600:1f16:160:aa01:1749:9160:1c6a:5e9f
	3.134.201.211	2600:1f16:160:aa02:b510:7929:d3e6:12e6

	44.225.123.220	2600:1f14:b5a:da01:a4c6:ab36:7bf9:915d
	34.214.132.181	2600:1f14:b5a:da02:2a4e:edb1:7409:dfb9
sa-east-1: South America (Sao Paulo)	54.207.7.119	2600:1f1e:653:3201:e41:9bc0:8071:cec0
	18.231.48.25	2600:1f1e:653:3202:2261:f67:9605:ebbe
	54.207.227.252	2600:1f1e:653:3201:eac8:161d:c0a:6915
	177.71.170.92	2600:1f1e:653:3202:3615:6e2c:7b0c:85c9
	18.228.169.208	2600:1f1e:653:3201:8fed:9a99:d38e:4855
	54.207.65.147	2600:1f1e:653:3202:d9f7:e5d7:ab2f:e684
	52.67.36.82	2600:1f1e:653:3201:b266:d210:941f:46bb
	18.229.224.63	2600:1f1e:653:3201:6d62:b616:3070:869f
	15.229.95.152	2600:1f1e:653:3202:cad1:1b69:28e2:ccea
	52.67.231.140	2600:1f1e:653:3201:503e:4983:215f:927e
	54.233.79.85	2600:1f1e:653:3202:5504:9120:fcb1:9b8f

FortiWeb Cloud scrubbing centers on Azure

Scrubbing centers	IPv4 addresses
West Europe	52.149.70.62
	52.149.99.16
	20.86.129.248
	20.86.49.155
	51.124.233.151
	20.4.62.24
	20.4.62.25
	13.95.206.25
	13.95.206.33
	104.40.255.125
	13.80.68.18
	13.80.71.152
West US2	40.90.196.194
	40.90.208.131
	20.29.202.53
	20.29.202.44
	20.29.202.61
	20.230.223.218
	20.230.221.119
East US	40.90.225.162
	40.90.250.88
	52.151.250.58

Scrubbing centers	IPv4 addresses
	20.62.192.27 20.127.74.161 20.127.74.103 20.127.74.143 172.190.214.230 172.190.214.225
East US2	20.69.235.177 20.81.153.33 20.110.208.49 20.110.186.177 20.14.167.255 20.65.95.32 20.10.155.255 172.176.244.200 172.176.244.209
Australia East	20.70.160.47 20.70.152.97 20.248.200.0 20.248.200.83 20.28.181.79 20.28.181.228
Brazil South (São Paulo State)	20.195.163.139 20.197.225.122 20.226.106.176 20.226.106.172 4.228.89.120 4.228.89.123
Brazil South3	4.228.89.120 4.228.89.123
Canada Central	20.63.56.203 20.63.58.199 20.48.236.10 20.48.236.225 20.220.63.30 20.220.59.101

FortiWeb Cloud scrubbing centers on Google Cloud

Scrubbing centers	IPv4 addresses
europe-west3 (Frankfurt)	35.242.209.119 35.242.218.171 34.159.173.59 35.198.124.236
europe-west8 (Milan)	34.154.63.30 34.154.60.54 34.154.148.78 34.154.84.52
me-west1 (Tel Aviv)	34.165.140.173 34.165.109.6 34.165.80.144 34.165.254.142 34.165.184.29 34.165.1.25
us-east1 (South Carolina)	34.74.199.185 35.227.112.86 34.148.6.49 34.138.149.79
us-west1 (Oregon)	34.83.129.59 34.82.233.199 34.83.15.189 34.168.224.208

FortiWeb Cloud scrubbing centers on OCI

Scrubbing centers	IPv4 addresses
US East (Ashburn)	193.122.181.94 129.159.75.103 129.159.74.168 (offline)
US West (Phoenix)	158.101.43.252 158.101.43.253 129.146.233.205 (offline)
Germany Central (Frankfurt)	158.101.176.179 193.122.55.66 132.145.248.29 (offline)

How does FortiWeb Cloud choose regions?

When you onboard application, FortiWeb Cloud checks the IP address of your origin server to get its location, then suggest a FortiWeb Cloud scrubbing center based on the following factors:

- First, we determine if your application server is deployed on AWS, Azure, OCI, or Google Cloud.
  - If yes, the scrubbing centers located on the same cloud platform with your application server will be picked out for further screening.
  - If no, the scrubbing center located in EU (Frankfurt) or US East (N. Virginia) region on AWS will be suggested for your application, depending on whether your application server is in Europe or the rest of the world.
- Among the ones picked out against the first criterion, we then determine whether there is a scrubbing center deployed in the same region with your application server.
  - If yes, we will suggest that scrubbing center.
  - If no, the following scrubbing centers will be suggested:

	AWS	Azure	Google Cloud	OCI
For application servers located in Europe	EU (Frankfurt)	West Europe (Netherlands)	Europe-west3 (Frankfurt)	Germany Central (Frankfurt)
For application servers located in the rest of the world	US East (N. Virginia)	East US (Virginia)	Us-east1 (South Carolina)	US East (Ashburn)

If you enable CDN, there will not be a fixed scrubbing center assigned to you. The traffic from your users around the world can be directed to any scrubbing center (depending on whether you have selected a specific continent or Global) which is the closest to them. Be aware that users can't be directed to a cross-platform scrubbing center, for example, if your application server is on AWS, then your users can only be directed to the scrubbing centers on AWS.

With CDN enabled, if your application server is not deployed on the above mentioned cloud platforms, for example, it's deployed in your private on-premise network, then your users will be directed to the AWS regions closest to their locations.

See this article for the regions where FortiWeb Cloud scrubbing centers are deployed.

CDN

If CDN is enabled, the data on your origin servers will be cached in FortiWeb Cloud scrubbing centers distributed around the world or within a certain continent. When users request data from your application, they can be directed to the nearest scrubbing center and rendered with the requested data. For the list of scrubbing centers, see Restricting direct traffic & allowing FortiWeb Cloud IP addresses on page 53.

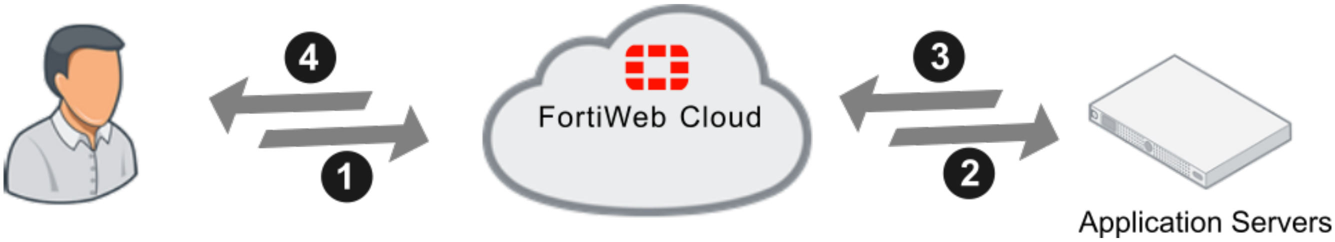
You can enable CDN when onboarding an application, or set this option in the **Application Settings** dialog (**Global > Applications**).

Traffic expenses with CDN enabled

The traffic expenses may increase if you enable CDN.

The following graph shows a typical traffic flow when a user initiates a request to the data stored on your application server. It helps you understand which part of traffic expense increases if CDN is enabled.

1. User's request first reaches FortiWeb Cloud scrubbing center for threat detection.
2. FortiWeb Cloud sends request to your application server to get the data requested by the user.
3. The application server sends response to FortiWeb Cloud.
4. FortiWeb Cloud sends response to the user.



Your traffic expense includes the following two parts:

- Expense for traffic flow number 4. That is, the traffic sent from FortiWeb Cloud to your application users. FortiWeb Cloud charges for this traffic with a fixed rate. It does not change whether CDN is enabled or not.
- Expense for traffic flow number 3. That is, the traffic outbound from your application server to FortiWeb Cloud. Your Internet Service Provider (ISP) charges you for this part of the expense. The unit price for this traffic might vary depending on whether CDN is enabled or not.

If CDN is not enabled, you will be assigned with a FortiWeb Cloud scrubbing center located in the same region with your application server, or a region closest to your application server.

If CDN is enabled, depending on whether you have selected a specific continent or Global, user requests are directed to the nearest FortiWeb Cloud scrubbing center (either globally or within the specified continent) closest to the user, but it could be far from the places where your application server is located.

So, for traffic flow number 3, the transmission path might be comparatively longer when CDN is enabled. Your ISP probably will charge you with a higher price for the long distance transmission. For example, AWS **intra-region** data transfer is considerably higher than **in-region** data transfer (See AWS pricing policy).

- If your application server is deployed on AWS, Azure, OCI, or Google Cloud, you will be charged for the intra-region data transfer if CDN is enabled.
- If your application server is deployed elsewhere, such as in your private on-premise environment, FortiWeb Cloud scrubbing centers located on AWS will process the traffic. Please consult your ISP about the price of data transfer between your application server and FortiWeb Cloud scrubbing center.

Please note that enabling CDN does not always cause the traffic expense to increase. In cases where user request hits the data cached on FortiWeb Cloud, FortiWeb Cloud directly sends response to the user. As there isn't any traffic flow from your application server to FortiWeb Cloud, no expense will incur. By caching data on FortiWeb Cloud, it saves the cost to fetch data from your application sever every time when users request it.

Understanding block mode and action

Block mode

On **Applications** page, you can turn on/off the **Block Mode** for each application.

When to enable block mode

- When Block Mode is enabled, FortiWeb Cloud will take actions as specified in Action of each WAF module. blocks requests if they trigger violations. Your application server does not receive these requests.
- When Block Mode is disabled, FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests.

Check the following prerequisites before you enable the Block Mode:

- The endpoints and servers are configured properly. The traffic flow between the clients, FortiWeb Cloud, and your application servers is stable.
- Observe the attack logs in **FortiView** or **Logs**. If legitimate traffic is falsely detected as attacks (also called false positives), add exceptions or modify the web protection configurations to avoid false positives in the future.

Action

When you have enabled **Advanced Configuration** in **Global > System Settings > Settings**, you can configure actions for each WAF feature specifically. If **Advanced Configuration** is disabled, the default actions of each WAF feature will work instead.

When Block Mode is disabled, FortiWeb Cloud will accept all requests and generate logs for all violations without considering the specified actions in each WAF feature.

When Block Mode is enabled, all requests will be blocked if they trigger the violation, and the specific actions you have configured in each WAF feature will prevail. For example, if you set the Action for Known Attacks as Alert & Deny, FortiWeb Cloud will block the request (or reset the connection) and generate a log message.

Global settings

Configure settings that are applied globally to your account.

- Application management
- Templates on page 67
- Admin management
- Role management
- Settings
- Contracts
- Cloud Connectors
- Custom block pages
- Audit logs on page 83
- Reports
- Usage on page 87

Application management

On the Applications page, you can manage configurations related to applications, including viewing application information, filtering applications, onboarding applications, enabling/disabling CDN, selecting FortiWeb Cloud scrubbing centers for your application.

- Viewing application information
- Onboarding applications
- Cloning the application configurations
- Enabling/disabling CDN
- Selecting FortiWeb Cloud scrubbing center

Viewing application information

The application table displays all the applications you have onboarded. You can view the following information about an application. Click **Add Filter** to create a filter based on Application table fields. Click the **Column Settings** icon ⚙ to select the columns being displayed in the table.

Domain Name	The domain name of the application. If you have added more than one domain name, click the number mark to view all the domain name. You can change the domain names in **Network > Endpoints**.
Platform	The platform where the FortiWeb Cloud scrubbing center assigned to your application is

	located. You can click the edit icon ✎ to change the region.
Region	The FortiWeb Cloud scrubbing center assigned to your application.
DNS Status	It shows **OK** if you have changed the DNS record to use the CNAME provided by FortiWeb Cloud. Refer to Example: Changing DNS records on AWS Route 53 on page 51.
Blocked Requests	The number of requests blocked by FortiWeb Cloud. To view the details, click the application name, then go to **Logs > Attack Logs**.
Requests	The number of requests destined to your application.
Data	The volume of data processed by FortiWeb Cloud, including the data accumulated by the blocked requests.
Block Mode	Enable or disable the block mode. Refer to Understanding block mode and action on page 63
Estimated Cost	The estimated cost that FortiWeb Cloud will charge you.

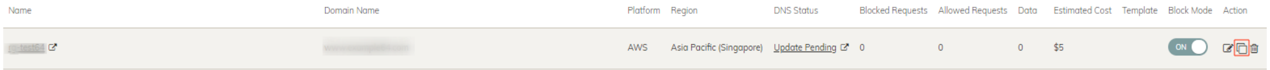
Onboarding applications

See Onboarding applications on page 47 for how to onboard applications.

Cloning the application configurations

You can create a new template by cloning an existing application's configuration.

1. Click the **Clone** icon on the application row.



Name	Domain Name	Platform	Region	DNS Status	Blocked Requests	Allowed Requests	Data	Estimated Cost	Template	Block Mode	Action
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	Update Pending	0	0	0	$5		ON	

2. Enter a name for the template.
3. Click OK.

The template will be displayed in **Global > Templates**.

Enabling/disabling CDN

Decide whether to enable or disable CDN. Refer to CDN on page 62

Selecting FortiWeb Cloud scrubbing center

If CDN is disabled, the system automatically assigns a FortiWeb Cloud scrubbing center located nearest to your application server. You can change it to another scrubbing center.

1. Go to **Global > Applications**.
2. Click the edit icon ✎ for the application.

3. Select the desired region.
4. Click **OK**.

Templates

The template is a collection of WAF configurations. When you assign a template to an application, the WAF configurations in this template will be automatically applied to the application.

Before you can configure a template, you need to enable **Advanced Configuration** in **Global > System Settings > Settings**.

FortiWeb Cloud provides the following predefined templates which contain the most commonly used WAF configurations for different scenarios:

- StandardProteciton
- SharePoint
- Drupal
- Exchange
- ExtendedProtection
- Wordpress

The WAF configurations in these predefined templates are un-editable. If you want to create an variation of the pre-defined template, click the Clone icon in the predefined template row to create a new template based on it.

To create a template:

1. Go to **Global > Templates**.
2. Click **Create Template**. Or click the **Clone** icon in the row of an existing template to create a new template which inherits the configurations of the selected template.
3. Enter a name for this template.
4. Select the application(s) to be applied with this template.
   You can skip this step, then go back selecting applications after you have finished configuring WAF settings for this template.
5. Click **OK**. The template will be created.

To configure WAF settings for a template:

1. Go to **Global > Templates**. Click the name of the template.
2. Configure WAF settings for this template. Click **Add Modules** to display WAF features in the left side menu. See WAF modules on page 126 for more information on each WAF feature.
3. After all the settings are done, click **SAVE** at the bottom right of the page to save the settings.

If you change the settings in a template, the changes will be applied to all the applications associated with this template.

To apply a template to application(s):

1. Go to **Global > Templates**.
2. Find the template you want to use, then click the Edit icon ✎ in this row.
3. Select the application(s) to be applied with the template, then click the right arrow to move them to the right column.
4. Click **OK**.

The configurations in the template will overwrite the existing configurations of the selected applications.

If certain configurations in the template do not fit the application, you can select the application in **Global > Applications**, and disable **Inherit Template** on the specific WAF module page, then edit configurations for the module. The configurations edited in an application apply only to this application.

Admin management

FortiWeb Cloud will cease to support Sub-user and Admin (Legacy) accounts starting from version 24.1, which is scheduled for release in January 2024. To ensure uninterrupted access, kindly migrate Sub-user and Admin (Legacy) to IAM user in advance. Failure to do so may result in the them losing access to FortiWeb Cloud. For more information, see Migrating to IAM user on page 70.

From release 21.3.b, user management for FortiWeb Cloud is integrated into FortiCloud. You can add or delete users, add IAM roles in FortiCloud.

There are two admin types:

- IAM (recommended)
  - IAM users do not need to be configured in FortiWeb Cloud. The configuration of permissions can be done solely in FortiCloud.
- Sub-user
  - Although this admin type is supported, we advise against creating new sub-users as we will no longer be providing updates or new features related to sub-user management.

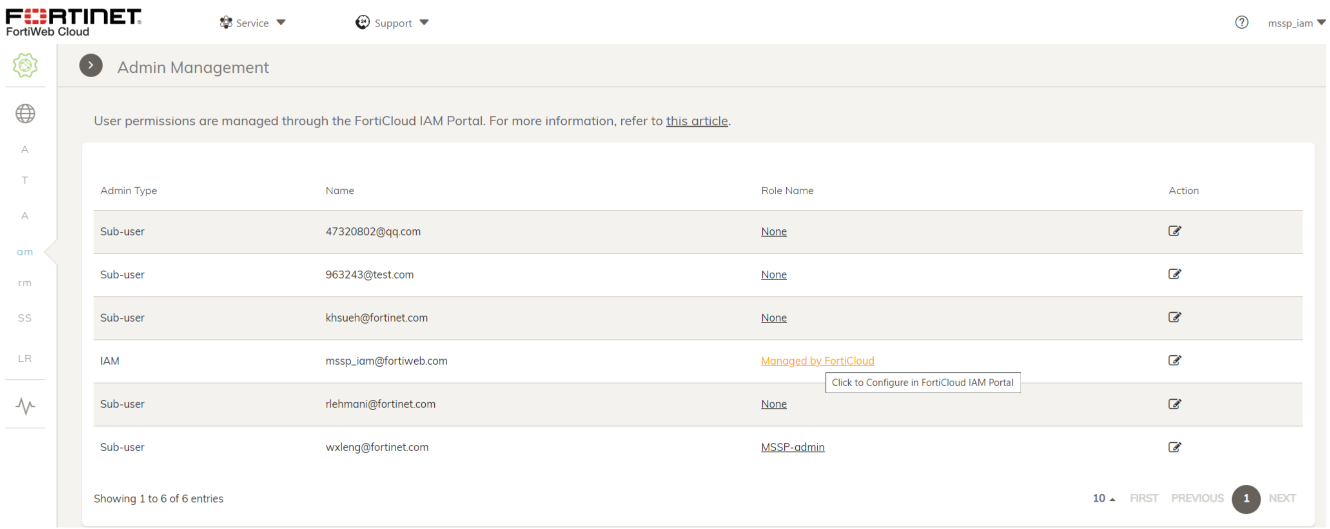
For more differences between sub-user and IAM user, refer to the FortiCloud Feature comparison chart.

The old admin users you have added before 21.3.b are still valid. It's admin type is shown as Admin (Legacy).

To add an IAM user:

Please see Adding IAM users for instructions on how to to add an IAM user in FortiCloud.

FortiWeb Cloud no longer supports configuring roles for IAM users.



Admin Management

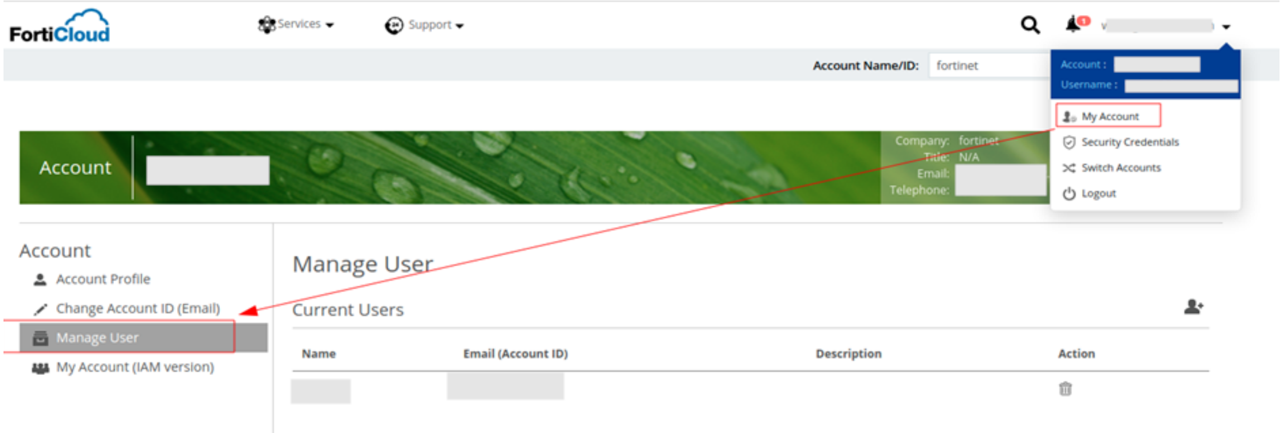
User permissions are managed through the FortiCloud IAM Portal. For more information, refer to this article.

Admin Type	Name	Role Name	Action
Sub-user	47320802@qq.com	None	✎
Sub-user	963243@test.com	None	✎
Sub-user	khsueh@fortinet.com	None	✎
IAM	mssp_iam@fortiweb.com	Managed by FortiCloud Click to Configure in FortiCloud IAM Portal	✎
Sub-user	rlehmani@fortinet.com	None	✎
Sub-user	wxleng@fortinet.com	MSSP-admin	✎

Showing 1 to 6 of 6 entries

To add a sub-user:

1. Log in to FortiCloud: https://support.fortinet.com/Account/Profile.aspx.
2. Click **My Account**, then select **Manage User**.



Manage User

Current Users

Name	Email (Account ID)	Description	Action

3. Click the Add User icon above the top right corner of the Current Users table.
4. Enter the required information for this user.
5. Click **Save**.
6. Log in to FortiWeb Cloud with super root account or other accounts which have the permission to edit Admin Management settings.
7. Go to **Global > Administrators > Admin Management**, you will see the user is automatically synchronized from FortiCloud. The user type is Sub-user.
8. The default role for the user is **None**, meaning the user has neither view nor edit permission. If you want to grant the user more permissions, click the **Edit** icon to assign a corresponding role.
9. On the **Edit User** page, from the **Role** drop-down list, select the role you want to assign to this user. The role defines whether the user has None, Read-only, or Read-Write permission to different parts of your account. To check the permissions of each role, go to **Global > Administrators > Role Management**.
10. By assigning the user a certain role, it will by default have permission to access applications as defined in the role. However, if you want this user to have different permissions when accessing different applications, you can enable **Custom Application Permissions**.
    The **Custom Application Permissions** settings will overwrite the **Application** permission you have set for this role

in **Role Management**.
If new application is onboarded in your account, the administrators will by default have **Default permission** to access it.
Please note the Read-Write permission of Application includes not only the privilege to edit configurations, but also the permission to onboard new applications.
Leaving **Custom Application Permissions** disabled means this account will have the Application permission defined in the corresponding role in **Global > Administrators > Role Management**.

To edit or delete the account:

You can edit or delete the account in FortiCloud through https://support.fortinet.com/Account/Profile.aspx. For more information, refer to FortiCloud Online Help.

The account you used to subscribe the service is super root account with read-write permission to all resources. To protect this account, it is not listed in the Admin Management page.

Migrating to IAM user

FortiWeb Cloud will cease to support Sub-user and Admin (Legacy) accounts starting from version 24.2.a, which is scheduled for release in June 2024. To ensure uninterrupted access, kindly migrate Sub-user and Admin (Legacy) to IAM user in advance. Failure to do so may result in users losing access to FortiWeb Cloud.

For how to migrate, refer to Migrating sub users.

For Admin (Legacy) accounts, if they don't appear in the active sub-users list, you should create an IAM user as needed. See Adding IAM users.

Please be aware that Sub-user and Admin (Legacy) accounts have their permissions currently configured under **Global > Administrators > Role Management**. However, upon migration to FortiCloud, these permissions will be managed by FortiCloud through permission profiles. Therefore, it's essential to create the appropriate permission profiles for them in FortiCloud. For how to create permission profiles in FortiCloud, see Permission profiles.

FortiCloud Organizational Units

FortiWeb Cloud now supports FortiCloud Organization. This centralized account management service consolidates multiple FortiCloud accounts into a structured system of Organization/Organizational Units (OUs).

To create an organization and invite member accounts to join:

In order to create an organization, you must have an active FortiCloud Premium contract in the Root account. If the contract is missing, expired, or soon to be expired, a warning message will appear, guiding the user to purchase the contract through a Fortinet Partner.

1. Log in to the FortiCloud organization portal and click **Create Organization.** See Creating an organization for detailed instructions.
2. Go to the **Invitation Token** page and click **Generate Token**. See Creating invitation tokens for more information.

3. If applicable, manually send the generated token(s) to any member accounts, and ask them to follow the steps below to join your organization:
   a. Log into their FortiCloud account.
   b. Click **Join Organization** from the landing page.
   c. Enter the token you provided to the **Invitation Token** field along with other relevant information on each page of the **Join Organization** procedure.
4. If needed, approve member accounts' join requests once they have entered the token(s) to join your organization. For more information, see Invitation Approval.

OU Admin

OU Admin users are IAM users with Permission Scope set to **Organization**. To understand the distinction between users with Local and Organization access types, see Permission scope with Organizations.

OU Admin abilities include transferring products between different OUs, and registering assets to member accounts. For help navigating your Asset Management portal, see Organizational Unit account views.

Organization User Management

FortiWeb Cloud now supports FortiCloud Organization. This centralized account management service consolidates multiple FortiCloud accounts into a structured system of Organizational Units (OUs).

This service implements role-based access control (RBAC) to restrict user access and privileges to applications and specific functions. You can use FortiCloud Organizational Units (OUs) to configure access to applications based on your organizational structure.

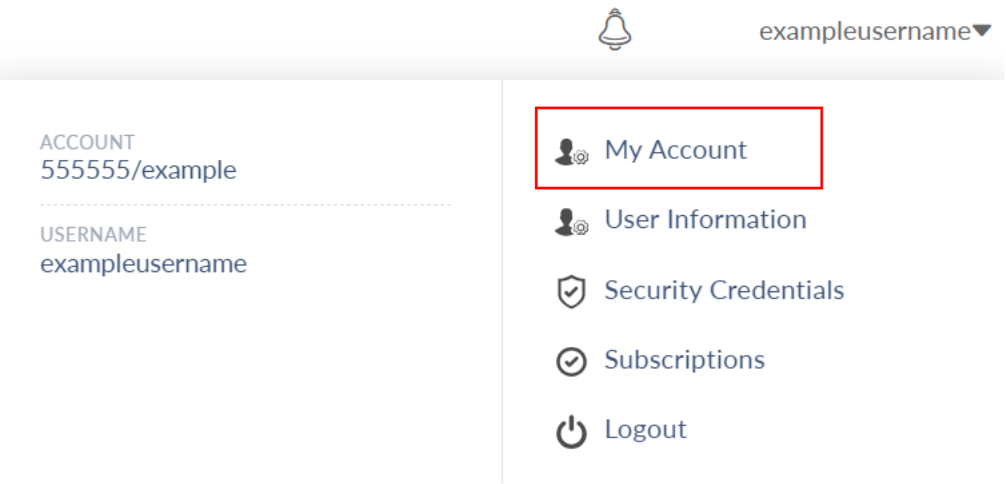
In OU Management, applications are tied to various organization member accounts. To manage your applications, simply log in to the respective member account.

The following items are required to set up OU Management in the Identity & Access Management portal:

- FortiCloud Account with a valid OU license
- Supported Browser

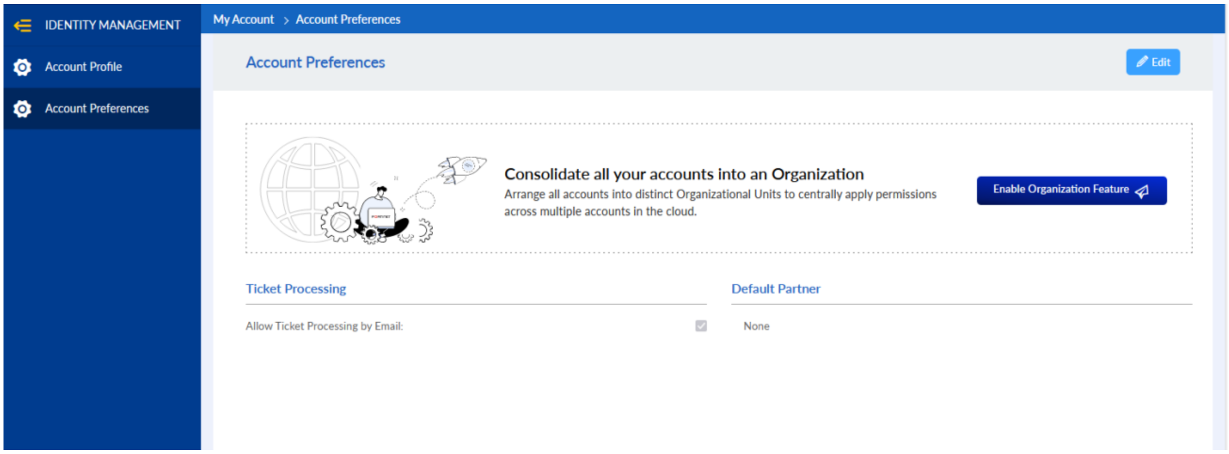
How to use Organizational Units with FortiWeb Cloud

1. Enable Organizational Units via FortiCloud.
   a. Login to the root account of your FortiCloud account.
   b. Navigate to **My Account > Account Preferences** and click **Enable Organization Feature**.



ACCOUNT
555555/example

USERNAME
exampleusername



Consolidate all your accounts into an Organization

Arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

Ticket Processing

Allow Ticket Processing by Email: ☑

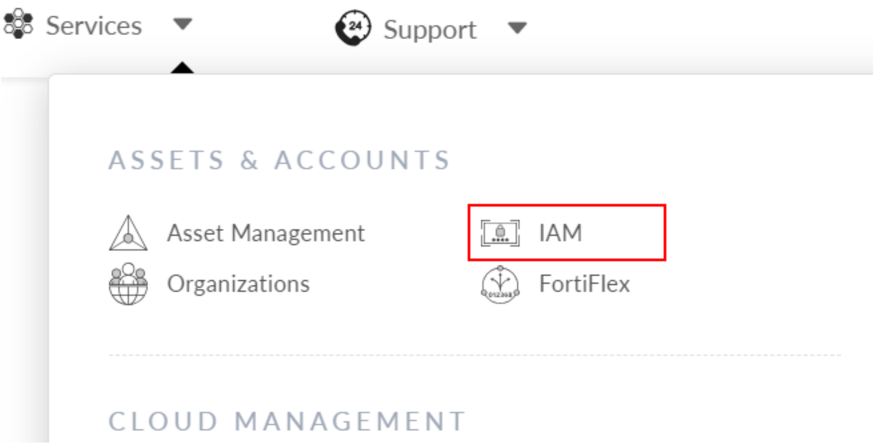
Default Partner

None

c. Click **Create Organization**. For more setup instructions, please see Creating an Organization.

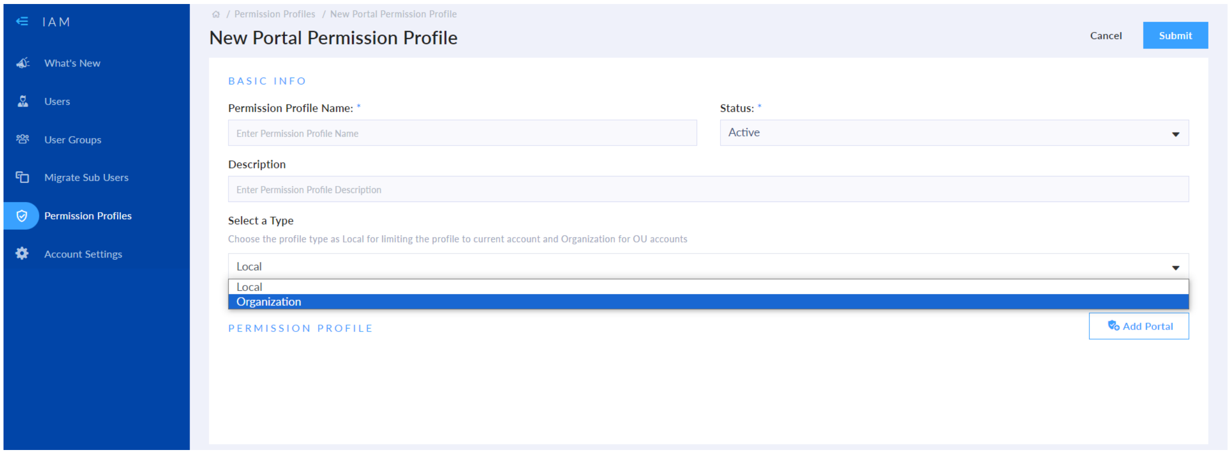
2. Enable and create permission profiles.

   a. Go to **Services > Assets&Accounts > IAM** in the top navigation bar.



   b. Click on **Permission Profiles** in the left-hand navigation bar.

   c. Click **Add New** to create a new Permission profile.



New Portal Permission Profile

BASIC INFO

Permission Profile Name: * Enter Permission Profile Name

Status: * Active

Description: Enter Permission Profile Description

Select a Type

Choose the profile type as Local for limiting the profile to current account and Organization for OU accounts

Local

- Local
- Organization

PERMISSION PROFILE

d. Enter a name for the profile in the Permission Profile Name field.

e. Set the **Status** to **Active**.

f. Enter a description of the portal permissions in the Description field.

g. To manage a new Organizational Unit, please set the Type to **Organization**. Later, you can create different permission profiles according to the needs of your organization.

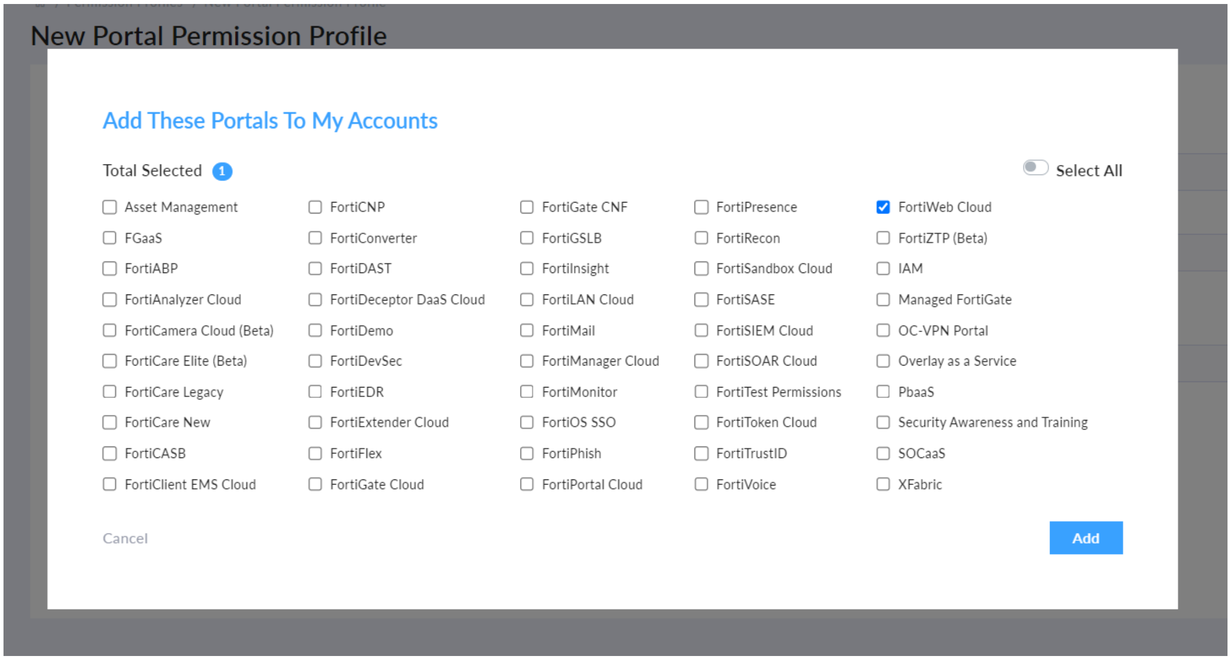
There are two types of permission profiles:

- **Local:** Default option. Users under profiles with this type can manage access for itself and its asset folders.
- **Organization:** This advanced option is only visible to those that have enabled Organizational Units (step 1). Permission profiles with this type allow its IAM users to configure settings for entire OUs.

For more detailed information, see Permission scope with Organizations.

Note: Once the permission profile is saved, the permission profile type cannot be changed.

h. Click **Add Portal**. A list of available portals is displayed.



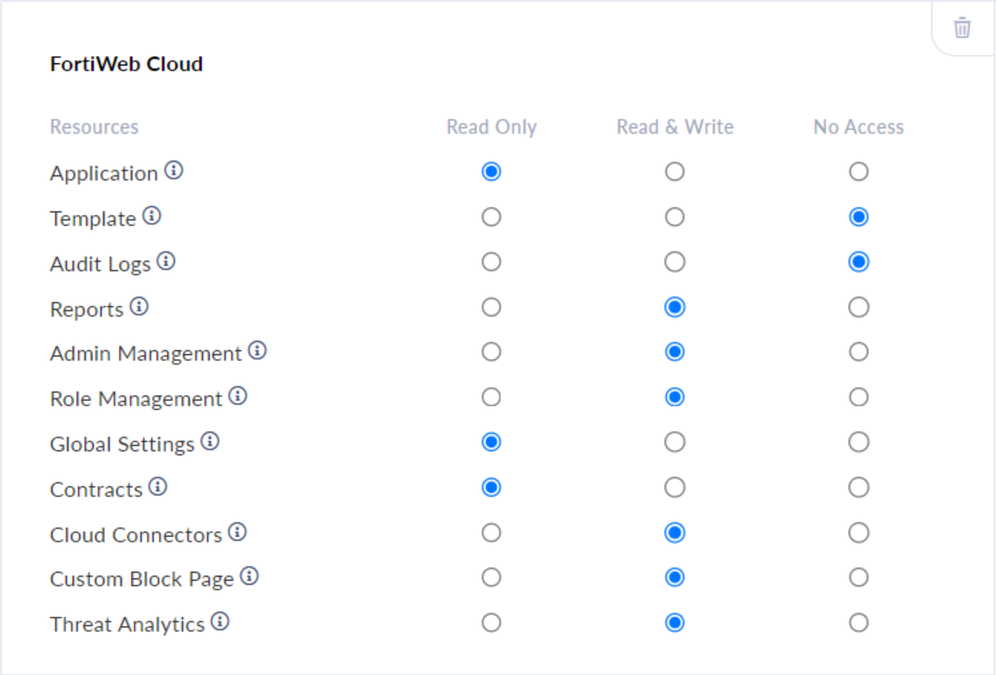
Add These Portals To My Accounts

Total Selected 1

□ Asset Management
□ FGaaS
□ FortiABP
□ FortiAnalyzer Cloud
□ FortiCamera Cloud (Beta)
□ FortiCare Elite (Beta)
□ FortiCare Legacy
□ FortiCare New
□ FortiCASB
□ FortiClient EMS Cloud
□ FortiCNP
□ FortiConverter
□ FortiDAST
□ FortiDeceptor DaaS Cloud
□ FortiDemo
□ FortiDevSec
□ FortiEDR
□ FortiExtender Cloud
□ FortiFlex
□ FortiGate Cloud
□ FortiGate CNF
□ FortiGSLB
□ FortiInsight
□ FortiLAN Cloud
□ FortiMail
□ FortiManager Cloud
□ FortiMonitor
□ FortiOS SSO
□ FortiPhish
□ FortiPortal Cloud
□ FortiPresence
□ FortiRecon
□ FortiSandbox Cloud
□ FortiSASE
□ FortiSIEM Cloud
□ FortiSOAR Cloud
□ FortiTest Permissions
□ FortiToken Cloud
□ FortiTrustID
□ FortiVoice
☑ FortiWeb Cloud
□ FortiZTP (Beta)
□ IAM
□ Managed FortiGate
□ OC-VPN Portal
□ Overlay as a Service
□ PbaaS
□ Security Awareness and Training
□ SOCaaS
□ XFabric

i. Select the portals you want to enable or deny access to. To use this Permission Profile with FortiWeb Cloud, select the FortiWeb Cloud portal.

j. Click **Add**. The portals are displayed in cards.
   - For portals with resource-based permission capabilities like FortiWeb Cloud, specify the Resources access type.



FortiWeb Cloud

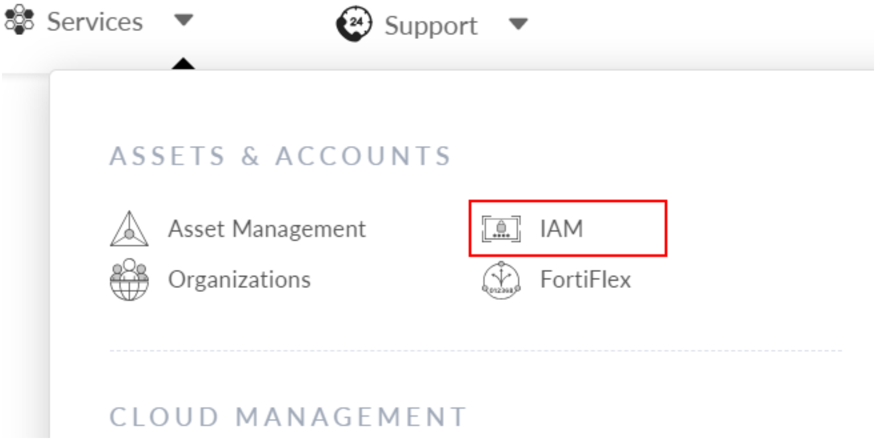
Resources	Read Only	Read & Write	No Access
Application ⓘ	●	○	○
Template ⓘ	○	○	●
Audit Logs ⓘ	○	○	●
Reports ⓘ	○	●	○
Admin Management ⓘ	○	●	○
Role Management ⓘ	○	●	○
Global Settings ⓘ	●	○	○
Contracts ⓘ	●	○	○
Cloud Connectors ⓘ	○	●	○
Custom Block Page ⓘ	○	●	○
Threat Analytics ⓘ	○	●	○

   - For other portals with role-based permissions, enable Access and specify the portal Access Type and any Additional Permissions.

k. Click **Save**. The permission profile is now available to be assigned to users.

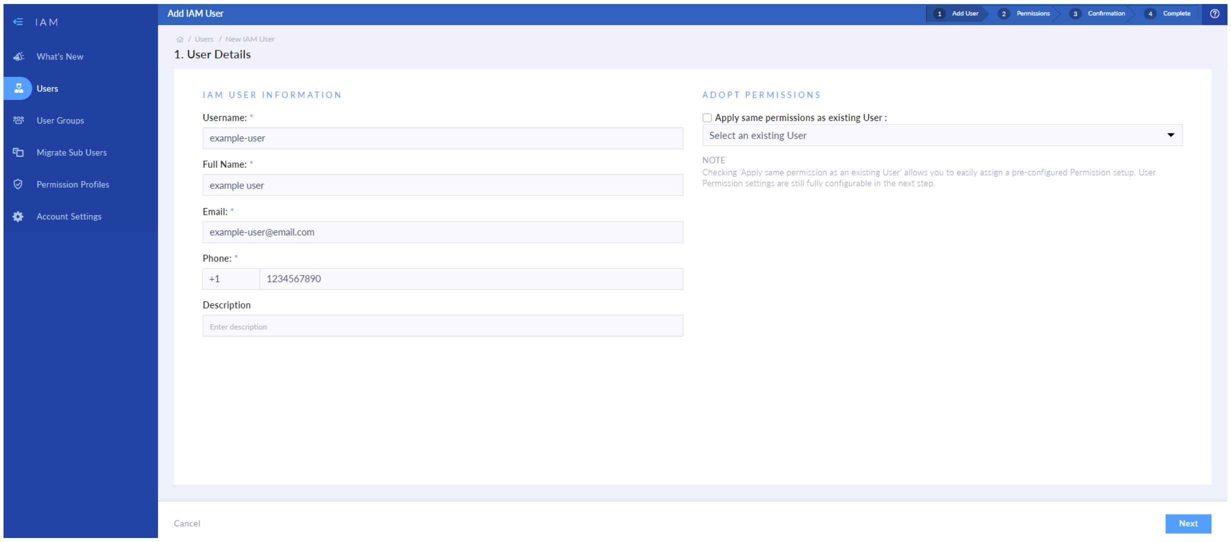
3. Create your first IAM user with Organization permissions. You can use this IAM user to create your first OU.

   a. Go to **Services > Assets&Accounts > IAM** in the top navigation bar.



   b. Navigate to **Users** in the left-hand navigation bar.

c. Click **Add New**, then select **IAM User**. Fill in the desired contact information and click **Next**.



1. User Details

IAM USER INFORMATION

Username: * example-user

Full Name: * example user

Email: * example-user@email.com

Phone: * +1 1234567890

Description: Enter description

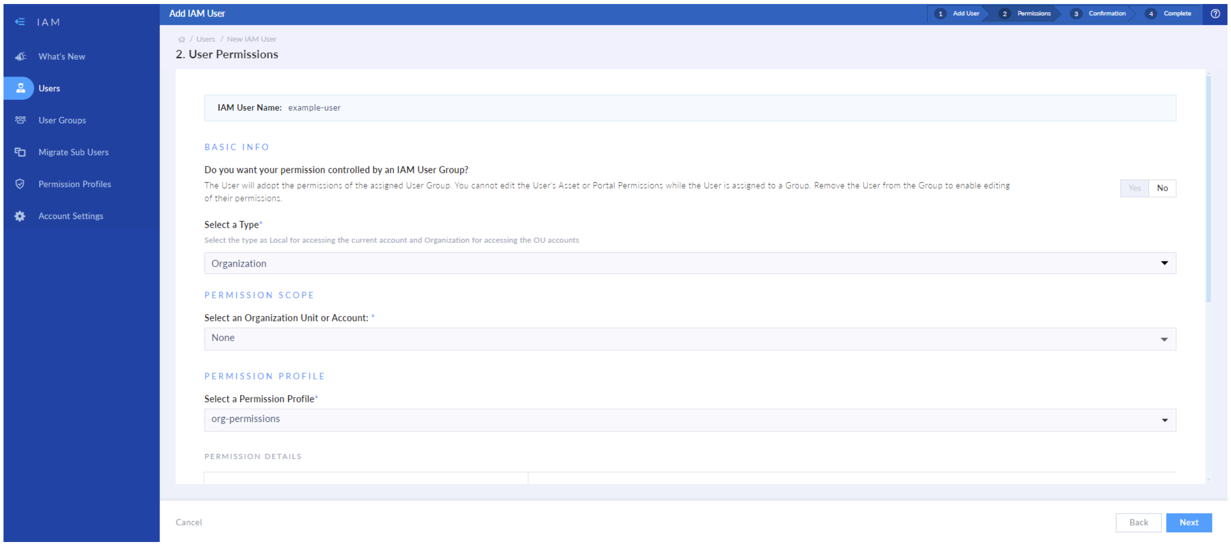
ADOPT PERMISSIONS

□ Apply same permissions as existing User : Select an existing User

NOTE

Checking 'Apply same permission as an existing User' allows you to easily assign a pre-configured Permission setup. User Permission settings are still fully configurable in the next step.

d. On the **User Permissions** page, set the Type to **Organization**, set the **Permission Scope** to the OU you would like the IAM user to manage, and set the **Permission Profile** to the profile with Organization type that you created in Step 2.



2. User Permissions

IAM User Name: example-user

BASIC INFO

Do you want your permission controlled by an IAM User Group?

The User will adopt the permissions of the assigned User Group. You cannot edit the User's Asset or Portal Permissions while the User is assigned to a Group. Remove the User from the Group to enable editing of their permissions.

Yes [✓ No]

Select a Type*

Select the type as Local for accessing the current account and Organization for accessing the OU accounts

Organization

PERMISSION SCOPE

Select an Organization Unit or Account: * None

PERMISSION PROFILE

Select a Permission Profile* org-permissions

PERMISSION DETAILS

e. Click **Next** and review your new IAM user information.

4. Set up additional permission profiles according to the needs of your organization, as well as other users, user groups, and roles within Organizations.

   Return to Step 2 for information about setting up permission profiles.

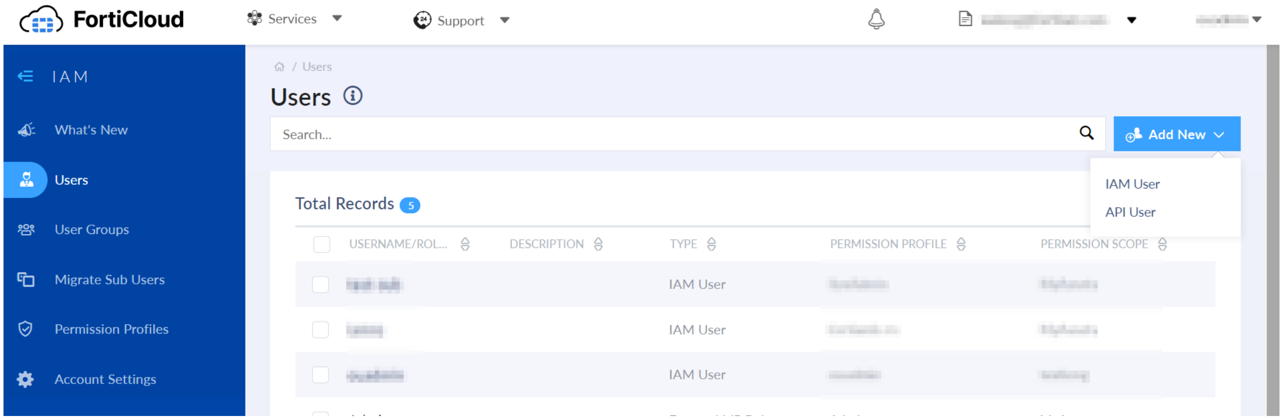
   Once you have your permission profiles set up, you can create users and designate permissions within your organization in the IAM portal.

   - **IAM user**: An IAM (Identity and Access Management) user with Organizational permissions has specific credentials and permissions, facilitating controlled access to FortiCloud resources and services.
   - **API User:** Please note that FortiWeb Cloud currently does not support use with API users.

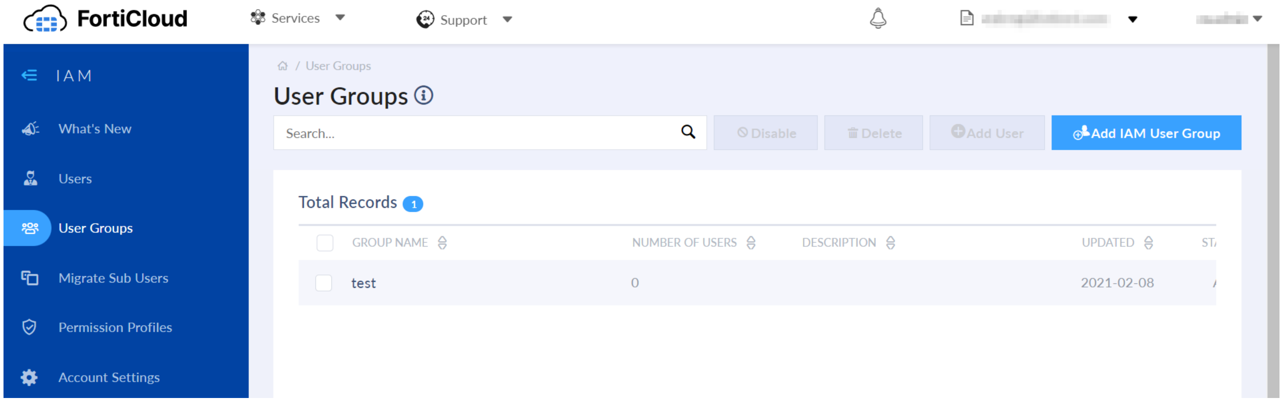
     For other compatible services, API users can access FortiCloud services through an API. API users can only use OAuth 2.0 for authentication then access web service APIs provided by each FortiCloud service portal.

- **User Groups:** User groups save time assigning asset and portal permissions to users. Use a group to create sets of conditions and then assign users to the group. A user can only belong to one group at a time.

For configuration details, see Creating users, user groups, and roles within Organizations.



USERNAME/ROL...	DESCRIPTION	TYPE	PERMISSION PROFILE	PERMISSION SCOPE
[redacted]		IAM User	[redacted]	[redacted]
[redacted]		IAM User	[redacted]	[redacted]
[redacted]		IAM User	[redacted]	[redacted]



GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	ST
test	0		2021-02-08	/

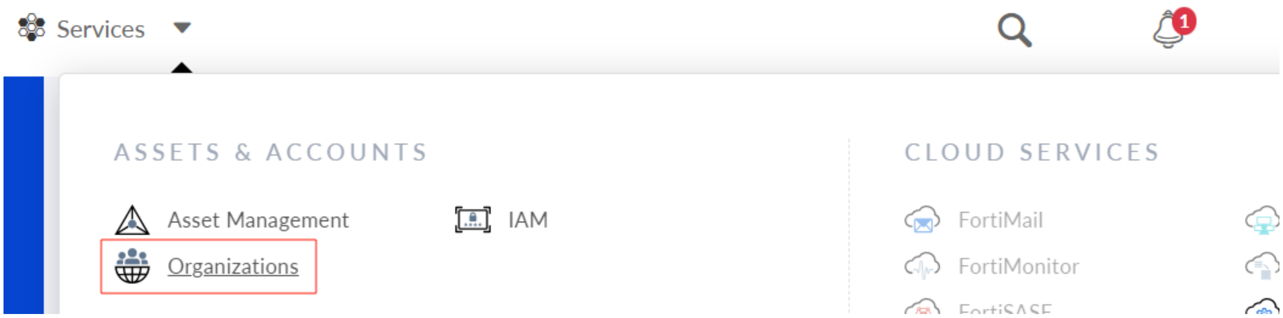
OU Admin

OU Admin users are IAM users with Permission Scope set to **Organization**. To understand the distinction between users with Local and Organization access types, see Permission scope with Organizations.

OU Admin abilities include transferring products between different OUs, and registering assets to member accounts. For help navigating your Asset Management portal, see Organizational Unit account views.

How to invite member accounts to join your Organization

1. Go to **Services > Assets&Accounts > Organizations** in the top navigation bar.



2. Go to the **Invitation Token** page and click **Generate Token**. See Creating invitation tokens for more information.
3. If applicable, manually send the generated token(s) to any member accounts, and ask them to follow the steps below to join your organization:
   a. Log into their FortiCloud account.
   b. Click **Join Organization** from the landing page.
   c. Enter the token you provided to the **Invitation Token** field along with other relevant information on each page of the **Join Organization** procedure.
4. If needed, approve member accounts' join requests once they have entered the token(s) to join your organization. For more information, see Invitation Approval.

Role management

FortiWeb Cloud has three permissions:

- When an administrator has only **read** access to a feature, the administrator can access the web UI page for that feature, but cannot make changes to the configuration. An exception is the API Key in **Global > System Settings > Settings** . The read-only user is also allowed to create API key.
- **Write** access is required for modification of any kind.
- **None** means the administrator can't access the feature.

Role management controls the specific job that each administrator does, such as user account creation, log auditing, or editing configurations of a specific feature. It can limit each administrator account to their assigned role.

To create a role:

1. Go to **Global > Administrators > Role Management**.
2. Click **Add Role**.
3. Enter a role name.
4. Enter a brief description for this role.
5. Select permissions to access different part of web GUI.
6. Click **OK**.

If you want to modify permission for a role or remove it, click the Edit ✎ or Delete 🗑 icon beside this role.

Use **Admin Management** to assign roles to administrator accounts.

Settings

Advanced Configuration

Once this option is enabled, you are allowed to configure the following:

- On each WAF module page, you can configure appropriate actions if the traffic violates WAF rules, such as Period Block, Alert, Alert & Deny.
- **Templates** page will appear under **Global** tab for you to push a collection of WAF settings across multiple applications.

- A **Bypass WAF** switch will appear on the **Vulnerability Scan** page, which allows you to check out the vulnerabilities exposed by your origin server assuming the protection from FortiWeb Cloud was off.

Audit Logs Export

Enable to export system-level events such as user login and server creation to specified log servers.

Notification Emails

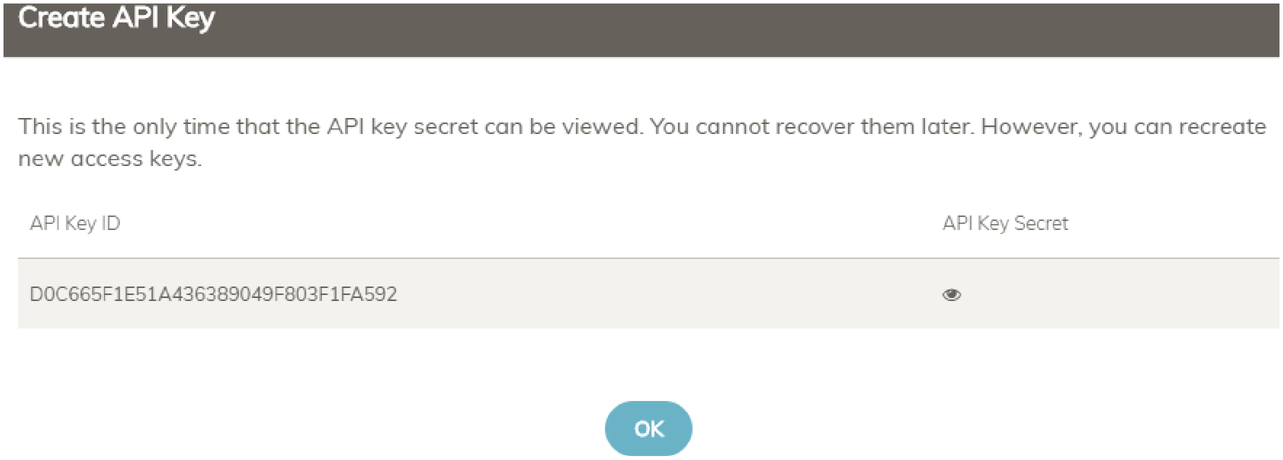
FortiWeb Cloud sends notifications to your email about the information related with subscription, new features in each release, system maintenance, certificate expiration and more.

Enable **Notification Emails** in **Global > System Settings > Settings** to send notification emails to your registered email address.

API Key

FortiWeb Cloud RESTful API requires API key authorization. You can generate the API key from the GUI directly. Please note that API key creation does not restrict only to users with write permission. Read-only users can also create API key.

1. Go to **Global > System Settings > Settings** .
2. Locate **API Key**.
3. Click **Create**.
   An API key ID and an API key secret are generated. Click the **View** icon to get the hidden key secret and use it for invoking APIs. You have got only one chance to view the key. The key will not be stored at the back-end server.



Create API Key

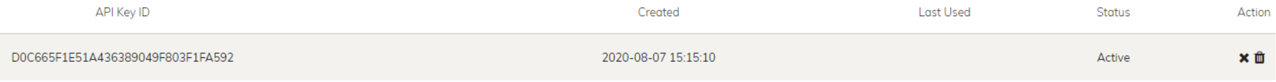
This is the only time that the API key secret can be viewed. You cannot recover them later. However, you can recreate new access keys.

API Key ID	API Key Secret
D0C665F1E51A436389049F803F1FA592	👁

In the API Key table, you can view the API key ID, the time when the key was created and last used, the active and inactive status.

You can inactivate the API key in case of any key security problem, and revoke it later.

Only one API key can be created for an account. You can delete an API key before you create a new one.



API Key ID	Created	Last Used	Status	Action
D0C665F1E51A436389049F803F1FA592	2020-08-07 15:15:10		Active	✖ 🗑

When using this API key, just put it in the HTTP authentication header as below:

```
authentication: Basic <api-key-secret>
```

Origin Server Lock

Lock your origin server's IP address to ensure it can only be used by your account. The Origin Server Lock prevents other accounts on FortiWeb Cloud from setting up an application targeting malicious traffic at your origin server.

The Origin Server Lock setup is only configurable through Fortinet support. Please contact the support team and provide your origin server's IP addresses. We will do the setup for you.

Fabric Connector

Connect to the Security Fabric with FortiGate version 7.0.0 or newer. For configuration instructions, see Fortinet Security Fabric on page 236.

Consumption Report

This feature is disabled by default. Enabling this feature will result in the automatic generation and delivery of monthly Consumption Reports to the email addresses entered in the **Recipients** box.

Consumption reports encompass usage details for all applications within the user's account, providing data on metrics like throughput and bandwidth. Consumption data for each month is generated on the 5th of the following month. For instance, data for October will be generated on November 5th.

Please refer to the table below on levels of access for different user types:

User Type	Level of Access
Organization root account	Can enable or disable consumption report for itself and all tenants.
Organization user, not root account	Cannot enable nor disable consumption report.
Non-OU user, excluding Tenants	Can enable or disable consumption report for itself.
Tenant	Cannot enable nor disable consumption report.

Contracts

The Contracts page shows the FortiWeb Cloud contracts you have registered. The contract automatically becomes valid on its start date.

FortiWeb Cloud contracts are annual. We recommend customers to align their contract to the highest monthly consumption level.

Contract Renewal

⚠ Please ensure that you renew your contracts before they expire or before reaching the bandwidth usage limit. Failure to do so may result in interrupted service and loss of access to controls.

After your contracts expire, FortiWeb Cloud continues protecting your applications for 21 days. During this period, you are not allowed to edit configuration for your applications unless the contract is renewed. After the 21-day extension, your applications will be deleted from your FortiWeb Cloud account.

If you possess at least one valid contract but have exceeded the allowed number of applications on your account, your UI will be locked to read-only access for all applications. To resolve this issue, you need to purchase an additional contract. The 21-day grace period is not activated until the last remaining contract expires.

Measuring bandwidth by the 95th Percentile

FortiWeb Cloud measures each account using a burstable model for overall account bandwidth calculation. The model is based on calculating the 95th percentile of bandwidth usage of clean traffic and is also common with other CDNs and Cloud solutions.

The 95th percentile bandwidth is calculated in the following way:

- Traffic for the entire month is measured in 5 minute buckets.
- At the end of the month, the 5% of buckets with the most Mbps are dropped, and the highest Mbps rate of the remaining buckets represents the 95th percentile value for the account.

At the beginning of every month, the 95th percentile bandwidth shown in FortiWeb Cloud might be very low, or even shown as 0. This is because there aren't enough 5-minute buckets collected to calculate a valid value. At the end of the month with more buckets generated, the value becomes more accurate.

Cloud Connectors

In some cases your application server's IP address may dynamically change, for example, when it's deployed in auto-scaling mode on public cloud platforms. Instead of manually updating the origin server's IP address in FortiWeb Cloud, you can configure a Cloud Connector to authorize FortiWeb Cloud to access your public cloud resources in order to automatically obtain the latest IP addresses.

To create a Cloud Connector:

1. Go to **Global > System Settings > Cloud Connectors**.
2. Click **Create Connector**.
3. Configure the following settings.

Name	Enter a name for the Cloud Connector.
Status	Turn on or off the Cloud Connector.
Type	Select the public cloud platform where your application server is deployed.

4. Configure the following settings if the type is **AWS**.
An access key on AWS grants programmatic access to your resources. If you have security considerations, it's recommended to create an IAM role specially for FortiWeb Cloud and grant read-only access. For how to create an access key, see this article.

Region	The region where your application server is deployed.
Access Key ID	The Access Key ID.

Secret Access Key	Secret Access Key.
VPC ID	The ID of the VPC where your application server is deployed.

5. Configure the following settings if the type is **Azure**.
   You must create an Azure AD application to generate the Azure client ID and corresponding Azure client secret. This application must be a service principal. Otherwise, the Fabric connector cannot read the inventory. You can find the complete instructions at Use portal to create an Azure Active Directory application and service principal that can access resources.
   Keep the following in mind when you get to the part about making a new application registration:
   - The Application type has two options. Choose Web app/API.
   - The Sign-on URL has the asterisk commonly associated with a required field, but this is not applicable in this case. Put in any valid URL in the field to complete the form and enable the Create button.

Server Region	The region where your application server is deployed.
Tenant ID	See instructions above for how to find the Tenant ID.
Client ID	See instructions above for how to find the Client ID.
Client Secret	See instructions above for how to find the Client Secret.
Subscription ID	The ID of the subscription where your application server is deployed.
Resource Group	The name of the resource group where your application server is deployed. Make sure that the service principal (app registration) is granted for the network contributor and VM contributor roles for the target resource group.

6. Configure the following settings if the type is **GCP**.
   A service account is a special type of Google account intended to represent a non-human user that needs to authenticate and be authorized to access data in Google APIs. See Understanding service accounts for how to create a service account and authenticate with private key.

Project ID	The ID of the project where your application server is deployed.
Service Account Email	The Service Account Email that FortiWeb Cloud uses to access your application server.
Private Key	The Private Key to for authentication.
Zone	The zone where your application server is deployed.

7. Click **Test** to verify whether FortiWeb Cloud can access the resources with the provided information. If the test succeeds, click **OK** to save the settings.

If you want to edit the settings or delete a Cloud Connector, click the Edit✎ or Delete🗑 icon in the Cloud Connector row.

After the Cloud Connector is created, you can go to **Network > Origin Servers** to configure the dynamic server settings so that FortiWeb Cloud can use the specified conditions to find the right VMs in our account and obtain their IP addresses. See Origin Servers on page 114.

Custom block pages

You can customize the following pages that FortiWeb Cloud displays to your users:

- The error page FortiWeb Cloud uses to respond to an HTTP request that violates a policy and the configured action is **Deny** or **Period Block**.
- The "Server Unavailable!" page that FortiWeb Cloud returns to the client when none of the server pool members are available either because their status is **Disable** or **Maintenance** or they have failed the configured health check.
- The Captcha enforcement pages that FortiWeb Cloud uses to differentiate between real users and automated users, such as bots.

Configuring a custom block page

Follow steps below to configure a custom block page:

1. Go to **Global > System Settings > Custom Block Pages**.
2. Under the **Messages** tab, click **Create New**.
3. Enter a name for the block page. The maximum length is 30 characters.
4. Enter description for the block page. The maximum length is 512 characters
5. Click the **Edit** icon for the message you want to edit.
6. In the **Edit Message** window, the left side pane displays the source code, and the right side is how the message shows in the browser.
   It's not allowed to change the macros such as `%%SOURCE_IP%%`. See Macros in custom block pages.
7. Click **Save** to save the changes of the message.
8. If you want to edit other messages, click the **Edit** icon in their rows.
9. Click **OK** to save the block page.
10. To apply a block page for an application, select it in the **Custom Block Pages** list in **Application > Network > Endpoints**.

FortiWeb Cloud supports up to 8 custom block pages (including the predefined page).

Macros in custom block pages

All the macros and parameters in the HTML code can't be removed or edited, while the text that shows in the Web UI is allowed to be modified.

For example, in the following code, the macros (e.g. `%%CAPTCHA_VCODE_STR%%`) and parameters (e.g. `req_data`) can't be removed or edited, but the text "Security check" can be replaced with any text as you desire.

```
<input type="hidden" name="vcode" value="%%CAPTCHA_VCODE_STR%%">
<input type="hidden" name="req_data" value="%%CAPTCHA_REQ_DATA%%">
<h2>
Security check
</h2>
```

Adding images in custom block pages

The default block pages contain predefined images. To use your own images, you need to upload the image file, then insert image macro in the message body.

Uploading image files

1. Go to **Global > System Settings > Custom Block Pages**.
2. Under the **Images** tab, Click **Create New**.
3. Specify a name for the image file, select its type, and then click **Choose File** to browse to the file and select it. Ensure the image is no larger than 24 KB and that its type matches the value you have selected for **Type**.
4. Click **OK**.

Inserting image file to messages

Use the following format to add an image macro anywhere in a custom block message:

```
%%IMAGE:<image_name>%%
```

where `<image_name>` is the name of the image you have uploaded.

For example, if you want to add the image `test` to the list of images, use `%%IMAGE%%:test%%` to add it to the HTML code.

```
h2.fgd_icon {
   background: url(%%IMAGE:test%%)
   width: 90px;
   height: 92px;
   margin: 48px auto;
}
```

Audit logs

Audit logs report system-level events such as user login, server creation. You can view the audit logs through **Global > Log & Report > Audit Logs** . A maximum of 10,000 audit logs are displayed per each filter.
An audit log is saved for three months. After that it will be deleted.

To configure the log display settings:

1. Go to **Global > Log & Report > Audit Logs**.
2. Configure the following settings.

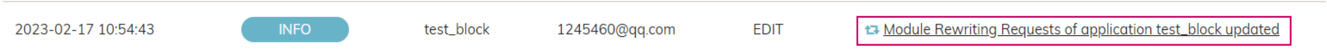
Reload	Click to update the page with any logs that have been recorded since you previously loaded the page.
Add Filter	Click to create a filter based on log message fields. Only messages that are in the most recent 100,000 messages and match the criteria in the filter are displayed.

When you search by time, all messages with the selected date are displayed.

To view before&after comparison:

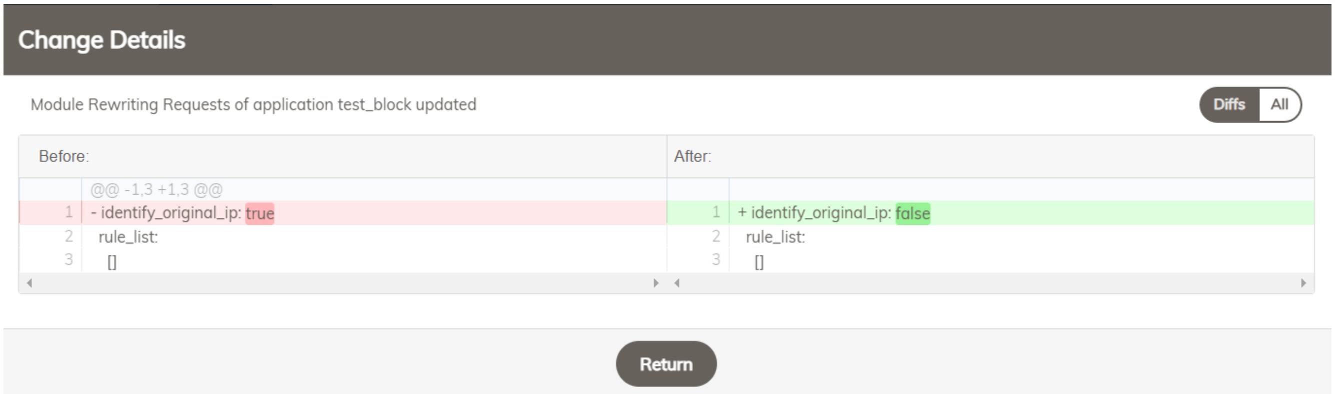
Audit logs provide details on the configuration changes with before&after information.

For the logs on configuration updates, the log item is a clickable link, as shown below.



2023-02-17 10:54:43	INFO	test_block	1245460@qq.com	EDIT	Module Rewriting Requests of application test_block updated

By clicking on the link, a before&after comparison view will display. You can click the **Diffs** or **All** at the top right corner to show only the differences or expand the whole configuration.



Module Rewriting Requests of application test_block updated

Before:	After:
@@ -1,3 +1,3 @@	
1 - identify_original_ip: true	1 + identify_original_ip: false
2 rule_list:	2 rule_list:
3 []	3 []

To export audit logs to log server:

1. Go to **Global > System Settings > Settings**.
2. Enable **Audit Logs Export**.

3. Configure the following settings.

Server Type	Select whether to export the logs to a log server or an ElasticSearch service. See the following instructions for SysLog and ElasticSearch.
SysLog	
IP/Domain and Port	Enter the IP/Domain and Port of the log server.
Protocol	Select the protocol used for log transfer.
Server Certificate Verification	When enabled, the system will enforces server certificate verification before it sends attack logs to the log server.
Custom Certificate and Key	• **Off:** FortiWeb Cloud automatically retrieves the SSL certificate used to encrypt the HTTPS connections between the log server and FortiWeb Cloud. • **On:** Manually enter the SSL certificate. Available only if you select **SSL** in **Protocol**.
Client Certificate	Fill in the Certificate field. Available only if you enabled **Custom Certificate and Key**.
Private Key	Fill in the Private Key field. Available only if you enabled **Custom Certificate and Key**.
Password	Enter the password of the private key. Available only if you enabled **Custom Certificate and Key**.
Log Format	• **Default:** Export logs in default format. • **Custom:** Customize the log format. All the supported parameters are listed by default. You can select the ones that you need, and delete the others. • **Splunk**: Export logs to Splunk log server. • **CEF:0 (ArcSight):** Export logs in CEF:0 format. • **Microsoft Azure OMS:** Export logs in Microsoft Azure OMS format. • **LEEF1.0(QRadar):** Export logs in LEEF1.0 format.
Log Facility	Select the source facility of the logs. We only support the local use facilities which are not reserved and are available for general use.
ElasticSearch ElasticSearch is a search engine providing a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.	
Address and Port	Enter the address and port to access your ElasticSearch service. The default port for ElasticSearch service is 9200.
User Name	Enter the user name of the ElasticSearch service.
Password	Enter the password of the ElasticSearch service user.

4. Click **SAVE**. The system exports newly generated audit logs to the log server every minute.

   To prevent log poisoning, it's recommended to set filters on your log server to allow only the traffic from FortiWeb Cloud. The source IPs are as follows:

- 3.226.2.163
- 3.123.68.65

Reports

In addition to the application-level threat data displayed on **Dashboard**, **FortiView** and **Logs** pages, you can customize weekly reports and configure FortiWeb Cloud to send the reports to your specified email addresses reporting the threat data for all the applications in your account.

For each report entry, you can use **Add Filter** to filter out reports based on the recipients or report names. Also, you can select actions in ⬇ ▶ ✎ 🗑 to download the report in PDF format, generate and send the report immediately, edit the report configuration, or delete the created report. For scheduled report, you can click ⏸ or ▶ to pause or restart scheduling the report.

1. Click **Create Report** in **Global > Log & Report > Reports**.
2. Configure these settings.

Report Name	Enter a name for the weekly report.
Time Range	Select the time span of the report.
Content	Select one or multiple queries that define the chart categories in the generated report. • Top Threats by Attack Category • Top Threats by Signature IDs • Top Threats by Source IPs • Top Threats by Countries • Top Threats by URLs • Top Threats by CVE • Threats By OWASP Top 10 • Applications Traffic Summary
Applications	Define the applications that you want to generate the weekly report for or not. You can add or remove all applications once.
Schedule	• Manually: Generate the report on demand. • Once: Generate the report for only one time. • Daily: Generate the report each day. • Weekly: Generate the report each week. • Monthly: Generate the report each month.
Recipients	Specify the email addresses that will receive the weekly report. Separate multiple email addresses with ",". A maximum of 10 email addresses are supported.

3. Click **OK**.

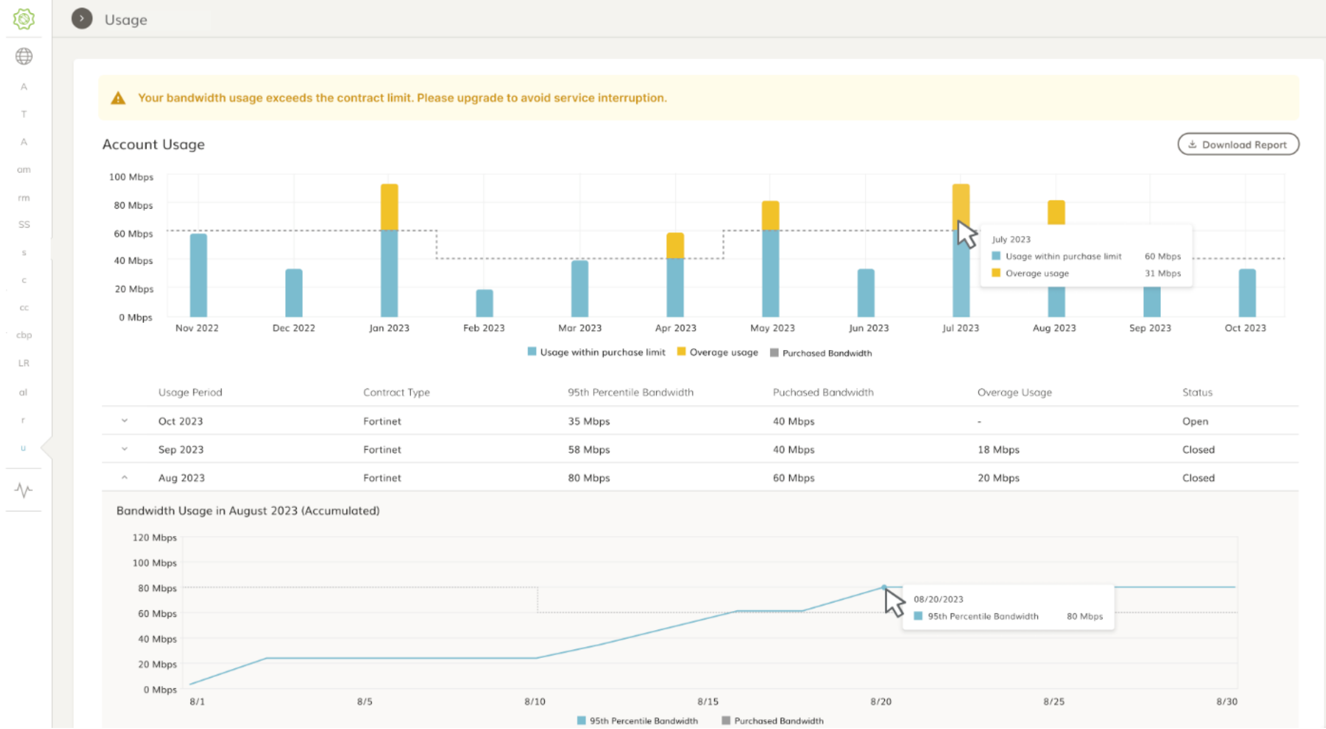
Usage

The Usage page gives you a clear overview of how your account has been used over time. It breaks down usage for each month of service, helping you easily identify your usage patterns and detect any overages in your account without delay.

This page will include different statistics depending on your contract type, which is in this case determined by the avenue from which you have purchased your contract.

- Fortinet and FortiFlex on page 87
- AWS, GCP, and Azure on page 88

Fortinet and FortiFlex



Usage

⚠ Your bandwidth usage exceeds the contract limit. Please upgrade to avoid service interruption.

Account Usage

	Usage Period	Contract Type	95th Percentile Bandwidth	Puchased Bandwidth	Overage Usage	Status
˅	Oct 2023	Fortinet	35 Mbps	40 Mbps	-	Open
˅	Sep 2023	Fortinet	58 Mbps	40 Mbps	18 Mbps	Closed
˄	Aug 2023	Fortinet	80 Mbps	60 Mbps	20 Mbps	Closed

Bandwidth Usage in August 2023 (Accumulated)

Account Usage graph

This bar chart displays your account's bandwidth usage history over a period of up to a year. Simply hover over a bar representing a specific month to view the exact usage figures for that month.

Usage table

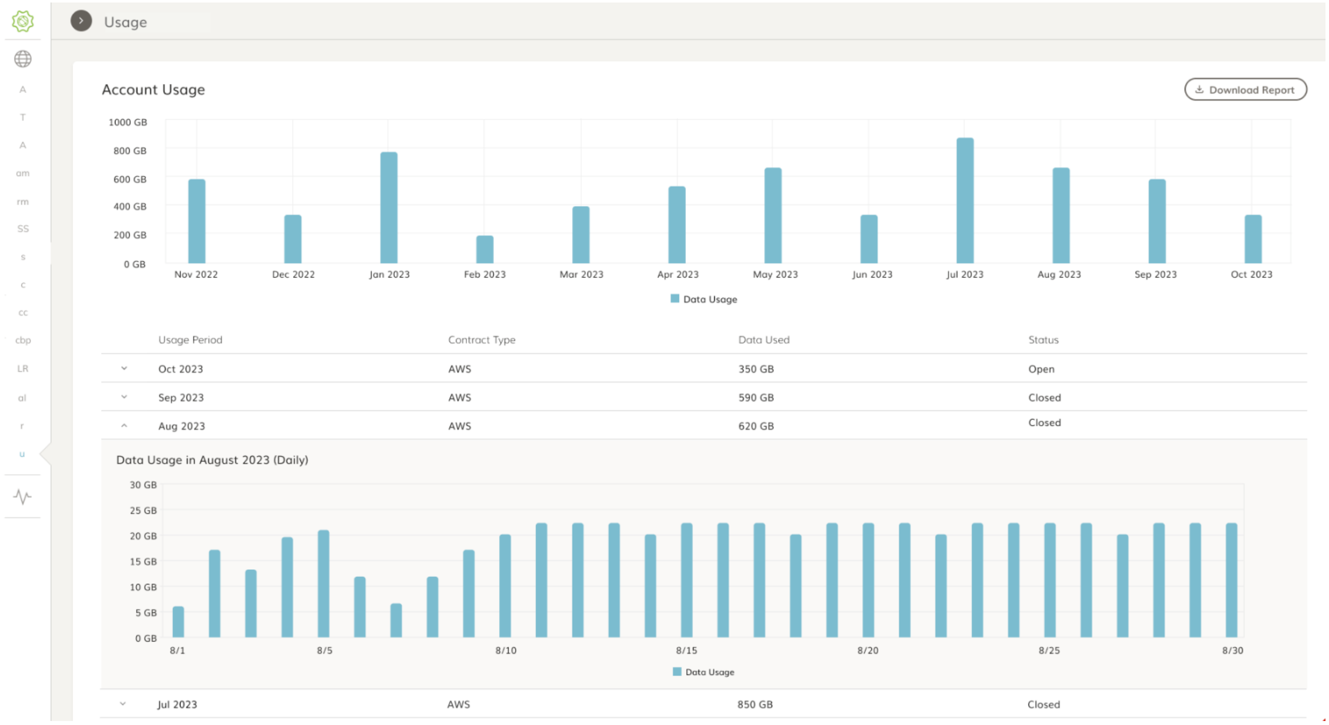
This table further breaks down the statistics for each month displayed in the Account Usage chart.

Field	Description
Contract Type	This field specifies the channel you used to subscribe to FortiWeb Cloud, such as Fortinet or FortiFlex.
95th percentile bandwidth	FortiWeb Cloud measures each account using a burstable model for overall account bandwidth calculation. The model is based on calculating the 95th percentile of bandwidth usage of clean traffic and is also common with other CDNs and Cloud solutions. The 95th percentile bandwidth is calculated in the following way: Traffic for the entire month is measured in 5 minute buckets. At the end of the month, the 5% of buckets with the most Mbps are dropped, and the highest Mbps rate of the remaining buckets represents the 95th percentile value for the account. At the beginning of every month, the 95th percentile bandwidth shown in FortiWeb Cloud might be very low, or even shown as 0. This is because there aren't enough 5-minute buckets collected to calculate a valid value. At the end of the month with more buckets generated, the value becomes more accurate.
Purchased Bandwidth	The bandwidth included in your contract.
Overage Usage	The data consumption exceeding your contracted limit.
Status	**Open**: The period is ongoing, and information collection is in progress. **Closed**: The period has ended, and informatione collection is complete.

Click on any row in this table to view a line graph illustrating usage trends for the selected month, along with the point when you reached the 95th percentile of bandwidth. These statistics can assist you in monitoring your usage habits and determining the appropriate amount of bandwidth to purchase in the future

AWS, GCP, and Azure

For contracts on AWS, GCP, and Azure, where bandwidth is unlimited, statistics regarding purchased bandwidth are not applicable.



Usage Period	Contract Type	Data Used	Status
Oct 2023	AWS	350 GB	Open
Sep 2023	AWS	590 GB	Closed
Aug 2023	AWS	620 GB	Closed

Jul 2023	AWS	850 GB	Closed

Account Usage graph

This bar chart displays your account's data usage history over a period of up to a year.

Usage table

Field	Description
Contract Type	This field specifies the channel you used to subscribe to FortiWeb Cloud, such as AWS, Azure, or Google Cloud.
Data Used	The amount of data (in GB) utilized in a given month.
Status	**Open**: The period is ongoing, and information collection is in progress. **Closed**: The period has ended, and information collection is complete.

Click on any row in this table to view a bar graph illustrating daily usage trends for the selected month.

Threat Analytics

Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application assets and aggregate them into security incidents and assign severity. It helps separate real threats from informational alerts and false positives and help you focus on the threats that matter.

- Incidents
- Insights
- Settings

Threat Analytics

Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application assets and aggregate them into security incidents and assign severity. It helps separate real threats from informational alerts and false positives and help you focus on the threats that matter.

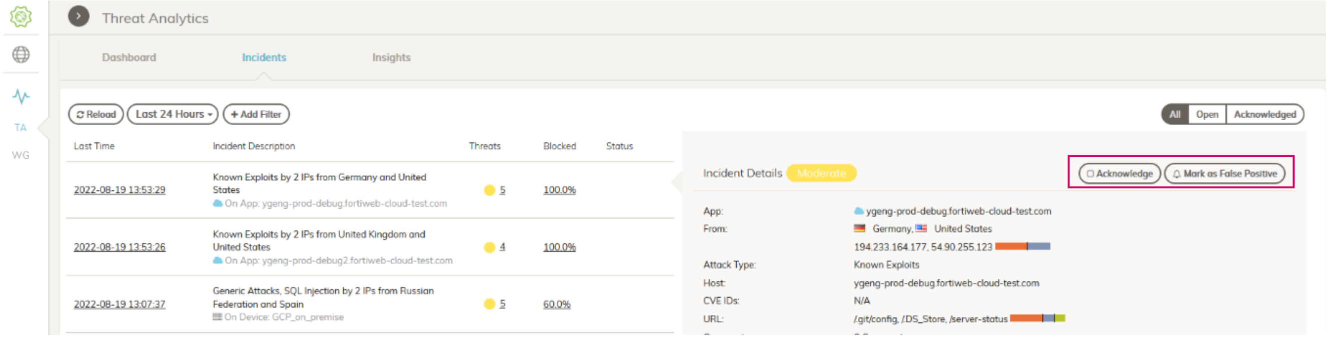
- Incidents
- Insights
- Settings

Incidents

Attack events are aggregated and then grouped into incidents by common characteristics. In this way, you can quickly find out which attack types occur frequently, the most malicious source IP addresses, etc.

By clicking the incident number, you will see the incident details including the attack type, the target application, source IPs, etc.

You can mark an incident as Acknowledged or False Positive, then the corresponding icons will display in the incident's **Status** column. Please note that marking **Acknowledge** or **False Positive** is only for your convenience to track the incidents. The system doesn't take this into account when it detects threats. You can also click the **Comments** link to add comments for the incident.

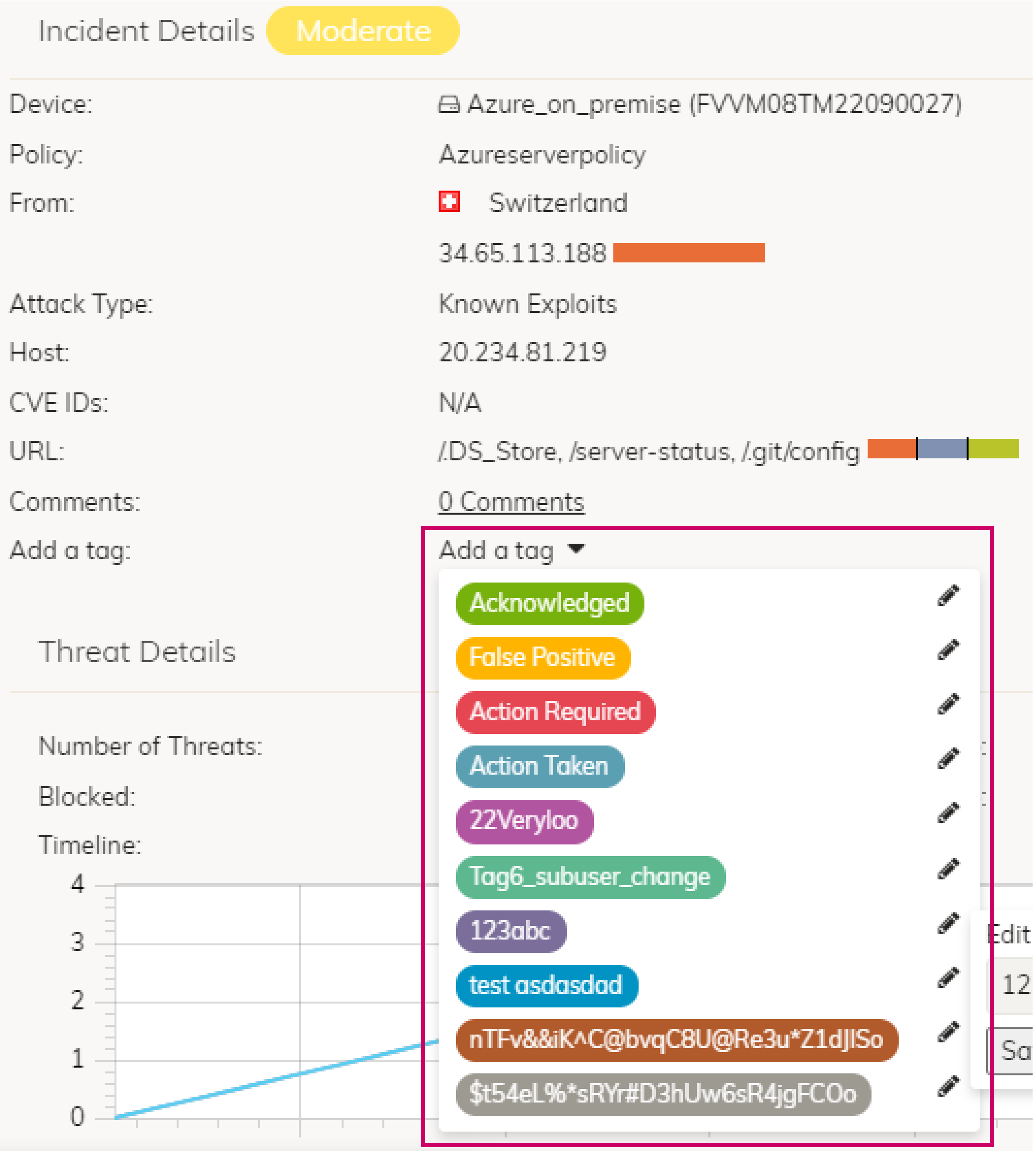


Last Time	Incident Description	Threats	Blocked	Status
2022-08-19 13:53:29	Known Exploits by 2 IPs from Germany and United States On App: ygeng-prod-debug.fortiweb-cloud-test.com	● 5	100.0%	
2022-08-19 13:53:26	Known Exploits by 2 IPs from United Kingdom and United States On App: ygeng-prod-debug2.fortiweb-cloud-test.com	● 4	100.0%	
2022-08-19 13:07:37	Generic Attacks, SQL Injection by 2 IPs from Russian Federation and Spain On Device: GCP_on_premise	● 5	60.0%	

Incident Details Moderate

App:	ygeng-prod-debug.fortiweb-cloud-test.com
From:	Germany, United States 194.233.164.177, 54.90.255.123
Attack Type:	Known Exploits
Host:	ygeng-prod-debug.fortiweb-cloud-test.com
CVE IDs:	N/A
URL:	/.git/config, /.DS_Store, /server-status

You can use predefined tags for Threat Analytics incidents. This helps in labeling incidents for future usage such as sorting, filtering and acknowledging incidents. It's supported to edit the tag name according to you needs.



Incident Details Moderate

Device: Azure_on_premise (FVVM08TM22090027)

Policy: Azureserverpolicy

From: Switzerland

34.65.113.188

Attack Type: Known Exploits

Host: 20.234.81.219

CVE IDs: N/A

URL: /.DS_Store, /server-status, /.git/config

Comments: 0 Comments

Add a tag: Add a tag

Threat Details

Number of Threats:

Blocked:

Timeline:

Roll down to the bottom of the **Incident Details** page, you can use the **Click to see details** button to open the threat view page which categorizes the attacks by Attack Type, Countries, Hosts, etc.

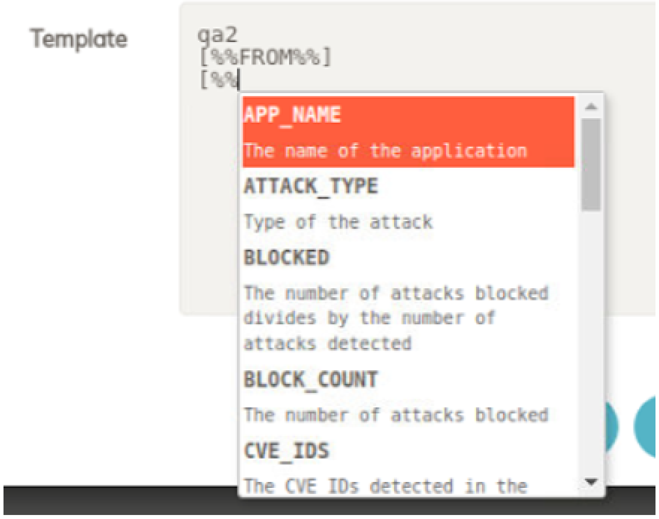
Settings

You can now define various rules to automatically create a Jira or ServiceNow ticket, or send an email when certain Incidents occur. This can help SOC analysts assign an incident to someone else in the organization.

To send email or create Jira tickets when certain incidents occur:

1. Go to **Threat Analytics > Threat Analytics**.
2. Select the **Settings** tab.

3. Click **Create Notification Template**.
4. Enter a name for the template.
5. For **Applications/Devices**, select:
   - **All Applications and Devices:** Notifications will be sent when incidents on any of the application or device occur.
   - **Customized:** Notifications will be sent only when incidents on the selected applications or devices occur.
6. Select the applications or devices you want to monitor, then move them to the **Selected** list. Please note that the applications in the list are those for which you have either read-write or read-only permission.
7. Turn on **Status** if you want this notification template to take effect.
8. Click **Next**.
9. Select **Notify me when** incident with certain risk level occurs.
   There may have multiple attack events with common characteristics aggregated in one incident. Incident with higher risk level means that there are more attack logs in it.
10. Select whether to send notification through email or Jira.
    - **Email**
      Configure the **Recipient**, **Subject**, **Template**. Separate multiple email addresses with ",".
      You can add macros as you want. Type "%%" then the available macro will be popped up.



Template

```
qa2
[%%FROM%%]
[%%
```

APP_NAME
The name of the application
ATTACK_TYPE
Type of the attack
BLOCKED
The number of attacks blocked divides by the number of attacks detected
BLOCK_COUNT
The number of attacks blocked
CVE_IDS
The CVE IDs detected in the

    - **Jira**
      i. Enter the Jira URL, then the **Account** and **Token** for FortiWeb Cloud to build up connection with Jira.
      ii. Click **Next**. FortiWeb Cloud will verify the token and account. It will not proceed to next page if the verification fails.
      iii. FortiWeb Cloud pulls the project names, issue types, and reporters from Jira, then populate them in the drop-down list. Select from the list. The Jira incident to be created will be tagged with the selected project name, issue type, and reporter.
      iv. Edit the **Summary** and **Description**. You can add macros as you want. Type "%%" then the available macro will be popped up.
      v. Click **Save**.
    - **ServiceNow**
      i. Enter the ServiceNow URL, then the **Client ID** and **Client Secret** for FortiWeb Cloud to build up connection with ServiceNow.
      ii. Click **Next**. FortiWeb Cloud will verify the token and account. It will not proceed to next page if the verification fails.

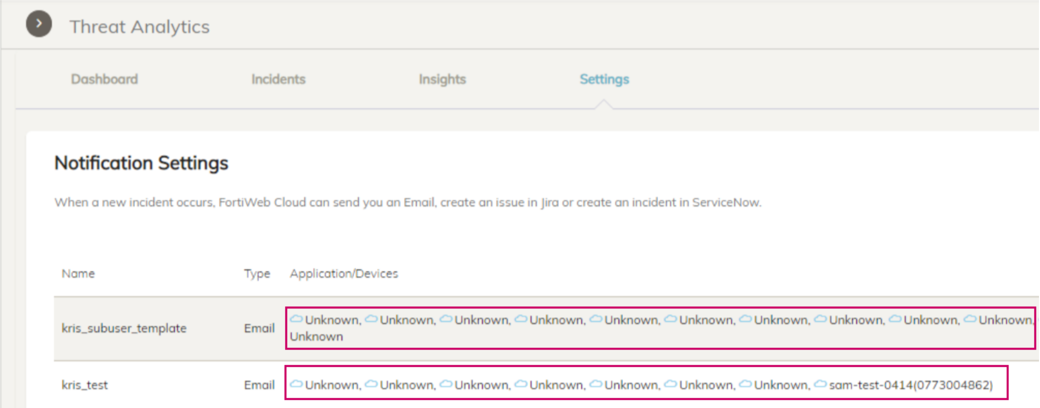
iii. FortiWeb Cloud pulls the Caller, Assignment Group from ServiceNow, then populate them in the drop-down list. Select from the list. The ServiceNow incident to be created will be tagged with the selected Caller and Assignment Group.

iv. Edit the **Summary** and **Description**. You can add macros as you want. Type "%%" then the available macro will be popped up.

v. Click **Save**.

The **Notification Settings** is globally applied, which means the **Notification Template** created or edited in your account will also be applied to other accounts under the same root account.

In certain cases you will see the application names shown as unknown. These are the applications to which you don't have Read-Only or Read-Write permission.



Notification Settings

When a new incident occurs, FortiWeb Cloud can send you an Email, create an issue in Jira or create an incident in ServiceNow.

Name	Type	Application/Devices
kris_subuser_template	Email	Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown
kris_test	Email	Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, Unknown, sam-test-0414(0773004862)

Forwarding FortiWeb attack logs to Threat Analytics

Attack logs on FortiWeb can be forwarded to FortiWeb Cloud, which allows you to leverage the powerful AI-based Threat Analytics service that helps identify significant threats and zoom in on the threats that matter.

Prerequisites for using Threat Analytics for FortiWeb's attack logs:

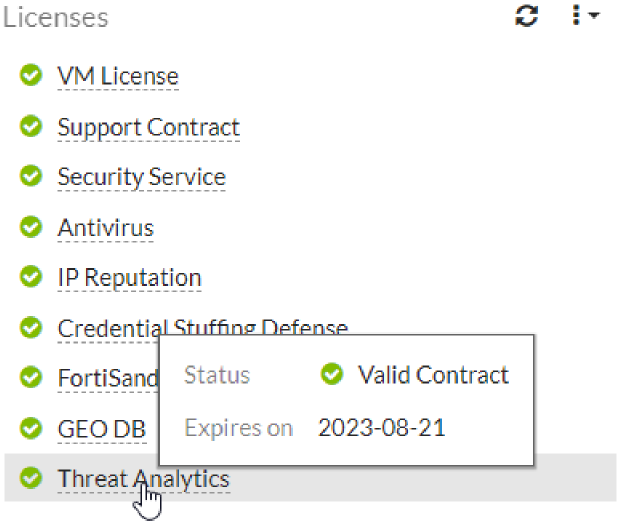
- You have a valid Threat Analytics service license.
- Threat Analytics service is enabled in FortiWeb.

Please note that when your license expires or becomes invalid, the log forwarding will stop immediately regardless whether the Threat Analytics service is enabled.

To enable Threat Analytics:

1. Contact Sales team to purchase a license with the Threat Analytics service, then register the license on Support site: HTTPs://support.fortinet.com
2. Log in to FortiWeb.

3. Check the status of Threat Analytics in the **Licenses** widget in **Dashboard > Status.** It should be displayed as Valid.

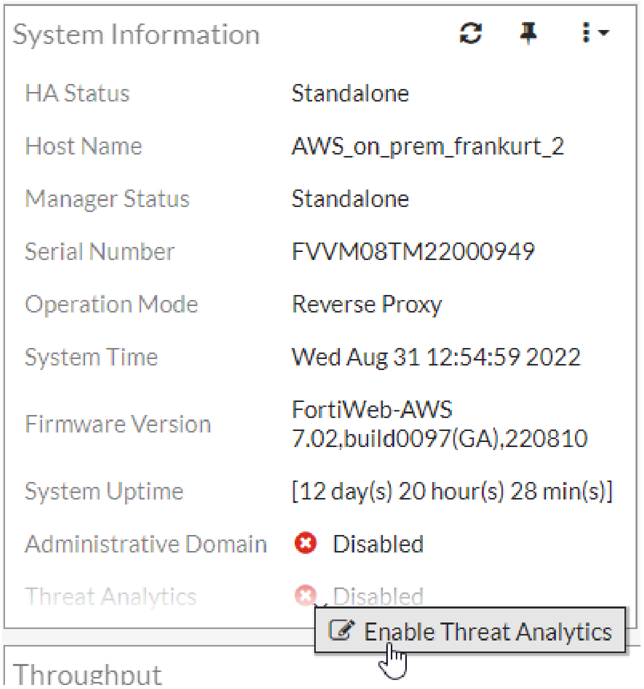


Licenses

- ✓ VM License
- ✓ Support Contract
- ✓ Security Service
- ✓ Antivirus
- ✓ IP Reputation
- ✓ Credential Stuffing Defense
- ✓ FortiSand
- ✓ GEO DB
- ✓ Threat Analytics

Status	✓ Valid Contract
Expires on	2023-08-21

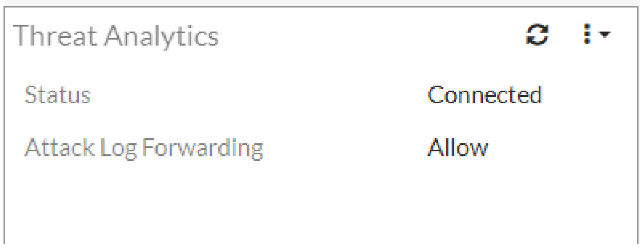
4. In the **System Information** Widget in **Dashboard > Status**, click **Enable Threat Analytics**, then click **OK** in the pop-up window.



System Information

HA Status	Standalone
Host Name	AWS_on_prem_frankurt_2
Manager Status	Standalone
Serial Number	FVVM08TM22000949
Operation Mode	Reverse Proxy
System Time	Wed Aug 31 12:54:59 2022
Firmware Version	FortiWeb-AWS 7.02,build0097(GA),220810
System Uptime	[12 day(s) 20 hour(s) 28 min(s)]
Administrative Domain	✗ Disabled
Threat Analytics	✗ Disabled

5. Make sure **Enable Attack Log** is switched on in **Log&Report > Log Config > Other Log Settings**.
6. Go to **Dashboard > Status**, click **Add Widget**, then select **Threat Analytics** in the **System** section. The **Threat Analytics** widget will be displayed on the **Status** page. You can view whether FortiWeb is successfully connected with FortiWeb Cloud and whether the attack logs are being forwarded.



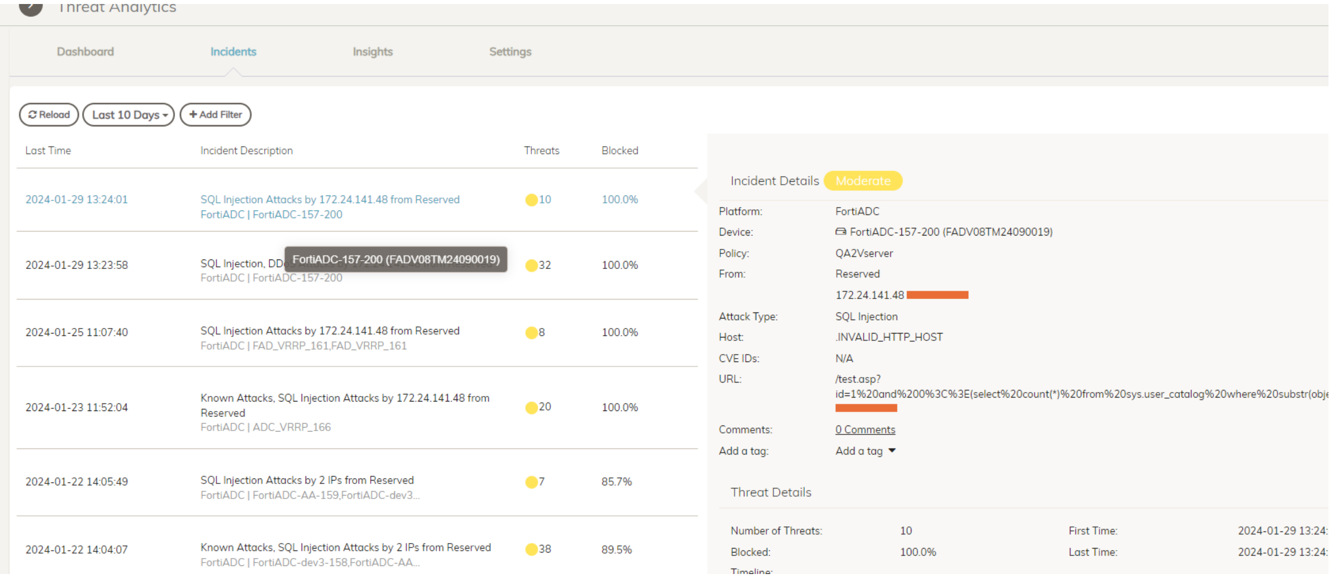
Threat Analytics

Status	Connected
Attack Log Forwarding	Allow

7. Wait for FortiWeb to generate attack logs.
8. Log in to FortiWeb Cloud with the account you used when registering your license on Fortinet Support site.

Forwarding FortiADC attack logs to Threat Analytics

Through the FortiADC integration with FortiWeb Cloud Threat Analytics, you can forward FortiADC attack logs to FortiWeb Cloud where the AI-based Threat Analytics engine identifies unknown attack patterns by parsing through all FortiADC attack logs and then aggregating similar or related attack logs into single incidents. This allows you to use these identified attack patterns to protect your application against the identified threats.



Last Time	Incident Description	Threats	Blocked
2024-01-29 13:24:01	SQL Injection Attacks by 172.24.141.48 from Reserved FortiADC | FortiADC-157-200	10	100.0%
2024-01-29 13:23:58	SQL Injection, DD FortiADC-157-200 (FADV08TM24090019) FortiADC | FortiADC-157-200	32	100.0%
2024-01-25 11:07:40	SQL Injection Attacks by 172.24.141.48 from Reserved FortiADC | FAD_VRRP_161,FAD_VRRP_161	8	100.0%
2024-01-23 11:52:04	Known Attacks, SQL Injection Attacks by 172.24.141.48 from Reserved FortiADC | ADC_VRRP_166	20	100.0%
2024-01-22 14:05:49	SQL Injection Attacks by 2 IPs from Reserved FortiADC | FortiADC-AA-159,FortiADC-dev3...	7	85.7%
2024-01-22 14:04:07	Known Attacks, SQL Injection Attacks by 2 IPs from Reserved FortiADC | FortiADC-dev3-158,FortiADC-AA...	38	89.5%

Incident Details Moderate

Platform:	FortiADC
Device:	FortiADC-157-200 (FADV08TM24090019)
Policy:	QA2Vserver
From:	Reserved 172.24.141.48 [redacted]
Attack Type:	SQL Injection
Host:	.INVALID_HTTP_HOST
CVE IDs:	N/A
URL:	/test.asp? id=1%20and%200%3C%3E(select%20count(*)%20from%20sys.user_catalog%20where%20substr(obj [redacted]
Comments:	0 Comments
Add a tag:	Add a tag

Threat Details

Number of Threats:	10	First Time:	2024-01-29 13:24:
Blocked:	100.0%	Last Time:	2024-01-29 13:24:

Timeline:

Prerequisites for using Threat Analytics for FortiADC attack logs:

- You must have a valid Threat Analytics service license.
- You must have the Threat Analytics service enabled in FortiADC.

Please note that when your license expires or becomes invalid, the log forwarding will stop immediately regardless of whether the Threat Analytics service is enabled.

14-Day Evaluation license

A 14-day Evaluation license is offered to customers who would want to evaluate the Threat Analytics service. This 14-day Evaluation license can only be used once. To activate the 14-day Evaluation license, enable Threat Analytics connector from **Security Fabric > Fabric Connectors**. During this 14-day trial period, you can disable and re-enable

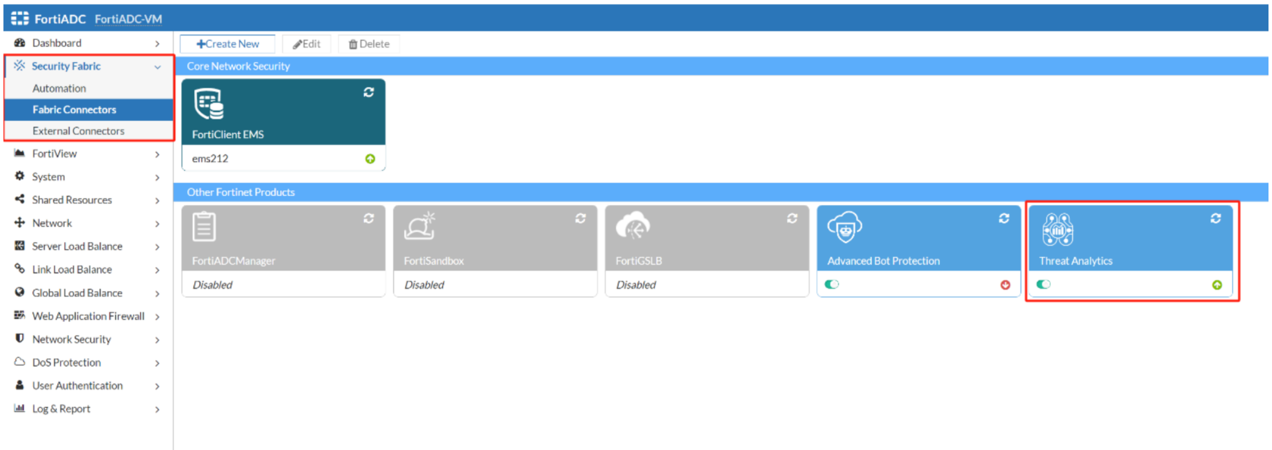
Threat Analytics anytime. The 14-day trial period starts from the first time Threat Analytics is enabled. When you are ready to purchase the full license with the Threat Analytics service, contact the Fortinet Sales team.

To enable Threat Analytics:

1. Register the license with the Threat Analytics feature on the Support site: HTTPs://support.fortinet.com
2. Log in to FortiADC.
3. In the **Dashboard > Status** License widget, check the status ofThreat Analytics. The status should be displayed as Valid.
4. Go to **Security Fabric > Fabric Connectors**. Under Other Fortinet Products section, locate the Threat Analytics connector.
5. Enable Threat Analytics.

GUI

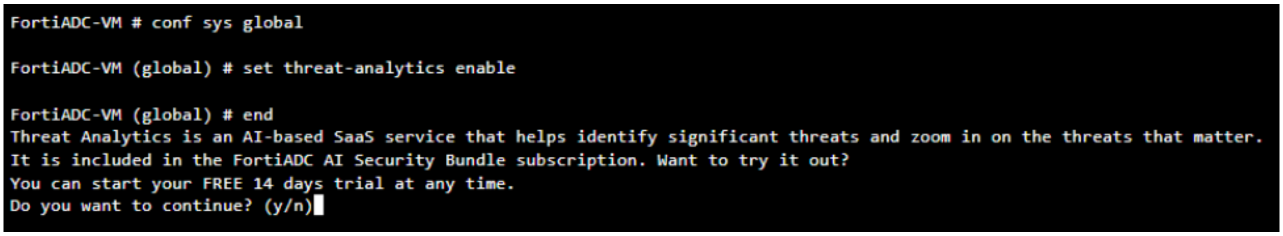
Go to **Security Fabric > Fabric Connectors** and enable the Threat Analytics connector.



CLI

```
config system global
       set threat-analytics enable
       set threat-analytics-authrul <auth-url>
end
```

If you do not have an active Threat Analytics contract, you will receive the following message:

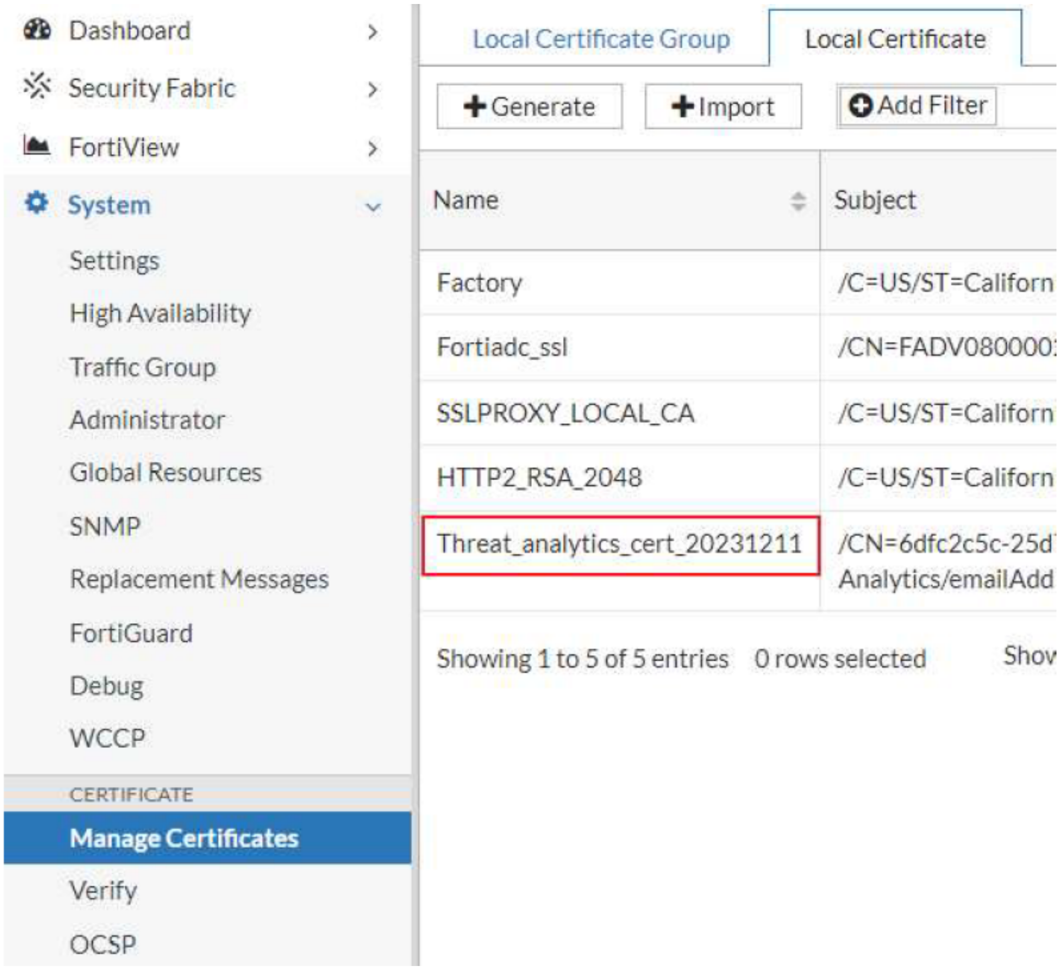


```
FortiADC-VM # conf sys global

FortiADC-VM (global) # set threat-analytics enable

FortiADC-VM (global) # end
Threat Analytics is an AI-based SaaS service that helps identify significant threats and zoom in on the threats that matter.
It is included in the FortiADC AI Security Bundle subscription. Want to try it out?
You can start your FREE 14 days trial at any time.
Do you want to continue? (y/n)
```

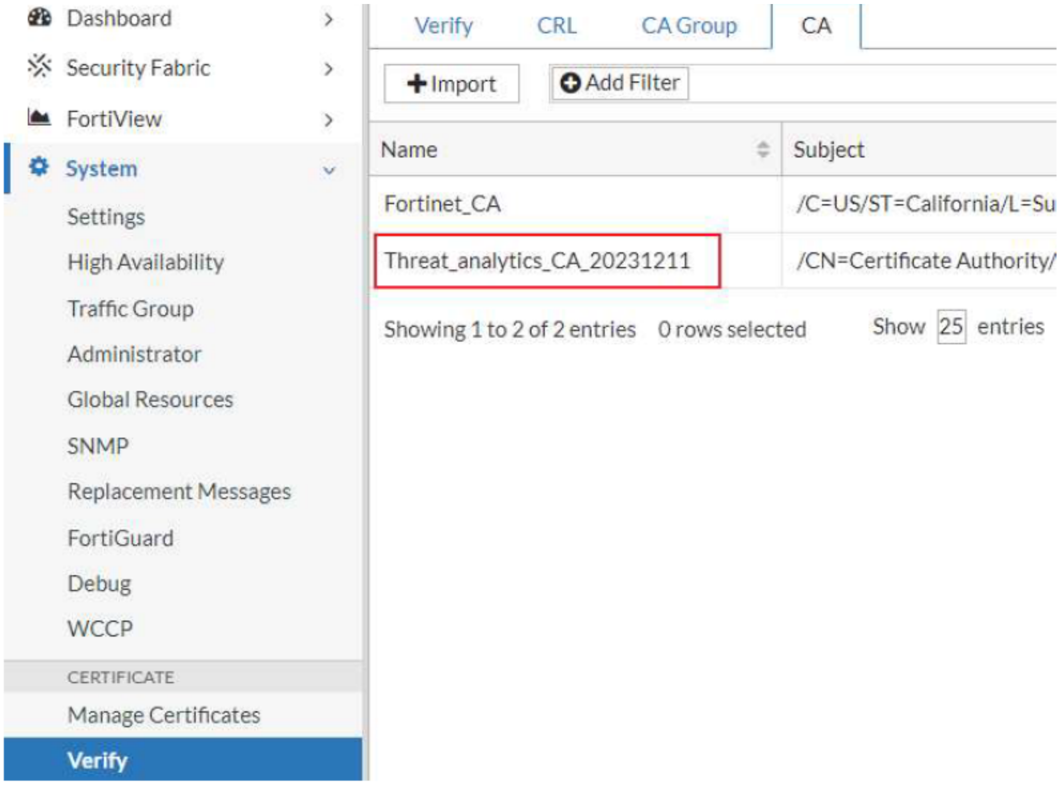
6. Once the Threat Analytics connector successfully connects FortiADC to the FortiWeb Cloud Threat Analytics service, a new local certificate and CA will be created. Check the certificates and CA to ensure they are present.
   a. Go to **System > Manage Certificates** to locate the new local certificate with the name *Threat_analytics_cert_ <date_of_today>*.



Name	Subject
Factory	/C=US/ST=Californ
Fortiadc_ssl	/CN=FADV080000:
SSLPROXY_LOCAL_CA	/C=US/ST=Californ
HTTP2_RSA_2048	/C=US/ST=Californ
Threat_analytics_cert_20231211	/CN=6dfc2c5c-25d Analytics/emailAdd

Showing 1 to 5 of 5 entries 0 rows selected Shov

b. Go to **System > Verify** to locate the new CA with the name *Threat_analytics_CA_<date_of_today>*.



Name	Subject
Fortinet_CA	/C=US/ST=California/L=Su
Threat_analytics_CA_20231211	/CN=Certificate Authority/

Showing 1 to 2 of 2 entries 0 rows selected Show 25 entries

c. A new syslog global_remote server will be created with the FQDN address type and with the comment *"fweb_cloud"*.

7. Wait to allow FortiADC to generate attack logs and forward them to FortiWeb Cloud.
8. Log In to FortiWeb Cloud with the account you used when registering your license on the Fortinet Support site.

Do not delete of modify the syslog remote and certificate/CA entry. Threat Analytics cannot be functional without these configurations.

Threat Analytics in VDOM

When Threat Analytics is enabled in VDOMs, Override in the Syslog Server configuration will be disabled in order to use the global syslog server. If you have previously enabled Override in the Syslog Server configuration, then the default global syslog server list would be removed and you may use a new syslog server list specifically defined in the VDOM. By default, the new syslog remote server would also be created in all the VDOMs with Threat Analytics enabled, which disables Override in order to use the global syslog server. When Threat Analytics is enabled, it will always use the global or root DNS, and not the VDOM's DNS.

Threat Analytics in HA

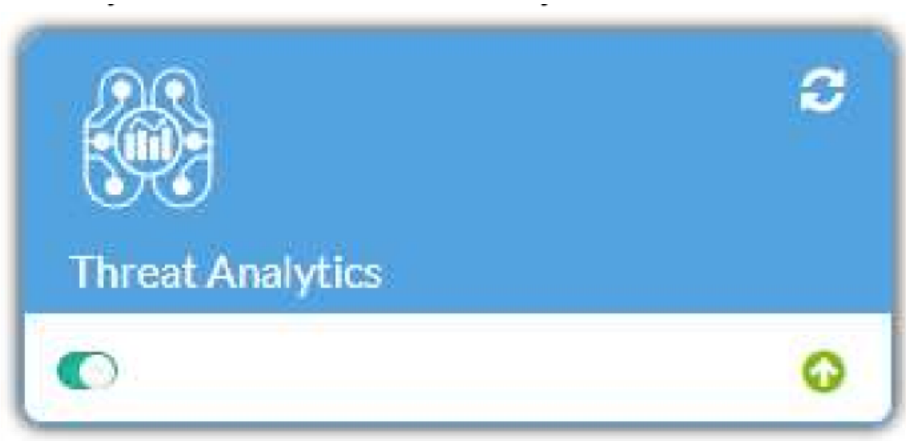
In HA mode, only the primary node is connected to FortiWeb Cloud Threat Analytics and then the certification and syslog configurations are synchronized to the secondary. This workflow is designed to prevent HA synchronization issues that can arise with having both the primary and secondary nodes connect to the FortiWeb Cloud at the same time. As only the primary node is connected to FortiWeb Cloud, the Threat Analytics status in the secondary node will show as "disconnected".

Threat Analytics troubleshooting and debugging

You can use the following tools to diagnose and troubleshoot Threat Analytics issues in FortiADC

Threat Anaytics connector

When you enable the threat analytics connector, the Threat Analytics service license status will display.



The ⬆ and ⬇ icons indicate whether the Threat Analytics connector has successfully connected to the FortiWeb Cloud server. If the connection is down , FortiADC will first perform an inspection of the Threat Analytics license status to determine whether the connection issue is caused by an invalid license. If a valid Threat Analytics license exists, then further troubleshooting may be required to determine the root cause of the Threat Analytics connection issue.

License Status	Description
0	No license
1	Advanced license
2	Standard license, has not enabled threat analytics before
3	Standard license, has enabled threat analytics before, has not expired.
4	Standard license, expired.

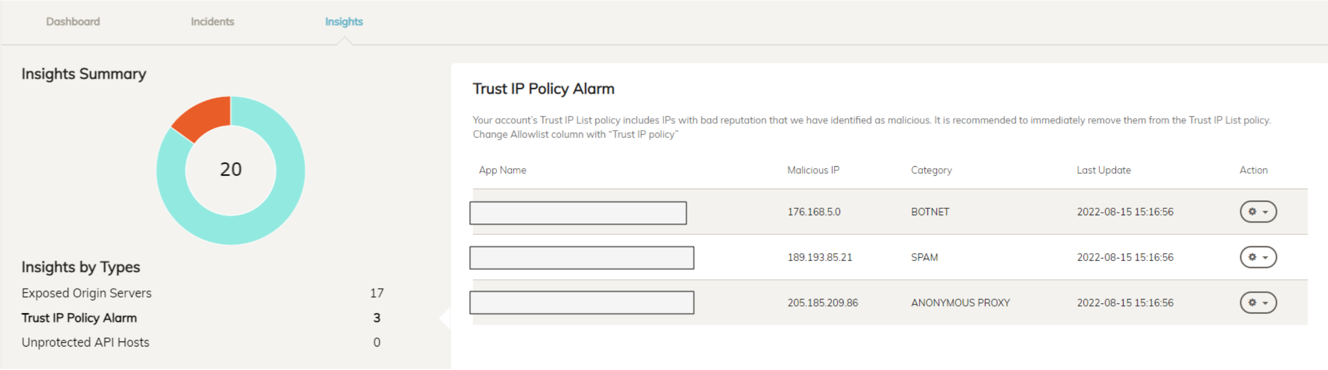
CLI commands to debug logs relating to Threat Analytics

Command	Guidelines
`diagnose debug module wassd`	To view the debug informatio of he wassd daemon. The wassd daemon forms the connection between FortiADC and FortiWeb Cloud and performs several integral functions when Threat Analytics is enabled. This includes the following:

Command	Guidelines
	• Establishing a web socket connection with the FortiWeb Cloud using a token. The wassd identifies whether a CA exists before registering to theFortiWeb Cloud. If a CA does exist, then the wassd will send the issue date of the CA certificate to the FortiWeb Cloud. • Updating FortiWeb Cloud with FortiADC configuration changes, such as HA status changes, member updates, or mode modification. • Updating device certificates received from the FortiWeb Cloud. Ifwassd registered to the FortiWeb Cloud without the issue date of the CA or that the certificate has expired, then FortiWeb Cloud will send new certificates (including the certificate, key, and CA) to wassd. The wassd will update to the local certificate and CA table, and register to FortiWeb Cloud again with the latest CA issue date. • Starting the forwarding of FortiADC attack logs to FortiWeb Cloud. If wassd has successfully registered to FortiWeb Cloud, then it will start the action with the log server and port from the FortiWeb Cloud. **Note:** The wassd daemon is create for Threat Analytics and executes the `wassd_ws` Python script when Threat Analytics is enabled. The backend log for the Python script is stored in `/var/log/wassd.log`
`diagnose sysem threat-analytics info`	To view the system information for Threat Analytics

Insights

The Insights page provides an additional layer of incident analysis and offers recommendations to improve your security posture.



Insights Summary

Insights by Types

Exposed Origin Servers	17
Trust IP Policy Alarm	3
Unprotected API Hosts	0

Trust IP Policy Alarm

Your account's Trust IP List policy includes IPs with bad reputation that we have identified as malicious. It is recommended to immediately remove them from the Trust IP List policy. Change Allowlist column with "Trust IP policy"

App Name	Malicious IP	Category	Last Update	Action
	176.168.5.0	BOTNET	2022-08-15 15:16:56	⚙ ▾
	189.193.85.21	SPAM	2022-08-15 15:16:56	⚙ ▾
	205.185.209.86	ANONYMOUS PROXY	2022-08-15 15:16:56	⚙ ▾

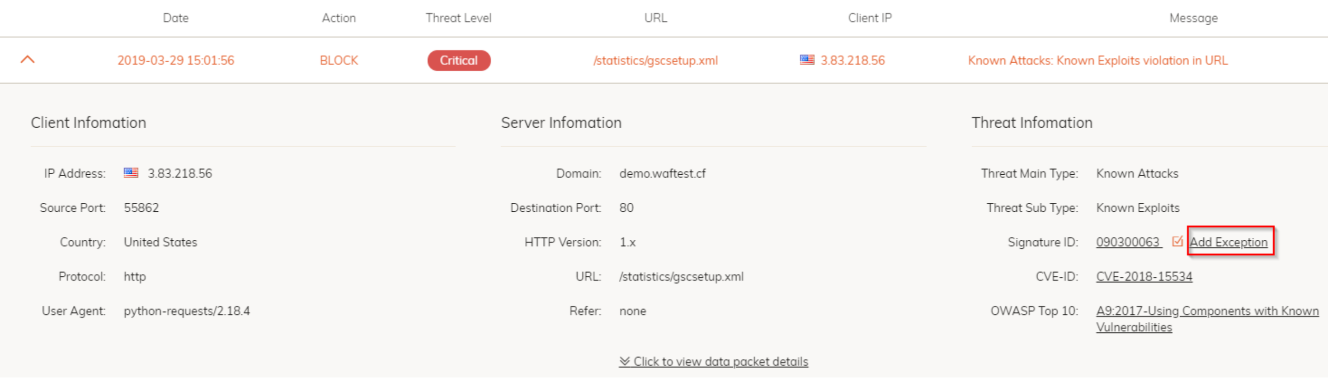
Attack logs

Unlike **FortiView** which displays threat data in different categories, **Attack Logs** straightforwardly lists all the threats.

Attack log now displays logs from all applications. In **Attack Logs**, You can click an entry to see threat details, or use **Add Filter** to filter out threats as desired. Click **Reload** to update the page with any logs that have been recorded since you previously loaded the page.

A maximum of 10,000 logs are displayed per each filter. FortiWeb Cloud saves the attack logs for two months. After that, they will be deleted.

If you know that certain URL tends to falsely trigger violations by matching an attack signature during normal use, you can click **Add Exception** beside the signature ID. The traffic to the specified URL and/or parameter in the exception rule will not be treated as an attack even if it matches this particular signature. For Request URL and Parameter Name, you should enable at least one. Please wait several minutes for the configuration to take effect.



	Date	Action	Threat Level	URL	Client IP	Message
^	2019-03-29 15:01:56	BLOCK	Critical	/statistics/gscsetup.xml	3.83.218.56	Known Attacks: Known Exploits violation in URL

Client Infomation

IP Address: 3.83.218.56
Source Port: 55862
Country: United States
Protocol: http
User Agent: python-requests/2.18.4

Server Infomation

Domain: demo.waftest.cf
Destination Port: 80
HTTP Version: 1.x
URL: /statistics/gscsetup.xml
Refer: none

Threat Infomation

Threat Main Type: Known Attacks
Threat Sub Type: Known Exploits
Signature ID: 090300063 ☑ Add Exception
CVE-ID: CVE-2018-15534
OWASP Top 10: A9:2017-Using Components with Known Vulnerabilities

Click to view data packet details

Request URL	Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`. • If **String Match** is selected, ensure the value starts with a forward slash (/) (for example, `/testpage.php`). You can enter a precise URL, such as /floder1/index.htm or use wildcards to match multiple URLs, such as /floder1/* ,or /floder1/*/index.htm. • If **Regular Expression Match** is selected, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. For details, see Frequently used regular expressions on page 237. Do not include a domain name because it's by default the domain name of this application.
Parameter Name	Specify a parameter name to match. For example, `http://www.test.com/testpage.php?a=1`, the parameter name is "a". To create a regular expression, see Frequently used regular expressions on page 237.

Please note that the number of attacks displayed in Attack Logs, FortiView , and Blocked Requests widget on Dashboard are slightly different.

- Certain attack types such as Bot and DDoS attacks generate a large amount of requests in a short time. To prevent numerous identical attack logs flooding the UI, FortiWeb Cloud only logs the first request in Attack Logs and FortiView , while it shows the actual count in Blocked Requests Widget so you can know how many actual attack requests were blocked.
- To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such items are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget.

- If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as Alert & Deny (no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget.
  To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below.

Attack ID	Security Rule
20000001	Allow Method
20000002	Protected Hostnames
20000003	Page Access
20000004	Start Pages
20000005	Parameter Validation
20000006	Black IP List
20000007	URL Access
20000008	Signature Detection
20000009	Custom Signature Detection
20000011	Hidden Fields
20000012	Site Publish
20000013	HTTP Parsing Error
20000014	DoS Protection
20000015	SYN Flood Protection
20000016	HTTPS Connection Failure
20000017	File Upload Restriction
20000018	GEO IP
20000019	Illegal XML Format
20000020	Illegal JSON Format
20000021	Custom Access
20000022	IP Reputation
20000023	Padding Oracle
20000024	CSRF Protection
20000025	Quarantined IPs
20000026	HTTP Protocol Constraints
20000027	Credential Stuffing Defense
20000028	User Tracking

Attack ID	Security Rule
20000029	XML Validation Violation
20000030	Cookie Security
20000031	FTP Command Restriction
20000032	FTP Parsing Error
20000033	Timeout Session
20000034	Other Attacks
20000035	FTP File Security
20000036	FTPS Connection Failure
20000037	Anomaly Detection
20000038	OpenAPI Validation Violation
20000039	WebSocket Security
20000040	MITB AJAX Security
20000041	Bot Detection
20000042	CORS Check Security
20000043	JSON Validation Security
20000044	Mobile API Protection
20000045	Bot Deception
20000046	Biometrics Based Detection
20000047	Threshold Based Detection
20000048	API Gateway
20000049	URL Encryption
20000050	SQL/XSS Syntax Based Detection
20000051	Known Bots Detection
20000053	Allow Only IP List
20000200	Known Attacks
20000201	Information Leakage
20000202	Cookie Security
20000203	File Protection
20000204	Client Security
20000205	Request Limits
20000206	URL Access

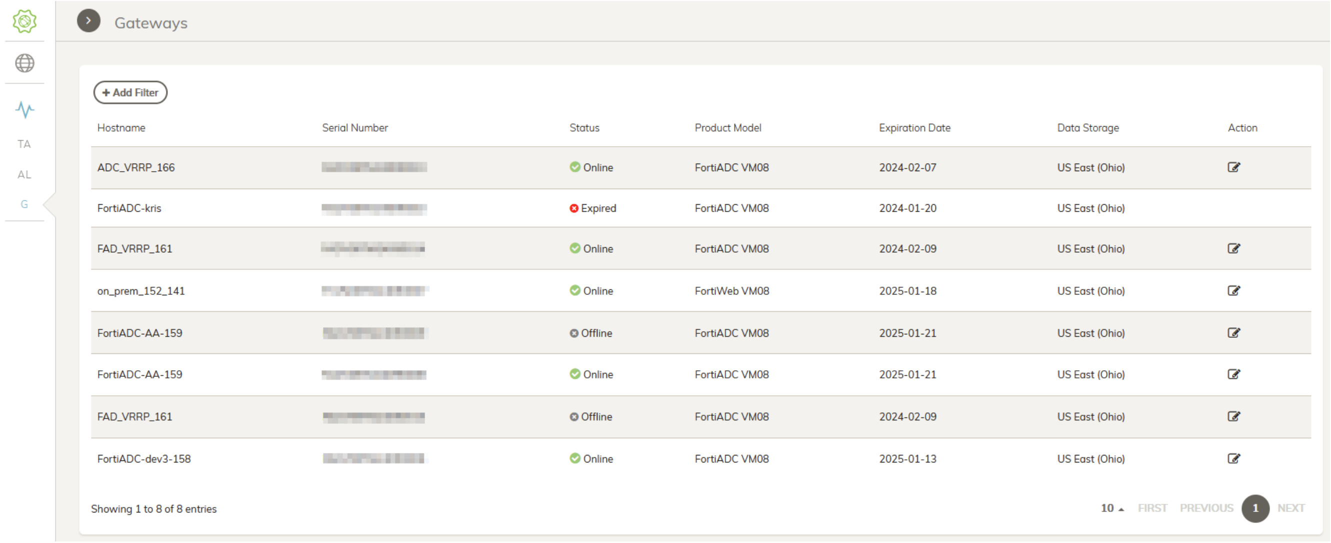
Attack ID	Security Rule
20000207	IP Protection
20000208	Bot Mitigation
20000209	DDoS Prevention
20000210	XML Security
20000211	OpenAPI Validation
20000212	WebSocket Security
20000213	Known Bots Detection
20000214	API Gateway
20000215	Mobile API
20000216	JSON Security

Gateways

FortiWeb Cloud now integrates with FortiWeb and FortiADC appliances. You can collect attack logs from all your FortiWeb platforms and leverage the power of threat analytics across your entire web assets.

You can configure FortiWeb to send its attack logs to FortiWeb Cloud. For more information, see Forwarding FortiWeb attack logs to Threat Analytics.

The devices connected with FortiWeb Cloud are displayed in **Gateways**.



Hostname	Serial Number	Status	Product Model	Expiration Date	Data Storage	Action
ADC_VRRP_166	[redacted]	✓ Online	FortiADC VM08	2024-02-07	US East (Ohio)	✎
FortiADC-kris	[redacted]	✕ Expired	FortiADC VM08	2024-01-20	US East (Ohio)	
FAD_VRRP_161	[redacted]	✓ Online	FortiADC VM08	2024-02-09	US East (Ohio)	✎
on_prem_152_141	[redacted]	✓ Online	FortiWeb VM08	2025-01-18	US East (Ohio)	✎
FortiADC-AA-159	[redacted]	✕ Offline	FortiADC VM08	2025-01-21	US East (Ohio)	✎
FortiADC-AA-159	[redacted]	✓ Online	FortiADC VM08	2025-01-21	US East (Ohio)	✎
FAD_VRRP_161	[redacted]	✕ Offline	FortiADC VM08	2024-02-09	US East (Ohio)	✎
FortiADC-dev3-158	[redacted]	✓ Online	FortiADC VM08	2025-01-13	US East (Ohio)	✎

Showing 1 to 8 of 8 entries

Log Settings

Exporting attack logs

To export the attack logs to a log server:

1. Go to **Log Settings**.
2. Enable **Attack Log Export**.
3. Click **Add Log Server**.
4. Configure the following settings.

Name	Enter a name for the log server.
Server Type	Select whether to export the logs to a log server, an ElasticSearch service, FortiAnalyzer, or FortiSIEM. See the following instructions for SysLog, ElasticSearch, FortiAnalyzer, and FortiSIEM
SysLog	
IP/Domain and Port	Enter the IP/Domain and Port of the log server.
Protocol	Select the protocol used for log transfer.
Server Certificate Verification	When enabled, the system will enforces server certificate verification before it sends attack logs to the log server.
Custom Certificate and Key	• **Off:** FortiWeb Cloud automatically retrieves the SSL certificate used to encrypt the HTTPS connections between the log server and FortiWeb Cloud. • **On:** Manually enter the SSL certificate. Available only if you select **SSL** in **Protocol**.
Client Certificate	Fill in the Certificate field. Available only if you enabled **Custom Certificate and Key**.
Private Key	Fill in the Private Key field. Available only if you enabled **Custom Certificate and Key**.
Password	Enter the password of the private key. Available only if you enabled **Custom Certificate and Key**.
Log Format	• **Default:** Export logs in default format. • **Custom:** Customize the log format. All the supported parameters are listed by default. You can select the ones that you need, and delete the others.

	• **Splunk:** Export logs to Splunk log server. • **CEF:0 (ArcSight):** Export logs in CEF:0 format. • **Microsoft Azure OMS:** Export logs in Microsoft Azure OMS format. • **LEEF1.0(QRadar):** Export logs in LEEF1.0 format.
Log Severity	Select the severity level of the logs. All the exported logs will be attached with the selected severity level.
Log Facility	Select the source facility of the logs. We only support the local use facilities which are not reserved and are available for general use.
ElasticSearch ElasticSearch is a search engine providing a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.	
Address and Port	Enter the address and port to access your ElasticSearch service. The default port for ElasticSearch service is 9200.
User Name	Enter the user name of the ElasticSearch service.
Password	Enter the password of the ElasticSearch service user.
FortiAnalyzer FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides centralized logging and analysis, plus end-to-end visibility. *Please note that while FortiAnalyzer is supported, FortiAnalyzer Cloud is not.	
IP/Domain and Port	Enter the IP/Domain and Port of the log server.
Protocol	Select the protocol used for log transfer.
Server Certificate Verification	When enabled, the system will enforces server certificate verification before it sends attack logs to the log server.
Log Format Preview	This box shows a preview of the log format, and is not editable.
Log Severity	Select the severity level of the logs. All the exported logs will be attached with the selected severity level.
Log Facility	Select the source facility of the logs. We only support the local use facilities which are not reserved and are available for general use.
FortiSIEM	
IP/Domain and Port	Enter the IP/Domain and Port of the log server.
Protocol	Select the protocol used for log transfer.
Server Certificate Verification	When enabled, the system will enforces server certificate verification before it sends attack logs to the log server.
Log Format Preview	This box shows a preview of the log format, and is not editable.
Log Severity	Select the severity level of the logs. All the exported logs will be attached with the selected severity level.
Log Facility	Select the source facility of the logs. We only support the local use facilities which are not reserved and are available for general use.

5. Click **OK**. The system exports newly generated attack logs to the log server every minute.

To prevent log poisoning, it's recommended to set filters on your log server to allow only the traffic from FortiWeb Cloud. The source IPs are as follows:

- 3.226.2.163
- 3.123.68.65

Configuring attack log alert

FortiWeb Cloud monitors the attack logs every five minutes, and sends alert email based on the set threat level. You can also customize a more complex rule for the alert email.

To configure an attack log alert:

1. Go to **Log Settings**.
2. Enable **Attack Log Alerts**.
3. For **Mode**, when you select **Basic**, configure the following settings

Threat Level	The attacks of different threat levels are marked with the following values: • Critical: 50 • High: 30 • Medium: 10 • Low: 5 The system counts the threat score every 5 minutes. For example, if there are 2 critical attacks and 1 high threat level attack in 5 minutes, the threat score is 50*2+30=130. **Basic** In basic mode, an alert email will be sent if the threat score is accumulated higher than the following value in 5 minutes: • 1 (low) • 100 (medium) • 400 (high) • 700 (critical) For example, if you set the **Threat Level** to medium, and the threat score is 130, then an alert email will be sent.
Notification Recipient	• **Default**—The alert email will be sent to the email address that is used to register your account. • **Custom**—Specify the email addresses to receive the alert.
Custom Recipient	Enter the email addresses. Separate multiple email addresses with ",". Available only if you select Custom for Notification Recipient.

4. For **Mode**, when you select **Advanced**, click **+Create Alert** to customize a more complex rule. You can create at most five rules.

5. Configure the following settings.

Name	Enter a name for the alert rule.
Threat Score	Specify a threat score for the attack log. The attacks of different threat levels are marked with the following values: • Critical: 50 • High: 30 • Medium: 10 • Low: 5 The system counts the threat score every 5 minutes. For example, if there are 2 critical attacks and 1 high threat level attack in 5 minutes, the threat score is 50*2+30=130. If the actual threat score is higher than the score value you set, an alert email will be sent.
Notification Recipient	• **Default**—The alert email will be sent to the email address that is used to register your account. • **Custom**—Specify the email addresses to receive the alert.
Custom Recipient	Enter the email addresses. Separate multiple email addresses with ",". Available only if you select Custom for Notification Recipient.

6. For **Filter Overview**, click **Add Filter** to create a filter based on attack log messages. Only messages that match the criteria in the filter will be calculated on the threat score.
7. Click **OK**.

Exporting traffic logs

Traffic logs record traffic events such as HTTP requests and responses, and the expiration of HTTP sessions. FortiWeb Cloud's Web UI doesn't show traffic logs, but you can export traffic logs to AWS S3 or Azure Blob bucket in real time for long-term storage, analysis, or alerting.

Please note that at this time, FortiWeb Cloud does not support exporting traffic logs to OCI (Oracle Cloud Infrastructure).

1. Go to **Log Settings**. w
2. Enable **Traffic Log Export**.

3. Configure the following settings.

Server Type	Select whether to export the logs to AWS S3 or Azure Blob.
AWS S3	
Bucket name	Enter the AWS S3 bucket name.
Region	Enter the region code, for example, ap-southeast-1.
Access Key ID	Enter the access key ID of the S3 bucket.
Secret Key ID	Enter the secret key ID of the S3 bucket.
Prefix / Folder	Enter the prefix / folder to store the traffic log.
Azure Blob	
Storage Account Name	Enter the Azure Blob storage account name
Account Access Key	Enter the Account Access Key for your storage account.
Container Name	Enter the name of the blob container to which you would like to export your traffic logs.

4. Click **Save**.

To prevent log poisoning, it's recommended to set filters on your S3 bucket to allow only the traffic from FortiWeb Cloud. The source IPs from FortiWeb Cloud are as follows:

- 3.226.2.163
- 3.123.68.65

We also recommend adding the source IP addresses of traffic log exporting centers into the filter, corresponding to the region of your application.

AWS:

ap-east-1: Asia Pacific (Hong Kong)	16.162.29.183
ap-south-1: Asia Pacific (Mumbai)	15.207.118.191
ap-southeast.prod: Asia Pacific (Singapore)	18.142.59.230
ap-southeast-2: Asia Pacific (Sydney)	13.238.126.108
ca-central-1: Canada (Central)	52.60.181.20
eu-central-1: Europe (Frankfurt)	3.64.92.136 3.79.38.161
eu-west-1: Europe (Ireland)	54.220.37.1
eu-west-2: Europe (London)	18.171.94.215
eu-west-3: Europe (Paris)	15.237.205.81
eu-south-1: Europe (Milan)	35.152.101.76
il-central-1: AWS Israel (Tel Aviv)	51.17.180.108
sa-east-1:L South America (Sao Paulo)	15.229.167.39
us-east-1: US East (N.Virginia)	44.215.25.31 44.216.53.179
us-east-2: US East (Ohio)	3.19.8.134
us-west-1: US West (N. California)	54.177.53.242

us-west-2: US West (Oregon)	34.208.62.10

Azure:

Australia East	4.196.242.12
Canada Central	20.104.248.13
Central US	20.9.90.86 40.83.6.169
East US	20.228.131.15
East US 2	172.203.55.132 172.177.166.112 172.176.82.138
West US 2	20.114.37.228
West Europe	40.118.51.192
Brazil South (São Paulo State)	20.197.180.231

Google Cloud:

europe-west3 (Frankfurt)	34.89.191.169
europe-west8 (Milan)	34.154.9.107
us-east1 (South Carolina)	34.73.79.95
us-west1 (Oregon)	34.83.110.1

Sensitive Data Masking

Configure **Sensitive Data Masking** as part of **Log Settings** to mask information deemed sensitive in log message fields, such as passwords or credit card numbers. The **Sensitive Data Masking** settings are applied at the application level, with each application able to support up to 16 sensitive data rules.

To create a sensitive data rule:

1. Go to **Log Settings**.
2. Enable **Sensitive Data Masking**.
3. Click **+Sensitive Data Rule**.

4. Configure the following settings.

Type	Select the type of data the rule will apply to. - **URL** - **Cookie** - **Parameter** - **Header**
Name	Type a regular expression that matches all and only the input names whose values you want to obscure. To create a regular expression, see Frequently used regular expressions on page 237. This field is not required if **URL** data type is selected.
Value	Type a regular expression that matches all and only input values that you want to obscure. To create a regular expression, see Frequently used regular expressions on page 237.

5. Click **OK**.

Retention and Periodic clean

All logs are periodically cleaned at the beginning of each month.

Please see table below for the retention information on each type of log:

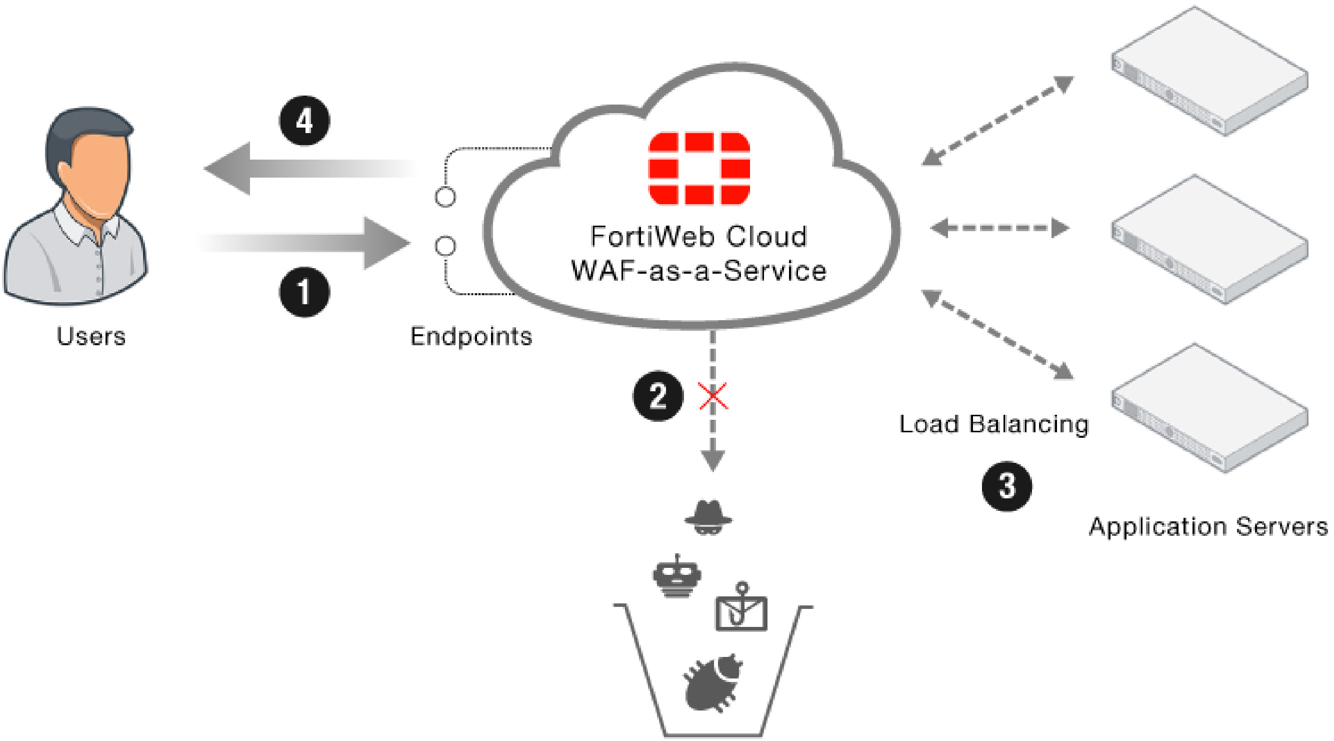
Category	Features	Retention
Incident	Dashboard - Incidents	90 days
	Dashboard - Top Incidents by Severity	
	Threat Analytics - Incidents	
Attack log	Threat Analytics -Attack log	60 days
	FortiView	
	Dashboard - OWASP Top 10 Threats	
	Dashboard - Threat Level History	
	Dashboard - Top Known Threats	
Traffic log	Dashboard - Traffic Statistics by Country	60 days
	Traffic Summary	
Audit log	Audit log	60 days
On-Premise Device Attack log	Threat Analytics - Attack log (on-premise device only)	90 days

Configuring network

After you complete the configurations in the Wizard, you can navigate to **Network** if you want to change the network settings, or configure advanced settings, such as specifying the SSL certificate for HTTPS connections, adding origin servers, etc.

- Endpoints
- Origin Servers

Before setting up the network, it is helpful to understand the traffic flow between the clients, FortiWeb Cloud, and origin servers.



The figure above illustrates the following points:

1. When users visit your application, the traffic is directed to the endpoints on FortiWeb Cloud.
2. FortiWeb Cloud filters the incoming traffic from users, blocking the OWASP Top 10 attacks, zero day threats, and other application layer attacks.
3. Legitimate traffic arrives at origin servers. Load balancing algorithm is used to distribute traffic among servers.
4. When FortiWeb Cloud sends responses to your users, it obfuscates sensitive data such as the credit card number and other information that are likely to be used by hackers to damage your business.

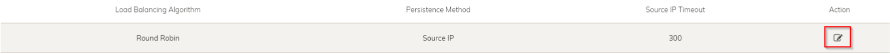
Origin Servers

Configure the origin servers which FortiWeb Cloud will send the traffic to. If there are multiple origin servers, configure Load Balancing rules to determine how the traffic should be distributed among servers.

You can lock your origin server's IP address to prevent other accounts on FortiWeb Cloud from setting up an application targeting malicious traffic at your origin server. Please contact the cloud provider to request for the Origin Server Lock setup.

To configure a Load Balancing rule:

1. Navigate to **Network > Origin Servers**.
1. Click the **Edit** icon for the Load Balancing rule.



Load Balancing Algorithm	Persistence Method	Source IP Timeout	Action
Round Robin	Source IP	300	✎

2. Configure the following settings.

Server Balance	After the application is onboarded, **Server Balance** is enabled by default to apply load balancing algorithm to origin servers. If you turn off this option, only one origin server is allowed, and both HTTPS and HTTP ports can be defined for this server. It's recommended to keep Server Balance on even if you have only one server, because switching the Server Balance status will delete all existing servers you have added. Turning off Server Balance only when you want FortiWeb Cloud to communicate with the origin server over both HTTP and HTTPS protocols.
The following options are available only when Server Balance is on.	
Load Balancing Algorithm	• **Round Robin**—Distributes new TCP connections to the next server, regardless of weight, response time, traffic load, or number of existing connections. • **Weighted Round Robin**—Distributes new TCP connections using the round-robin method, except that members with a higher weight value receive a larger percentage of connections. • **Least Connection**—Distributes new TCP connections to the member with the fewest number of existing, fully-formed TCP connections. When the status of a server is set to **Disabled**, or a health check indicates it is down. FortiWeb Cloud will transfer any remaining HTTP transactions in the TCP stream to an active server according to the Load Balancing Algorithm.
Persistence	After FortiWeb Cloud has forwarded the first packet from a client to a server, some protocols require that subsequent packets also be forwarded to the same server until a period of time passes or the client indicates that it has finished transmission. **Persistence** specifies how FortiWeb Cloud determines a request is the subsequent request from a client. • **Source IP**—The requests with the same client IP address and subnet as

	the initial request will be forwarded to the same server. • **Insert Cookie**—The requests with the same cookie name as the initial request will be forwarded to the same server. If you select **None**, the subsequent requests will be forwarded to random servers according to the Load Balancing Algorithm.
Persistence Timeout	Specifies the maximum amount of time between requests that FortiWeb Cloud maintains persistence, in seconds. FortiWeb Cloud stops forwarding requests according to the established persistence after this amount of time has elapsed since it last received a request from the client with the associated property (for example, an IP address or cookie). Instead, it again selects a server using the Load Balancing Algorithm.
Cookie Name	Specifies a value to match or the name of the cookie that FortiWeb Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Cookie Path	Specifies a path attribute for the cookie that FortiWeb Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Cookie Domain	Specifies a domain attribute for the cookie that FortiWeb Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Health Check	Enable to periodically test for server availability. If FortiWeb Cloud determines the server is unresponsive, it will not forward traffic to this server until it becomes responsive again. Enable **Health Check** only if there are more than one origin servers associated with this application. When **Health Check** is enabled, you can click the Test icon in the origin server list to get the real-time status of a single server.
URL Path	Type the URL that the HTTP or HTTPS request uses to verify the responsiveness of the server (for example, `/index.html`). If the web server successfully returns this URL, and its content matches the **Response Code**, it is considered to be responsive. By default, FortiWeb Cloud uses the URL path "/" to test responsiveness of the server when you click **Test Origin Server** in the ADD APPLICATION wizard, then populates the response code received from the server in the **Response Code** field.
Interval	Type the number of seconds between each server health check. Valid values are 1 to 300. Default value is 10.
Timeout	Type the maximum number of seconds that can pass after the server health check. If the web server exceeds this limit, it will indicate a failed health check. Valid values are 1 to 30. Default value is 3.
Retry Times	Type the number of times, if any, that FortiWeb Cloud retries a server health check after failure. If the web server fails the server health check this number of times consecutively, it is considered to be unresponsive. Valid values are 1 to 10. Default value is 3.

Method	Specify whether the health check uses the HEAD, GET, or POST method.
Response Code	Enter the response code that you require the server to return to confirm that it is available.

3. Click **OK**.

To add a server:

1. Navigate to **Network > Origin Servers**.
2. Click **Create Server**.
3. Configure the following settings.

Status	• **Active**—Specifies that this server can receive new sessions from FortiWeb Cloud. • **Disable**—Specifies that this server does not receive new sessions from FortiWeb Cloud and it closes any current sessions as soon as possible. • **Maintenance**—Specifies that this server does not receive new sessions from FortiWeb Cloud but it maintains any current connections.
Server Type	Select either **IP** or **Domain** to indicate how you want to define the server. Select **Dynamic** if the server's IP address dynamically changes. This applies only to servers on AWS, Azure, and Google Cloud.
IP/Domain	Specify the IP address or fully-qualified domain name (FQDN) of the server. For domain servers, FortiWeb Cloud queries a DNS server to resolve each web server's domain name to an IP address/FQDN. For improved performance, it's recommended to use physical servers instead. Available only if the **Server Type** is **IP** or **Domain**.
Cloud Connector	Select the Cloud Connector so that FortiWeb Cloud can be authorized to access the resources in your public cloud account. See Cloud Connectors on page 80. Available only if the **Server Type** is **Dynamic**.
Filter	Once you select the fabric collector that you have created, the available filter options for your VMs in your public cloud account will be listed here. You can select multiple filter options among instance IDs, image IDs, tags, etc. FortiWeb Cloud will find the VM instance, for example, whose instance ID is i-12345678 in your AWS account, then obtain the IP address of this instance and record it as the origin server's IP. **AWS** • instance-id (e.g. instance-id=i-12345678) • image-id (e.g. image-id=ami-123456) • key-name (e.g. key-name=aws-key-name) • subnet-id (e.g. subnet-id=sub-123456) • tag:*TagName* (The tag attached to the instance. *TagName* is a variable. It can be any value you have named for the tag. e.g. tag:Type=appserver. Up to 8 tags are supported.) **Azure** • vm-name (e.g. vm-name=myVM01) • tag:*TagName* (The tag attached to the virtual machine. *TagName* is a

	variable. It can be any value you have named for the tag, e.g. tag:Type=appserver. Up to 8 tags are supported.) **GCP** • instance-id (e.g. instance-id=3528415166015934407) • instance-name (e.g. instance-name=myInstance) • labels.*LabelName*(The label attached to the instance. *LabelName* is a variable. It can be any value you have named for the tag, e.g. labels.Type=appserver. Up to 8 labels are supported.) Available only if the **Server Type** is **Dynamic**.
IP List	Click **Test** button. FortiWeb Cloud will find the instances/virtual machines according to the filters selected above, then list their IP addresses. Available only if the **Server Type** is **Dynamic**.
Protocol & Port	Select whether this server connects with FortiWeb Cloud through HTTP or HTTPS, then type the port number for the HTTP or HTTP protocol. The valid range is from 1 to 65,535. Only available when the Server Balance on page 114 is on.
HTTPS Port & HTTP Port	When the Server Balance on page 114 is off, FortiWeb Cloud can communicate with the origin server over both HTTP and HTTPS protocols. Specify the port number for both HTTP and HTTPS protocols. Only available when the Server Balance on page 114 is off.
HTTP/2	When HTTPS is enabled, you can enable HTTP/2.
Weight	If TCP connections are distributed among the servers using the **Weighted Round Robin** load-balancing algorithm, servers with a greater weight receive a greater proportion of connections. Weighting servers can be useful when, for example, some servers are more powerful or if a server is already receiving fewer or more connections due to its role in multiple websites.
Backup	When other servers fail their server health check, FortiWeb Cloud routes any connections for the failed server to this server. If you have enabled Backup for more than one server, FortiWeb Cloud uses the load balancing algorithm to determine which servers to use. The backup server mechanism does not work if you do not enable Health check in the loading balancing configurations.
Sever Certificate Authentication	Enable this option to secure the connection between FortiWeb Cloud and the server. Please note this option is available to configure only when you have successfully added the server.
CA Certificate	If **Sever Certificate Authentication** is enabled, then you need to click **Import** to upload the SSL certificate to encrypt the HTTPS connection.
Certificate Revocation Lists	Click **Import** to upload the Certificate Revocation Lists. To ensure that FortiWeb Cloud validates only certificates that have not been revoked, you should periodically upload current certificate revocation lists (CRL) that may be provided by certificate authorities (CA).

> FortiWeb Cloud continuously verifies the IP address paired with the domain name, and if the IP address changes, FortiWeb Cloud automatically updates the origin server IP in its configuration. The frequency that FortiWeb Cloud updates the IP depends on the TTL of the DNS record, which is usually 60 seconds in AWS ALB/ELB.

4. If HTTPS protocol is selected, you need to configure which versions of TLS protocol to use and the SSL encryption level.
   - **TLS Versions**: Select which versions of TLS protocols are allowed for the HTTPS connections between FortiWeb Cloud and the server.
   - **SSL Encryption Level**: The HTTPS traffic is encrypted or decrypted with ciphers. **SSL Encryption Level** controls which ciphers are supported.
     - **Mozilla-Modern:** For services with clients that support TLS 1.3 and don't need backward compatibility, Mozilla-Modern is the recommended configuration as it provides an extremely high level of security.
     - **Mozilla-Intermediate:** For services that don't need compatibility with legacy clients such as Windows XP or old versions of OpenSSL, Mozilla-Intermediate is the recommended configuration as it is highly secure and in the meanwhile compatible with nearly every client released in the last five (or more) years.
     - **Mozilla-Old:** For services accessed by very old clients or libraries, such as Internet Explorer 8 (Windows XP), Java 6, or OpenSSL 0.9.8.
     - **Customized** – Supports a customizable list of all ciphers.
5. Click **OK**.
6. For each created origin server, from the **Action** tab, you can delete the server, or edit the server information; also, you can click the Test icon to get the real-time server status.

   You can add at most 128 origin servers to the server pool of an application.

> As the Health Check test packet is just a simulating one, the test result may not show the real server status.

Endpoints

Domain name

List the domains to protect. The protection policy configured for this application applies to all the domains.

- You can add up to 10 domains. They should belong to the same root domain, such as www.example.com and mail.example.com.
- Wildcard is supported except the first entry in the list. Make sure that the domain name entries do not overlap, for example, “www.example.com” can't be added together with “*.example.com” . The wildcard only matches with the string within the same domain level, for example, "a.example.com" matches with “*.example.com”, while "a.a.example.com" doesn't.
- Once the application is onboarded, you are not allowed to change the first domain. Highly recommend to use root domain for the first domain, e.g. example.com or www.example.com.

Traffic Type

Select HTTP, HTTPS, HTTP/2, or IPv6 to define the traffic types allowed to arrive at the domains of your application.

HTTP	Select the port number for HTTP service.
HTTPS	If HTTPS is allowed, you will be required to configure the **Local Certificate** and **SSL/TLS** settings. **Notes:** • With both HTTP and HTTPS enabled, selecting port 80 for HTTP will by default allow 443 for HTTPS, even if you select a different port number for HTTPS. For example, if you select 80 for HTTP and 7443 for HTTPS, the HTTPS connections can be transferred through either 443 or 7443. • If the port number for HTTPS service is not 443, FortiWeb Cloud can't redirect HTTP traffic to HTTPS.

FortiWeb Cloud uses the following ports for HTTP and HTTPS services. These ports are open on FortiWeb Cloud scrubbing center clusters. There won't be security concerns because if the port is not set as the service port for your application, any request to this port for the application will be rejected.

- HTTP: 80, 81, 3881, 3883, 8000, 8014, 8069, 8080, 8087, 8888, 9003, 9013, 9080, 9091, 9092, 9219, 10082, and 10083
- HTTPS: 443, 444, 1443, 1760, 2087, 4333, 4334, 4430, 4440, 4466, 4993, 5001, 5454, 7003, 7443, 7741, 8010, 8012, 8076, 8078, 8081, 8085, 8086, 8088, 8090, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8099, 8181, 8282, 8443, 8444, 8448, 8585, 8723, 8787, 8866, 9052, 9090, 9093, 9440, 9443, 9797, 44395, 44443, 52233, and 55553

If the HTTP and HTTPS port number you want to use is not in the list, please contact Fortinet Support or your sales engineer to customize the port number. Notice not all non-standard ports can be used, and HTTP and HTTPS services must use different ports.

SSL Certificate

The SSL certificate is used to encrypt the HTTPS connections between users and FortiWeb Cloud. Without a valid certificate, users will see a certificate invalid warning when they visit your application.

By default, FortiWeb Cloud automatically retrieves SSL certificates from the Certificate Authority Let's Encrypt. If it fails, or if you would like to use your own certificate, you can manually upload it to FortiWeb Cloud.

FortiWeb Cloud will not apply automatic certificate if your application uses AWS CloudFront service.

Automatic Certificate

Before configuring Automatic Certificate, make sure:

- You must have changed your DNS record to the CNAME or A record shown in the last step of the ADD APPLICATION wizard.

- You must have enabled HTTP service and uses port 80 for it on the endpoint if you use **HTTP Challenge**, because the Certificate Authority sends HTTP requests to FortiWeb Cloud to validate the DNS CNAME record.
- You must add "letsencrypt.org" in the CAA value if you have configured a CAA record at your DNS service. For more information, search CAA in FAQs.
- You should not block requests from United States in IP Protection > Geo IP Block, otherwise FortiWeb Cloud can't retrieve certificates from Let's Encrypt.
- The server health check status should be OK. If not, you should first disable health check so that it won't interrupt certificate retrieval. After the certificate is successfully retrieved, you can go ahead enable health check and troubleshoot the server connection issue.

Selecting the Challenge Type:

Let's Encrypt sends challenges to validate that you control the domain names you have listed while onboarding the application.

You can select **HTTP Challenge** or **DNS Challenge**. Please note that DNS challenge will be used for the wildcard domains regardless which challenge type you have chosen.

- **HTTP Challenge**
  To pass the challenge, you must change all the DNS entries for the domains you listed.
- **DNS Challenge**
  To pass the challenge, you need to create a new CNAME record for automatic certificate as well as change the DNS entries for the domains you listed. To avoid users encounter the "certificate invalid" error, you can first create the CNAME record (beginning with "_acme-challenge") to get the automatic certificate. After DNS status turns to **OK**, which means the certificate is successfully installed, you can then change the DNS records for your application's domains to direct the traffic to FortiWeb Cloud.

The challenge is handled automatically, but if you need to make some more complex configuration decisions, it’s useful to know more about them. See Challenge Types posted by Let's Encrypt.

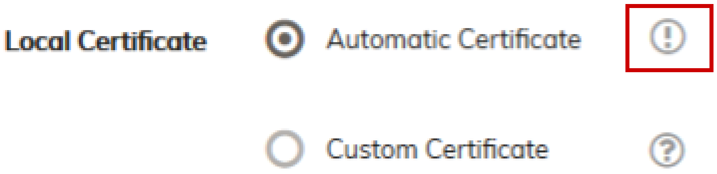
Several minutes after the challenge is successful, FortiWeb Cloud obtains an SSL certificate on your behalf from Let’s Encrypt and installs it on your application. It will be used in HTTPS connections to encrypt or decrypt the traffic. If FortiWeb Cloud fails to retrieve the certificate, it will try again every 12 minutes on the 1st day, then once an hour on the 2nd and 3rd days. After that, it downgrades the frequency to once a day, until the certificate is successfully retrieved.

To retrieve the certificate immediately, click the **Retrieve** button beside **Automatic Certificate** to restore the interval count to the 1st day. FortiWeb Cloud will then retrieves certificate every 12 minutes, and so on.

Thirty days before your certificate expires, FortiWeb Cloud verifies again that your DNS CNAME record is still correct. If it is, FortiWeb Cloud renews your certificate for another 90 days, so it never expires.

Custom Certificate

FortiWeb Cloud may fail to retrieve the certificate for some reasons, for example, the HTTP traffic is not allowed on the endpoints. An exclamation mark will appear beside the **Automatic Certificate** option indicating the certificate fails to be retrieved.

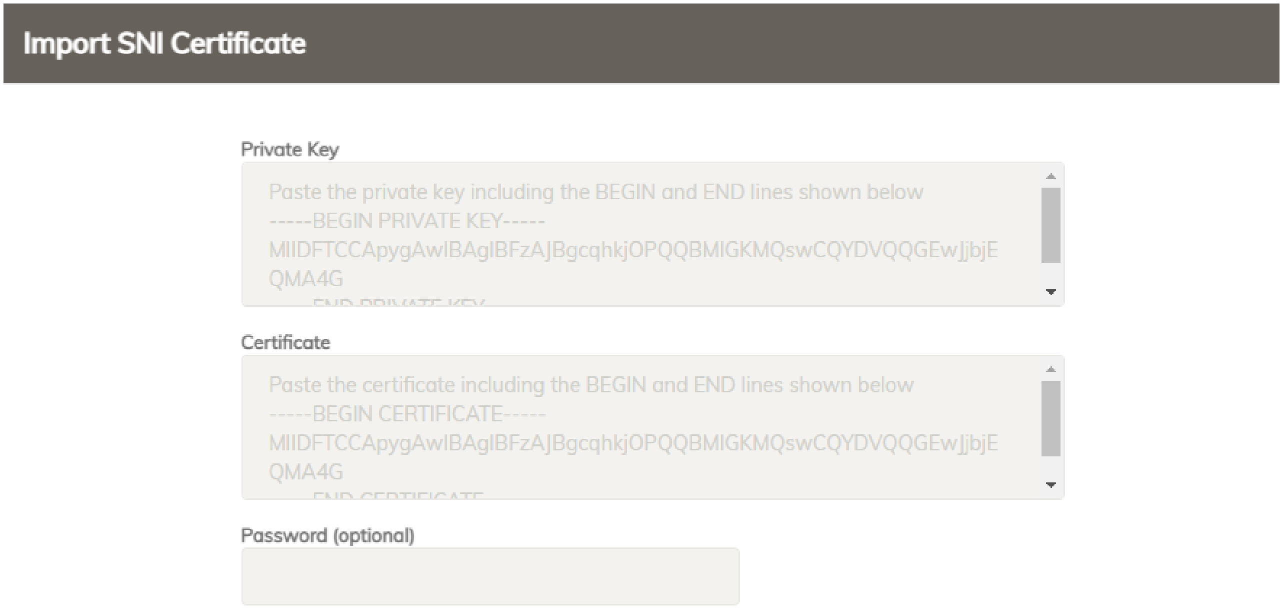


Local Certificate ● Automatic Certificate ⓘ

○ Custom Certificate ?

In this case, or in case you would like to use your own certificate, you can import SNI certificates or intermediate certificates (optional).

1. Select **Custom Certificate** on the **Endpoints** page.
2. For **SNI Certificate**, click **Import** and copy the Private Key and Certificate values provided by your Certificate Authority.
   FortiWeb Cloud automatically parses information of the SNI certificates including issuance, expiration, status, and certificate chain, and changes them to recognizable formats.
   For status, when FortiWeb Cloud verifies the private key and certificate values are consistent, the status is OK; when FortiWeb Cloud verifies the certificate has expired, the status is Expired; when FortiWeb Cloud verifies the certificate is valid, while the certificate chain verification fails, the status is Invalid Chain.
   FortiWeb Cloud requires you to import the private key and certificate in separate fields. If you use a PKCS#12 certificate, refer to this article to extract the key and certificate: https://www.ssl.com/how-to/export-certificates-private-key-from-pkcs12-file-with-openssl



Import SNI Certificate

Private Key

Paste the private key including the BEGIN and END lines shown below
-----BEGIN PRIVATE KEY-----
MIIDFTCCApygAwIBAgIBFzAJBgcqhkjOPQQBMIGKMQswCQYDVQQGEwJjbjE
QMA4G

Certificate

Paste the certificate including the BEGIN and END lines shown below
-----BEGIN CERTIFICATE-----
MIIDFTCCApygAwIBAgIBFzAJBgcqhkjOPQQBMIGKMQswCQYDVQQGEwJjbjE
QMA4G

Password (optional)

3. For **Intermediate Certificate (optional)**, click **Import** and copy the certificate value provided by your intermediate Certificate Authority.
   FortiWeb Cloud automatically parses information of the intermediate certificates including issuance, and expiration, and changes them to recognizable formats. Also, FortiWeb Cloud verifies the status and certificate chain.
   When an indeterminate certificate is successfully imported or deleted, FortiWeb Cloud reverifies the expiration and certificate chain.

You can import at most 32 SNI certificates and intermediate certificates respectively. Contact support team if you want to extend the limits. See Contacting customer service on page 286 for how to submit a support ticket.

SSL/TLS

SSL/TLS Versions: Select which versions of SSL or TLS protocols are allowed for the HTTPS connections between FortiWeb Cloud and the clients.

SSL/TLS Encryption Level: The HTTPS traffic is encrypted or decrypted with ciphers.

The **SSL/TLS Encryption Level** controls how many ciphers are supported and the settings provides the following options:

- **Mozilla-Modern:** For services with clients that support TLS 1.3 and don't need backward compatibility, Mozilla-Modern is the recommended configuration as it provides an extremely high level of security.
- **Mozilla-Intermediate:** For services that don't need compatibility with legacy clients such as Windows XP or old versions of OpenSSL, Mozilla-Intermediate is the recommended configuration as it is highly secure and in the meanwhile compatible with nearly every client released in the last five (or more) years.
- **Mozilla-Old:** For services accessed by very old clients or libraries, such as Internet Explorer 8 (Windows XP), Java 6, or OpenSSL 0.9.8. Mozilla-old is the recommended configuration as it is compatible with most of the clients.
- **Customized** – Supports a customizable list of all ciphers.

For a complete list of the ciphers of each Encryption Level, see Supported cipher suites & protocol versions.

When **HTTP/2** is enabled, only certain **TLS 1.3** and **TLS 1.2** ciphers will be supported for all SSL/TLS encryption levels.

Redirect all HTTP traffic to HTTPS: Select to automatically redirect all HTTP requests to the HTTPS service with the same URL and parameters. Do not enable this option if you have only one origin server and want FortiWeb Cloud to communicate with the origin server over both HTTP and HTTPS protocols.

If you want to provide different content over HTTP and HTTPS protocols, Please refer to Network settings for applications serving different content over HTTP and HTTPS on page 227

HTTP Strict Transport Security (HSTS): Enable to combat MITM attacks on HTTP by injecting the RFC 6797 (http://tools.ietf.org/html/rfc6797) strict transport security header into the reply, such as: `Strict-Transport-Security: max-age=31536000`.

This header forces clients to use HTTPS for subsequent visits to this domain. If the certificate is invalid, the client’s web browser receives a fatal connection error and does not display a dialog that allows the user to override the certificate mismatch error and continue.

HSTS Max-age: Specify the time to live in seconds for the HSTS header. The HSTS enforcement will be lifted after the specified max-age. Subsequent visits will not be required to use HTTPS.

Secure flag for internal Cookie: Enable to add the secure flag to cookies, which forces browsers to return the cookie only when the request is for an HTTPS page. When enabled, only the HTTPS request contains cookie, while the HTTP is cookieless.

HTTP Only flag for internal Cookie: Enable to add the "HTTP Only" flag to internal cookies, which prevents client-side scripts from accessing the cookie.

Advanced Settings

Configure the following settings:

HTTP/2	Enable to accept HTTP/2 traffic.
Client Certificate Authentication	Enable it so that FortiWeb Cloud requires a client to provide a client certificate during the SSL handshake. When enabled, if a client doesn't provide a client certificate during the SSL handshake, FortiWeb Cloud won't accept the request. • Click **Import** to upload the trusted CA certificates so that FortiWeb Cloud can authenticate client certificates. How to obtain CA certificate: ◦ If you are using a commercial CA, your web browser should already contain a copy in its CA trust store. Export a copy of the file to your desktop or other folder. ◦ If you are using your own private CA, download a copy from your CA's server. For example, on Windows Server 2003, you would go to: `HTTPs://<ca-server_ipv4>/certsrv/` where `<ca-server_ipv4>` is the IP address of your CA server. Log in as `Administrator`. Other accounts may not have sufficient privileges. The **Microsoft Certificate Services** home page for your server's CA should appear, and you can download a CA certificate, certificate chain, or CRL from there. **Note:** Verify that your private CA's certificate does not contain its private keys. Disclosure of private keys compromises the security of your network, and will require you to revoke and regenerate all certificates signed by that CA. • Click **Import** to upload the Certificate Revocation Lists. To ensure that FortiWeb Cloud validates only certificates that have not been revoked, you should periodically upload current certificate revocation lists (CRL) that may be provided by certificate authorities (CA).
IPv6	If IPv6 is enabled, both IPv4 and IPv6 are allowed to your application. If disabled, only IPv4 traffic is allowed.
Custom Block Page	Select the block page that FortiWeb Cloud displays to your users. It contains the following messages: • The error page FortiWeb Cloud uses to respond to an HTTP request that violates a policy and the configured action is **Deny** or **Period Block**. • The "Server Unavailable!" page that FortiWeb Cloud returns to the client when none of the server pool members are available either because their status is **Disable** or **Maintenance** or they have failed the configured health check. • The Captcha enforcement pages that FortiWeb Cloud uses to differentiate between real users and automated users, such as bots. The custom block page is configured in **Global > System Settings > Custom Block Pages**.

Supported cipher suites & protocol versions

A secure connection’s protocol version and cipher suite, including encryption bit strength and encryption algorithms, is negotiated between the client and the SSL/TLS terminator during the handshake.

The **SSL/TLS Encryption Level** controls how many ciphers are supported and the settings provides the following options:

- **Mozilla-Modern:** For services with clients that support TLS 1.3 and don't need backward compatibility, Mozilla-Modern is the recommended configuration as it provides an extremely high level of security.
- **Mozilla-Intermediate:** For services that don't need compatibility with legacy clients such as Windows XP or old versions of OpenSSL, Mozilla-Intermediate is the recommended configuration as it is highly secure and in the meanwhile compatible with nearly every client released in the last five (or more) years.
- **Mozilla-Old:** For services accessed by very old clients or libraries, such as Internet Explorer 8 (Windows XP), Java 6, or OpenSSL 0.9.8. Mozilla-old is the recommended configuration as it is compatible with most of the clients.
- **Customized** – Supports a customizable list of all ciphers.

Ciphers supported by Mozilla-Modern/Intermediate/Old levels

Cipher	Mozilla Modern	Mozilla Intermediate	Mozilla Old
TLS_AES_256_GCM_SHA384	Yes	Yes	Yes
TLS_CHACHA20_POLY1305_SHA256	Yes	Yes	Yes
TLS_AES_128_GCM_SHA256	Yes	Yes	Yes
ECDHE-ECDSA-AES128-GCM-SHA256		Yes	Yes
ECDHE-RSA-AES128-GCM-SHA256		Yes	Yes
ECDHE-ECDSA-AES256-GCM-SHA384		Yes	Yes
ECDHE-RSA-AES256-GCM-SHA384		Yes	Yes
ECDHE-ECDSA-CHACHA20-POLY1305		Yes	Yes
ECDHE-RSA-CHACHA20-POLY1305		Yes	Yes
DHE-RSA-AES128-GCM-SHA256		Yes	Yes
DHE-RSA-AES256-GCM-SHA384		Yes	Yes
DHE-RSA-CHACHA20-POLY1305			Yes

Cipher	Mozilla Modern	Mozilla Intermediate	Mozilla Old
ECDHE-ECDSA-AES128-SHA256			Yes
ECDHE-RSA-AES128-SHA256			Yes
ECDHE-ECDSA-AES128-SHA			Yes
ECDHE-RSA-AES128-SHA			Yes
ECDHE-ECDSA-AES256-SHA384			Yes
ECDHE-RSA-AES256-SHA384			Yes
ECDHE-ECDSA-AES256-SHA			Yes
ECDHE-RSA-AES256-SHA			Yes
DHE-RSA-AES128-SHA256			Yes
DHE-RSA-AES256-SHA256			Yes
AES128-GCM-SHA256			Yes
AES256-GCM-SHA384			Yes
AES128-SHA256			Yes
AES256-SHA256			Yes
AES128-SHA			Yes
AES256-SHA			Yes
DES-CBC3-SHA			Yes

WAF modules

When you onboard a new application on FortiWeb Cloud, the system will automatically assign a security policy for your application, with the Security Rules and Access Rules modules enabled. You can select additional protection rules using the Modules tab.

For information on adding and removing a module, refer to How to add or remove a module.

The following modules are available for FortiWeb Cloud:

- Security Rules
- Client Security
- Access Rules
- Bot Mitigation
- DDoS Prevention
- Advanced Applications
- API Protection
- Account Takeover
- Application Delivery
- Global Trustlist

For any configuration you made in a module, it may take several minutes for the configuration to take effect.

How to add or remove a module

Each module allows you to customize a feature or add a particular type of security to your application.

Adding a module

To add a module

1. Go to **ADD MODULES**.
2. In the module list, locate the modules you want to add.
3. Click to enable them.
4. Click **OK**.

The modules you have added appear in the left navigation bar, and they are automatically enabled.

Removing a module

When you remove a module, the settings associated with it are reset to the initial configuration, and the data is deleted and cannot be recovered.

You can always add the module again to customize the settings.

To remove a module

1. Go to **ADD MODULES**.
2. In the module list, locate the modules you want to remove.
3. Click to disable them.
4. Click **OK**.

The modules you have removed will disappear from the left navigation bar.

When you click to disable a module, the enabled fields remain ON status to help you track the previous configurations.

Security Rules

With security rules configured, FortiWeb Cloud detects messages in HTTP requests that access web servers to prevent web servers from known attacks, protect the privacy-sensitive information in the messages such as Cookie, and restrict, scan uploaded files.

This module is enabled by default, as the Known Attacks option is enabled automatically once an application is added.

- Known Attacks
- Anomaly Detection
- Parameter Validation
- Information Leakage
- Cookie Security
- File Protection

Known Attacks

FortiWeb Cloud defends against attacks in OWASP Top 10 such as Cross-site scripting (XSS), SQL Injection, Generic Attacks, Known Exploits, and Trojans, etc using continuously updated signatures. FortiWeb Cloud parses messages in the packet, compares them with the signatures, and takes specified actions on the packets.

To configure attacks to defend

1. Go to **SECURITY RULES > Known Attacks**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. For **Signature Based Detection**, you can use attack signatures to detect application layer attacks that try to exploit a known web vulnerability.
   Configure these settings.

Sensitivity Level	Choose from four categories of attack signatures (L1 to L4) based on their sensitivity to false positives and their requirement for a higher security level. Increasing the level adds additional signatures but also adds the chance of blocking legitimate traffic. We recommend to use the different level according to the following rules: **Level 1:** Baseline security with the least false positives. Use it if you are running an HTTP server on the internet. **Level 2:** This level is adequate when real user data like user name and password is involved. Perhaps an off-the-shelf online shop. **Level 3:** The online banking level security with lots of false positives, so it’s important to learn how to write rule exclusions.

	Level 4: Rules that are so strong that they're adequate to protect the top confidential data. Be sure you have enough time to process the false positives. Please expect that with this amount of false positives, user experience might be greatly compromised. **Notes:** This setting also applies to the Server Information Disclosure and Personally Identifiable Information options in Information Leakage.
Cross Site Scripting	Enable to prevent a variety of cross-site scripting (XSS) attacks, such as varieties of CSRF (cross-site request forgery).
SQL Injection	Enable to prevent SQL injection attacks, such as blind SQL injection.
Generic Attacks	Enable to prevent other common attacks, including a variety of injection threats that do not use SQL, such as local file inclusion (LFI) and remote file inclusion (RFI).
Known Exploits	Enable to prevent known exploits.
Trojans	Enable to prevent malware attacks and prevent accessing Webshell located on server.

If you want to view the details of a specific signature, click **Search Signature** to find it by CVE number, Keywords, Attack Category, or signature ID.

3. Click **+Create Exception Rule** under **Signature Based Detection** section to omit attack signature scans when you know that some parameters or URLs cause false positives by matching an attack signature during normal use.

4.

Request URL	Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`. • If **String Match** is selected, ensure the value starts with a forward slash (/) (for example, `/testpage.php`). You can enter a precise URL, such as /floder1/index.htm or use wildcards to match multiple URLs, such as /floder1/* ,or /floder1/*/index.htm. • If **Regular Expression Match** is selected, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. For details, see Frequently used regular expressions on page 237. Do not include a domain name because it's by default the domain name of this application.
Parameter Name	Specify a parameter name to match. For example, `http://www.test.com/testpage.php?a=1`, the parameter name is "a".
Cookie Name	Specify a cookie name to match. Both **String Match** and **Regular Expression Match** are supported.
JSON Elements	Specify the name of the JSON element to match. Both **String Match** and **Regular Expression Match** are supported.
Attack Category	Select an attack category in which you want to create an exception for its attacks therein.
Signature ID	The ID for the signature applied to the attack.

Signature Information	Signature description and examples are listed here. You can select any signature ID for the attack and view the signature details.

5. In addition to Signature Based Detection, FortiWeb Cloud also supports Syntax Based Detection for SQL injection or Cross Site Scripting (XSS).
   a. In **SQL Syntax Based Detection**, enable the options to detect the corresponding SQL injection types. FortiWeb Cloud uses an SQL parser to validate whether the pattern is real SQL language. It helps identify true attacks while minimizing false positives.
   The syntax-based detection detects an SQL injection attack by analyzing the lexeme and syntax of SQL language rather than using a pattern matching mechanism as the signature-based detection does.
   b. In **XSS Syntax Based Detection**, enable the option to detect the corresponding XSS attack types. FortiWeb Cloud detects an XSS injection attack by analyzing the HTML/JavaScript syntax.
   It does HTML document parsing and JavaScript compiling, and checks whether the compiled results include valid HTML and JavaScript codes.
6. Click **+Create Exception Rule** to omit Syntax Based attack scans when you know that some parameters or URLs may trigger Syntax Based Detection false positives during normal use.

Request URL	Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`. • If **String Match** is selected, ensure the value starts with a forward slash (/) (for example, `/testpage.php`). You can enter a precise URL, such as /floder1/index.htm or use wildcards to match multiple URLs, such as /floder1/* ,or /floder1/*/index.htm. • If **Regular Expression Match** is selected, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. For details, see Frequently used regular expressions on page 237. Do not include a domain name because it's by default the domain name of this application.
Parameter Name	Specify a parameter name to match. For example, `http://www.test.com/testpage.php?a=1`, the parameter name is "a".
Cookie Name	Specify a cookie name to match. Both **String Match** and **Regular Expression Match** are supported.
Attack Category	Select an attack category in which you want to create an exception for its attacks therein.
Attack Name	Select the attack name. • Stacked queries SQL injection: The snippet of this attack can be something like "1; delete from users". • Embedded queries: The snippet of this attack can be something like "1 union select username, password from users 1 /*! ; drop table admin */ ".

For Request URL and Parameter Name, you shall enable at least one. The request matching the specified URL and/or parameter in exception rule would not be treated as an attack.

7. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

8. Click **SAVE**.

Anomaly Detection

Use machine learning enabled Anomaly Detection to block zero day threats and other sophisticated attacks. Machine learning automatically and continuously builds and maintains a model of normal user behavior and uses it to identify malicious application traffic. To learn about whether a request is legitimate or a potential malicious attack attempt, it performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed access
- Matches anomalies against pre-trained threat models
- Detects attacks

Once an anomaly is triggered by the mathematical model, FortiWeb Cloud uses pre-built trained threat models to confirm whether it's a real attack or just a benign anomaly that should be ignored. Each threat model is already trained based on analysis of thousands of attack samples and is continuously updated using the FortiWeb Security Service.

Model settings

FortiWeb Cloud parses all the URLs in a domain, and builds anomaly detection models for all parameters attached to the URLs.

After anomaly detection model is built, the system will keep on calculating the probability of the new samples and compare it against the model. If the probability of the new samples varies to a large extent for a long period, the system determines this parameter has changed and automatically rebuilds the model based on the new samples.

To configure anomaly detection:

1. Go to **SECURITY RULES> Anomaly Detection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure the following settings.

IP List Type	• **Trust:** The system will collect samples only from the IP ranges in the **Source IP list**. • **Block:** The system will collect sample from any IP addresses except the ones in the **Source IP list**. Whichever option you choose, if you leave the **Source IP list** blank, the system will collect traffic data samples from any IP address.
Source IP List	Click **Create New** to list the IP ranges of the samples. Depending on whether you select **Trust** or **Block**, FortiWeb Cloud will or will not collect samples from the specified IP ranges.

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.

4. Click **SAVE**.

Due to database migration, the Anomaly Detection machine learning data will be removed after upgrade to 23.1. The system will rebuild the model after upgrade.

Overview

The Overview tab provides a high level summary of data collected for the domain, including Top 10 URLs by Hit, Violations triggered by anomalies, HMM learning process, Event Dashboard.

Domain overview

The top of the Overview page provides a summary of the data that the machine-learning module has learned about the domain.

Parameters	Description
Access Frequency	Indicates how frequently this application is being accessed. • Level1 (over 500 requests) • Level2 (over 1000 requests) • Level3 (over 1500 requests) • Level4 (over 2000 requests) • Level5 (over 2500 requests) • Level6 (over 3000 requests) • Level7 (over 3500 requests)
Start Time	The date and time when the machine-learning module started to learn about the domain.
URL Number	The total number of URLs that the machine-learning module has learned.
Block	The total number of block actions that have been triggered since the start time up to the present moment.
Service(HTTP/HTTPS)	The total amount of the HTTP and the HTTPS traffic from the start time up to now.
Page Charset	The charset of URLs in the domain, such as UTF-8.

Top 10 URLs by Hit

This chart displays the top 10 URLs for page hits counts.

Violations Triggered by Anomalies

This chart displays the total number of the potential anomalies and definite anomalies found by the anomaly detection profile.

Learning Progress

This chart displays the statistics of machine learning states of all parameters in the domain. Hover over the circle to check how many parameters are in Collecting, Building, Testing, Running, or Discarded stages respectively. For the explanation of each stage, see Anomaly Detection on page 131.

Machine Learning Events

This chart displays the anomaly detection events, such as sample collection, model running, building and testing, along with the time periods when these events take place.

Tree View

This tab displays the entire URL directory of the domain in a tree view. You can choose either one of the URLs to view its violation statistics.

Web site directory

The left panel of the **Tree View** page shows the directory structure of the website. The / (backslash) indicates the root of the site. You can click a URL in the directory tree, then the violation statistics of this URL will be displayed on the right side of the Tree View page. You can also click a directory, then click **Relearn Directory** or **Rebuild Directory** to relearn or rebuild anomaly detection models for all the URLs under the selected directory.

URL summary

This part of the Tree View page shows the statistics of a specific URL.

Parameters	Description
Access Frequency	The frequency at which this URL was accessed in last 24 hours. The frequency is divided into 7 levels, as defined below: • Level1 (over 500 requests) • Level2 (over 1000 requests) • Level3 (over 1500 requests) • Level4 (over 2000 requests) • Level5 (over 2500 requests) • Level6 (over 3000 requests) • Level7 (over 3500 requests)
Model Initialization Date	The date and time when the mathematical model of this URL was initialized. It shows when FortiWeb Cloud began to learn about the data of this URL.
Block	The total number of block actions that have been triggered against this URLsince the start time up to the present moment.
Anomaly	The anomalies detected by the anomaly detection model.

Violation Trend

This chart shows the trend of violations in last 24 hours.

Parameter list

The Parameters list shows all the parameters attached to the URL. For example, if the URL is http://www.demo.com/1.php?user_name=jack, then user_name is the parameter. The system builds machine learning model for each parameter, and detects the abnormal parameter values.

Parameter Validation

Define validation rules to only permit requests that meet specific parameter (input) requirements to your web applications. According to the defined rules, FortiWeb Cloud can deny any invalid requests or block the request's IP for a period of time, as well as record the invalid requests in the attack log.

A parameter validation rule is composed of a validation operation that will be applied to a URL and one or more validation restrictions to limit parameters, such as to specify whether or not the parameter is required, its maximum allowed length, or its data type.

FortiWeb Cloud requires at least one parameter rule to be added for each request URL to successfully apply parameter validations. Otherwise, FortiWeb Cloud will accept all requests if there are no restrictions placed on any parameters.

To create a parameter validation rule:

1. Go to **Security Rules > Parameter Validation**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Enable **Parameter Validation**.
3. Click **+Create Rule**.
4. Configure the following to set the validation operation.

Name	Enter a name for the parameter validation rule.
Request URL	Enter the URL to which the validation rule will be applied.
Operation	Select the action that will be triggered by the validation rule: • **Alert** – FortiWeb Cloud will record the invalid request in the attack log. • **Deny** – FortiWeb Cloud will block the invalid request and send a "block page" back to the browser, as well as record the request in the attack log. • **Deny (no log)** – FortiWeb Cloud will block the invalid request and send a "block page" back to the browser. • **Period Block** – Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs. If **Period Block** is selected, specify the time period between 1 to 3600 seconds.

5. Click **Add Rule**.

6. Configure the following to define the parameter restriction rule.

Parameter Name	Type a regular expression that matches the parameter whose values you want to validate. To create a regular expression, see Frequently used regular expressions on page 237.
Max Length	Specify the maximum allowed length of the parameter between 0 to 1024 characters.
Required	Specify whether or not the parameter is required. **Note:** If there isn't any parameter in the request URL, the parameter validation will not be triggered, which means the traffic will let go even if you have configured required parameters in the parameter restriction rule. Parameter validation takes effect only when there is at least one parameter in the request URL.
Use Type Check	Specify whether or not to check the data-type of the parameter.
Argument Type	Specify the argument type of the parameter: • **Data Type** • **Regular Expression** Available only if you enabled **Use Type Check**.
Data Type	Select a predefined data type from the drop-down list to limit the format of the parameter value. Available only if you enabled **Use Type Check** and selected **Data Type** as the **Argument Type**.
Regular Expression	Type a regular expression to limit the format of the parameter value. To create a regular expression, see Frequently used regular expressions on page 237. Available only if you enabled **Use Type Check** and selected **Regular Expression** as the **Argument Type**.

7. Click **Save Rule**.

Information Leakage

FortiWeb Cloud can detect server error messages and other sensitive messages in the HTTP headers.

To configure attacks to defend

1. Go to **SECURITY RULES > Information Leakage**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Server Information Disclosure	Enable to detect and erase server specific sensitive information in headers and response page, with no alerts generated. • **Log ON**—Check to record logs for any information leakage. • **Log OFF**—Uncheck to not record logs for any information leakage.
Personally Identifiable Information	Enable to identify personally identifiable information (PII).

Cloak Error Pages	Enable to replace 403, 404, and 5XX with 500 error code.
Erase HTTP Headers	Enable to cloak server replied HTTP headers. You can add multiple HTTP headers in which the sensitive information will be hidden.

3. Click **+Create Exception Rule** (optional).
   You can also configure FortiWeb Cloud to omit attack signature scans by creating exception rules.
4. Configure these settings.

URI	Specify a Uniform Resource Identifier (URI), for example, `http://www.example.com`.
Request URL	Specify a URL value to match. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php`. • If **String Match** is selected, ensure the value starts with a forward slash (/) (for example, `/testpage.php`). You can enter a precise URL, such as /floder1/index.htm or use wildcards to match multiple URLs, such as /floder1/* ,or /floder1/*/index.htm. • If **Regular Expression Match** is selected, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. For details, see Frequently used regular expressions on page 237. Do not include a domain name because it's by default the domain name of this application.
Parameter Name	Specify a parameter name to match. For example, `http://www.test.com/testpage.php?a=1`, the parameter name is "a".
Cookie Name	Specify a cookie name to match. Both **String Match** and **Regular Expression Match** are supported.
JSON Elements	Specify the name of the JSON element to match. Both **String Match** and **Regular Expression Match** are supported.
Attack Category	You can select an attack category between: • **Server Information Disclosure** • **Personally Identifiable Information**
Signature ID	The ID for the signature applied to the attack.
Signature Information	Signature description and examples are listed here. You can select any signature ID for the attack and view the signature details.

For Request URL and Parameter Name, you shall enable at least one. The request matching the specified URL and/or parameter in exception rule would not be treated as an attack even if it matches a particular signature.

5. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message. To avoid log flooding, the minimum interval between logs is 1 second.
Erase & Alert	Hide or remove sensitive information in replies from the web server (sometimes called “cloaking”) and generate a log message. To avoid log flooding, the minimum interval between logs is 1 second.
Deny & Erase(no log)	For violations of the **Server Information Disclosure**, **Cloak Error Pages**, and the **Erase HTTP Headers** categories, hide or remove sensitive information in replies from the web server but do not generate log messages.

6. Click **SAVE**.
   You can continue creating multiple exception rules for specific attacks.

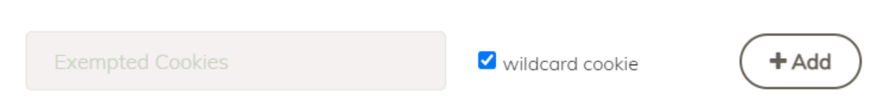
Cookie Security

FortiWeb Cloud can protect against cookie poisoning and other cookie-based attacks. When **Cookie Security** module is added FortiWeb Cloud signs all cookies by default.

To create cookie security rules

1. Go to **SECURITY RULES > Cookie Security**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Cookie Replay Protection	Enable to select whether FortiWeb Cloud uses the IP address of a request to determine the owner of the cookie and protect against replay attacks.
Set Max Cookie Age	Enter the maximum age (in minutes) permitted for cookies that do not have an “Expires” or “Max-Age” attribute. To configure no expiry age for cookies, enter `0`.
Security Mode	• **None**—FortiWeb Cloud does not apply cookie tampering protection or encrypt cookie values. • **Signed**—Prevents tampering (cookie poisoning) by tracking the cookie value. When FortiWeb Cloud receives the first HTTP or HTTPS request from a client, it uses a cookie to track the session. When you select this option, the session-tracking cookie includes a hash value that FortiWeb Cloud uses to detect tampering with the cookie from the backend server response. If FortiWeb Cloud determines the cookie from the client has changed, it takes related action. • **Encrypted**—Encrypts cookie values the back-end web server sends to clients. Clients see only encrypted cookies. FortiWeb Cloud decrypts cookies submitted by clients before it sends them to the back-end server.
Set Secure Cookie	Enable to add the secure flag to cookies, which forces browsers to return the cookie only when the request is for an HTTPS page.

	This function applies to the cookie from origin server. If you want to modify the cookie from browser, please refer to **Secure flag for internal Cookie** in Endpoints.
Set HTTP Only Cookie	Enable to add the "HTTP Only" flag to cookies, which prevents client-side scripts from accessing the cookie. This function applies to the cookie from origin server. If you want to modify the cookie from browser, please refer to **HTTP Only flag for internal Cookie** in Endpoints.
Don't Block Until	If **Allow Suspicious Cookies** is **Custom**, enter the date on which FortiWeb Cloud starts to take the specified action against suspicious cookies.
Exempted Cookies	If you want to specify cookies that are exempted from the cookie security policy, click + to add cookie names. If you use wildcard in cookie name, please check the box beside the cookie name field.  Exempted Cookies ☑ wildcard cookie + Add

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.
Remove Cookie	Accept the request, but remove the cookie from the datagram before it reaches the web server, and generate a log message.

4. Click **SAVE**.

Select whether FortiWeb Cloud allows requests that contain cookies that it does not recognize or that are missing cookies.

In many cases, when you first introduce the cookie security features, cookies that client browsers have cached earlier generate false positives.

To avoid this problem, either select **Never**, or select **Custom** and enter an appropriate date on which to start taking the specified action against suspicious cookies.

- **Never**—FortiWeb Cloud does not take the action specified against suspicious cookies.
- **Always**—FortiWeb Cloud always takes the specified action against suspicious cookies.
- **Custom**— FortiWeb Cloud takes the specified action against suspicious cookies starting on the date specified by **Don't Block Until**.

File Protection

You can configure FortiWeb Cloud to perform the following tasks.

- Restrict file uploads based upon file type and size.
- Scan uploaded files for viruses and Trojans.
- Submit uploaded files for evaluation and generate attack log messages for files that FortiWeb Cloud has identified as threats.

1. Go to **SECURITY RULES > File Protection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Trojans/Backdoor	Attackers may attempt to upload Trojan horse code (written in scripting languages such as PHP and ASP) to the back-end web servers. The Trojan then infects clients who access an infected web page. Enable to detect Trojans in the uploaded files.
Antivirus Scan	Enable to scan for viruses, malware, and greyware.
Advanced Threat Protection	Enable to send matching files to FortiSandbox for evaluation. Sandbox file evaluation is performed in the same region where the FortiWeb Cloud cluster is located. This ensures compliance with various data regulations such as GDPR. This option works only when your application is hosted on AWS or Azure.
File Size Limit	Define the maximum allowed size for the file to upload.
File Type Validation	Define the allowed and blocked file types. Select file types by clicking **Change** button, and then select to allow or block such files with **Allow** and **Block** buttons. **Note:** The ".zip" file compressed from the compression software (not the command line) that comes with the MacOS and Linux GUI operating systems has the same binary code with the ".jar" file. As a result, blocking the ".jar" file may incorrectly block the ".zip" file. To solve this problem, either warn your users not to use the compression methods mentioned above, or do not block the **Java Archive(.jar)** type.
Target URL	Define the target URL that accepts the uploads.

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Deny(no log)	Block the request (or reset the connection) but do not generate log messages.

4. Click **SAVE**.

Client Security

You can configure FortiWeb Cloud to prevent web-related attacks such as clickjacking, CSRF attacks, and MITB attacks.

- CSRF Protection
- HTTP Header Security
- MITB Protection

HTTP Header Security

HTTP response security headers are a set of standard HTTP response headers proposed to prevent or mitigate known XSS, clickjacking, and MIME sniffing security vulnerabilities. These response headers define security policies to client browsers so that the browsers avoid exposure to known vulnerabilities when handling requests.

When enabling this feature, headers with specified values are inserted into HTTP responses coming from the backend web servers. This is a quick and simple solution to address the security vulnerabilities on your website without code and configuration changes. The following includes the security headers that FortiWeb Cloud can insert into responses.

To configure HTTP Header Security, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

X-Frame-Options	This header prevents browsers from **Clickjacking attacks** by providing appropriate restrictions on displaying pages in frames.
X-Content-Type-Options	This header prevents browsers from **MIME content-sniffing attacks** by disabling the browser's MIME sniffing function.
X-XSS-Protection	This header enables a browser's built-in **Cross-site scripting (XSS)** protection.
Content-Security-Policy	Enable to prevent certain types of attacks, including XSS and data injection attacks by inserting this header (e.g. default-src 'self'; script-src 'self'; object-src 'self').

CSRF Protection

A cross-site request forgery (CSRF) is an attack that exploits the trust that a site has in a user's browser to transmit unauthorized commands. FortiWeb Cloud uses a dedicated, per user token to track access to protected pages. To protect back-end servers from CSRF attacks, you create two lists of items, a list of web pages to protect against CSRF attacks, and a corresponding list of the URLs found in the requests that the pages generate.

To configure CSRF Protection, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

To create a page list

1. Click **+Create Page List Table**.
2. Configure these settings.

Full URL	Enter a literal URL, for example, `/www.test.com`.
Parameter Filter	Enable to specify a parameter name and value to match. The parameter can be located in either the URL or the HTTP body of a request.
Parameter Name	Enter the parameter name to match.
Parameter Value	Enter a value for the parameter.

3. Click **OK**.

You can continue creating multiple page lists.

To create a URL list

1. Under **URL List Table**, click **+Add URL List Table**, configure these same settings as for adding a page list.
2. Click **SAVE**.

You can continue creating multiple URL lists.

To configure actions

1. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

2. Click **SAVE**.

MITB Protection

The Man-in-the-Browser (MITB) attack uses Trojan Horse to intercept and manipulate calls between the browser and its security mechanisms or libraries on-the-fly. The Trojan Horse sniffs or modifies transactions as they are formed on the browser, but still displays back the user's intended transaction. The most common objective of this attack is to cause financial fraud by manipulating transactions of Internet Banking systems, even when other authentication factors are in use.

To protect the user inputs from being attacked by MITB, FortiWeb Cloud implements security rules including obfuscation, encryption, anti-keylogger, and Ajax request allowlist.

Obfuscation

To prevent the MITB attack from identifying the names of the user input field , FortiWeb Cloud obfuscates it into meaningless character strings based on Base64 encoding rule.

For example, for the account name, passwords, and other sensitive user input fields on a transaction page, the obfuscation rule is used to disguise the real values of the input field names.

Encryption

To protect the password that users enter into the web page, FortiWeb Cloud encrypts the password from a readable form to an encoded version based on Base64 encoding rule. The encrypted password can only be decoded by FortiWeb Cloud.

Anti-Keylogger

Sometimes the MITB attack installs a key logger on users' browsers and records each key pressed. Sensitive data such as passwords can be intercepted and recorded, compromising the user account.

If the Anti-Keylogger rule is enabled for the password parameter, FortiWeb Cloud prevents it from being recorded even if there is a key logger installed on user's browser.

AJAX Request allowlist

The MITB attack may use a malicious AJAX worm to hack into the user's browser. It creates an AJAX based sniffer to override the OPEN and SEND function of the AJAX request, and then send the data to a program on a different domain.

FortiWeb Cloud supports configuring an allowlist for AJAX requests. If the user's browser sends AJAX requests to an external domain which is not in the allowlist, FortiWeb Cloud will take action according to your configuration.

To configure MITB Protection, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

- Configure the settings below to define the URL to protect.

Request URL	Enter the literal URL which hosts the web page containing the user input fields you want to protect.
POST URL	When the user inputs (e.g. password) are posted to the web server, a new URL will open. This is the POST URL. The format of the POST URL field is similar to that of the Request URL field. Note: The AJAX request rule only checks the Request URL, and it doesn't involve POST URLs, so the POST URL of the AJAX request rule should be set as "*" to match any URLs.

- To protect the standard user input and passwords, click **+Create Protected Parameter**, and configure these settings.

Input Name	Enter the name of the user input field, which shall be exactly the same with the name of user input field in the source code of the web page.
Type	Select either **Standard Input** or **Password Input**.
Obfuscate	Available when the Type is either **Standard Input** or **Password Input**.
Encrypt	Available when the Type is **Password Input**.
Anti-KeyLogger	Available when the Type is **Password Input**.

- To add an allowlist for the AJAX Request, click **+Create External Domain**, and enter the external domain address. If the user's browser sends AJAX request to an external domain which is not in the domain list you have entered, FortiWeb Cloud will take actions (alert, or alert & deny) accordingly.
- Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner. To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings >**

Settings.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.

- Click **SAVE**.

Access Rules

You can control clients' access to your web applications and limit the rate of requests. Multiple ways are available for this, depending on whether you are to act based upon the URL, the client's source IP, or something more complex.

This module is enabled by default, as the Request Limits option is enabled automatically once an application is added.

- Request Limits
- URL Access
- IP Protection

Request Limits

Request limits enforces limitations at the HTTP protocol level to make sure all client requests adhere to the HTTP RFC standard and security best practice. With this feature, you can prevent exploits such as malicious encoding and buffer overflows that can lead to Denial of Service (DoS) and server takeover.

Specifying allowed HTTP methods

You can configure FortiWeb Cloud to allow only specific HTTP request methods.

Mark the check boxes for all HTTP request methods that you want to allow. Methods that you do not select will be denied.

Configuring HTTP protocol constraints

Protocol constraints govern features such as the HTTP header fields in the protocol itself, as well as the length of the HTML, XML, or other documents or encapsulated protocols carried in the HTTP body payload.

Use protocol constraints to prevent attacks such as buffer overflows. Buffer overflows can occur in web servers and applications that do not restrict elements of the HTTP protocol to acceptable lengths, or that mishandle malformed requests. Such errors can lead to security vulnerabilities.

To configure an HTTP protocol constraint profile

1. Go to **ACCESS RULES > Request Limits**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

HTTP Header	
Header Length	Specifies the maximum acceptable size in bytes of all HTTP header lines. Attack log messages contain `Total Size of All Headers Too Large` when this feature detects a header size buffer overflow attempt.
Header Name Length	Specifies the maximum acceptable size in bytes of a single HTTP header name (for example, `Host:`, `Content-Type:`, `User-Agent:`).
Header Value Length	Specifies the maximum acceptable size in bytes of a single HTTP header

		value.
	Number of Cookies in Request	Specifies the maximum acceptable number of cookies in an HTTP request. Attack log messages contain `Too Many Cookies in Request` when this feature detects a cookie count buffer overflow attempt.
	Number of Ranges in Range Header	Specifies the maximum acceptable number of range: lines in each HTTP header. Attack log messages contain `Too Many Range Headers` when this feature detects too many `Range:` header lines.
	Illegal Character in Header Name	Enable to check whether the HTTP header name contains illegal characters. Illegal characters in HTTP headers include spaces, non-printable ASCII characters, or other special characters
	Illegal Character in Header Value	Enable to check whether the HTTP header value contains illegal characters. Illegal characters in HTTP headers include spaces, non-printable ASCII characters, or other special characters
	Redundant HTTP Headers	Enable to check whether a HTTP request contains multiple instances of `Content-Length` (only for HTTP/1.x), `Content-Type` (for both HTTP/1.x and HTTP/2) and `Host` (for both HTTP/1.x and HTTP/2) header fields. These header fields are required to appear only once in a request by the RFC. Redundant HTTP headers are most probably involved in possible attacks.
HTTP Parameter		
	Total URL Parameter Length	Specifies the total maximum acceptable length in bytes of all parameters, including their names and values, in the URL. Parameters usually appear after a `?`, such as: `/url?`**parameter1=value1&parameter2=value2**. The count does not include: • Question mark (?), ampersand (&), and equal (=) characters are not included. • Parameters in the HTTP body, which can occur with HTTP `POST` requests. Attack log messages contain `Total URL Parameters Length Exceeded` when this feature detects a URL parameter line length buffer overflow attempt.
	Number of URL Parameter	Specifies the maximum number of parameters in the URL. It does **not** include parameters in the HTTP body, which can occur with HTTP `POST` requests. Attack log messages contain `Too Many Parameters in Request` when this feature detects a URL parameter count buffer overflow attempt.
	Maximum URL Parameter Name Length	Specifies the maximum acceptable length in bytes of each URL parameter name in a request. Enable to check whether a parameter name exceeds the limitation (the default is 4096). For example, `user` in the request `GET /index.php?user=test&sid=1234` is an illegal parameter name if you set the limitation as 3.

Maximum URL Parameter Value Length	Specifies the maximum acceptable length in bytes of each URL parameter value in a request. Enable to check whether a parameter value exceeds the limitation (the default is 4096). For example, `1234` in the request `GET /index.php?user=test&sid=1234` is an illegal parameter value if you set the limitation as 3.
Illegal Character in Parameter Name	Enable to check whether a URL parameter name contains the characters that are not allowed by the RFC. These illegal characters are usually non-printable ASCII characters or other special characters.
Illegal Character in Parameter Value	Enable to check whether a URL parameter value contains the characters that are not allowed by the RFC. These illegal characters are usually non-printable ASCII characters or other special characters.
Duplicate Parameter Name	Enable to check whether a duplicate parameter name is in the header or body parameters. This protocol constraint will be triggered if: • There are duplicate parameter names in the header. • There are duplicate parameter names in the body. • A parameter name in the header is also in the body.
HTTP Request	
HTTP Request Filename Length	Specifies the maximum acceptable length in bytes of the HTTP request filename.
Number of Header Lines in Request	Specifies the maximum acceptable number of lines in the HTTP header. Attack log messages contain `Too Many Headers` when this feature detects a header line count buffer overflow attempt.
Null Character in URL	Enable to check whether the URL (or path for HTTP/2) in a request contains null characters (such as `\0` or `%00`). This feature checks the part between the host prefix and parameters in the URL (if they exist), for example, the `/index.php` in `GET http://www.server.com/index.php?name=value HTTP 1.1`. Attackers might embed NULL characters in URL to evade detections.
Illegal Character in URL	Enable to check whether the URL (or path for HTTP/2) in a request contains characters that are not allowed by the RFC. These illegal characters are usually non-printable ASCII characters or other special characters (such as ASCII 0 - 31 and ASCII 127). This feature checks the part between the host prefix and parameters in the URL (if they exist), for example, the `/index.php` in `GET http://www.server.com/index.php?name=value HTTP 1.1`.
Malformed URL	Enable to check whether the URL (or path for HTTP/2) in a request conform the spec by beginning with a slash ("/") character or a slash character follows the protocol prefix and host prefix in the URL (e.g. `http://myserver.com/default.asp`). If the slash characters are missing, it is typically a malicious access to other protocols (e.g. SMTP) using the back-end web servers.
HTTP/2 Max Requests	Enable to specify the maximum acceptable number of requests in an HTTP/2 connection.

HTTP/2 RST Stream	Enable to specify the maximum acceptable number of HTTP/2 RST Streams in an HTTP/2 connection.
HTTP/2 RST Stream Frequency	Enable to specify the maximum occurrences of the HTTP/2 RST Stream per second.

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.

4. Click **SAVE**.

URL Access

You can configure URL access rules that define which HTTP requests FortiWeb Cloud accepts or denies based on their `Host:` name and URL.

To create a URL access rule

1. Go to **ACCESS RULES > URL Access**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Create Rule**.
3. Configure these settings.

Name	Enter a unique name that can be referenced in other parts of the configuration.
Request URL	Enter a regular expression that matches the target URL. To create a regular expression, see Frequently used regular expressions on page 237.
Action	Select the action that FortiWeb Cloud takes when it detects a violation of the rule. • **Alert & Deny**—Block the request (or reset the connection) and generate an alert email and/or log message. • **Pass—**Allow the request. Do **not** generate an alert and/or log message. • **Continue—**Continue by evaluating any subsequent rules defined in the web protection profile. If the request does not violate any other rules, FortiWeb Cloud allows the request. If the single request violates multiple rules, it generates multiple attack log messages.

4. Click **OK**.
   You can continue creating at most 12 URL access rules for an application.

IP Protection

You can block requests from clients based upon their source IP address directly, their current reputation known to FortiGuard, or which country or region the IP address is associated with.

Conversely, you can also exempt clients from scans typically included by the policy.

To configure IP Protection, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

IP reputation

To block the following attacks, you can configure FortiWeb Cloud to block client access based on up-to-date threat intelligence.

- botnets
- spammers
- phishers
- malicious spiders/crawlers
- virus-infected clients
- clients using anonymizing proxies
- DDoS participants

IP reputation leverages many techniques for accurate, early, and frequently updated identification of compromised and malicious clients so you can block attackers before they target your servers. Data about dangerous clients derives from many sources around the globe, including:

- FortiGuard service statistics
- honeypots
- botnet forensic analysis
- anonymizing proxies
- 3rd party sources in the security community

From these sources, Fortinet compiles a reputation for each public IP address. Clients will have poor reputations if they have been participating in attacks, willingly or otherwise. Because blocking innocent clients is equally undesirable, Fortinet also restores the reputations of clients that have improved their behaviors. This is crucial when an infected computer is cleaned, or in DHCP or PPPoE pools where an innocent client receives an IP address that was previously leased by an attacker.

Check whether an IP address is malicious through FortiGuard IP Web Application Security Service: https://www.fortiguard.com/services/ws.

If you believe an IP address is wrongly classified as a malicious IP, you can report it here: https://www.fortiguard.com/faq/contact-web-security.

Go to **ACCESS RULES > IP Protection** to enable IP Reputation.

Geo IP Block

To configure blocking by geography, select one or more geographical regions that you want to block from the Country list, then click the right arrow or double click the countries to move them to the Selected Country list on the right.

In addition to countries, the Country list also includes distinct territories within a country, such as Puerto Rico, and regions that are not associated with any country, such as Antarctica.

The action taken for the GEO IP violations is Period Block (600 seconds).

IP list

You can define which source IP addresses are trusted or distrusted clients, or allowed ones.

In **IP List** section, configure these settings.

IP List Input	There are two ways of adding IP list: • **Manually input IP/IP range one by one** Type the client's source IP address, then click **Add** to add more. You can enter either a single IP address or a range of addresses (for example, 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100). Each entry should contain only one IP address or IP range. Both IPv4 and IPv6 addresses are supported only on AWS platform currently. **Note:** A maximum number of 30,000 IPs/IP Ranges is supported, 10,000 for each IP/IP Range type. • **Upload a CSV file to add IPs in batch** Click **Upload CSV** to import a CSV file that contains multiple IPs. The type should be one of "BLOCK", "ALLOW","TRUST" . Use the following format for each IP/IP range (enter one IP/IP range per line) in the CSV file: BLOCK,<IP Address> ALLOW,<IP Address> TRUST,<IP Address>-<IP Address>
Type	• **Block IP**—The source IP address that is distrusted, and is permanently blocked from accessing your web servers, even if it would normally pass all other scans. Note: If multiple clients share the same source IP address, such as when a group of clients is behind a firewall or router performing network address translation (NAT), blocking the source IP address could block innocent clients that share the same source IP address with an offending client. • **Trust IP**—The source IP address is trusted and allowed to access your web servers, bypassing any further scanning by subsequent security modules.

	By default, if the IP address of a request is neither in the Block IP nor Trust IP list, FortiWeb Cloud will pass this request to other scans to decide whether it is allowed to access your web servers. However, you can define the **Allow Only** list so that such requests can be screened against this list before it's passed to other scans. • **Allow Only**—If the source IP address is in the **Allow Only** list, it will be passed to other scans to decide whether it's allowed to access your web servers. If not, it will be blocked. If this list is empty, then the source IP addresses which are not in the Block IP and Trust IP list will be passed directly to other scans. The scan sequence for processing IP addresses is as follows: **Block IP > Trust IP > Allow Only**. For example, if an IP address is present in the **Block IP** list, the system will block it immediately without proceeding to scan against the **Trust IP** and **Allow Only** IP lists. In other words, if an IP address appears in multiple IP lists, it will be processed only against the list which is scanned first. For example, if you wish to trust an IP range but block specific IP addresses within that range, then you can add those IP addresses to the **Block IP** list and the IP range in the **Trust IP** list. This approach will allow the IP range to be trusted while the specified IP addresses are blocked, since the **Block IP** list is scanned first. Requests that are blocked according to the IP Protection lists will receive a warning message as the HTTP response. The warning message page includes **ID: 70007**, which is the ID of all attack log messages about requests from blocked IPs.

Click **SAVE**.

If you have enabled **Use X-Header to Identify Original Clients' IP** in **Rewriting Requests**, the IP address in the header will be identified as the client IP and be scanned by **IP Protection**.

CORS protection

If you have enabled Cross-Origin Resource Sharing (CORS) for your application, the resources of your application can be accessed by other applications using JavaScript within the browser. Use the CORS Protection feature on FortiWeb Cloud so that only legitimate CORS requests from allowed web applications can reach your application.

To create a CORS protection rule

1. Go to **ACCESS RULES > CORS protection**.
2. Enter a **Request URL** to protect. It can be either:
   - A literal URL, such as `/folder1/index.htm` that the HTTP request must contain in order to match the rule, or use wildcards to match multiple URLs, such as `/folder1/*` or `/folder1/*/index.htm`. The URL must begin with a slash (`/`).
   - A regular expression, such as `^/*.php`. This pattern does not require beginning with a slash (/); however, it must match URLs that begin with a slash.
     To create and test a regular expression, click the **RegEx Test**. This opens the **Regular Expression Validator** window where you can fine-tune the expression. For details, see Frequently used regular expressions.
3. Enable **Block CORS Traffic** to block all the CORS traffic to the above specified URL.
   Disable this option to allow CORS traffic, in the meantime configure the settings below to add restrictions for the CORS traffic.
4. Click **Create New** to add **Allowed Origins**. Configure the following settings.

Protocol	Select which type of protocols is allowed for the connections between foreign applications and your application.
Origin Name	Enter the foreign application's domain name. Wildcards are supported. Please note that the Origin Name only matches with domains in the same level, for example, *.com matches with a.com but not a.b.com; while *.b.com matches with a.b.com.
Port	Type the TCP port number for the CORS connections. The valid range is from 0 to 65,535. 0 means the CORS requests can reach at any TCP port number.
Include Sub Domains	Enable this option so that the **Origin Name** matches with domains of its sub level. For example, if this option is enabled, *.com matches with all domain names.

5. Click **OK**.
6. Configure the following settings.

Allowed Credentials	Specify whether CORS requests from foreign applications can include user credentials. • **None**: Allow CORS requests with or without user credentials. • **TRUE**: Allow only CORS requests with user credentials. The CORS specification requires a specific value for `Access-Control-Allow-Origin` in the response package if the `Access-Control-Allow-Credentials` is true. If you leave the **Allowed Origins** list empty, please be careful to select **TRUE** for **Allowed Credentials** unless you are sure the back-end server will not set `*` for `Access-Control-Allow-Origin` in the response package. • **FALSE**: Allow only CORS requests without user credentials.
Allowed Maximum Age	The maximum time period before the result of a preflight request expires. The valid range is from 0 to 86,400. 0 means using the Allowed Maximum Age configured in the back-end server.

	For example, if the Allowed Maximum Age is set to 3,600 seconds, and the initial preflight request is allowed, then the subsequent CORS requests in the next 3,600 seconds can be sent directly without a precedent preflight request. This applies only to the CORS preflighted requests, not the simple requests.
Allowed Methods	Click **Add** to add the allowed methods so that FortiWeb Cloud can verify whether the allowed methods used in the CORS requests are legitimate.
Allowed Headers	Click **Add** to add the allowed headers so that FortiWeb Cloud can verify whether the headers used in the CORS requests are legitimate.
Exposed Headers	Click **Add** to add the exposed headers so that FortiWeb Cloud can expose the specified headers in JavaScript and share with foreign applications.

7. Click **Save**.

Bot Mitigation

To quickly protect websites, mobile apps and APIs from automated threats, you can configure the bot mitigation feature to check more specific signatures such as client events, and occurrence of suspicious behaviors, etc. of regular clients.

- Biometrics Based Detection
- Threshold Based Detection
- Known Bots
- Bot Deception
- ML Based Bot Detection

Biometrics Based Detection

By checking the client events such as mouse movement, keyboard, screen touch, and scroll, etc in specified period, FortiWeb Cloud judges whether the request comes from a human or from a bot.

1. Go to **BOT MITIGATION > Biometrics Based Detection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Monitor Client Events	Select at least one client event according to your need. • Mouse Movement • Click • Keyboard • Screen Touch • Scroll
Event Collection Period	Specify the time period that the events will be collected from the client.
Bot Effective Time	For the identified bot, choose the time period before FortiWeb Cloud tests and verifies the bot again.

3. Click **+Create Rule**.
4. For **URL**, enter the literal URL, such as `/index.php`, or a regular expression, such as `^/*.php` that the HTTP request must contain in order to match the rule. Multiple URLs are supported.
5. Click **OK**.
6. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.

Deny(no log)	Block the request (or reset the connection).

7. Click **SAVE**.

Threshold Based Detection

With the occurrence, time period, and severity of the following suspicious behaviors predefined, FortiWeb Cloud judges whether the request comes from a human or a bot.

- Known Bad Bots
- Known Search Engines
- Crawler
- Vulnerability Scanning
- Slow Attack
- Content Scraping
- Credential Based Brute Force

To configure Threshold Based Detection:

1. Go to **BOT MITIGATION > Threshold Based Detection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Crawler	Enable to detect web crawlers that are usually used to map out your application structure. If 403 and 404 response codes occur more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Vulnerability Scanning	Enable to detect tools that scan your application for vulnerabilities. If attack signatures are triggered more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Slow-Attack	Enable to detect automatic tools that try to go undetected by generating traffic in low thresholds. If the timeout HTTP Transaction occurs more than 5 times within 100 seconds, FortiWeb Cloud will take actions.
Content-Scraping	Enable to detect malicious tools that try to download large amounts of content such as text/html and application/xml from your web site. If the download activity occurs more than 100 times within 30 seconds, FortiWeb Cloud will take actions.
Credential Based Brute Force	Enable to block brute force attacks that try to obtain user credentials. To enable Credential Based Brute Force, Account Takeover must be enabled.
Request URL	The URL that you want to protect from brute force login. Here we only support **Regular Expression Match**. The value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. For details, see Frequently used regular expressions on page 237. Only available when Credential Based Brute Force is enabled.
Occurrence **Within**	When the brute force login occurs more than a certain times in a certain time period, FortiWeb Cloud will periodically block the request. The Occurrence defines "how many times", while the Within (Seconds) defines the "time period". Only available when Credential Based Brute Force is enabled.

Challenge	You can select among: • **Disable**—Disables this option to not to challenge users when a rule is triggered. • **Real Browser Enforcement**—Specifies whether FortiWeb Cloud returns a JavaScript to the client to test whether it is a web browser or automated tool when it meets any of the specified conditions. If the client fails the test or does not return results in 20 seconds, FortiWeb Cloud applies specified actions. If the client appears to be a web browser, FortiWeb Cloud allows the client to exceed the action. • **CAPTCHA Enforcement**—Requires the client to successfully fulfill a CAPTCHA request. If the client cannot successfully fulfill the request within 3 times or doesn't fulfill the request within 20 seconds, FortiWeb Cloud applies related actions and sends the CAPTCHA block page. **Note:** Configurable only when either of Crawler, Vulnerability Scanning, Slow Attack, or Content Scraping is enabled.

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.

   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

   The default action for Threshold Based Detection is Period Block. It is not recommended to change this configuration.

   For Threshold Based Detection, Period Block is the most reasonable action to take. When the count of suspicious behaviors reaches the threshold and triggers the Period Block action, all the subsequent requests from the suspected IP address in the next 10 minutes will be blocked, while if the action is Alert & Deny or Deny (no log), only the request that hits the threshold will be denied, and the subsequent requests will be let go until the threshold count is hit again.

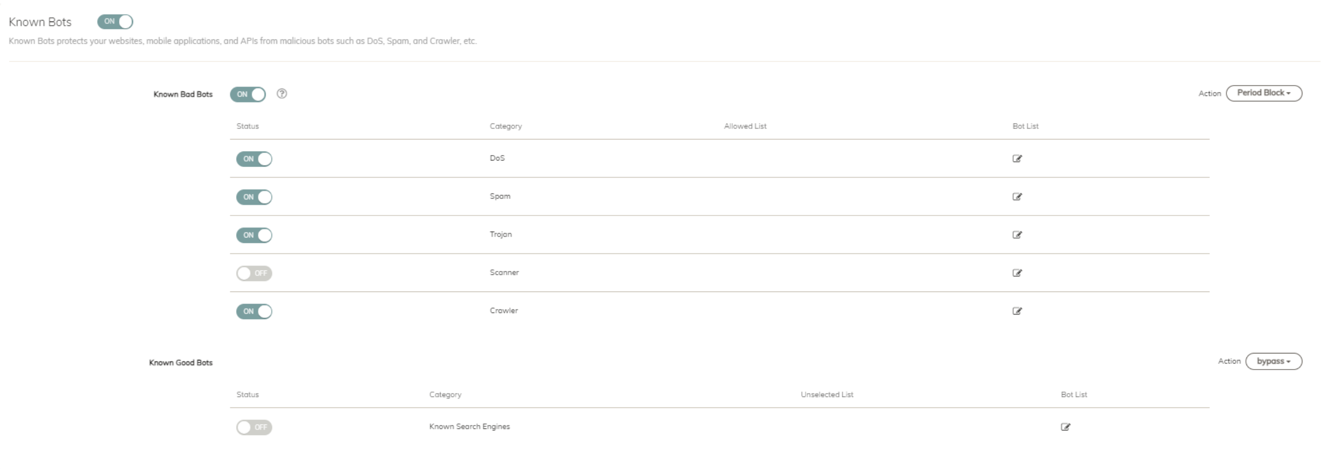
Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.

4. Click **SAVE**.

Known Bots

Configuring Known Bots protects your websites, mobile applications, and APIs from known malicious bots (e.g., DoS, Spam, Crawlers) while allowing activity from beneficial bots like search engines. This ensures both security and the smooth flow of essential traffic.

This feature identifies and manages a wide range of attacks from automated tools no matter where these applications or APIs are deployed.



Known Bots ON

Known Bots protects your websites, mobile applications, and APIs from malicious bots such as DoS, Spam, and Crawler, etc.

Known Bad Bots ON — Action: Period Block

Status	Category	Allowed List	Bot List
ON	DoS		✎
ON	Spam		✎
ON	Trojan		✎
OFF	Scanner		✎
ON	Crawler		✎

Known Good Bots — Action: bypass

Status	Category	Unselected List	Bot List
OFF	Known Search Engines		✎

To configure Known Bots rule

1. Go to **BOT MITIGATION > Known Bots**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.
3.

Known Bad Bots	Enable to take the configured action against bad bots using predefined signatures. Click the **Edit** icon on each Bot List if you want specific bots to be exempted. The signatures moved to the **Allowed List** will not be screened against.
Known Good Bots	Enable to take the configured action on known good bots (we recommend configuring bypass or alert for this option). By default, all popular predefined search engines (Google, Bing, Yahoo, etc.) are on the **Selected List**. Click the **Edit** icon on each Bot List if you want specific bots to be exempted. The search engines moved to the **Unselected List** will not be screened against.

4. Select the action that FortiWeb Cloud takes when it detects a Known Good or Bad Bot.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Bypass	Accept the request with no generated log or alert.
Alert	Accept the request and generate an alert email and/or log message
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.

5. Click **SAVE**.

Bot Deception

To prevent bot deception, you can configure to insert link into HTML type response pages. For regular clients, the link is invisible, while for malicious bots like web crawler, they may request the resources which the invisible link points at.

To configure bot deception

1. Go to **BOT MITIGATION > Bot Deception**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. For **Deception URL**, specify the deception URL to be inserted in the HTML response page, which can be either an absolute path or a relative path.
3. Click **+Create Rule** to enter the literal URL, such as `/index.php`, or a regular expression, such as `^/*.php` that the HTTP request must contain in order to match the rule. Multiple URLs are supported.
4. Click **OK**.
5. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.

6. Click **SAVE**.

ML Based Bot Detection

The AI-based bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots and CC attacks that can sometimes go undetected.

Compared with the traditional mechanisms to detect bots, the ML based bot detection model saves you the trouble to experiment on an appropriate threshold to detect abnormal user behaviors. For example, how could you know how many times of HTTP requests initiated by a user should be considered as abnormal? With the traditional mechanism, you may need to experiment on different threshold values and continuously check the attack log until no related attack logs are reported for the regular traffic.

Things are much easier if you use the ML based bot detection model. FortiWeb Cloud uses SVM (Support Vector Machine) algorithm to build up the bot detection model that self-learns the traffic profiles of regular clients. When the traffic from a new client flows in, it is compared against that of the regular clients. If they don't match, the bot detection model classifies the new client as an anomaly. When the traffic profiles of the regular clients vary dramatically (e.g. the functions of your application have changed, so that users behave differently when they visit your application),FortiWeb Cloud automatically refreshes the bot detection model to adapt to the changes.

Moreover, test shows that the bot detection model performs much better, specially when it detects crawlers and scrapers. The traffic is comprehensively evaluated from 13 dimensions. It helps increase the detection accuracy and decrease the false positive rate.

To configure a ML based bot detection rule:

1. Go to **BOT MITIGATION > ML Based Detection (Beta)**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Select the **Model Settings** tab.
3. Configure the following settings.

Client Identification Method	FortiWeb Cloud collects samples from the real users to build a machine learning model. Select whether to use **IP**, **IP and User-Agent**, or **Cookie** to identify a user. • **IP**: The traffic data in one sample should come from the same source IP. • **IP and User-Agent**: The traffic data in one sample should come from the same source IP and User-Agent (the browser). • **Cookie**: The traffic data in one sample should have the same cookie value.
Model Type	Multiple models are built during the model building stage. The system uses training accuracy, cross-validation value, and testing accuracy to select qualified models. The **Model Type** is used to select the one final model out of all the qualified models. • If you configure the Model Type to **Moderate**, the system chooses the model which has the **highest** training accuracy among all the qualified models. • If you configure the Model Type to **Strict**, the system chooses the model which has the **lowest** training accuracy among all the qualified models. The Strict Model has a higher likelihood of identifying anomalies, but also carries the risk of incorrectly identifying regular users as bots. The Moderate Model is relatively lenient making it less prone to false positive detections, but comes with the risk of allowing actual bots to go undetected. There isn't a perfect option for every situation. Whichever model type you choose, you can always leverage the options in **Anomaly Detection Settings** and **Action Settings** to mitigate the side effects, for example, using **Bot Confirmation** to avoid false positive detections.
Anomaly Count	If the system detects certain times of anomalies from a user, it takes actions such as sending alerting emails or blocking the traffic from this user. **Anomaly Count** controls how many times of anomalies are allowed for each user. For example, the Anomaly Count is set to 4, and the system has detected 3 anomalies in the last 6 samples. If the 7th sample is detected again as an anomaly, the system will take actions. Please note that if no valid traffic is collected for the 7th sample (for example, the user leaves your application), the system will clear the anomaly count and the user information. If the user revisits your application, he/she will be treated as new users and the system starts anomaly counting afresh. Since this option allows certain times of anomalies from a user, it might be a good choice if you want to avoid false positive detections.
Challenge	If a bot is detected, the system will use the following methods to confirm it's indeed a bot. • **Real Browser Enforcement**: The system sends a JavaScript to the client to verify whether it is a web browser. • **CAPTCHA Enforcement**: The system requires clients to successfully fulfill a CAPTCHA request.

	It will trigger the action policy if the traffic is not from web browser.
Block Duration	Enter the number of seconds that you want to block the requests. The valid range is 1–3,600 seconds (1 hour). This option only takes effect when you choose **Period Block** in **Action**.
Source IP List	Click **Create New** to list the source IP ranges of the samples. FortiWeb Cloud will collect samples from the specified IP ranges.
Exception URLs	Due to the nature of some web pages, such as the stock list web page, even regular users may behave like bots because they tend to frequently refresh the pages. You may need to add these URLs in the exception list, otherwise the model may be invalid because too many bot-like behaviors are recorded in the samples. Click **Create New** to list exception URLs. The system will collect samples for any URL except the ones in the **Exception URLs** list.

4. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate a log message.
Alert & Deny	Block the request (or reset the connection) and generate a log message.
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.
Deny (no log)	Block the request (or reset the connection) without generating a log message.

5. Click **SAVE**.

DDoS prevention

FortiWeb Cloud DDoS prevention is a service that protects you against DDoS high-volume attacks.

A Distributed Denial of Service attack (DDoS attack) is a cyber attack in which an attacker attempts to overwhelm a web server/site, making its resources unavailable to its intended users. Most DDoS attacks use automated tools (not browsers) on one or more hosts to generate the harmful flood of requests to a web server.

DDoS attacks can be prevented at Application layer (HTTP or HTTPS) and Network layer (TCP/IP).
As public cloud platforms already execute basic Network layer TCP Flood Prevention checks afront, when traffic comes into FortiWeb Cloud, it only detects DDoS attacks at Application layer (HTTP or HTTPS).

To configure **DDoS prevention** , you must have already enabled this module in **Add Modules**. See How to add or remove a module.

Configuring application-layer DDoS prevention

For some DDoS prevention features, FortiWeb Cloud uses session management to track requests.

1. When FortiWeb Cloud receives the first request from any client, it adds a session cookie to the response from the web server in order to track the session. The client will include the cookie in subsequent requests.
2. If a client sends another request before the session timeout, FortiWeb Cloud examines the session cookie in the request.
    - If the cookie does not exist or its value has changed, FortiWeb Cloud drops the request.
    - If the same cookie exists, the request is treated as part of the same session. FortiWeb Cloud increments its count of connections and/or requests from the client. If the rate exceeds the limit, FortiWeb Cloud drops the extra connection or request.

You can configure settings below to limit the number of HTTP requests and TCP connections.

HTTP Access Limit	Enable to limit the number of HTTP requests per second from a certain IP.
HTTP Request Limit	Type a rate limit for the maximum number of HTTP requests per second from each source IP address that is a single HTTP client. For example, if loading a web page involves: • 1 HTML file request • 1 external JavaScript file request • 3 image requests The rate limit should be at least 5, but could be some multiple such as 10 or 15 in order to allow 2 or 3 page loads per second from each client. It's recommended to use an initial value of 1000.
Malicious IPs	Enable to limit the number of TCP connections with the same session cookie.
TCP Connection Number Limit	Type the maximum number of TCP connections allowed with a single HTTP client. It's recommended to use an initial value of 100.

HTTP Flood Prevention	Enable to limit the number of HTTP connections with the same session cookie.
HTTP Request Limit	Type the maximum rate of requests per second allowed from a single HTTP client. It's recommended to use an initial value of 500.
Challenge	• **Real Browser Enforcement**—Specifies whether FortiWeb Cloud returns a JavaScript to the client to test whether it is a web browser or automated tool when it meets any of the specified conditions. • **CAPTCHA Enforcement**—Requires the client to successfully fulfill a CAPTCHA request.

Configuring actions

1. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.

Advanced Applications

With this module, you can configure XML protection to ensure no potential attacks in requests containing XML; also, you can configure FortiWeb Cloud to secure WebSocket traffic with various security controls.

- Custom Rule
- WebSocket Security

Custom Rule

Custom Rule provides advanced access control capabilities to match complex conditions specific to your web application.

You use the rule's filters to specify all criteria that you require allowed traffic to match.

The filters apply to request traffic only, with the following exceptions:

- **HTTP Response Code** and **Content Type** apply to responses.
- **Signature Violation** applies to either requests or responses, depending on which signatures you enable.
- **Occurrence** applies to either requests or responses.

To create a custom rule

1. Go to **ADVANCED APPLICATIONS > Custom Rule**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Create Rule**.
3. Configure these settings.

Name	Type a unique name for the custom rule.
Operation	Select which action the FortiWeb Cloud will take when it detects a violation of the rule: • **Deny**—Block the request (or reset the connection). • **Deny (no log)**—Block the request (or reset the connection) without generating a log message. • **Period Block**—Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.
Challenge	Choose how to challenge users when a custom rule is triggered. • **Disable**—Disable this option to not to challenge users when a rule is triggered. • **Real Browser Enforcement**—Specifies whether FortiWeb Cloud returns a JavaScript to the client to test whether it is a web browser or automated tool when it meets any of the specified conditions. If the client fails the test or does not return results in 20 seconds, FortiWeb Cloud applies specified actions. If the client appears to be a web browser, FortiWeb Cloud allows

	the client to exceed the action. • **CAPTCHA Enforcement**—Require the client to successfully fulfill a CAPTCHA request. If the client cannot successfully fulfill the request within 3 times or doesn't fulfill the request within 20 seconds, FortiWeb Cloud applies related actions and sends the CAPTCHA block page.

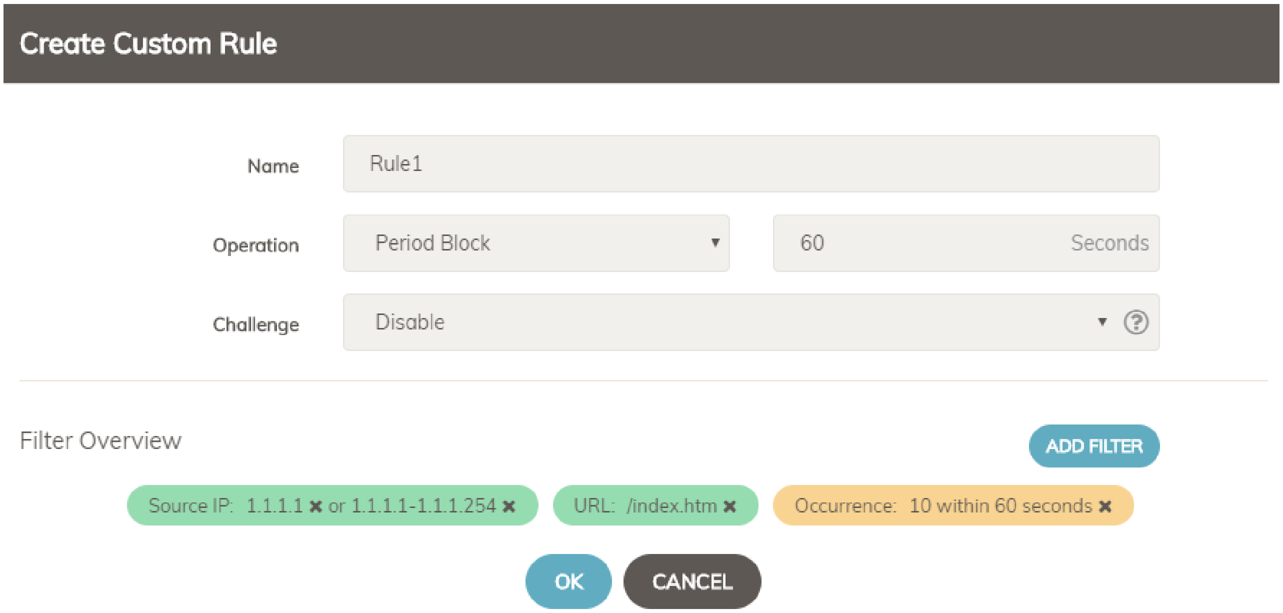
4. Click **ADD FILTER** to select the filter types.
5. Configure these settings.

Filter Type	Select the filter types that a request must match in order not to be allowed, and configure their settings respectively.
Source IP	The request containing the IP/IP Range will not be allowed. • **IP/IP Range**—Type the IP address of a client that is not allowed. You can enter either a single IP address or a range of addresses (for example, 172.22.14.1-172.22.14.255 or 10:200::10:1-10:200:10:100). Each entry should contain only one IP address or IP range. Both IPv4 and IPv6 addresses are supported only on AWS platform currently. • **Reverse Matching**—Once enabled, only the specified IP/IP range will be allowed by FortiWeb Cloud.
User	The request containing the user name will not be allowed. • **User Name**—Enter a user name captured in Account Takeover module to match. You must enable Account Takeover module for this user type. • **Reverse Matching**—Once enabled, the request containing the specified user name will be allowed by FortiWeb Cloud.
URL	The request matching the specified URL will not be handled. • **URL Pattern**—Type a regular expression that matches one or more URLs, such as `/index\.jsp`. • **Reverse Matching**—Once enabled, only the specified URL will be handled.
Parameter	The request containing specified Name Pattern and Value Pattern will not be handled. • **Name Pattern**—Define the name pattern of a parameter using regular expression. • **Value Pattern**—Define the value pattern of a parameter using regular expression.
HTTP Header	The request matching all or part of the specified HTTP header name values will not be handled. • **HTTP Header**—Indicate a single HTTP Header Name such as `Accept:`, and all or part of its value in Value Pattern. ◦ **Predefined Header** **Header Name**—Select a single HTTP header name from the drop down list. **Value Pattern**—Define the value pattern using regular expression. **Reverse Matching**—Once enabled, the request that matches the specified value pattern will be handled.

	◦ **Custom Header** **Name Pattern**—Define the name pattern of a single HTTP header name. **Value Pattern**—Define the value pattern using regular expression. **Reverse Matching**—Once enabled, the request will be handled if the HTTP header contains the regular expression. • **HTTP Method** ◦ **Method Pattern**—Configure a regular expression for the HTTP method that FortiWeb Cloud will search for in the header field. ◦ **Reverse Matching**—Once enabled, the request will be handled if the HTTP header contains the HTTP method's regular expression.
Content Type	The request will not be handled if an HTTP response for a file matches one of the specified types. Use icons ➡ and ⬅ to add or remove the content types to or from the Allow Content Types list.
HTTP Response Code	The request will not be handled if a HTTP response code matches the specified code or range of codes. • **Code**—Enter a response code or code range. For example, `404` or `500-503`.
Known Attacks	The request will not be handled if FortiWeb Cloud detects selected attack signature categories in the request or response. • Cross Site Scripting • SQL Injection • Generic Attacks • Known Exploits • Trojans Refer to Known Attacks for information about the attacks above.
Access Rate Limit	The request will not be handled if the number of requests per second per client IP exceeds the specified value. • **Request per Second**—Enter a value to indicate the number of requests per second per client IP.
Packet Interval Timeout	The request will not be handled if the time period between packets arriving from either the client or server (request or response packets) exceeds the specified value in seconds. • **Timeout**—Enter a value to indicate the time period between packets arriving from either the client or server.
Transaction Timeout	The request will not be handled if the lifetime of a HTTP transaction exceeds the specified transaction timeout. • **Timeout**—Enter a value in seconds to indicate the lifetime of a HTTP transaction.
Occurrence	The request will not be handled if a transaction matches other filter types in the current rule at a rate that exceeds the specified threshold. • **Occurrence**—Enter a rate that a transaction matches other filter types.

	• **Within**—Enter a time period in seconds for the occurrence.
Time Period	The request will not be handled if the time period of the request matches what you specify. • **Type**—Select Daily or Once for the time period. • **Time Period**—Enter a time period.

Note: Two colors green and yellow are adapted to classify the filter types; green means filtering HTTP traffic, include Source IP, URL, Parameter, HTTP Header, HTTP Response Code, and Content Type; while yellow is related to security, including Security Rules, Packet Interval Timeout, Transaction Timeout, and Occurrence.



Create Custom Rule

Name	Rule1
Operation	Period Block ▾ 60 Seconds
Challenge	Disable ▾

Filter Overview

Source IP: 1.1.1.1 ✖ or 1.1.1.1-1.1.1.254 ✖

URL: /index.htm ✖

Occurrence: 10 within 60 seconds ✖

6. Click **OK**.
   You can continue creating at most 12 custom rules for an application.
7. You can click ✎ ↑ ↓ 🗑 to edit, reorder, or remove each created rule.

WebSocket Security

WebSocket Protocol is a TCP-based network protocol, which enables full-duplex communication between a web browser and a server.

FortiWeb Cloud now secures WebSocket traffic with a variety of security controls such as allowed formats, frame and message size and signature detection.

You can create WebSocket security rules to detect traffic that uses the WebSocket TCP-based protocol.

To create a WebSocket security rule

1. Go to **ADVANCED APPLICATIONS > XML Protection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Add WebSocket Security Rule**.

3. Configure these settings.

Name	Type a name that can be referenced by other parts of the configuration.
Request URL	Enter the literal URL, such as `/index.php`, that the HTTP request must contain in order to match the rule.
Allow WebSocket	Enable to detect the WebSocket traffic, and FortiWeb Cloud will check any WebSocket related traffic. The following fields can be configured only when this option is enabled.
Allow Formats	When the WebSocket connection is established , data is transmitted in the form of frame. Select the allowed frame formats that are acceptable matches. By default, both **Plain Text** and **Binary** are checked.
Max Frame Size	Specify the maximum acceptable frame header and body size in bytes. The valid range is 0–2147483647 bytes.
Max Message Size	Specify the maximum acceptable message header and body size in bytes. The valid range is 0–2147483647 bytes.
Block Extensions	Enable to not check the extension header in WebSocket handshake packet. By default, this option is disabled.
Block Known Attacks	Enable to protect against known attacks, common vulnerabilities and exposures (CVEs), and other exploits as part of the OWASP Top 10.

4. Enter the allowed origin.
   For example, `121.40.165.18:8800`. Only traffic from the allowed origins can be accepted. You can add multiple origins here.
5. Click **OK**.
   You can create at most 12 WebSocket security rules for an application.

To configure actions

1. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

2. Click **SAVE**.

API Protection

FortiWeb Cloud secures your API interfaces that are implemented using XML, JSON API, or OpenAPI.

Depending on how your API interfaces are implemented, you can use **OpenAPI Validation**, **JSON Protection**, or **XML Protection** to import a schema/validation file defining how a client should request the resources being fetched or modified. FortiWeb Cloud parses the contents of each API call against the schema/validation file and take appropriate actions to protect you from malicious traffic.

FortiWeb Cloud has the ability to manage API users, verify API keys, control API access and rate limits, etc. It can also check whether the request initiated from a mobile device carries a JWT-token header and whether the token is valid. These settings are available in **API Gateway** and **Mobile API Protection**.

- ML Based API Protection
- OpenAPI Validation
- JSON Protection
- XML Protection
- Mobile API Protection
- API Gateway

ML Based API Protection

The AI-based API Protection builds mathematical models for Schema Protection and Threat Protection. The Schema Protection model learns the REST API data structure from user traffic samples and then compiles a schema file to screen out malformed API requests. The Threat Protection model learns the patterns of the parameter value in the API request body and then builds models to screen out requests which have abnormal values in its body.

Model Settings

To configure an API Protection rule:

1. Go to **API PROTECTION > ML Based API Protection.**
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Select the **Model Settings** tab.
3. Based on the samples collected, the system learns the patterns of the parameter value in the API request body and then builds **Threat Protection** models to screen out requests which have abnormal values in their body.
   Select the action to take when abnormal parameter values are detected:
   - **Alert:** Accept the request and generate a log message.
   - **Alert&Deny:** Block the request (or reset the connection) and generate a log message.
   - **Standby:** Do not take any action.

   Please note that in addition to the Threat Protection model that screens out API requests with abnormal parameter values, the system also builds an Schema Protection model to detect API requests which are malformed. It compiles an API schema file and screens out malformed API requests against the schema file. The Schema Protection data can be viewed in the **API Collection** tab.

4. Configure the Data Collection Settings.

IP List Type	• **Trust**: FortiWeb Cloud collects API request samples only from the **Trust** source IP addresses. • **Block**: FortiWeb Cloud collects API request samples from all source IP addresses except the ones in the **Block** list. If the IP List Type is **Trust** and the **Source IP List** is empty, FortiWeb Cloud will not collect samples from any Source IP address. If the IP List Type is **Block** and the **Source IP List** is empty, FortiWeb Cloud will collect samples from all Source IP addresses. The IP list only restricts where the samples come from. Once the model is built, requests from other source IP addresses will also be scanned by the IP Protection model.
Source IP List	Click **Create New** to add the source IP list. This option is used together with **IP List Type**.
API Learning Patterns	If you want to limit the API protection learning to certain API paths, click **Create New** in the **API Learning Patterns** section, then enter either a string match API path or regular expression. Please note that only the specified API paths will be protected by the API Protection module.

API Collection

To view and edit API paths learned by the Schema Protection model:

1. Go to **API PROTECTION > ML Based API Protection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Select the **API Collection** tab. This page lists all the API paths learned by machine learning model.
   Please note that the default action for Schema Protection is **Standby**. You can click into each API path and change the action.
3. Click the Edit icon ✎ on the API path row to view and edit the parameter, request body, and response body learned by the model.
4. Select the action to take when malformed API request to this API path is detected.
   - **Alert:** Accept the request and generate a log message.
   - **Alert&Deny:** Block the request (or reset the connection) and generate a log message.
   - **Standby:** Do not take any action.
5. Click the **Parameter** tab under **Request** section, check the parameters learned by the machine learning model. If some parameters are missing, you can click **Create Parameter** to add them.
   If you don't want certain parameter to be protected, click the **Remove** icon on the corresponding parameter row.
6. To edit the parameter, click the **Edit** ✎ icon of the parameter to be edited. Configure the following settings.

Name	Enter a name for the parameter.
Description	Enter a brief description for this parameter.
In	Currently FortiWeb Cloud only support adding the query parameters in API schema. The path parameters in API schema is not supported yet.

Required	**True:** This parameter is required. If the API request doesn't contain this parameter, it will be detected as a violation. **False:** This parameter is optional.

Schema	Enter the data structure of this parameter. For example:
	`{`
	`"type": "string",`
	`"maxLength": 5,`
	`"minLength": 1`
	`}`
	For more information, refer to Supported parameter and body structure.

7. Click the **body** tab under **Request** section. Check the request body learned by the machine learning model. You can click **Edit** ✎ icon to modify them. For more information, refer to Supported parameter and body structure.
8. Under **Response** section, check the response body to be sent to the client. You can click the **Edit** ✎ icon to modify them. For more information, refer to Supported parameter and body structure.
9. Click **OK**.

Supported parameter and body structure

The parameters and the body schema should follow the API 2.0 specification. Refer to : https://swagger.io/specification/

FortiWeb Cloud supports the following types in parameter:

- boolean
- number
- string
- object (one level)

FortiWeb Cloud supports the following types in body:

- boolean
- number
- string
- array
- object

For the "string" type in parameter and body, the following formats are supported:

- data-time (rfc3339)
- date (rfc3339)
- time (rfc3339)
- email (rfc5322)
- hostname (rfc1034)
- ipv4 (rfc2673)
- ipv6 (rfc2373)

Examples:

```
{
“type”: “string”,
"maxLength": 5,

"minLength": 1,

"pattern": "^(\\([0-9]{3}\\))?[0-9]{3}-[0-9]{4}$"

}
```

```
{

“type”: “string”,

“format” : “email”

}
```

Please note the "format" and "pattern" can be learned by the Schema Protection model, but you can manually add it for the system to validate the API requests against.

```
{

“type”: “number”,

"minimum": 0,

"maximum": 100

}
```

```
{

“type”: “array”,

"items": {

"type": "number"

}

"minItems": 2,

"maxItems": 3

}
```

```
{

“type”: “object”,

"properties": {

"number": { "type": "number" },

"street_name": { "type": "string" }

},

"required": [" number "]

}
```

Combined types in schema are supported. For example:

```
{
"oneOf": [
{ "type": "number"},
{ "type": "string" }
]
}
```

OpenAPI Validation

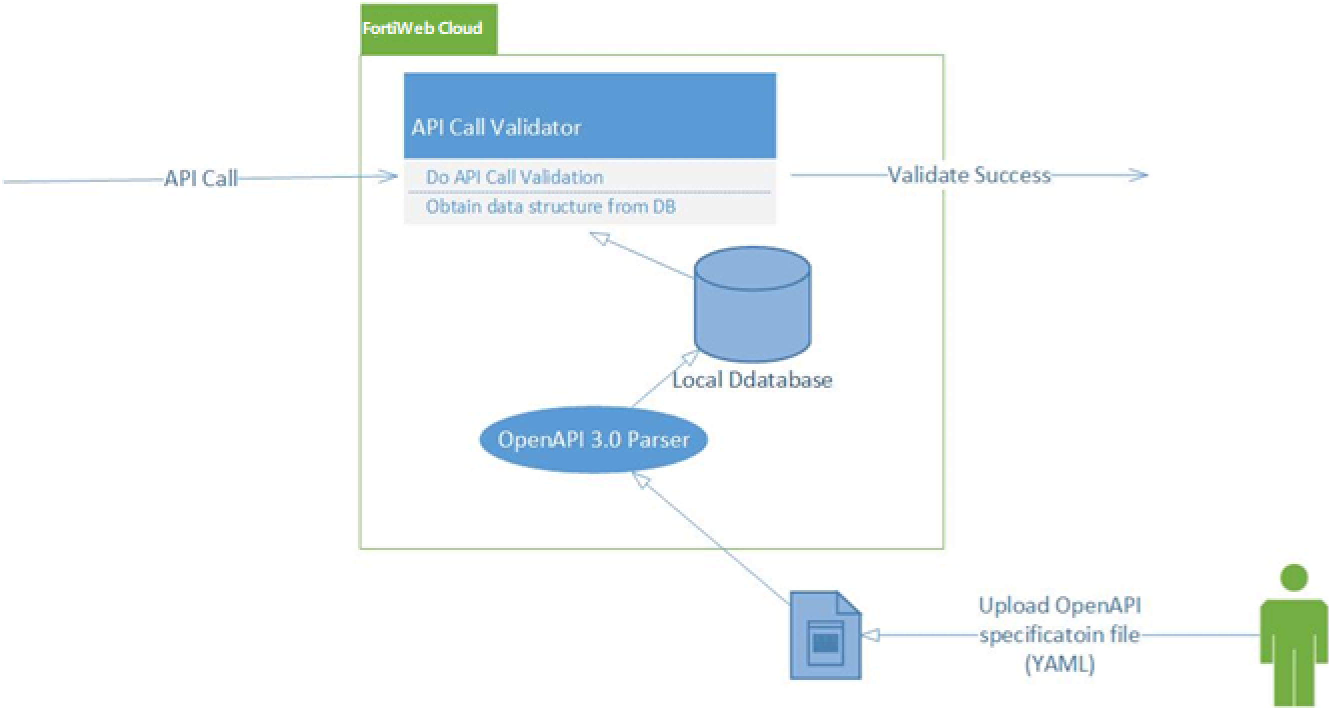
The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs, which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection.

If your API interfaces are implemented using OpenAPI, you can configure an OpenAPI Validation rule, and import a validation file which defines the data structure of the OpenAPI request, such as the request URL, the parameter names in the URL, the value of the parameters (string, integer, etc.), where are parameters submitted (URL, header, body, etc.), and so on.

The validation file specifies the scope for FortiWeb Cloud to scan against. For example, if request URLs are defined in the validation file, FortiWeb Cloud applies OpenAPI Validation rule only to the requests whose URLs match with the ones defined in the validation file, and take actions if they violate the data structure. For those requests whose URLs are not defined in the validation file, FortiWeb Cloud will skip the OpenAPI Validation rule and pass the requests to be scanned against other rules. For use cases, see "OpenAPI Validation" in FortiWeb Administration Guide.

FortiWeb Cloud only supports OpenAPI 3.0.

The figure below shows how FortiWeb Cloud supports OpenAPI.



To configure an OpenAPI Validation rule

1. Go to **API PROTECTION > OpenAPI Validation**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+ Create OpenAPI Validation Rule**.
3. In **Edit OpenAPI Validation Rule** dialog, click **Choose File** to upload a valid OpenAPI file. Make sure the OpenAPI file doesn't contain any structural error, otherwise the OpenAPI Validation Rule will not take effect.

   It is RECOMMENDED you use **Swagger Editor** to generate your OpenAPI file, https://swagger.io/tools/swagger-editor/.

4. Click **OK**.
   The file title, description, server URL information will be listed in the table if any automatically. You can also click ✎ 🗑 🗋 to edit, delete the file, or view the file details.

   You can continue creating at most 10 OpenAPI Validation rules for an application.
5. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

6. Click **SAVE**.

JSON Protection

JSON is a lightweight data-interchange format, and attackers may try to exploit sensitive information in JSON code to attack web servers.

If your API interfaces are implemented using JSON API, you can configure JSON protection rules to define and enforce acceptable JSON content.

To create a JSON protection rule

1. Go to **API Protection > JSON PROTECTION**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Create JSON Protection Rule**.
3. Configure these settings.

Name	Enter a name for the JSON protection rule.
Request URL	Type the URL used to match requests, such as `/upload.php`, or use wildcards to match multiple URLs, such as `/folder1/*` or `/folder1/*/index.htm`. The URL must begin with a slash (/). **Notes:** For those requests whose URLs don't match with the **Request URL**, FortiWeb Cloud will not apply JSON Validation rule on them.
JSON Limits	Enable to use the following default limits for data size, key, and value, etc. • Key size: 512 Bytes • Key number: 1024 • Value size: 10240 Bytes • Value number: 1024 • Value number in array: 1024 • Object depth: 1028
Schema Validation	Enable to import JSON schema files to check JSON contents in HTTP requests. The JSON schema file defines JSON data structure and the valid JSON data contents. Make sure the schema file doesn't contain any structural error, otherwise the JSON Protection Rule will not take effect.
Schema File	Upload an acceptable JSON schema file. Available only when Schema Validation is enabled.

4. Click **OK**.
5. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

6. Click **SAVE**.

XML Protection

XML is commonly used for data exchange, and hackers sometimes try to exploit security holes in XML code to attack web servers. XML Protection examines client requests for anomalies in XML code, and also attempts to validate the structure of XML code in client requests using trusted XML schema files.

If your API interfaces are implemented using XML, you can configure XML protection rules to ensure that the content of XML API requests does not contain any potential attacks.

To create an XML protection rule

1. Go to **API PROTECTION > XML Protection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Create XML Protection Rule**.
3. Configure these settings.

Name	Enter a name for the XML protection rule.
Request URL	Type the URL used to match requests, such as `/upload.php`, or use wildcards to match multiple URLs, such as `/folder1/*` or `/folder1/*/index.htm`. The URL must begin with a slash (/). **Notes:** For those requests whose URLs don't match with the **Request URL**, FortiWeb Cloud will not apply XML Validation rule on them.
XML Limits	Enable to define limits for attributes, CDATA, and elements.
Schema Validation	Enable to import XML schema files to check XML contents in HTTP requests. XML schema files specify the acceptable structure of and elements in an XML document. Make sure the schema file doesn't contain any structural error, otherwise the XML Protection Rule will not take effect.
Schema File	Upload an acceptable XML schema file. Available only when Schema Validation is enabled.
Forbid XML Entities	Enable to configure limits for the XML entities.

4. Click **OK**.
5. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

6. Click **SAVE**.

Mobile API Protection

When a client accesses a web server from a mobile application, the Mobile API Protection module checks whether the request carries the JWT-token header and whether the token carried is valid for the following three cases:

- The request doesn't carry the JWT-token header;
- The request carries the JWT-token header and the token is valid;
- The request carries the JWT-token header and the token is invalid.

Based on the token and request URL, FortiWeb Cloud takes related actions to avoid potential attacks.

1. Go to **API Protection > Mobile API Protection**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Token Secret	Enter the JWT-token secret that you get from the Approov platform. Refer to Approov doc for how to get the token.
Token Header	Indicate the header that carries the JWT-token in the request.
Request URL	Type the URL used to match requests, such as `/upload.php`, or use wildcards to match multiple URLs, such as `/folder1/*` or `/folder1/*/index.htm`. The URL must begin with a slash (/).

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

4. Click **SAVE**.

API Gateway

API Gateway allows to manage API users, verify API keys, control API access and rate limits, as well as rewrite API calls.

Creating API users

You can define API users to restrict access to APIs based on API keys.

1. Go to **API PROTECTION > API Gateway**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **+Create API User**.
3. Configure these settings.

Name	Enter a name that identifies the user.
Email	Type the email address of the user that is used for contact purpose.

Comments	Optionally, enter a description or comments for the user.
Restrict Access IPs	Restrict this API key so that it may only be used from the specified IP addresses. Both single IP addresses or IP ranges are supported. You can enter multiple IP addresses by clicking + .
Restrict HTTP Referers	Restrict this API key so that it may only be used when the specified URLs are present in the Referer HTTP header. This can be used to prevent an API key from being reused on other client-side web applications that don’t match this URL (but note that this does not prevent server-side reuse where the referer could be forged). Now only full URL such as `https://example.com/foo` is supported. You can enter multiple referers by clicking + .

4. Click **OK**.
   You can continue creating multiple API users.

Once the API user is created successfully, an API key and UUID are automatically assigned to this user by FortiWeb Cloud. The API key and UUID can not be changed, while you can append IP or HTTP referer restrictions for this user.

Configuring API gateway rules

To restrict API access, you can configure certain rules involving API key verification, API key carryover, sub-URL setting.

1. Click **+Create API Gateway Rule**.
2. For **Name**, type a name for the API gateway rule.
3. For **Match URL Prefixes**, configure the URL prefixes to be routed to the backend.
   - Enter the Frontend Prefix; the frontend prefix is the URL path in a client call, for example, `/good/`, the URL is like this `https://172.22.14.244/good/example.json?param=value`.
   - Enter the Backend Prefix; the backend prefix is the path which the client request will be replaced with, for example, `/api/v1.0/System/Status/`.
     After the URL rewriting, the URL is like this:
     `https://10.200.3.183:90/api/v1.0/System/Status/example.json?param=value`.

   You can enter multiple URL prefixes, which means multiple URL paths may match the API gateway rule.

4. For **Request Settings**, configure these settings:

API Key Verification	When an user makes an API request, the API key will be included in HTTP header or parameter, FortiWeb Cloud obtains the API key from the request. When this option is enabled, FortiWeb Cloud verifies the key to check whether the key belongs to an valid API user.
API Key In	Indicate where FortiWeb Cloud can find your API key in HTTP request: • HTTP Parameter • HTTP Header Available only when API Key Verification is enabled.
Parameter Name	Enter the parameter name in which FortiWeb Cloud can find the API key when API Key In is HTTP Parameter. Available only when API Key Verification is enabled.
Header Field Name	Enter the header filed name in which FortiWeb Cloud can find the API key when API Key In is HTTP Header. Available only when API Key Verification is enabled.
Allow Users	Select API users created to define which users have the persmission to access the API. Available only when API Key Verification is enabled.
Rate Limit	Type the number of API call requests in certain time period.
Requests in	Type the time period during which the API call requests are made.

5. Click **OK**.

Configuring actions

1. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked. The default blocking period is 10 minutes. You can configure this value according to your own needs.

2. Click **SAVE**.

Account Takeover

Account takeover feature allows you to detect and protect against account takeover threats. FortiWeb Cloud tracks the authentication URL to your website and identifies all user access. Attack logs will reference the username and additional protection capabilities such as Credential Stuffing Protection and Session Fixation Protection.

FortiWeb Cloud uses a user tracking rule to track users. When FortiWeb Cloud detects users that match the criteria you specify in the user tracking rule, it stores the session ID and username.

FortiWeb Cloud tracks only users who have logged in successfully. It uses one of the following methods to determine whether a log in is successful:

- The response matches a condition you specify in the user tracking rule, such as a return code, a specific redirect URL or a string in the response body. You create these conditions in Authentication Successful Condition on page 178.
- If the response does not match a condition in Authentication Successful Condition on page 178, FortiWeb Cloud uses the default results `failed`.

FortiWeb Cloud stops tracking users when either of the following two events occur:

- The client request contains the log off URL that you specify in the user tracking rule. (The log off URL setting is optional.)
- The session is idle for longer than the session timeout value `14400 seconds`.

To configure a user tracking rule

1. Go to **ACCOUNT TAKEOVER**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Configure these settings.

Authentication URL	Enter the URL to match in authorization requests. Ensure that the value begins with a forward slash (/).
Log Off URL	Optionally, enter the URL of the request that a client sends to log out of the application. When the client sends this URL, FortiWeb Cloud stops tracking the user session. Ensure that the value begins with a forward slash (/).
Username Field	Enter the username field value to match in authorization requests.
Password Field	Enter the password field value to match in authorization requests.
Session ID Name	Type the name of the session ID that is used to identify each session. Examples of session ID names are `sid, PHPSESSID`, and `JSESSIONID`.
Authentication Successful Condition	
Return Code	Enter the value of the return code when the authentication is successful. It should be a regular expression.
Redirect URL	Enter the redirect URL when the authentication is successful. It should be a regular expression.

Response Body	The response body when the authentication is successful. It should be a regular expression.
Credential Stuffing Protection	Enable to use FortiGuard's Credential Stuffing Defense database to prevent against Credential Stuffing attacks. When this setting is enabled, FortiWeb Cloud will evaluate the username (Username Field) and password (Password Field) of the matched login requests against the Credential Stuffing Defense database to identify whether the paired username/password has been spilled.
Session Fixation Protection	Enable to configure FortiWeb Cloud to erase session IDs from the cookie and argument fields of a matching login request. FortiWeb Cloud erases the IDs for non-authenticated sessions only. For web applications that do not renew the session cookie when a user logs in, it is possible for an attacker to trick a user into authenticating with a session ID that the attacker acquired earlier. This feature prevents the attacker from accessing the web app in an authenticated session. When this feature removes session IDs, FortiWeb Cloud does not generate a log message because it is very common for a legitimate user to access a web application using an existing cookie. For example, a client who leaves his or her web browser open between sessions presents the cookie from an earlier session.

3. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
   To configure the actions, you must first enable the **Advanced Configuration** in **Global > System Settings > Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).

4. Click **SAVE**.

Application Delivery

You can configure FortiWeb Cloud to rewrite URLs and headers to prevent the disclosure of underlying technology or website structures to HTTP clients; the Caching and Compression feature can help you improve performance of your back-end network and servers by reducing their traffic and processing load.

- Rewriting Requests
- Caching and Compression
- Waiting Room

Rewriting Requests

Rewriting URLs and headers allows changing the structure of the request from clients before forwarding them to the web application.

Some web applications need to know the IP address of the client where the request originated in order to log or analyze it. Thus, you need to enable FortiWeb Cloud to add or append to an `X-Forwarded-For:` or `X-Real-IP:` header. The web server can instead use this HTTP-layer header to find the public source IP and path of the IP-layer session from the original client.

To configure **Rewriting Requests**, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

Add X-Forwarded-For	Enable to include the `X-Forwarded-For:` HTTP header in requests forwarded to your web servers. If the HTTP client or web proxy does not provide the header, FortiWeb Cloud adds it, using the source IP address of the connection. If the HTTP client or web proxy already provides the header, it appends the source IP address to the header's list of IP addresses. This option can be useful if your web servers log or analyze clients’ public IP addresses, if they support the `X-Forwarded-For:` header. If they do not, disable this option to improve performance.
Add Source Port	If enabled, the `X-Forwarded-For:` header will record the connection's source port as well as the source IP.
Add X-Forwarded-Port	If enabled, an `X-Forwarded-Port:` header will be added to record the connection's original destination port.
Add X-Real-IP	Enable to include the `X-Real-IP:` HTTP header on requests forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any, see Add X-Forwarded-For. Like `X-Forwarded-For:`, this header is also used by some proxies and web servers to trace the path, log, or analyze based upon the packet’s original source IP address.
Use X-Header to Identify Original Client's IP	If you have a front-end load balancer or proxy, enable this option to derive the original clients’ IP from the X-Header, rather than from the connection's source IP. FortiWeb Cloud will detect violations and report logs based on the IP derived from X-Header.

To configure a rewriting rule

1. Go to **APPLICATION DELIVERY > Rewriting Requests**.
2. Click **+Add Rule**.
3. Configure these settings.

Name	Type a name that can be referenced by other parts of the configuration.
Action	Select the item that this rule will rewrite HTTP requests from clients. • Rewrite Host Rewrite the `Host:` field in the header of an HTTP request.

	• Rewrite URL Rewrite the URL line in the header of an HTTP request. • Rewrite Referer Rewrite the `Referer:` field in the header of an HTTP request. • Insert Header In Header Name and Header Value, insert the name of the header field that you want to insert to a request, and the value of the header field accordingly. • Redirect URL (301 Permanently) Type a URL, such as /catalog/item1, to which a client will be redirected to. It is used in the `301 Moved Permanently` response. • Redirect Host (301 Permanently) Type either a host name or IP address (e.g. http://store.example.com or https://2.2.2.2), to which a client will be redirected. It is used in the `301 Moved Permanently` response. **Note:** Only literal form is supported for the **Rewrite/Redirect To** field, but regular expression is supported for the **Rewrite/Redirect From** field. For example, the following configuration can redirect "a.com" to "www.a.com": • **Redirect From:** ^a\.com$ • **Redirect To:** https://www.a.com To achieve the opposite effect, you can use the following configuration to redirect from "www.a.com" to "a.com", excluding the "www": • **Redirect From:** ^www\.a\.com$ • **Redirect To:** https://a.com For both examples above, the Action would be set to "Rewrite Host".
Action: Rewrite HTTP Header Advanced	This action enables FortiWeb Cloud to rewrite HTTP header when multiple conditions are met. **Rewriting Condition:** Specify one or more conditions that the HTTP request must match. The conditions are in an "AND" relationship. • Match Host: Enter the value of the `Host:` field to match. • Match URL: Enter the URL to match. • Match Referer: Enter the value of `Referer:` field to match. • Protocol Filter: Select the protocol if you want to restrict the condition only for either HTTP or HTTPS. **Rewriting Behavior:** Replace the corresponding elements in HTTP request with the values specified below. Multiple behaviors will be applied as specified. • Rewrite Host: Enter the `Host:` value to replace with. • Rewrite URL: Enter the URL to replace with. • Rewrite Referer: Enter the value of `Referer:` field to replace with. • Insert Header: Enter the header name and value to insert into the HTTP request. • Remove Header: Remove the header from HTTP request.

Action: Redirect Advanced (301 Permanently)	This action enables FortiWeb Cloud to redirect HTTP request when multiple conditions are met. **Rewriting Condition:** Specify one or more conditions that the HTTP request must match. The conditions are in an "AND" relationship. • Match Host: Enter the value of the `Host:` field to match. • Match URL: Enter the URL to match. • Match Referer: Enter the value of `Referer:` field to match. • Protocol Filter: Select the protocol if you want to restrict the condition only for either HTTP or HTTPS. **Rewriting Behavior:** Redirect the request to the specified location when the above conditions are met. • Rewrite Location: The location can be a URL, a host name, or an IP address.
URL Translation	Enable it to keep the URL path while redirecting clients to a new host or IP address in a “301 Permanently” response. For example, clients visiting "www.aaa.com/test.html" can be redirected to "www.bbb.com/test.html". Available only if the action is **Redirect Host (301 Permanently)**.
Protocol Filter	Enable if you want to match this condition only for either HTTP or HTTPS. For example, you could redirect clients that accidentally request the login page by HTTP to a more secure HTTPS channel—but the redirect is not necessary for HTTPS requests. As another example, if URLs in HTTPS requests should be exempt from rewriting, you could configure the rewriting rule to apply only to HTTP requests.
Protocol	Select which protocol will match this condition, either **HTTP** or **HTTPS**. This option appears only if **Protocol Filter** is enabled.

4. Click **OK**.
   You can continue creating at most 12 rewriting rules for an application. Please be aware that the rules operate under "OR" conditions. This implies that FortiWeb Cloud will process the request based on the first matching rule, subsequently forwarding the request to the next scan.

Caching and Compression

To improve performance of your back-end network and servers by reducing their traffic and processing load, you can configure FortiWeb Cloud to cache and compress responses from your servers.

To configure **Caching and Compression**, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

⚠ When enabling caching make sure you correctly configured the web server’s no-cache/no-store directives to avoid caching sensitive data.

1. Configure these settings.

Default Cache Timeout	Type the time to live for each entry in the cache. Expired entries will be removed. A subsequent request for the URL will cause FortiWeb Cloud to forward the request to the server in order to cache the response again. Any additional requests will receive FortiWeb Cloud's cached response until the URL's cache timeout occurs.
Allow HTTP Method	Select whether to cache the response contents according to the HTTP method you use. • GET, HEAD (Recommended) • GET, HEAD, OPTIONS • GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
Allow Return Code	Select whether to cache the response contents according to the response code. • 200 (Recommended) • 200, 206 • 200, 206, 301, 302
Allow File Type	Select whether to cache the response contents according to the content type. • Text • Picture • Media • Binary • Other
Key Generation Factor	Select the protocol variable that you want to use to generate the cache key. • Method, such as GET, POST, HEAD, etc. • Protocol, the string can be either "http://" or "https://"; • Host • URL • Arguments, for example in request `http://host.com/test.php?a=1&b=2` , the Arguments string is "`a=1&b=2`". • Cookies—Once you have created a web cache rule, you can edit the rule to indicate cookies in HTTP requests and append them to the key string to generate the cache key.

2. Click **Create New** to configure the URLs not to be cached.
3. Configure these settings.

HTTP Method	Select the HTTP method in which the request URL is included.
URL Expression	Enter a regular expression, such as `^/*.php`, matching the sub URLs to which the rule should apply. The pattern does not require a slash (`/`), but it must match sub URLs that begin with a slash, such as `/index.cfm`. For details, see "Regular expression syntax" on page 1.

Bypass Arguments	Enable this option and enter the argument name so that the request matches the bypass URL only when the request brings the specific arguments.
Bypass Cookies	Enable this option and enter the cookie name so that the request matches the bypass URL only when the request brings the specific cookies.

4. Click **OK**. You can continue creating multiple Bypass Sub URL lists.
5. Enable **Compression** to completely offload compression to FortiWeb Cloud to save resources on your web servers.
6. Select the content types that you want to compress. Click **Change**, select the content type, and then click the right arrow (**->**) to move them to the **Allow Content Types** list.
7. Click **SAVE**.

You can click the **Clear Cache** button at the top right corner of the page to clear the responses cached on FortiWeb Cloud.

What can be cached?

Caching generally works best with data that doesn't change. Things like static web pages, images, movies, and music all typically work well.

When content changes often, caching provides overhead by consuming RAM without its usual benefit of reduced latency. Some HTTP headers and other factors indicate dynamic content which FortiWeb Cloud will not cache.

FortiWeb Cloud will not cache responses if the request:

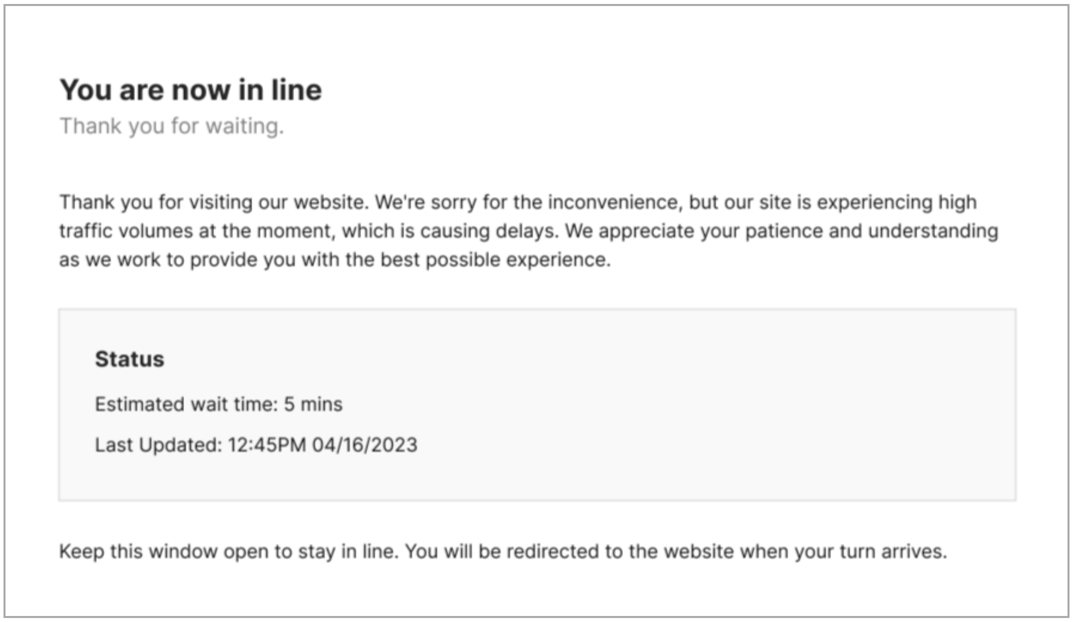
- Has fields such as `Cache-Control: no-cache/no-store/`; `Pragma:no-cache`
- Contains the header:
  - `Authorization`
  - `Proxy-Authorization`

FortiWeb Cloud will not cache if the response:

- Has a Set-Cookie: field
- Has a Vary: field
- Has fields such as `Cache-Control: no-cache/no-store/private; Pragma:no-cache; Cache-Control: max-age=0`
- Contains the header:
  - `Proxy-Authorization`
  - `Connection`
  - `Keep-Alive`
  - `Proxy-Authenticate`
  - `TE`
  - `Trailers`
  - `Transfer-Encoding`
  - `Upgrade`

Waiting Room

To manage visitor traffic and avoid server overload delays, you can enable a virtual holding space and queuing system, allowing new users to enter a Waiting Room where they can view estimated wait times before accessing your application.



You are now in line

Thank you for waiting.

Thank you for visiting our website. We're sorry for the inconvenience, but our site is experiencing high traffic volumes at the moment, which is causing delays. We appreciate your patience and understanding as we work to provide you with the best possible experience.

Status

Estimated wait time: 5 mins

Last Updated: 12:45PM 04/16/2023

Keep this window open to stay in line. You will be redirected to the website when your turn arrives.

This feature may be configured for your entire website, or specific URL paths.

Before you configure Waiting Room, you must have already enabled this module in **Add Modules**. See How to add or remove a module.

Overview

Waiting room's **Overview** tab highlights key traffic insights for your application.

Total Active Users	The total number of users accessing your application.
New Users	The number of users joining your application at one time.
Total Waiting Users	The number of users currently in the Waiting Room.
Estimated Waiting Time	The length of time a new user is expected to wait before accessing your application.

You have the option to configure the time period for each graph of the above values, allowing you to select from the last hour, the last 24 hours, or the last 7 days.

Use the displayed information to make adjustments and optimize your configured settings for the Waiting Room feature.

Settings

To configure Waiting Room Settings:

1. Go to **Application Delivery > Waiting Room > Settings** and toggle the switch ON.
2. Configure these settings:

   Please note, you are required to configure at least one of **Total Active Users** and **New Users Per Minute**. In addition, **Path** and **Maximum Idle Time** cannot be empty.

Total Active Users	Control the size of traffic accessing your application. When enabled, if the number of active users reaches the configured value, additional users will enter the Waiting Room.
New Users per Minute	Prevent your application from being flooded by new users in a short time span. When enabled, if the number of new users per minute reaches the configured value, additional users will enter the Waiting Room.
Path	The waiting room will only be enabled for the configured URL. Use /.* to match all. Path can be an exact string, wildcard, or regular expression. It is also case sensitive. This value cannot be empty.
Maximum Idle Time	Users who have remained idle for the configured time will be considered as a new user. Users who have ended and restarted the session will also be considered as a new user. This value cannot be empty.
Bypass Rules	Allow users with certain IP addresses to access your application directly, even if they trigger the above limiting conditions. Click **Create New** and enter an IP address or range in the **Value** field to configure a new Bypass rule.

3. Click **SAVE**.

Global Trustlist

You can configure FortiWeb Cloud to ignore scanning parameters specified for modules of signature based detection, syntax based detection, and anomaly detection across the entire application.

1. Go to **SECURITY RULES > Global Trustlist**.
   You must have already enabled this module in **Add Modules**. See How to add or remove a module.
2. Click **Create New**.
3. Configure these settings.

Parameter Name	Enter a unique name for the parameter as it appears in the URL or HTTP body.
Request Status	Optionally, you can enable to indicate a regular expression designed to match multiple URLs, which carry the trustlist parameters.

Request URL	Specify a URL value to match, such as `^/*.php`, which matches requests for `http://www.test.com/^/*.php`. The pattern does not require a slash (/); however, it must at match URLs that begin with a slash, such as `/index.cfm`. See Frequently used regular expressions on page 237. Do not include a domain name because it's by default the domain name of this application.

4. Click **OK**.

   In the global trustlist table, you can click buttons in ✎ ✖ 🗑 to edit, or delete the parameter rule; also, you can choose to enable or disable to indicate the URL to match.

Vulnerability Scan

The Vulnerability Scan module helps identify OWASP Top 10 flaws in web applications. You can get a comprehensive report with remediation recommendations to protect your web applications.

You now have the option to subscribe to the Vulnerability Scan service with a monthly plan on AWS, Azure, and Google Cloud.

By default, the Vulnerability Scan report is based on your current WAF configuration. It highlights the vulnerabilities that are still exposed to attackers given the existing configuration, so that you can fine tune the WAF settings to strengthen the security.

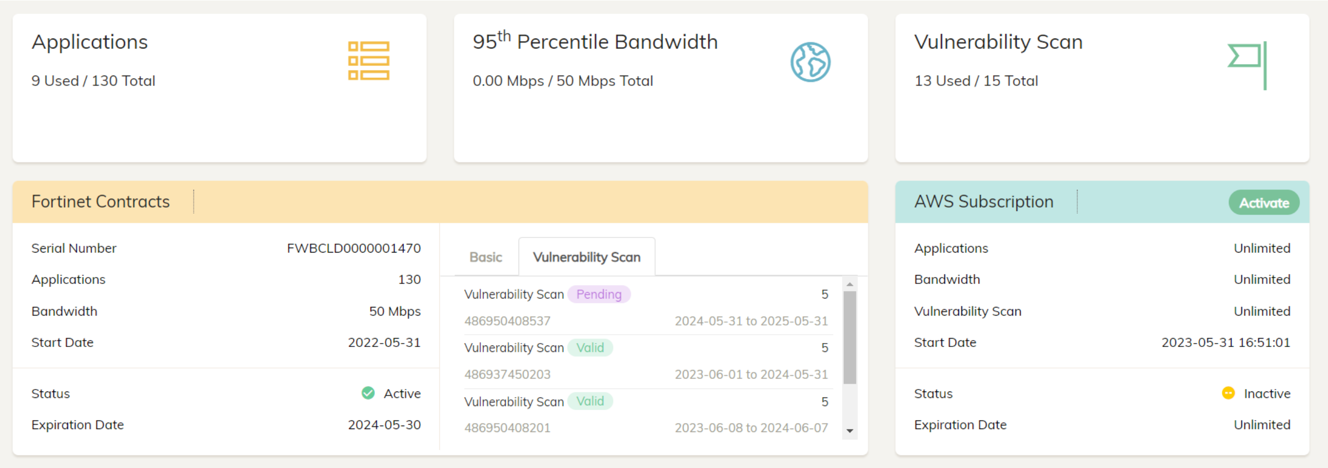
However, if you want to check out the vulnerabilities assuming the protection from FortiWeb Cloud was off, you can enable the **Bypass WAF** option at the top right corner of the **Vulnerability Scan** page. Please note this option is only available when the **Advanced Configuration** on the **Global > System Settings > Settings** page is switched on.

To add applications for vulnerability Scan:

1. Go to **Vulnerability Scan**.
2. Click **Create New**.
3. In **Add Asset** window, select the **FQDN** and **Port**. These are the domain names and port numbers you have defined in **Network > Endpoints**.
4. Click **OK**.

The maximum number of applications allowed are defined in your contracts. You can check it in **Global > System Settings > Contracts**.

In the following screenshot, "0/5" means you can add at most 5 applications across all applications, while 0 seat is available now.



Applications
9 Used / 130 Total

95th Percentile Bandwidth
0.00 Mbps / 50 Mbps Total

Vulnerability Scan
13 Used / 15 Total

Fortinet Contracts

Serial Number	FWBCLD0000001470
Applications	130
Bandwidth	50 Mbps
Start Date	2022-05-31
Status	Active
Expiration Date	2024-05-30

Basic | Vulnerability Scan

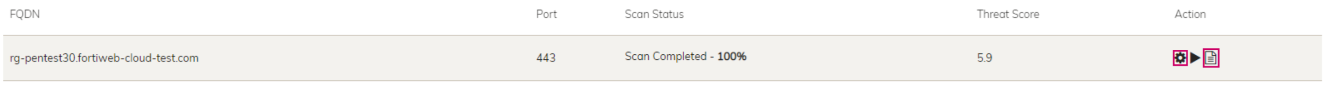
Vulnerability Scan Pending	5
486950408537	2024-05-31 to 2025-05-31
Vulnerability Scan Valid	5
486937450203	2023-06-01 to 2024-05-31
Vulnerability Scan Valid	5
486950408201	2023-06-08 to 2024-06-07

AWS Subscription — Activate

Applications	Unlimited
Bandwidth	Unlimited
Vulnerability Scan	Unlimited
Start Date	2023-05-31 16:51:01
Status	Inactive
Expiration Date	Unlimited

To configure and view the vulnerability report:

Click the **Settings** button to configure scanning settings and the **Reports** button to view the reports. For more information, check FortiDAST User Guide: https://docs.fortinet.com/product/FortiDAST



FQDN	Port	Scan Status	Threat Score	Action
rg-pentest30.fortiweb-cloud-test.com	443	Scan Completed - **100%**	5.9	

To configure your Vulnerability Scan subscription from a public cloud marketplace:

Go to **Global > System settings > Contracts**.

Billing

The billing cycle for Vulnerability Scan occurs monthly, and you will be charged on the date you initially add an application and subsequently on the same date each month. For instance, if you add an application on May 1st, your next billing date will be June 1st. If you happen to remove the application on May 15th and then re-add it on May 20th, you will be charged once at the time of re-adding the application. Following this, your next billing date will be on June 20th.

Please note that Vulnerability Scan seats are nontransferable. Removing applications does not open a seat in your contract that can be replaced with a different application.

FortiView

FortiWeb Cloud detects attacks to your application and displays the threats in FortiView in the following categories:

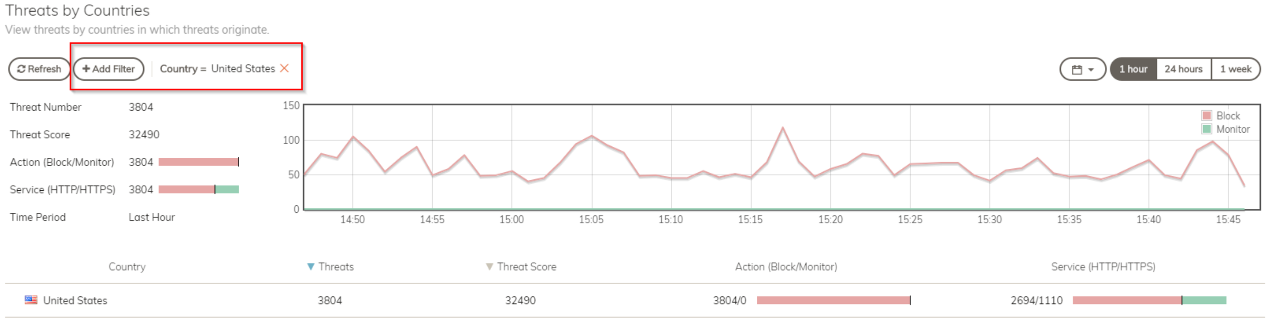
- **Threat by OWASP TOP10:** Displays threats by OWASP top10 to analyze the 10 most critical attacks targeted to your application.
- **Threats by Types:** Displays threats in specific types, such as Known Attacks, Information Leakage, etc.
- **Blocked IPs:** Displays IP addresses that have been blocked for security reasons, either by your application's security policy or by actions triggered by other applications that caused the load balancers to block them. See detailed instructions to Review and release blocked IP addresses on page 191 below.
- **Threat by Source IPs:** Displays threats by source IP to provide a deep insight in the IP addresses from which attacks originate.
- **Threats by Countries:** Displays threats by countries in which attacks originate.
- **Threat Map:** Displays threats by geographic region. You can see a global map that shows threats in real-time from specific countries.
- **Traffic Summary**: Displays traffic statistics such as source IP addresses, URL, User Agent, Return Code, and Request Method.

You can see the overview of the threats, such as the total number of threats, threat scores, the types of actions FortiWeb Cloud carries out in response to specific types of attacks, and how severe attacks are.

You can also drill down from a high-level overview to a detailed analysis of particular threat. Below is an example using the **Threats by Countries** menu to illustrate how the filtering and drilling down process works.

To view the detailed analysis of a particular threat:

1. Go to **FortiView > Threats by Countries**.
2. Click **Add Filter**, select **Country**, and either enter the name of the country or select the country from the drop-down menu. In this case, United States is selected.



Threats by Countries

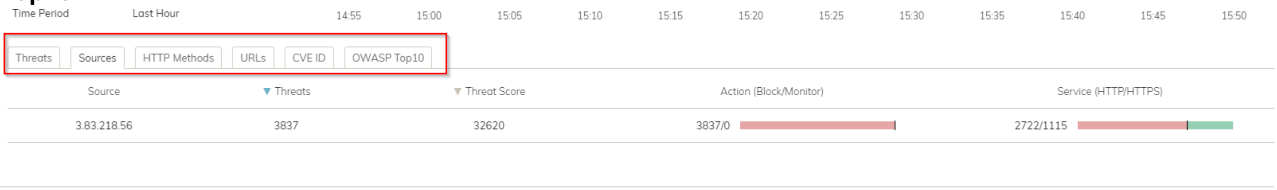
View threats by countries in which threats originate.

Country = United States

Threat Number	3804
Threat Score	32490
Action (Block/Monitor)	3804
Service (HTTP/HTTPS)	3804
Time Period	Last Hour

Country	▼ Threats	▼ Threat Score	Action (Block/Monitor)	Service (HTTP/HTTPS)
United States	3804	32490	3804/0	2694/1110

3. Double-click the country row to view a summary of the threat data from this country.
4. Select tabs to view the threat data categorized by **Threats**, **Sources**, **HTTP Methods**, **URLs**, **CVE ID**, and **OWASP Top10**.

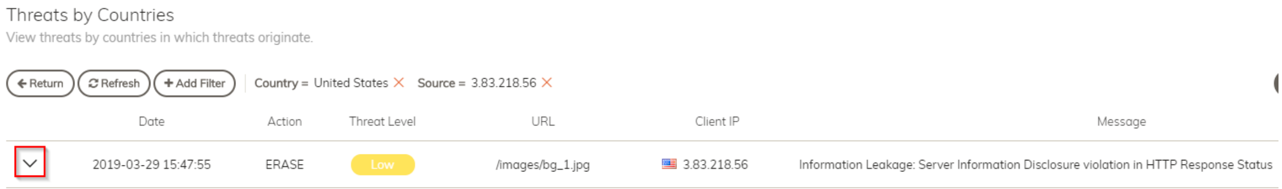


Time Period Last Hour

Source	▼ Threats	▼ Threat Score	Action (Block/Monitor)	Service (HTTP/HTTPS)
3.83.218.56	3837	32620	3837/0	2722/1115

5. In this example, we double click the row of 3.83.218.56 to view the threats originated from this source IP address.

6. Click the arrow icon to unfold the detailed analysis of a particular threat.



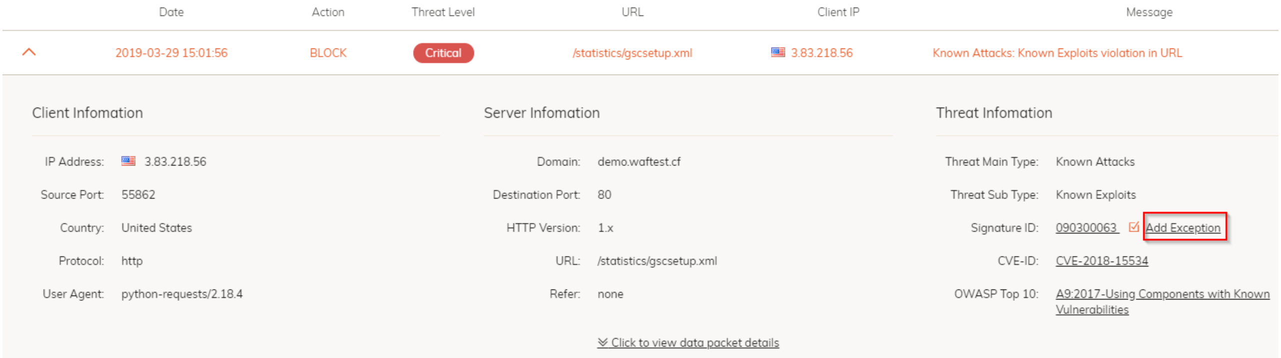
Threats by Countries

View threats by countries in which threats originate.

Country = United States ✕ Source = 3.83.218.56 ✕

Date	Action	Threat Level	URL	Client IP	Message
2019-03-29 15:47:55	ERASE	Low	/images/bg_1.jpg	3.83.218.56	Information Leakage: Server Information Disclosure violation in HTTP Response Status

7. If you know that certain URL tends to falsely trigger violations by matching an attack signature during normal use, you can click **Add Exception** beside the signature ID. The traffic to that URL will not be treated as an attack even if it matches this particular signature.



Date	Action	Threat Level	URL	Client IP	Message
2019-03-29 15:01:56	BLOCK	Critical	/statistics/gscsetup.xml	3.83.218.56	Known Attacks: Known Exploits violation in URL

Client Infomation

IP Address: 3.83.218.56
Source Port: 55862
Country: United States
Protocol: http
User Agent: python-requests/2.18.4

Server Infomation

Domain: demo.waftest.cf
Destination Port: 80
HTTP Version: 1.x
URL: /statistics/gscsetup.xml
Refer: none

Threat Infomation

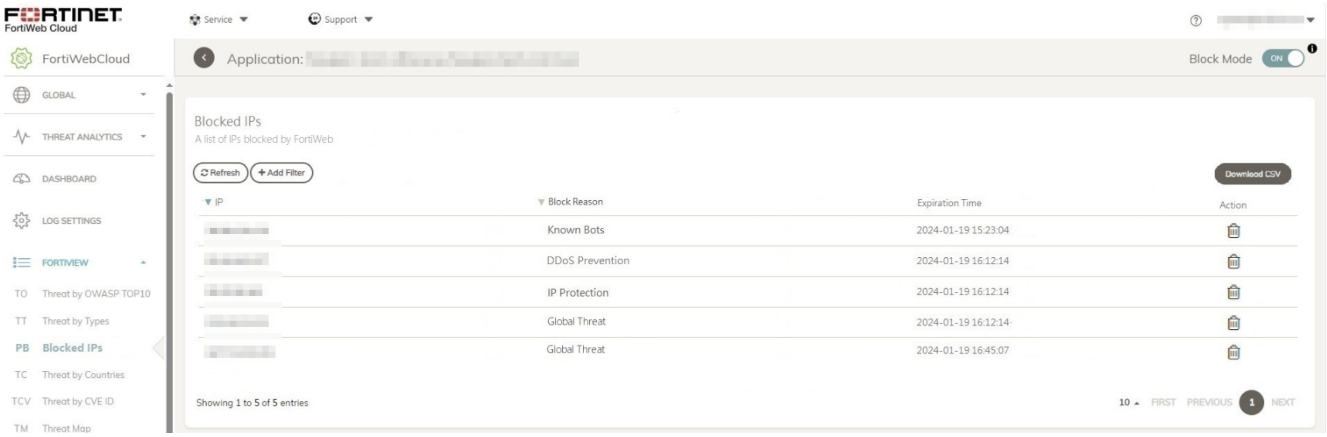
Threat Main Type: Known Attacks
Threat Sub Type: Known Exploits
Signature ID: 090300063 Add Exception
CVE-ID: CVE-2018-15534
OWASP Top 10: A9:2017-Using Components with Known Vulnerabilities

Please note that the number of attacks displayed in Attack Logs, FortiView , and Blocked Requests widget on Dashboard are slightly different.

- Certain attack types such as Bot and DDoS attacks generate a large amount of requests in a short time. To prevent numerous identical attack logs flooding the UI, FortiWeb Cloud only logs the first request in Attack Logs and FortiView , while it shows the actual count in Blocked Requests Widget so you can know how many actual attack requests were blocked.
- To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such items are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget.
- If you have set FortiWeb Cloud to block attacks but do not generate a log when certain violation occurs, such as Deny(no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget.

Review and release blocked IP addresses

This page displays the list of IP addresses that have been blocked by FortiWeb Cloud, either by your application's security rules or by actions triggered by other applications that caused the load balancers to block them.



Blocked IPs

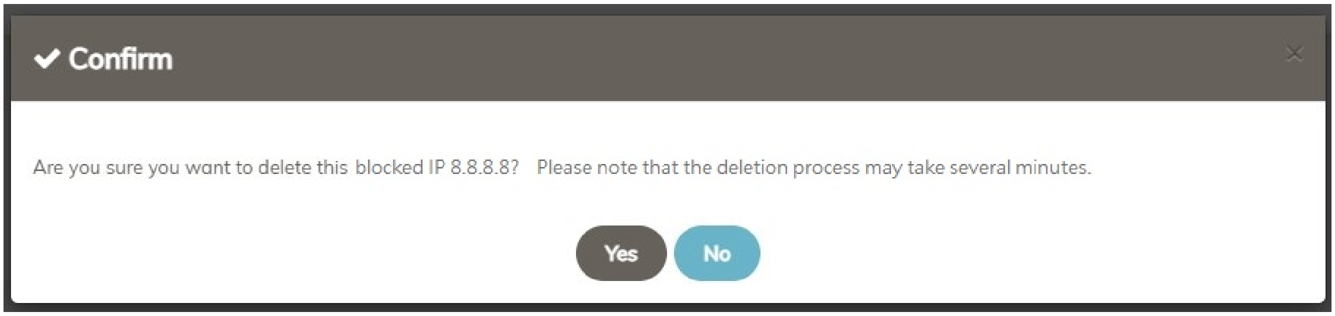
A list of IPs blocked by FortiWeb

IP	Block Reason	Expiration Time	Action
[redacted]	Known Bots	2024-01-19 15:23:04	🗑
[redacted]	DDoS Prevention	2024-01-19 16:12:14	🗑
[redacted]	IP Protection	2024-01-19 16:12:14	🗑
[redacted]	Global Threat	2024-01-19 16:12:14	🗑
[redacted]	Global Threat	2024-01-19 16:45:07	🗑

Showing 1 to 5 of 5 entries

When searching for a specific IP address on this list, you can click **Add Filter** to narrow down the number of IP addresses displayed on this page.

To remove an item from this list, click on the delete icon 🗑 in the same row as the desired IP address to effectively unblock it.



Are you sure you want to delete this blocked IP 8.8.8.8? Please note that the deletion process may take several minutes.

Using FortiWeb Cloud with DevOps tools

FortiWeb Cloud supports DevOps tools including Terraform, Jekins, and Ansible to provide more ways to efficiently deploy, manage, and automate application security. You can use DevOps tools to automatically onboard or delete applications from FortiWeb Cloud. You can also change the IP list in IP Protection using Ansible.

Configuring FortiWeb Cloud with Terraform

The following example demonstrates how to use the Terraform FortiWeb Cloud provider to perform simple configuration changes on FortiWeb Cloud. It requires the following:

- FortiWeb Cloud 20.2.d or later
- FortiWeb Cloud Provider: This example uses terraform-provider-fortiwebcloud 1.0.0.
- Terraform: This example uses Terraform 0.12.26.
- Download the template from Github repository: https://github.com/fortinet/fortiwebcloud-terraform

To configure FortiWeb Cloud with Terraform Provider module support:

1. Download the *terraform-provider-fortiwebcloud* to your local directory "~/.terraform.d/plugins".
2. Create a new file with the .tf extension for configuring your FortiWeb Cloud:

   ```
   $touch main.tf

   $ ls

   main.tf
   ```

3. Edit the main.tf Terraform configuration file:
   In this example, you may connect the FortiWeb Cloud API gateway and provide your username/password which have write privilege on FortiWeb Cloud. You can also use API Key to authenticate if you have created one in **Global > System Settings > Settings**. Your provider information may like this:

   ```
   provider "fortiwebcloud" {

     hostname   = "api.fortiweb-cloud.com"

   api_token = "specify you API key Secret value" #specify this parameter only when you
   choose API Key authentication#

   username   = "your username" #specify this parameter only when you choose username
   authentication#

   password   = "your password" #specify this parameter only when you choose username
   authentication#

   }
   ```

4. Create the resources for onboarding your application. Specify your application name, domain name, and served service.

   ```
   resource "fortiwebcloud_app" "app_example" {
   ```

```
  app_name = "from_terraform"
  domain_name = "www.example.com"
  app_service = {
    http= 80
    https= 443
  }
  origin_server_ip = "93.184.216.34"
  origin_server_service = "HTTPS"
  block = false
}
```

5. Save your Terraform configuration file.
6. In the terminal, enter terraform init to initialize the working directory.

```
$ terraform init
Initializing the backend...
Initializing provider plugins...
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see any
changes
that are required for your infrastructure. All Terraform commands should now work.

If you ever set or change modules or backend configuration for Terraform, rerun this
command to reinitialize your working directory. If you forget, other commands will
detect it and remind you to do so if necessary.
```

7. Run `terraform -v` to verify the version of the loaded provider module:

```
$ terraform -v
Terraform v0.12.26
+ provider.fortiwebcloud v1.0.0
```

8. Enter `terraform plan` to parse the configuration file and read from the FortiWeb Cloud configurations to see what Terraform changes:
   This example onboards an application to FortiWeb Cloud.

```
$ terraform plan
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.
------------------------------------------------------------------------
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
```

```
+ create
Terraform will perform the following actions:
# fortiwebcloud_app.app_example will be created
+ resource "fortiwebcloud_app" "app_example" {
+ app_name               = "from_terraform"
+ app_service            = {
+ "http"  = 80
+ "https" = 443
}
+ block                  = false
+ cdn                    = false
+ cname                  = (known after apply)
+ domain_name            = "www.example.com"
+ ep_id                  = (known after apply)
+ id                     = (known after apply)
+ origin_server_ip       = "93.184.216.34"
+ origin_server_port     = 443
+ origin_server_service = "HTTPS"
}
Plan: 1 to add, 0 to change, 0 to destroy.
------------------------------------------------------------------------
Note: You didn't specify an "-out" parameter to save this plan, so Terraform
can't guarantee that exactly these actions will be performed if
"terraform apply" is subsequently run.
```

9. Enter `terraform apply` to continue the configuration:

```
$ terraform apply
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
+ create
Terraform will perform the following actions:
# fortiwebcloud_app.app_example will be created
+ resource "fortiwebcloud_app" "app_example" {
+ app_name               = "from_terraform"
+ app_service            = {
+ "http"  = 80
```

```
    + "https" = 443
    }
    + block                 = false
    + cdn                   = false
    + cname                 = (known after apply)
    + domain_name           = "www.example.com"
    + ep_id                 = (known after apply)
    + id                    = (known after apply)
    + origin_server_ip      = "93.184.216.34"
    + origin_server_port    = 443
    + origin_server_service = "HTTPS"
    }
    Plan: 1 to add, 0 to change, 0 to destroy.

    Do you want to perform these actions?
    Terraform will perform the actions described above.
    Only 'yes' will be accepted to approve.

    Enter a value: yes

    fortiwebcloud_app.app_example: Creating...
    fortiwebcloud_app.app_example: Creation complete after 4s [id=from_terraform]

    Apply complete! Resources: 1 added, 0 changed, 0 destroyed.
```

The application is now onboarded on FortiWeb Cloud.

To delete the application, enter `terraform destroy` to delete the configuration from FortiWeb Cloud.

```
$ terraform destroy
fortiwebcloud_app.app_example: Refreshing state... [id=from_terraform]

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
- destroy

Terraform will perform the following actions:
# fortiwebcloud_app.app_example will be destroyed
- resource "fortiwebcloud_app" "app_example" {
```

```
- app_name               = "from_terraform" -> null
- app_service            = {
- "http"  = 80
- "https" = 443
} -> null
- block                  = false -> null
- cdn                    = false -> null
- domain_name            = "www.example.com" -> null
- id                     = "from_terraform" -> null
- origin_server_ip       = "93.184.216.34" -> null
- origin_server_port     = 443 -> null
- origin_server_service = "HTTPS" -> null
}

Plan: 0 to add, 0 to change, 1 to destroy.

Do you really want to destroy all resources?
Terraform will destroy all your managed infrastructure, as shown above.
There is no undo. Only 'yes' will be accepted to confirm.

Enter a value: yes

fortiwebcloud_app.app_example: Destroying... [id=from_terraform]
fortiwebcloud_app.app_example: Destruction complete after 3s

Destroy complete! Resources: 1 destroyed.
```

For now, modify operation isn't supported. You can modify the application via GUI/API.

Configuring FortiWeb Cloud with Ansible

The following example demonstrates how to use Ansible to perform simple configuration changes on FortiWeb Cloud. It requires the following:

- FortiWeb Cloud 20.2.d or later
- Ansible: This example uses Ansible 2.9.
- Download the template from Github repository: https://github.com/fortinet/fortiwebcloud-ansible

To perform configuration changes with Ansible, prepare the following files:

1. Create the `hosts` inventory file to specify FortiWeb Cloud host and the authentication information.

   Username/password authentication

   If you use username/password authentication, specify them as shown below.

   ```
   [fortiwebcloud] fortiwebcloud01 ansible_host="api.fortiweb-cloud.com" ansible_user="example@example.com" ansible_password="Your Password"
   [fortiwebcloud:vars] ansible_network_os=fortinet.fortiwebcloud.fortiwebcloud
   ```

   API key authentication

   If you have created an API Key in **Global > System Settings > Settings**, specify the key in `hosts` file as shown below, so that you can use the API key instead of specifying the username and password.

   ```
   fortiwebcloud_api_token="API_key"
   ```

   In the configuration files, add the following line to refer to the API key. Here we take the `cloudwaf_app_sni_cert_get.yml` file the as an example:

   ```
   ---


   - hosts: fortiwebcloud01
     name: Execute cloud api
     collections:
       - fortinet.fortiwebcloud
     gather_facts: no
     connection: httpapi
     vars:
       ansible_httpapi_validate_certs: False
       ansible_httpapi_use_ssl: True
       ansible_httpapi_port: 443
       application_name: "YOUR_APP_NAME"
     tasks:
       - name: Get SNI certificates.
         cloudwaf_sni_cert_method:
           api_token: "{{api_key}}"
           app_name: "{{application_name}}"
           action: get
   ```

2. Create files to perform the following configurations:
   - Onboarding or deleting an application on page 199
   - Creating an IP protection policy on page 200
   - Updating endpoint settings on page 202
   - Importing/Getting/Deleting intermediate certificates on page 204
   - Importing/Getting/Deleting SNI certificates on page 205

3. Run the test:

   ```
   ansible-playbook -i hosts <the_name_of_the_file_created_in_step_2>.yml
   ```

   or

   ```
   ansible-playbook <the_name_of_the_file_created_in_step_2>.yml -i hosts  -e 'ansible_python_interpreter=/usr/bin/python3'
   ```

To prepare the files, DO NOT copy the example text in this guide. There might be format issue which causes the operation to fail. Download the template from Github repository: https://github.com/fortinet/fortiwebcloud-ansible.

Onboarding or deleting an application

Example: onboard an application

```
---


- name: Execute cloud api
  hosts: fortiwebcloud01
  gather_facts: no
  collections:
    - fortinet.fortiwebcloud
  connection: httpapi
  vars:
    ansible_httpapi_validate_certs: False
    ansible_httpapi_use_ssl: true
    ansible_httpapi_port: 443
    application_name: "YOUR_APP_NAME"
  tasks:
    - name: Create an application.
      cloudwaf_app_create:
        app_name: "{{application_name}}"
        domain_name: "www.example.com"
        extra_domains:
          - a.example.com
          - b.example.com
        app_service:
          http: 80
          https: 443
        origin_server_ip: "166.111.4.100"
        origin_server_service: "HTTPS"
        origin_server_port: "443"
        cdn: False
        block: False
        template: "your-template-name-or-empty"
```

ansible_httpapi_validate_certs	Whether to validate certificates for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `False`.
ansible_httpapi_use_ssl	Whether to use SSL protocol for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `true`.
ansible_httpapi_port	The port number used for the SSL connection. Specify `443`.
domain_name	Specify the domain name of your application. See Domain name for more information.
extra_domains	up to 9 extra domains can be added. See Domain name for more information.

app_service	The traffic types allowed to arrive at the domains of your application. See Traffic Type for more information.
origin_server_ip	The IP address of your origin server.
origin_server_service	Specify `HTTP` or `HTTPS`.
origin_server_port	Specify the port number used for the HTTP or HTTPS connection between FortiWeb Cloud and your origin server.
cdn	`False`: Disable CDN. `True`: Enable CDN. For more information, see CDN.
block	`False`: Disable Block mode. `True`: Enable Block mode. For more information, see Understanding block mode and action.
template	Specify the template name. The configurations in the template will be applied to this application. You can also leave it empty.

Example: delete an application

```
---

- name: Execute cloud api

   hosts: fortiwebcloud01
   gather_facts: no
   collections:
      - fortinet.fortiwebcloud
   connection: httpapi
   vars:
      ansible_httpapi_validate_certs: False
      ansible_httpapi_use_ssl: true
      ansible_httpapi_port: 443
      application_name: "YOUR_APP_NAME"
   tasks:
      - name: Delete the application.
         cloudwaf_app_delete:
            app_name: "{{application_name}}"
```

Creating an IP protection policy

Example: create an IP protection policy

```
---

- name: Execute cloud api

   hosts: fortiwebcloud01
   gather_facts: no
   collections:
    - fortinet.fortiwebcloud
  connection: httpapi
  vars:
    ansible_httpapi_validate_certs: False
    ansible_httpapi_use_ssl: true
    ansible_httpapi_port: 443
    application_name: "YOUR_APP_NAME"
  tasks:
    - name: Configure IP Protection.
      cloudwaf_ip_protection_method:
        api_token: "You must specify a token"
        app_name: "{{application_name}}"
        template_status: disable
        status: enable
        IPProtection:
          ip-reputation: enable
          geo-ip-block:
            members:
              - Antigua And Barbuda
              - Aland Islands
              - Afghanistan
          ip-list:
            members:
              - type: trust-ip
                ip: '1.1.1.1,2.2.2.21-2.2.2.27'
              - type: block-ip
                ip: '3.1.1.1,3.1.1.11-3.1.1.17'
              - type: allow-only-ip
                ip: '4.1.1.1-4.1.1.17,4.1.1.19'
```

ansible_httpapi_validate_certs	Whether to validate certificates for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `False`.
ansible_httpapi_use_ssl	Whether to use SSL protocol for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `true`.
ansible_httpapi_port	The port number used for the SSL connection. Specify `443`.
template_status	Specify whether to `enable` or `disable` inheriting the configurations of the template that you have applied to this application.
status	Specify whether to `enable` or `disable` IP reputation module.
ip-reputation	Specify whether to `enable` or `disable` blocking client access based on up-to-date threat intelligence gathered by FortiGuard.
geo-ip-block members:	Specify one or more geographical regions that you want to block. All requests from the specified regions will be blocked.
ip-list type: trust-ip	Specify the trust IPs.

ip-list type: block-ip	Specify the block IPs.
ip-list type: allow-only-ip	Specify the allow only IPs. For more information about the trust IP, block IP, and allow only IP, see IP Protection.

Updating endpoint settings

Example: Updating endpoint settings

```
---

- name: Execute cloud api

  hosts: fortiwebcloud01
  gather_facts: no
  collections:
    - fortinet.fortiwebcloud
  connection: httpapi
  vars:
    ansible_httpapi_validate_certs: False
    ansible_httpapi_use_ssl: true
    ansible_httpapi_port: 443
    application_name: "YOUR_APP_NAME"
  tasks:
    - name: Update an endpoint.
      cloudwaf_endpoint_update:
        app_name: "{{application_name}}"
        http_status: 1
        https_status: 1
        http2_status: 0
        ipv6_option: 0
        extra_domains: []
        cert_type: 1
        ssl_options:
          tls_1_0: 0
          tls_1_1: 0
          tls_1_2: 1
          tls_1_3: 1
          encryption_level: 1
          http_2_https: 1
        custom_block_page: disable
        block_url: ''
        custom_http_port: 80
        custom_https_port: 443
```

ansible_httpapi_validate_certs	Whether to validate certificates for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `False`.

ansible_httpapi_use_ssl	Whether to use SSL protocol for the connections between your Ansible host and FortiWeb Cloud's API gateway. Specify `true`.
ansible_httpapi_port	The port number used for the SSL connection. Specify `443`.
http_status	`0`: Disable HTTP. `1`: Enable HTTP.
https_status	`0`: Disable HTTPS. `1`: Enable HTTPS.
http2_status	`0`: Disable HTTP/2. `1`: Enable HTTP/2.
ipv6_option	`0`: Disable IPv6. `1`: Enable IPv6. For more information about the HTTP, HTTPS, HTTP/2, and IPv6 settings, see Traffic Type.
extra_domains	Specify up to 9 extra domains. For more information, see Domain name.
cert_type	`0`: Automatic certificate. `1`: Custom certificate. If you use custom certificate, make use to import SNI certificates and intermediate certificates. See Importing/Getting/Deleting SNI certificates and Importing/Getting/Deleting intermediate certificates For more information about certificate type, see SSL Certificate.
tls_1_0	`0`: Disable TLS 1.0 `1`: Enable TLS 1.0.
tls_1_1	`0`: Disable TLS 1.1 `1`: Enable TLS 1.1.
tls_1_2	`0`: Disable TLS 1.2. `1`: Enable TLS 1.2.
tls_1_3	`0`: Disable TLS 1.3. `1`: Enable TLS 1.3. For more information, see SSL/TLS.
http_2_https	`0`: Disable redirecting HTTP traffic to HTTPS. `1`: Enable redirecting HTTP traffic to HTTPS. For more information, see SSL/TLS.
custom_block_page	`disable`: Disable the custom page settings. `enable`: Enable the custom page settings.
block_url	Specify the URL path of the block page so that FortiWeb Cloud can return it to your user's client when its request violates WAF rules, for example: /blockpage.html.

custom_http_port	The HTTP port number of the block page.
custom_https_port	The HTTPS port number of the block page.

Importing/Getting/Deleting intermediate certificates

Example: Import an intermediate certificate

```
---


- hosts: fortiwebcloud01
  name: Execute cloud api
  collections:
    - fortinet.fortiwebcloud
  gather_facts: no
  connection: httpapi
  vars:
    ansible_httpapi_validate_certs: False
    ansible_httpapi_use_ssl: True
    ansible_httpapi_port: 443
    application_name: "YOUR_APP_NAME"
  tasks:
    - name: Configure intermediate certificates.
      cloudwaf_inter_cert_method:
        app_name: "{{application_name}}"
        action: import
        certificate: <YOUR-CERTIFICATE>
```

Example: Get an intermediate certificate

```
---


- hosts: fortiwebcloud01
  name: Execute cloud api
  collections:
    - fortinet.fortiwebcloud
  gather_facts: no
  connection: httpapi
  vars:
    ansible_httpapi_validate_certs: False
    ansible_httpapi_use_ssl: True
    ansible_httpapi_port: 443
    application_name: "YOUR_APP_NAME"
  tasks:
    - name: Get intermediate certificates.
      cloudwaf_inter_cert_method:
        app_name: "{{application_name}}"
        action: get
```

Example: Delete an intermediate certificate

```
---


- hosts: fortiwebcloud01
  name: Execute cloud api
  collections:
     - fortinet.fortiwebcloud
  gather_facts: no
  connection: httpapi
  vars:
     ansible_httpapi_validate_certs: False
     ansible_httpapi_use_ssl: True
     ansible_httpapi_port: 443
     application_name: "YOUR_APP_NAME"
  tasks:
     - name: Delete intermediate certificates.
        cloudwaf_inter_cert_method:
           app_name: "{{application_name}}"
           action: delete
           id: 1
```

For more information about intermediate certificates, see Custom Certificate.

Importing/Getting/Deleting SNI certificates

Example: Import an SNI certificate

```
---


- hosts: fortiwebcloud01
  name: Execute cloud api
  collections:
     - fortinet.fortiwebcloud
  gather_facts: no
  connection: httpapi
  vars:
     ansible_httpapi_validate_certs: False
     ansible_httpapi_use_ssl: True
     ansible_httpapi_port: 443
     application_name: "YOUR_APP_NAME"
  tasks:
     - name: Configure SNI certificates.
        cloudwaf_sni_cert_method:
           app_name: "{{application_name}}"
           action: import
           certificate: <YOUR-CERTIFICATE>
           private_key: <YOUR_PRIVATE_KEY>
           passwd: 123456
```

Example: Get an SNI certificate

```
---


- hosts: fortiwebcloud01
   name: Execute cloud api
   collections:
      - fortinet.fortiwebcloud
   gather_facts: no
   connection: httpapi
   vars:
      ansible_httpapi_validate_certs: False
      ansible_httpapi_use_ssl: True
      ansible_httpapi_port: 443
      application_name: "YOUR_APP_NAME"
   tasks:
      - name: Get SNI certificates.
         cloudwaf_sni_cert_method:
            app_name: "{{application_name}}"
            action: get
```

Example: Delete an SNI certificate

```
---


- hosts: fortiwebcloud01
   name: Execute cloud api
   collections:
      - fortinet.fortiwebcloud
   gather_facts: no
   connection: httpapi
   vars:
      ansible_httpapi_validate_certs: False
      ansible_httpapi_use_ssl: True
      ansible_httpapi_port: 443
      application_name: "YOUR_APP_NAME"
   tasks:
      - name: Configure SNI certificates.
         cloudwaf_sni_cert_method:
            app_name: "{{application_name}}"
            action: delete
            id: 1
```

For more information about SNI certificates, see Custom Certificate.

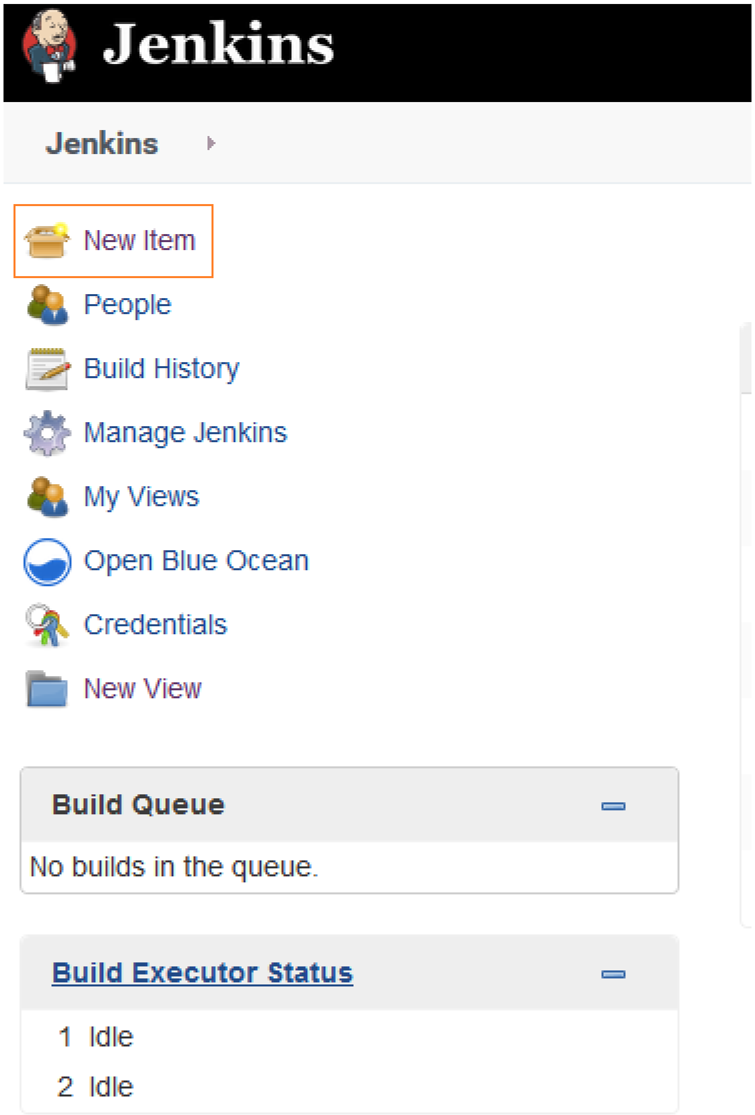
Configuring FortiWeb Cloud with Jenkins

The following example demonstrates how to use Jenkins to perform simple configuration changes on FortiWeb Cloud. It requires the following:

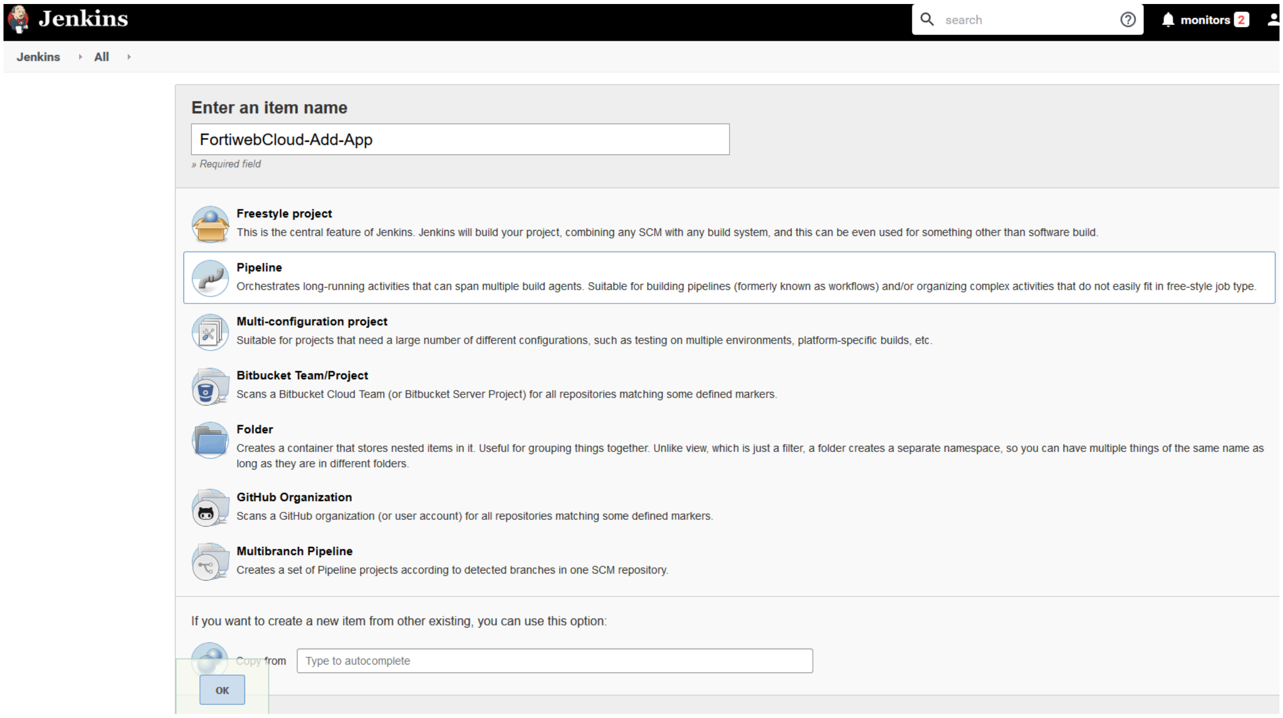
- FortiWeb Cloud 20.2.d or later
- Jekins: This example uses Jekins 2.222.3+.

To onboard an application with Jenkins, follow the steps below:

1. Log in to your Jenkins account.
2. Click **New Item**.



3. Name the item and select **Pipeline**, then click **OK**.



Enter an item name

FortiwebCloud-Add-App

» Required field

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

Bitbucket Team/Project
Scans a Bitbucket Cloud Team (or Bitbucket Server Project) for all repositories matching some defined markers.

Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

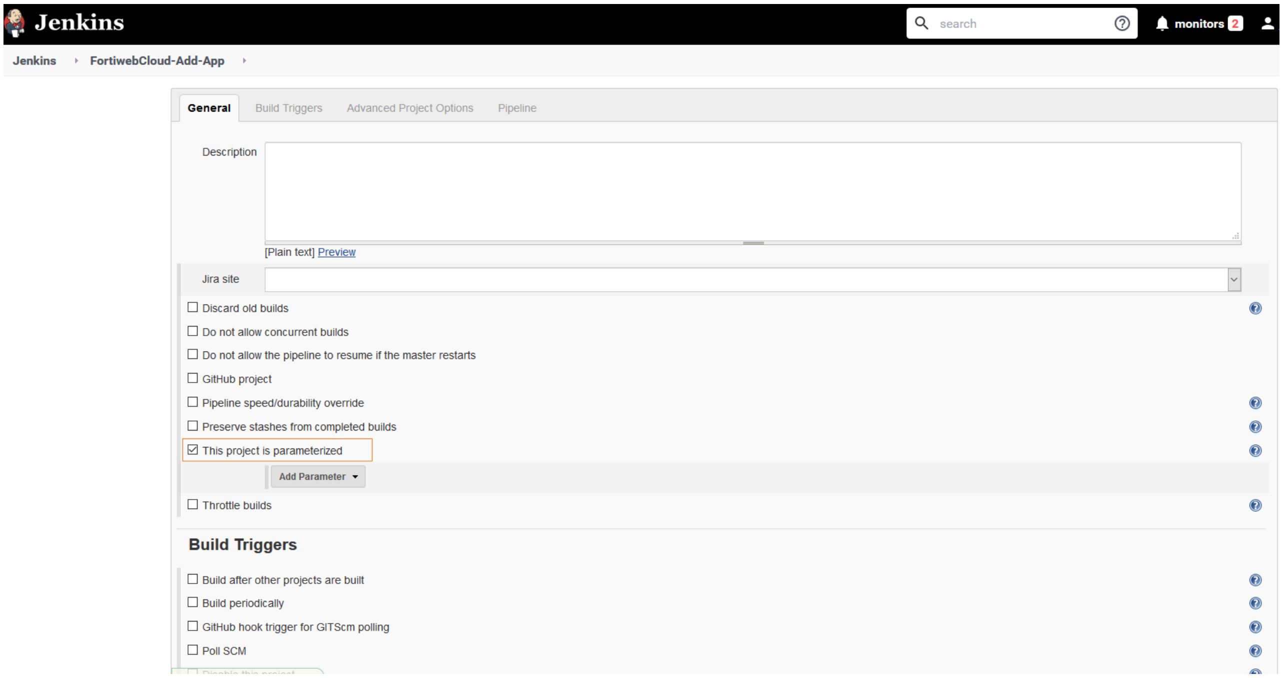
GitHub Organization
Scans a GitHub organization (or user account) for all repositories matching some defined markers.

Multibranch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

If you want to create a new item from other existing, you can use this option:

Copy from Type to autocomplete

4. Select **This project is parameterized**.



Description

[Plain text] Preview

Jira site

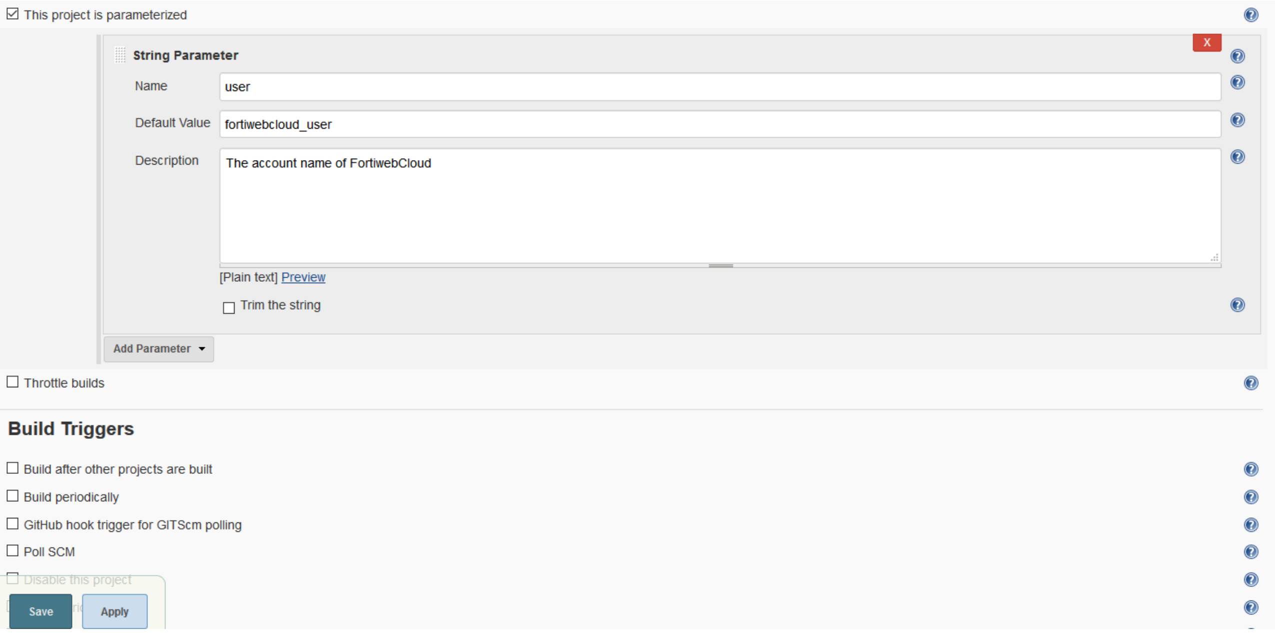
☐ Discard old builds
☐ Do not allow concurrent builds
☐ Do not allow the pipeline to resume if the master restarts
☐ GitHub project
☐ Pipeline speed/durability override
☐ Preserve stashes from completed builds
☑ This project is parameterized

☐ Throttle builds

Build Triggers

☐ Build after other projects are built
☐ Build periodically
☐ GitHub hook trigger for GITScm polling
☐ Poll SCM

5. In **String Parameter**, enter **user** in **Name**, then enter your FortiWeb Cloud's account name in **Default Value**. The account should have write privilege on FortiWeb Cloud.



☑ This project is parameterized

String Parameter

Name: user

Default Value: fortiwebcloud_user

Description: The account name of FortiwebCloud

[Plain text] Preview

□ Trim the string

□ Throttle builds

Build Triggers

□ Build after other projects are built

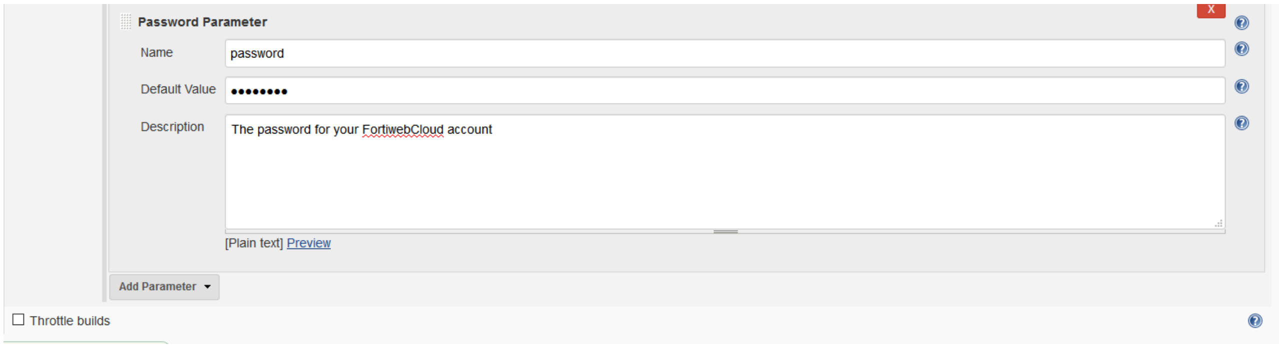
□ Build periodically

□ GitHub hook trigger for GITScm polling

□ Poll SCM

□ Disable this project

6. In **Password Parameter**, enter **password** in **Name**, then enter the password of the specified account in **Default Value**.



Password Parameter

Name: password

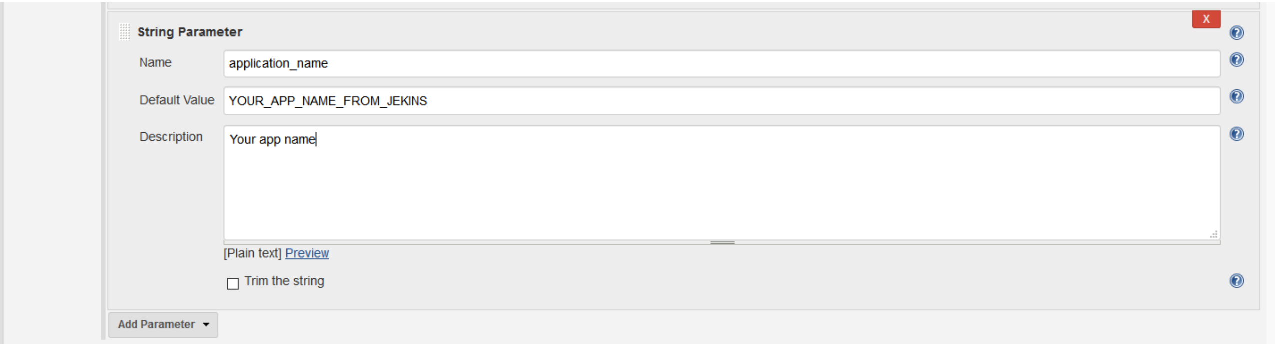
Default Value: ••••••••

Description: The password for your FortiwebCloud account

[Plain text] Preview

□ Throttle builds

7. In **String Parameter**, enter **application_name** in **Name**, then enter a name for your application. It will be displayed on FortiWeb Cloud's GUI to identify your application.



String Parameter

Name: application_name

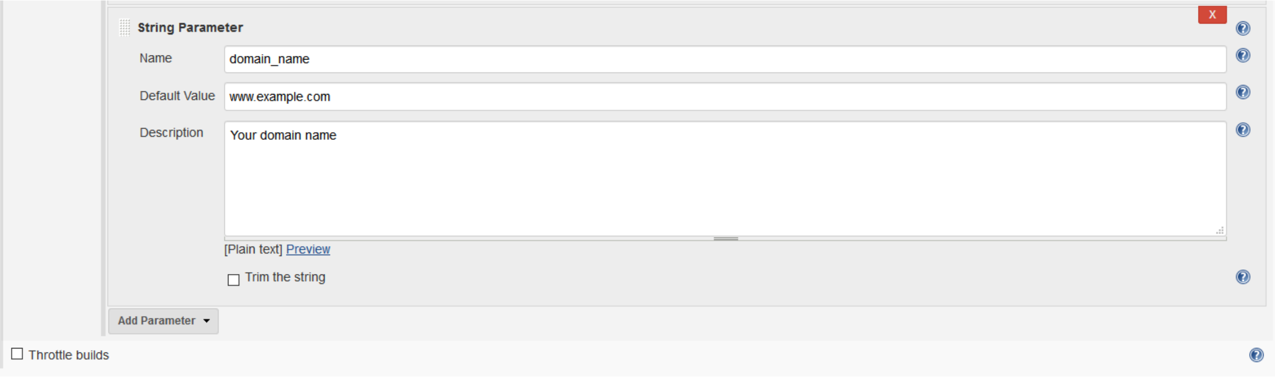
Default Value: YOUR_APP_NAME_FROM_JEKINS

Description: Your app name

[Plain text] Preview

□ Trim the string

8. In **String Parameter**, enter **domain_name** in **Name**, then enter your application's domain name in **Default Value**.



String Parameter

Name: domain_name

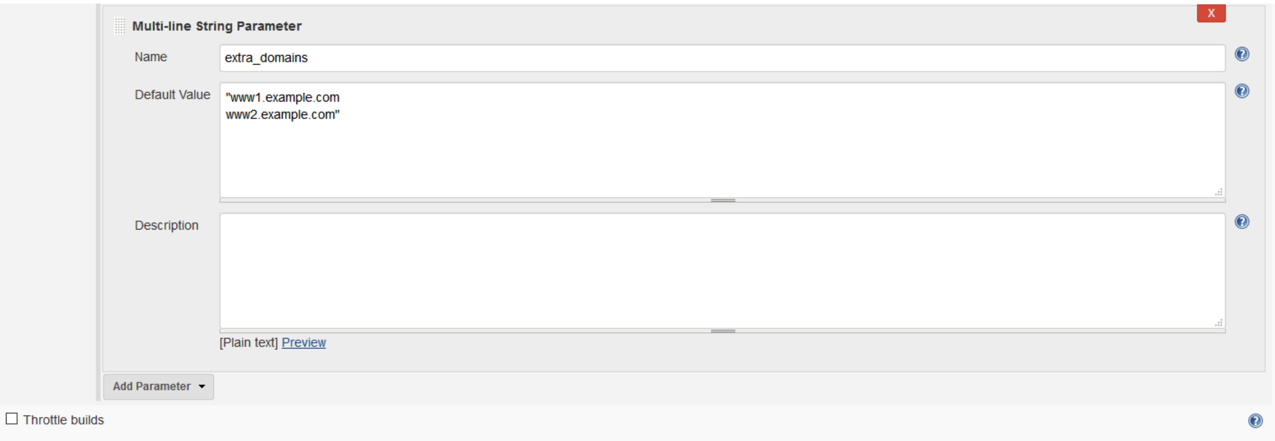
Default Value: www.example.com

Description: Your domain name

[Plain text] Preview

□ Trim the string

9. In **Multi-line String Parameter**, enter **extra_domains** in **Name**, then enter the domain names if your application has multiple domains.



Multi-line String Parameter

Name: extra_domains

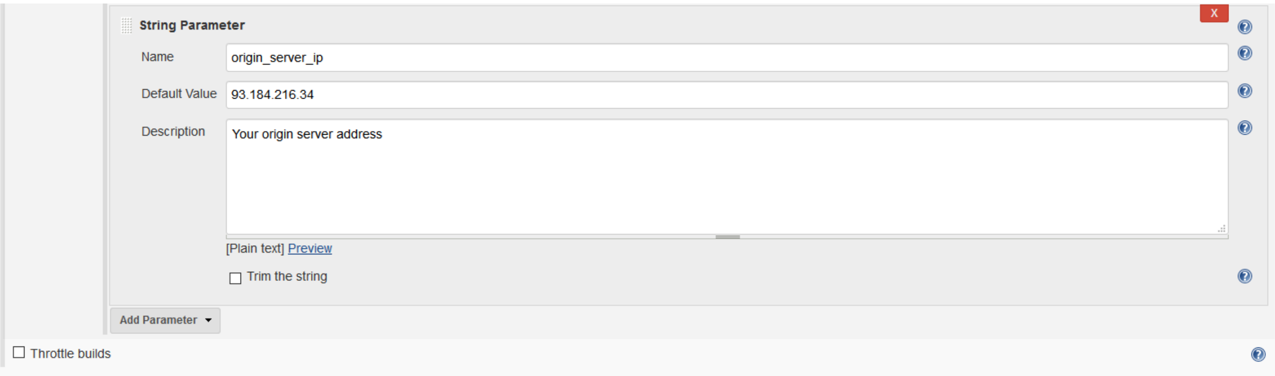
Default Value:

```
"www1.example.com
www2.example.com"
```

Description:

[Plain text] Preview

10. In **String Parameter**, enter **origin_server_ip** in **Name**, then enter your origin server's IP address in **Default Value**.



String Parameter

Name: origin_server_ip

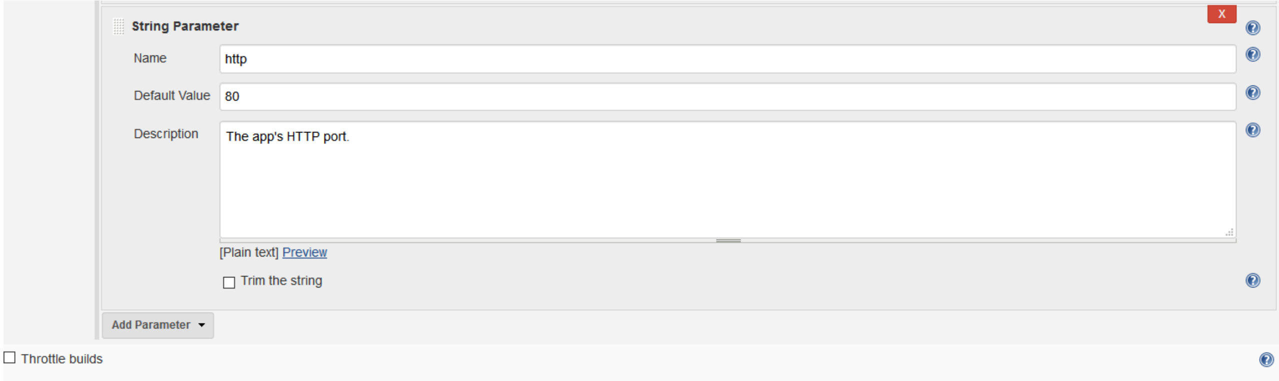
Default Value: 93.184.216.34

Description: Your origin server address

[Plain text] Preview

□ Trim the string

11. In **String Parameter**, enter **HTTP** in **Name**, then enter the port number used for HTTP service in **Default Value.**You must enter 80 as the default value.



String Parameter

Name: http

Default Value: 80

Description: The app's HTTP port.

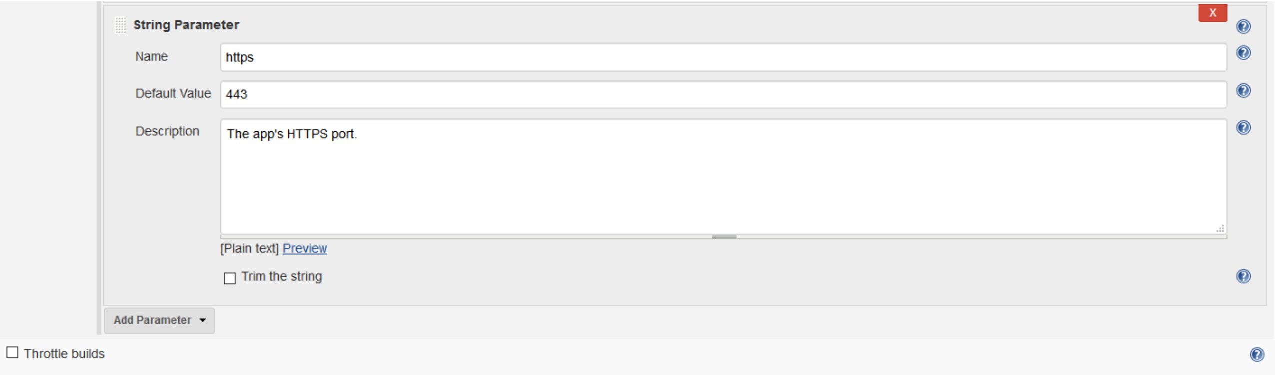
[Plain text] Preview

□ Trim the string

Add Parameter

□ Throttle builds

12. In **String Parameter**, enter **HTTPS** in **Name**, then enter the port number used for HTTPS service in **Default Value**. You must enter 443 as the default value.



String Parameter

Name: https

Default Value: 443

Description: The app's HTTPS port.

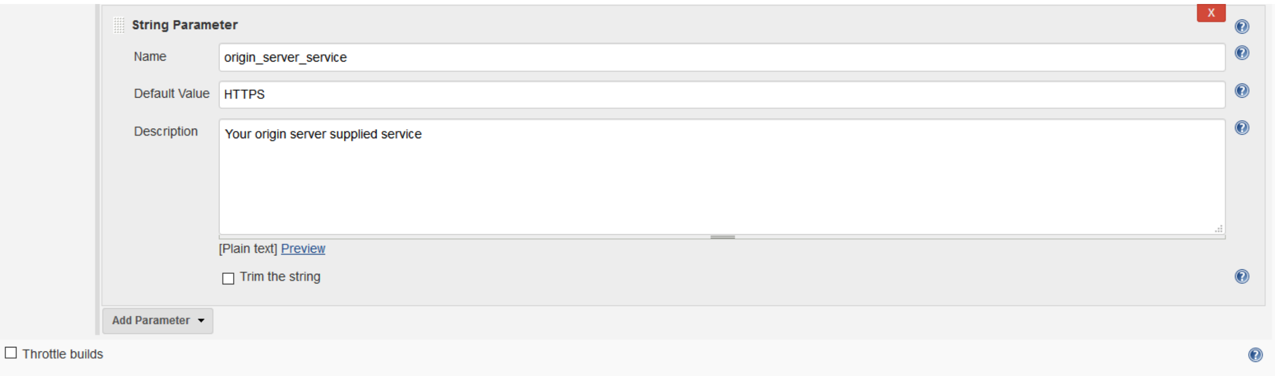
[Plain text] Preview

□ Trim the string

Add Parameter

□ Throttle builds

13. In **String Parameter**, enter **origin_server_service** in **Name**, then enter your origin server's service type in **Default Value**. You must input HTTP or HTTPS as the default value.



String Parameter

Name: origin_server_service

Default Value: HTTPS

Description: Your origin server supplied service

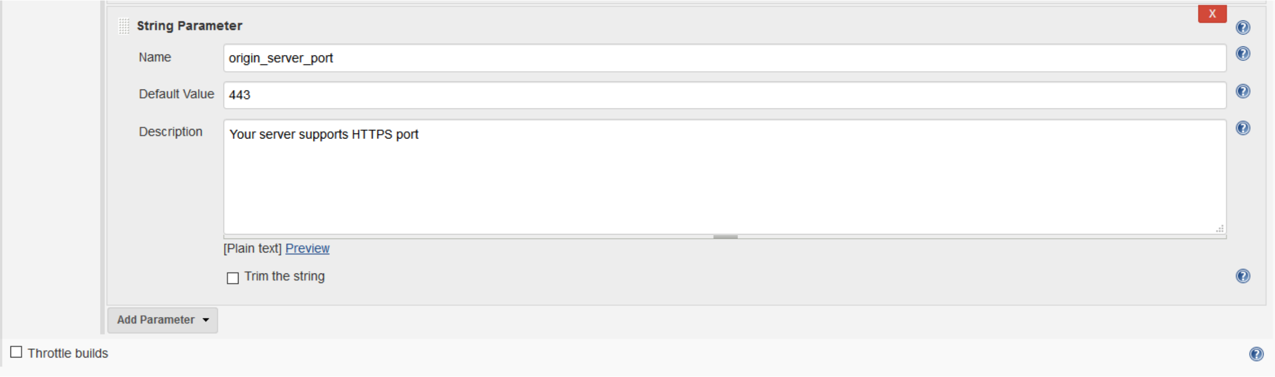
[Plain text] Preview

□ Trim the string

Add Parameter

□ Throttle builds

14. In **String Parameter**, enter **origin_server_port** in **Name**, then enter your origin server's listening port in **Default Value**. You can input 80 for HTTP or 443 for HTTPS as the default value.



String Parameter

Name: origin_server_port

Default Value: 443

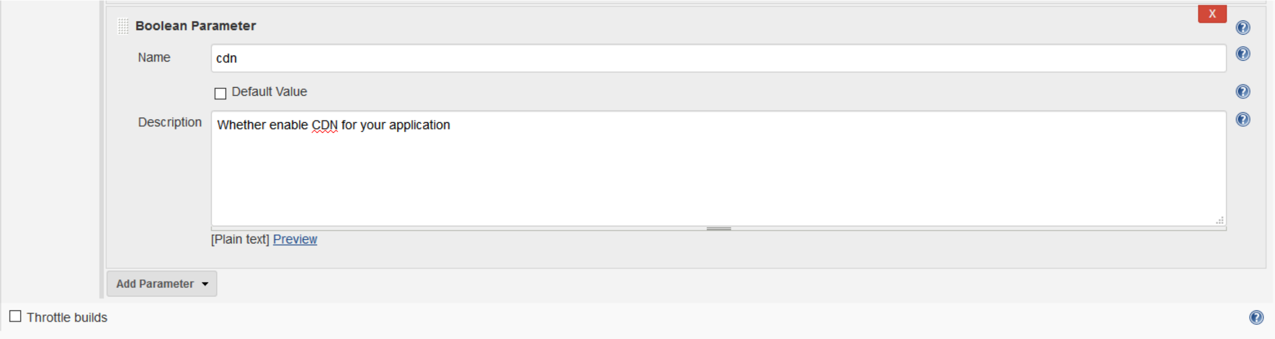
Description: Your server supports HTTPS port

[Plain text] Preview

☐ Trim the string

☐ Throttle builds

15. In **Boolean Parameter**, enter **cdn** in **Name**, then enable this option if you want your application to be accelerated in the global network.



Boolean Parameter

Name: cdn

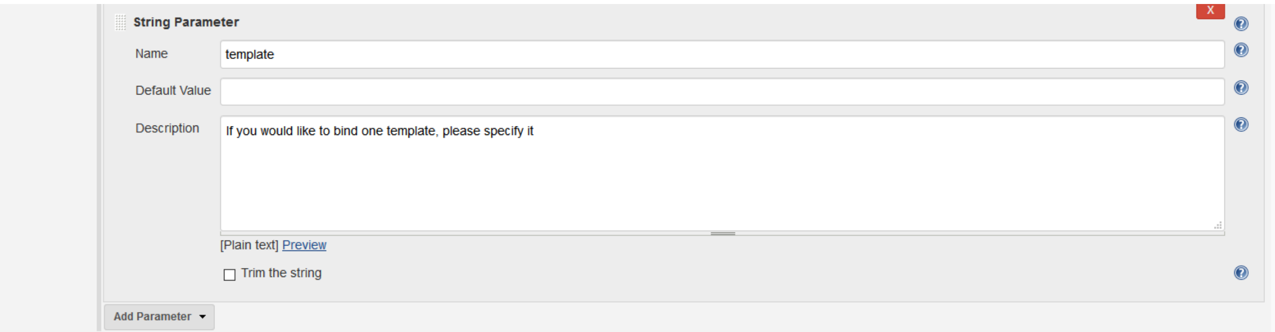
☐ Default Value

Description: Whether enable CDN for your application

[Plain text] Preview

☐ Throttle builds

16. In **Boolean Parameter**, enter **block** in **Name**, then enable this option if you want FortiWeb Cloud to block the attacks and abnormal traffic.
17. In **String Parameter**, enter **template** in **Name**, then enter the name of the template if you want your application to inherit configuration from the template.



String Parameter

Name: template

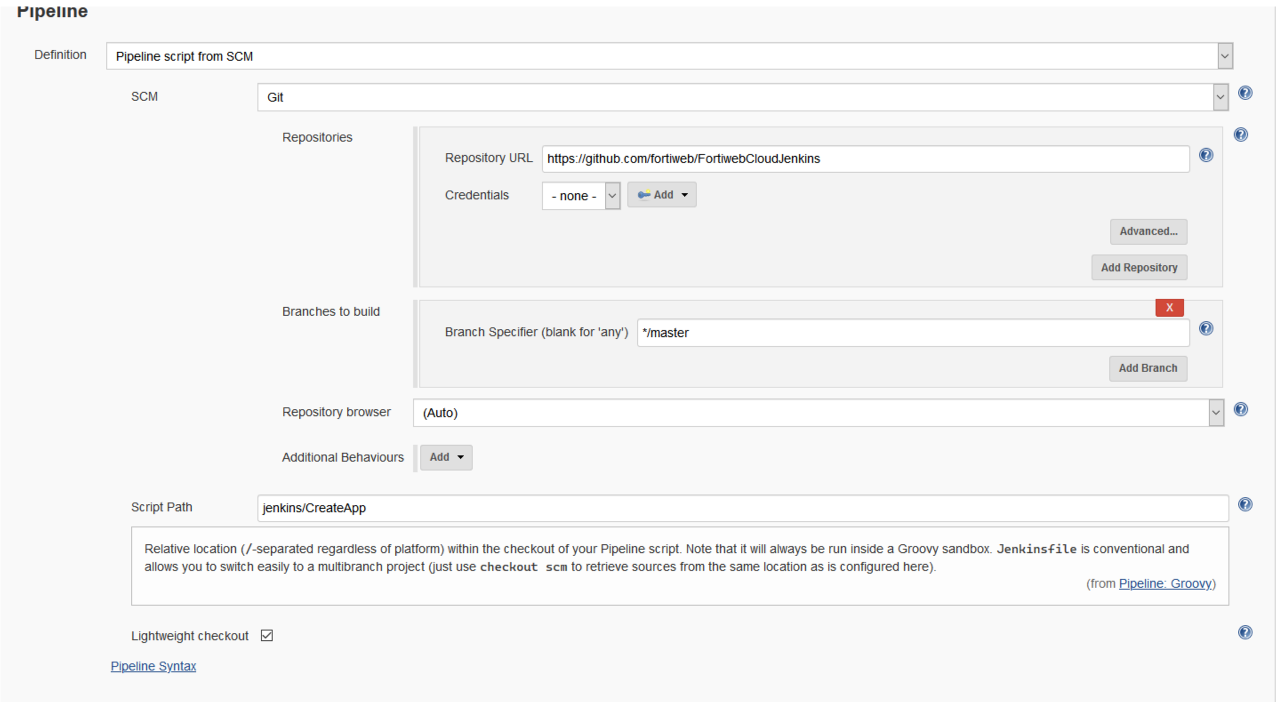
Default Value:

Description: If you would like to bind one template, please specify it

[Plain text] Preview

☐ Trim the string

18. Specify the repositories in the pipeline. The repository URL is https://github.com/fortinet/fortiwebcloud-jenkins and the script path is "jenkins/CreateApp". Click **Save** to finish the setup.



Pipeline

Definition: Pipeline script from SCM

SCM: Git

Repositories

Repository URL: https://github.com/fortiweb/FortiwebCloudJenkins

Credentials: - none -

Branches to build

Branch Specifier (blank for 'any'): */master

Repository browser: (Auto)

Additional Behaviours

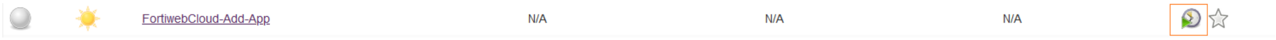
Script Path: jenkins/CreateApp

Relative location (/-separated regardless of platform) within the checkout of your Pipeline script. Note that it will always be run inside a Groovy sandbox. `Jenkinsfile` is conventional and allows you to switch easily to a multibranch project (just use `checkout scm` to retrieve sources from the same location as is configured here).

(from Pipeline: Groovy)

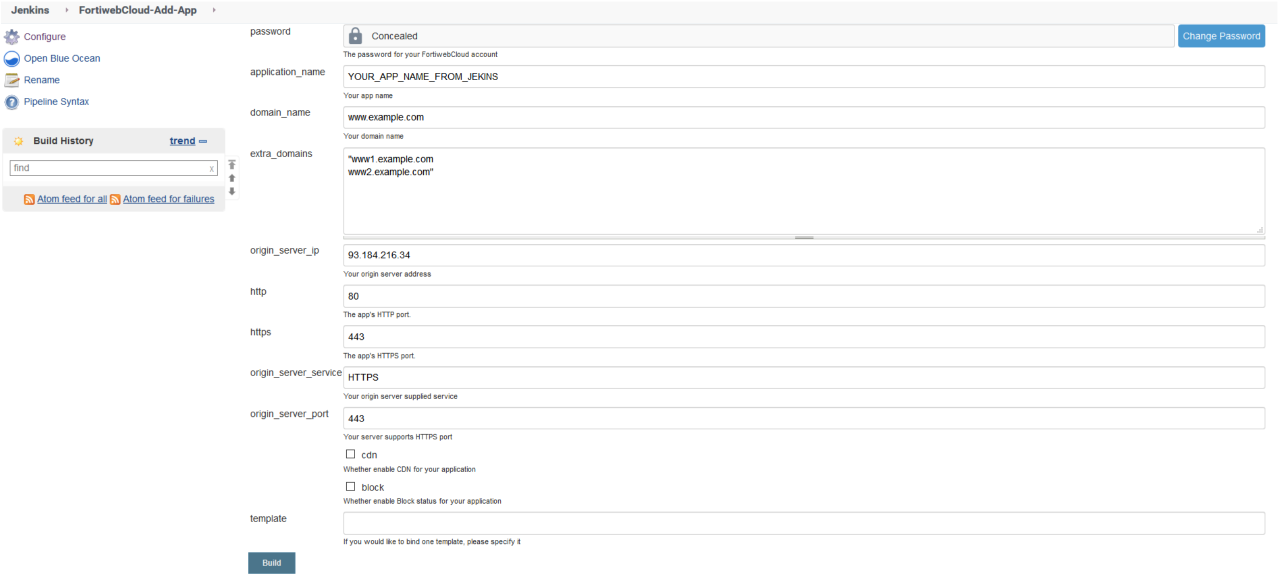
Lightweight checkout ☑

19. Now you can schedule the build.



		FortiwebCloud-Add-App	N/A	N/A	N/A	

20. Review the configuration before running the build. Click **Build**.



Jenkins › FortiwebCloud-Add-App ›

password: Concealed
The password for your FortiwebCloud account

application_name: YOUR_APP_NAME_FROM_JEKINS
Your app name

domain_name: www.example.com
Your domain name

extra_domains: "www1.example.com
www2.example.com"

origin_server_ip: 93.184.216.34
Your origin server address

http: 80
The app's HTTP port.

https: 443
The app's HTTPS port.

origin_server_service: HTTPS
Your origin server supplied service

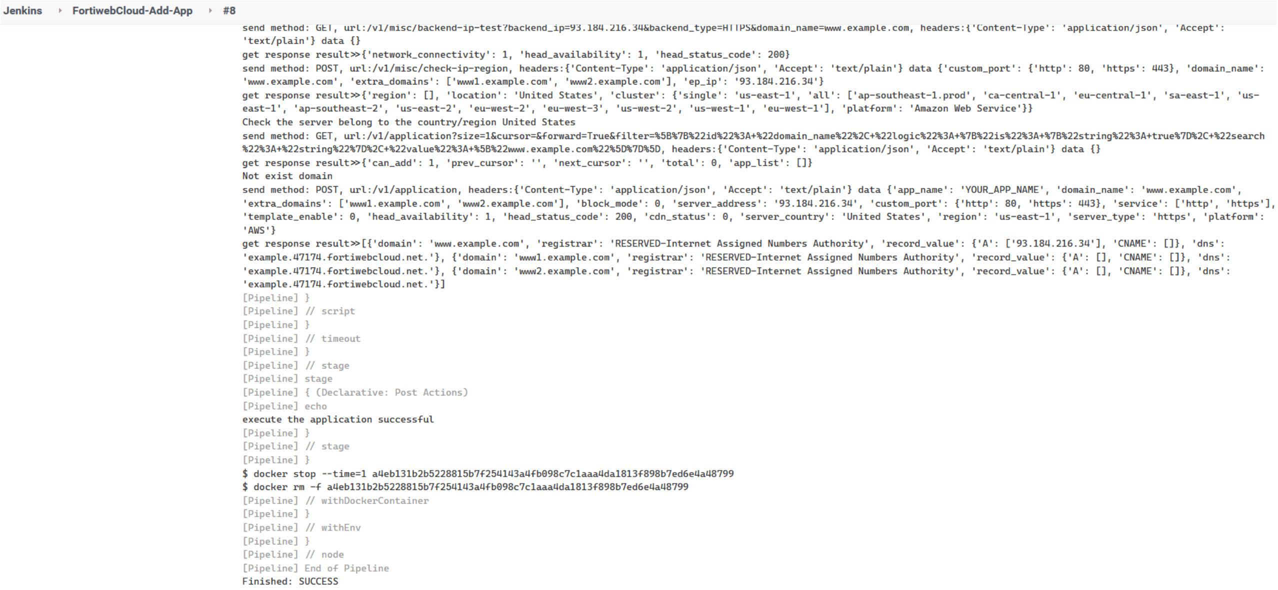
origin_server_port: 443
Your server supports HTTPS port

☐ cdn
Whether enable CDN for your application

☐ block
Whether enable Block status for your application

template:
If you would like to bind one template, please specify it

21. If nothing is wrong, you will see the successful operation via Console Output.

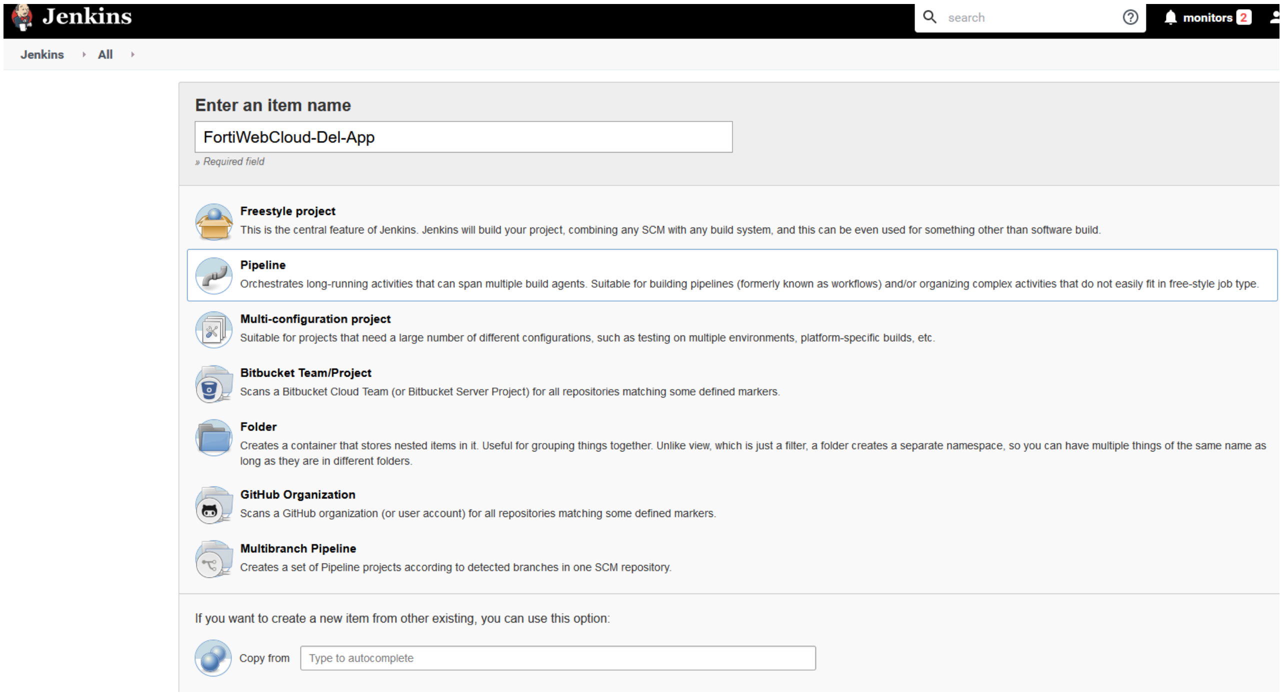


Jenkins › FortiwebCloud-Add-App › #8

```
send method: GET, url:/v1/misc/backend-ip-test?backend_ip=93.184.216.34&backend_type=HTTPS&domain_name=www.example.com, headers:{'Content-Type': 'application/json', 'Accept':
'text/plain'} data {}
get response result>>{'network_connectivity': 1, 'head_availability': 1, 'head_status_code': 200}
send method: POST, url:/v1/misc/check-ip-region, headers:{'Content-Type': 'application/json', 'Accept': 'text/plain'} data {'custom_port': {'http': 80, 'https': 443}, 'domain_name':
'www.example.com', 'extra_domains': ['www1.example.com', 'www2.example.com'], 'ep_ip': '93.184.216.34'}
get response result>>{'region': [], 'location': 'United States', 'cluster': {'single': 'us-east-1', 'all': ['ap-southeast-1.prod', 'ca-central-1', 'eu-central-1', 'sa-east-1', 'us-
east-1', 'ap-southeast-2', 'us-east-2', 'eu-west-2', 'eu-west-3', 'us-west-2', 'us-west-1', 'eu-west-1'], 'platform': 'Amazon Web Service'}}
Check the server belong to the country/region United States
send method: GET, url:/v1/application?size=1&cursor=&forward=True&filter=%5B%7B%22id%22%3A+%22domain_name%22%2C+%22logic%22%3A+%7B%22is%22%3A+%7B%22string%22%3A+true%7D%2C+%22search
%22%3A+%22string%22%7D%2C+%22value%22%3A+%5B%22www.example.com%22%5D%7D%5D, headers:{'Content-Type': 'application/json', 'Accept': 'text/plain'} data {}
get response result>>{'can_add': 1, 'prev_cursor': '', 'next_cursor': '', 'total': 0, 'app_list': []}
Not exist domain
send method: POST, url:/v1/application, headers:{'Content-Type': 'application/json', 'Accept': 'text/plain'} data {'app_name': 'YOUR_APP_NAME', 'domain_name': 'www.example.com',
'extra_domains': ['www1.example.com', 'www2.example.com'], 'block_mode': 0, 'server_address': '93.184.216.34', 'custom_port': {'http': 80, 'https': 443}, 'service': ['http', 'https'],
'template_enable': 0, 'head_availability': 1, 'head_status_code': 200, 'cdn_status': 0, 'server_country': 'United States', 'region': 'us-east-1', 'server_type': 'https', 'platform':
'AWS'}
get response result>>[{'domain': 'www.example.com', 'registrar': 'RESERVED-Internet Assigned Numbers Authority', 'record_value': {'A': ['93.184.216.34'], 'CNAME': []}, 'dns':
'example.47174.fortiwebcloud.net.'}, {'domain': 'www1.example.com', 'registrar': 'RESERVED-Internet Assigned Numbers Authority', 'record_value': {'A': [], 'CNAME': []}, 'dns':
'example.47174.fortiwebcloud.net.'}, {'domain': 'www2.example.com', 'registrar': 'RESERVED-Internet Assigned Numbers Authority', 'record_value': {'A': [], 'CNAME': []}, 'dns':
'example.47174.fortiwebcloud.net.'}]
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // timeout
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Declarative: Post Actions)
[Pipeline] echo
execute the application successful
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
$ docker stop --time=1 a4eb131b2b5228815b7f254143a4fb098c7c1aaa4da1813f898b7ed6e4a48799
$ docker rm -f a4eb131b2b5228815b7f254143a4fb098c7c1aaa4da1813f898b7ed6e4a48799
[Pipeline] // withDockerContainer
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

To delete app via Jenkins, follow the steps below:

1. Click **New Item** to add a new item.
2. Name the item and select **Pipeline**, then click **OK**.



Enter an item name

FortiWebCloud-Del-App

» Required field

Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

Bitbucket Team/Project
Scans a Bitbucket Cloud Team (or Bitbucket Server Project) for all repositories matching some defined markers.

Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

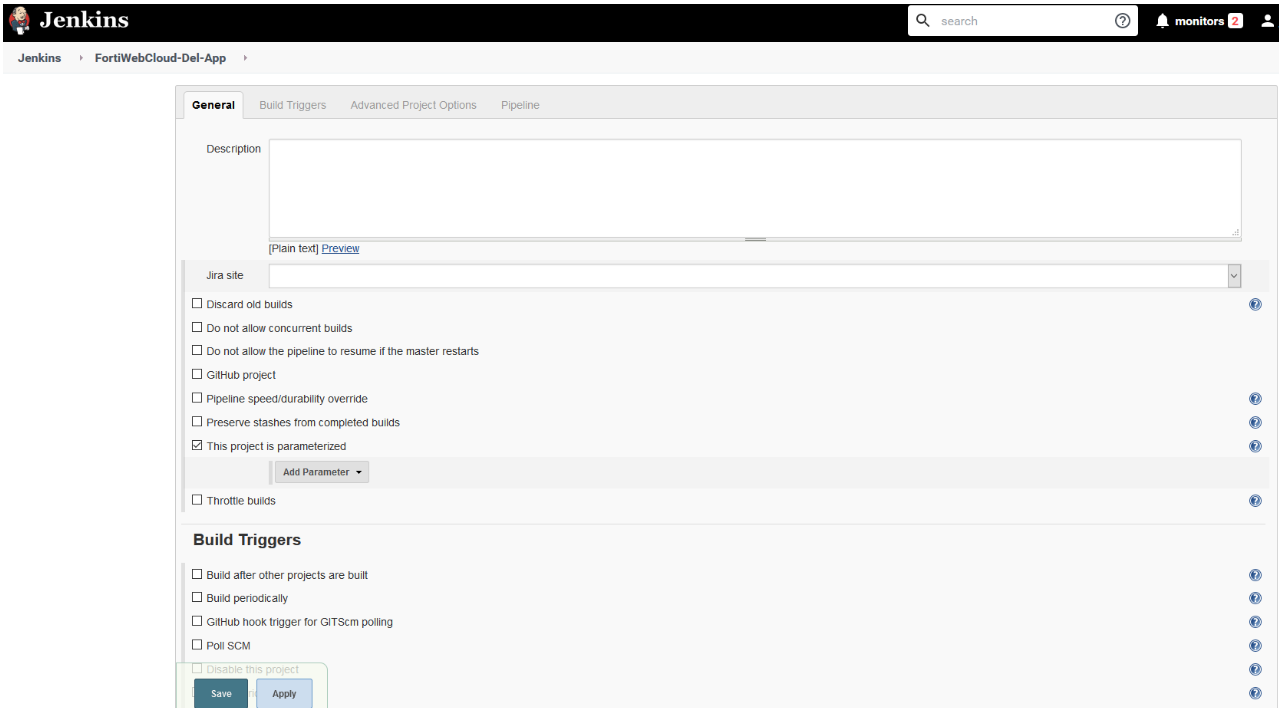
GitHub Organization
Scans a GitHub organization (or user account) for all repositories matching some defined markers.

Multibranch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

If you want to create a new item from other existing, you can use this option:

Copy from: Type to autocomplete

3. Select **This project is parameterized**.



Jenkins

search

monitors 2

Jenkins › FortiWebCloud-Del-App ›

General | Build Triggers | Advanced Project Options | Pipeline

Description

[Plain text] Preview

Jira site

□ Discard old builds

□ Do not allow concurrent builds

□ Do not allow the pipeline to resume if the master restarts

□ GitHub project

□ Pipeline speed/durability override

□ Preserve stashes from completed builds

☑ This project is parameterized

Add Parameter ▾

□ Throttle builds

Build Triggers

□ Build after other projects are built

□ Build periodically

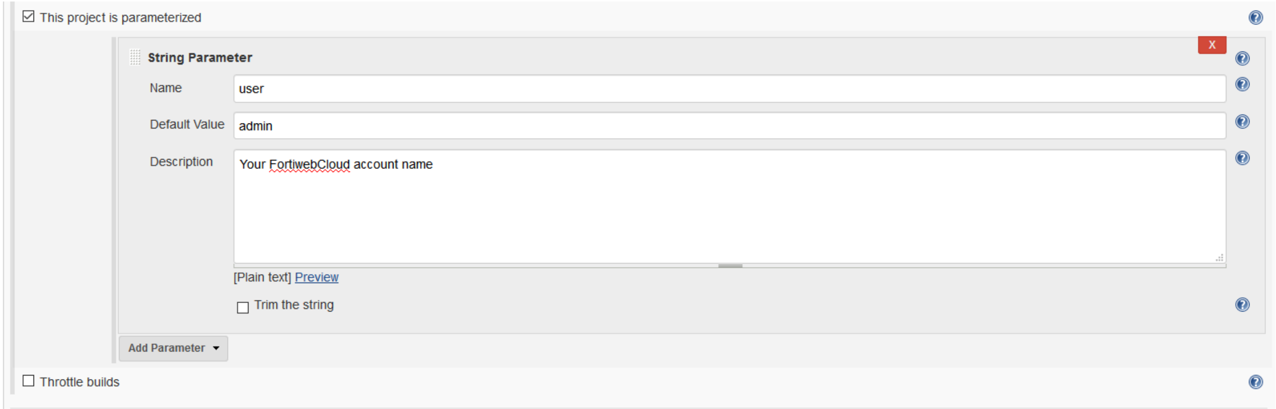
□ GitHub hook trigger for GITScm polling

□ Poll SCM

□ Disable this project

Save | Apply

4. In **String Parameter**, enter **user** in **Name**, then enter your FortiWeb Cloud's account name as its default value.



☑ This project is parameterized

String Parameter

Name: user

Default Value: admin

Description: Your FortiwebCloud account name

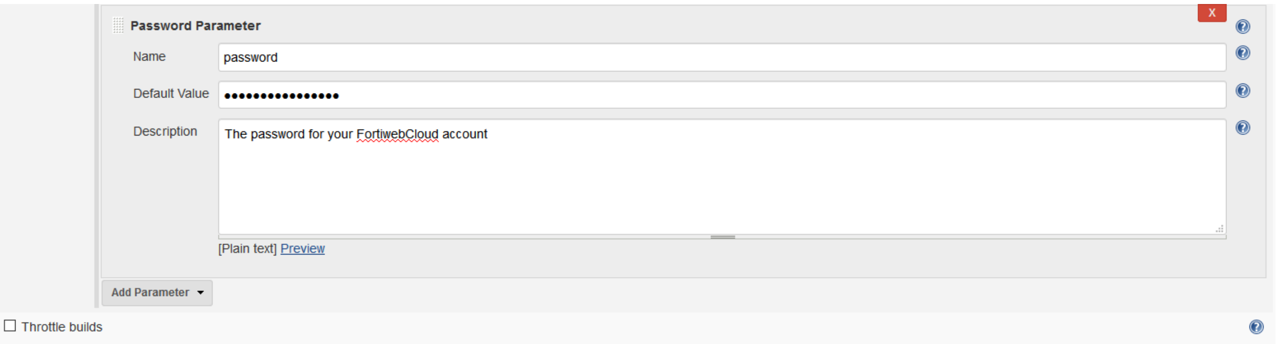
[Plain text] Preview

□ Trim the string

Add Parameter ▾

□ Throttle builds

5. In **Password Parameter**, enter **password** in **Name**, then enter the password of the specified account in **Default Value**.



Password Parameter

Name: password

Default Value: ••••••••••••••••

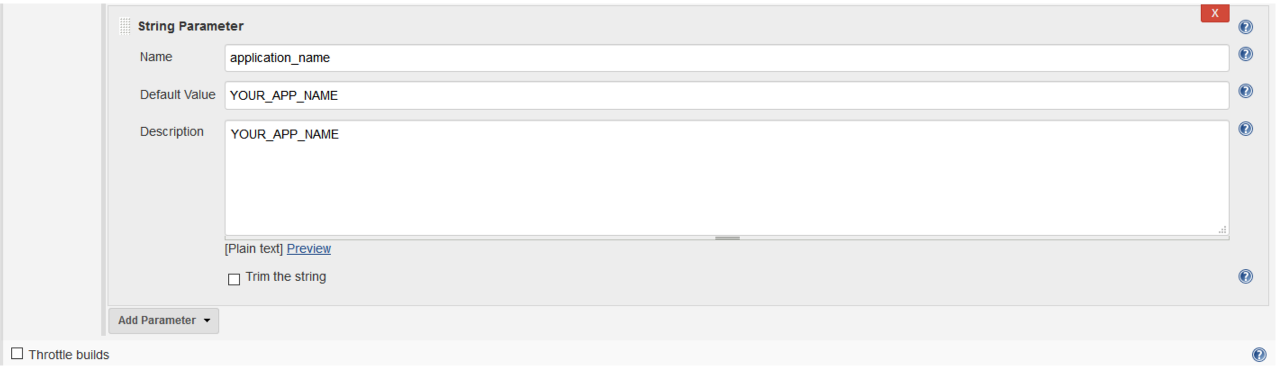
Description: The password for your FortiwebCloud account

[Plain text] Preview

Add Parameter ▾

□ Throttle builds

6. In **String Parameter**, enter **application_name** in **Name**, then enter the name of your application to be deleted.



String Parameter

Name: application_name

Default Value: YOUR_APP_NAME

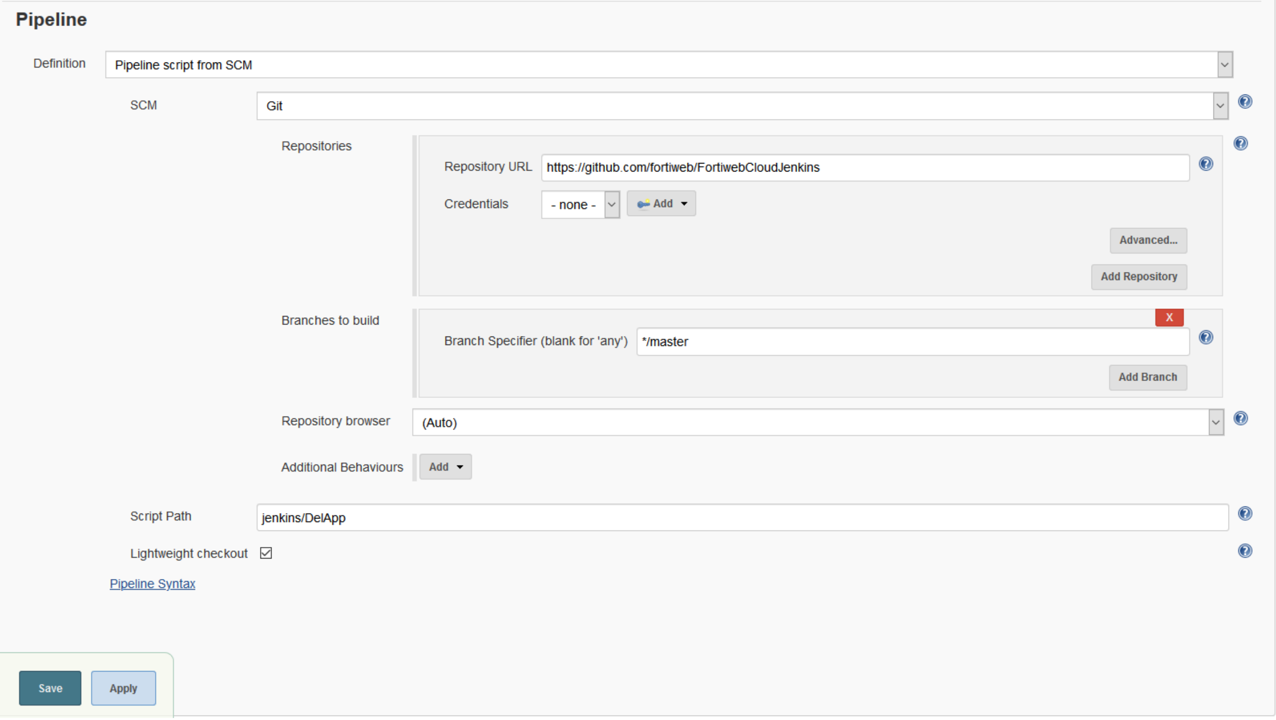
Description: YOUR_APP_NAME

[Plain text] Preview

□ Trim the string

□ Throttle builds

7. Specify the repositories in the pipeline. The repository URL is https://github.com/fortiweb/FortiwebCloudJenkins and the script path is "jenkins/DelApp". Then click **Save** to finish the setup.



Pipeline

Definition: Pipeline script from SCM

SCM: Git

Repositories

Repository URL: https://github.com/fortiweb/FortiwebCloudJenkins

Credentials: - none -

Branches to build

Branch Specifier (blank for 'any'): */master

Repository browser: (Auto)

Additional Behaviours

Script Path: jenkins/DelApp

Lightweight checkout ☑

8. Run the build. If nothing is wrong, then the delete process will be output and your application will be deleted from FortiWeb Cloud.

Use cases

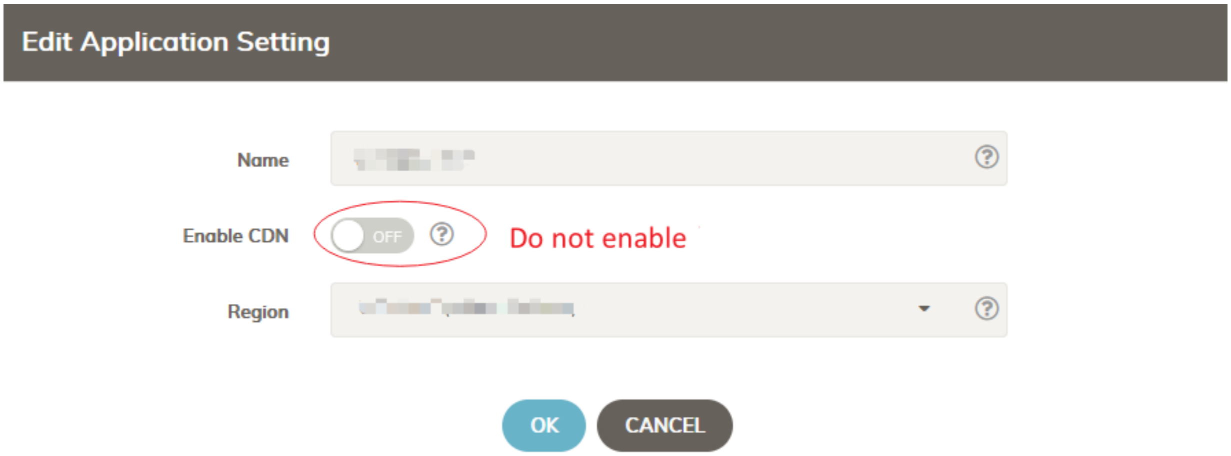
This chapter introduces the special configurations for different use cases.

Using FortiWeb Cloud behind a Content Distribution Service

If the traffic to your application server should be first forwarded to a Content Distribution Service, then flows to FortiWeb Cloud for threat detection, perform the following steps so that the traffic can correctly go through. In this example we assume the Content Distribution Service is AWS CloudFront.

Onboarding your application on FortiWeb Cloud

1. Refer to Getting Started in FortiWeb Cloud Online Help to onboard your application.
   - DO NOT enable **CDN**. A FortiWeb Cloud scrubbing center located nearest to your application server will be assigned. In your scenario, it's unnecessary to use the CDN feature of FortiWeb Cloud because AWS CloudFront already serves this purpose.



Edit Application Setting

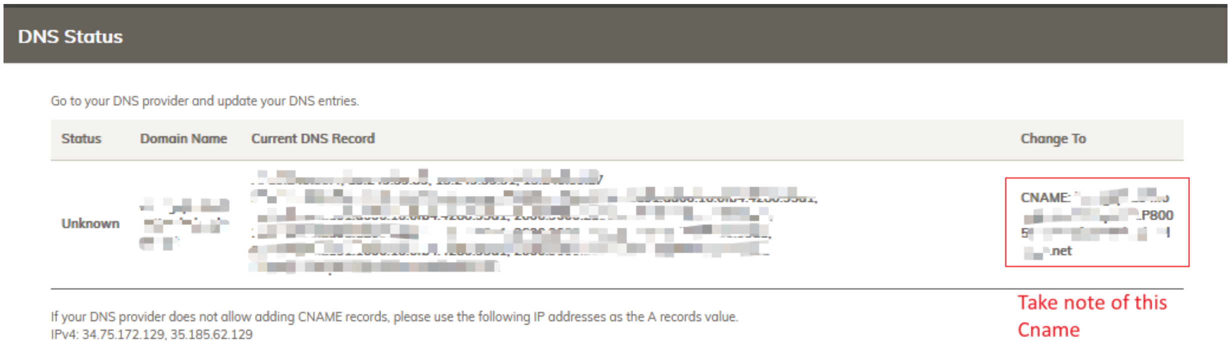
Name: [redacted]

Enable CDN: OFF

Do not enable

Region: [redacted]

- Take note of the CNAME provided by FortiWeb Cloud.



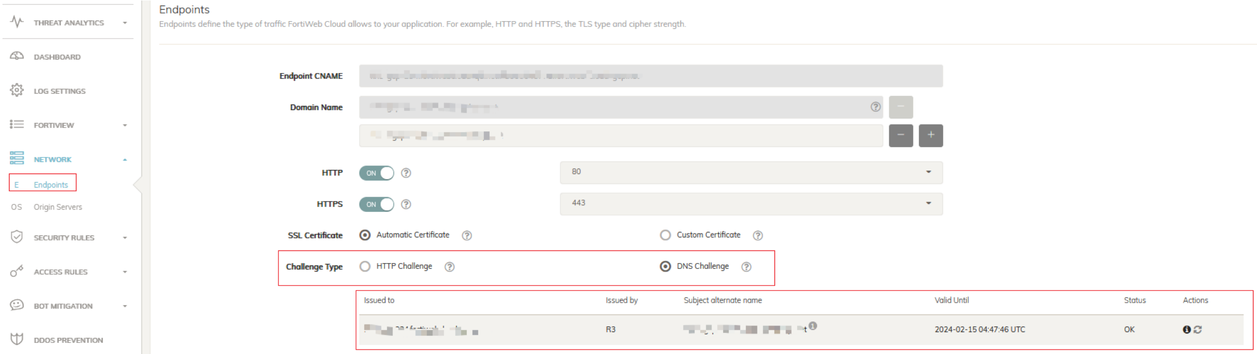
Go to your DNS provider and update your DNS entries.

Status	Domain Name	Current DNS Record	Change To
Unknown	[redacted]	[redacted]	CNAME: [redacted]

If your DNS provider does not allow adding CNAME records, please use the following IP addresses as the A records value.
IPv4: 34.75.172.129, 35.185.62.129

Take note of this Cname

2. Refer to Endpoints on page 118 to configure the **SSL Certificate** settings. If you use **Automatic Certificate**, make sure to select **DNS Challenge** type, otherwise the SSL certificate cannot be successfully retrieved.

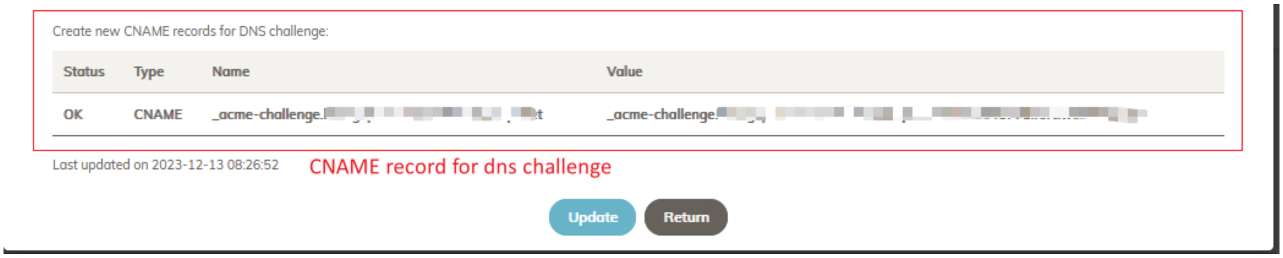


Endpoints
Endpoints define the type of traffic FortiWeb Cloud allows to your application. For example, HTTP and HTTPS, the TLS type and cipher strength.

Endpoint CNAME: [redacted]
Domain Name: [redacted]
[redacted]
HTTP: ON 80
HTTPS: ON 443
SSL Certificate: ● Automatic Certificate ○ Custom Certificate
Challenge Type: ○ HTTP Challenge ● DNS Challenge

Issued to	Issued by	Subject alternate name	Valid Until	Status	Actions
[redacted]	R3	[redacted]	2024-02-15 04:47:46 UTC	OK	

Additionally, make sure to include a CNAME record for the DNS challenge. You can locate this record in **Global > Applications > DNS Status**.



Create new CNAME records for DNS challenge:

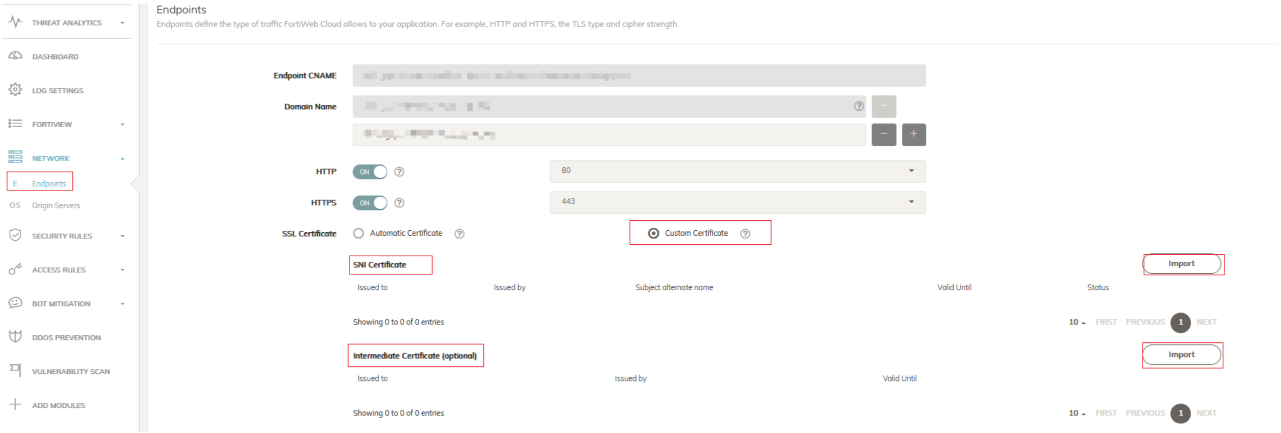
Status	Type	Name	Value
OK	CNAME	_acme-challenge.[redacted]	_acme-challenge.[redacted]

Last updated on 2023-12-13 08:26:52

CNAME record for dns challenge

Please note that DNS status may show as "Unknown". This is an expected issue when using CloudFront in front of FortiWeb Cloud. It does not affect the retrieval of the certificate, so there is no need to be concerned about it.

If you would like to use your own SSL certificate instead of the certificate issued by Let's Encrypt, you can select **Custom Certificate** in **Network > Endpoint** to upload your own SSL certificate.



Endpoints

Endpoints define the type of traffic FortiWeb Cloud allows to your application. For example, HTTP and HTTPS, the TLS type and cipher strength.

Endpoint CNAME [redacted]

Domain Name [redacted]

[redacted]

HTTP ON 80

HTTPS ON 443

SSL Certificate ○ Automatic Certificate ● Custom Certificate

SNI Certificate

Issued to	Issued by	Subject alternate name	Valid Until	Status

Showing 0 to 0 of 0 entries

Intermediate Certificate (optional)

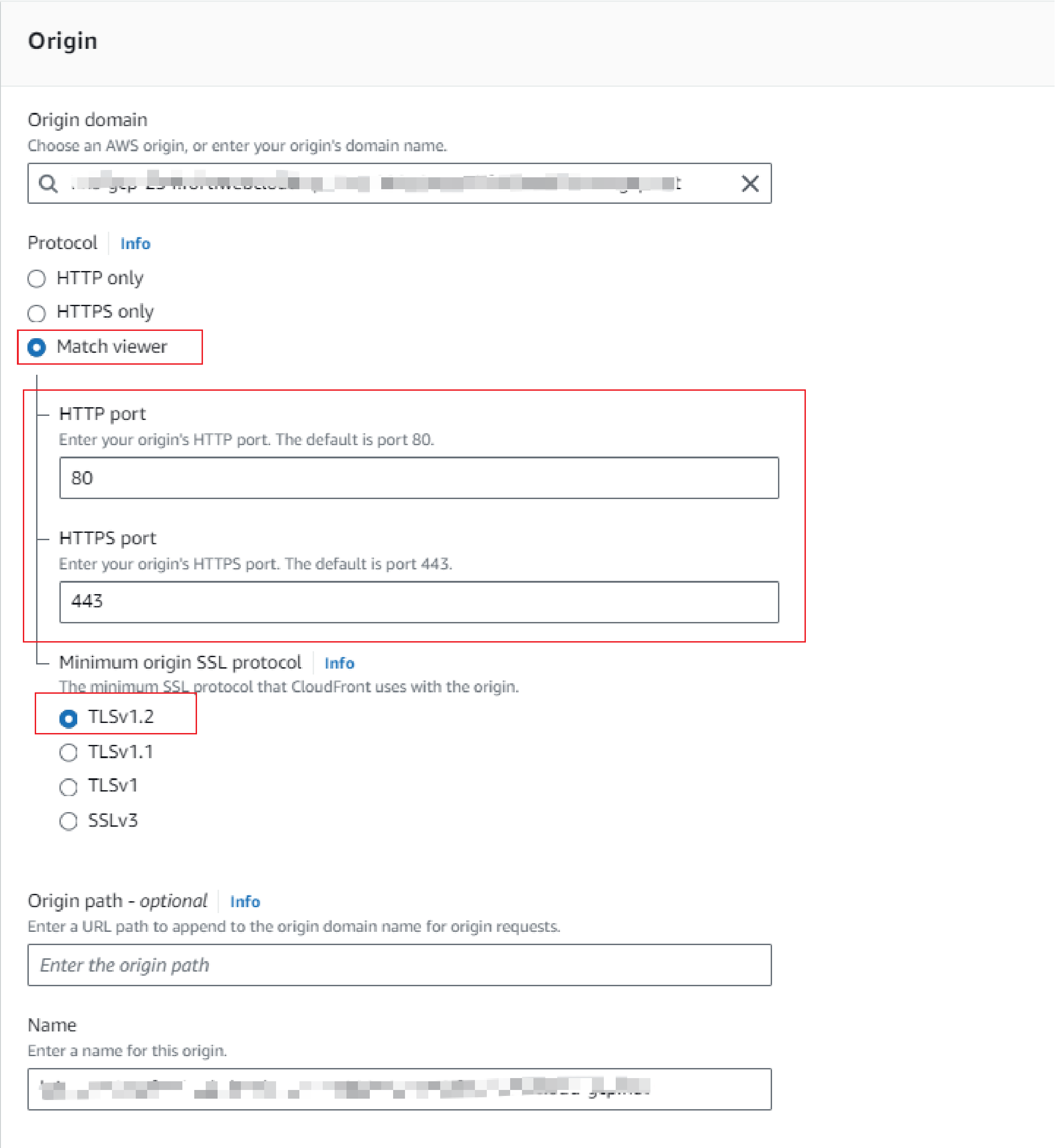
Issued to	Issued by	Valid Until

Showing 0 to 0 of 0 entries

Creating a Distribution in CloudFront

1. Log in to AWS cloud portal. Navigate to **CloudFront**.
2. Click **Create Distribution**.
3. Configure the following options as described. You can set any option not specified here according to your preference. Refer to AWS online help for more information.

Origin	
Origin Domain	Enter the CNAME provided by FortiWeb Cloud.
Origin Protocol Policy	Select **Match Viewer** so that the protocol used for the connections between CloudFront and FortiWeb Cloud can be HTTP or HTTPS. It matches with the protocol used by the viewer, for example, if the viewer connects to CloudFront using HTTPS, CloudFront will connect to FortiWeb Cloud using HTTPS.
HTTP Port	Set HTTP port value to 80.
HTTPS Port	Set HTTPS port value to 443.
Minimum origin SSL protocol	Select **TLSv1.2**.



Origin

Origin domain

Choose an AWS origin, or enter your origin's domain name.

[redacted]

Protocol | Info

○ HTTP only

○ HTTPS only

● Match viewer

HTTP port

Enter your origin's HTTP port. The default is port 80.

80

HTTPS port

Enter your origin's HTTPS port. The default is port 443.

443

Minimum origin SSL protocol | Info

The minimum SSL protocol that CloudFront uses with the origin.

● TLSv1.2

○ TLSv1.1

○ TLSv1

○ SSLv3

Origin path - *optional* | Info

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

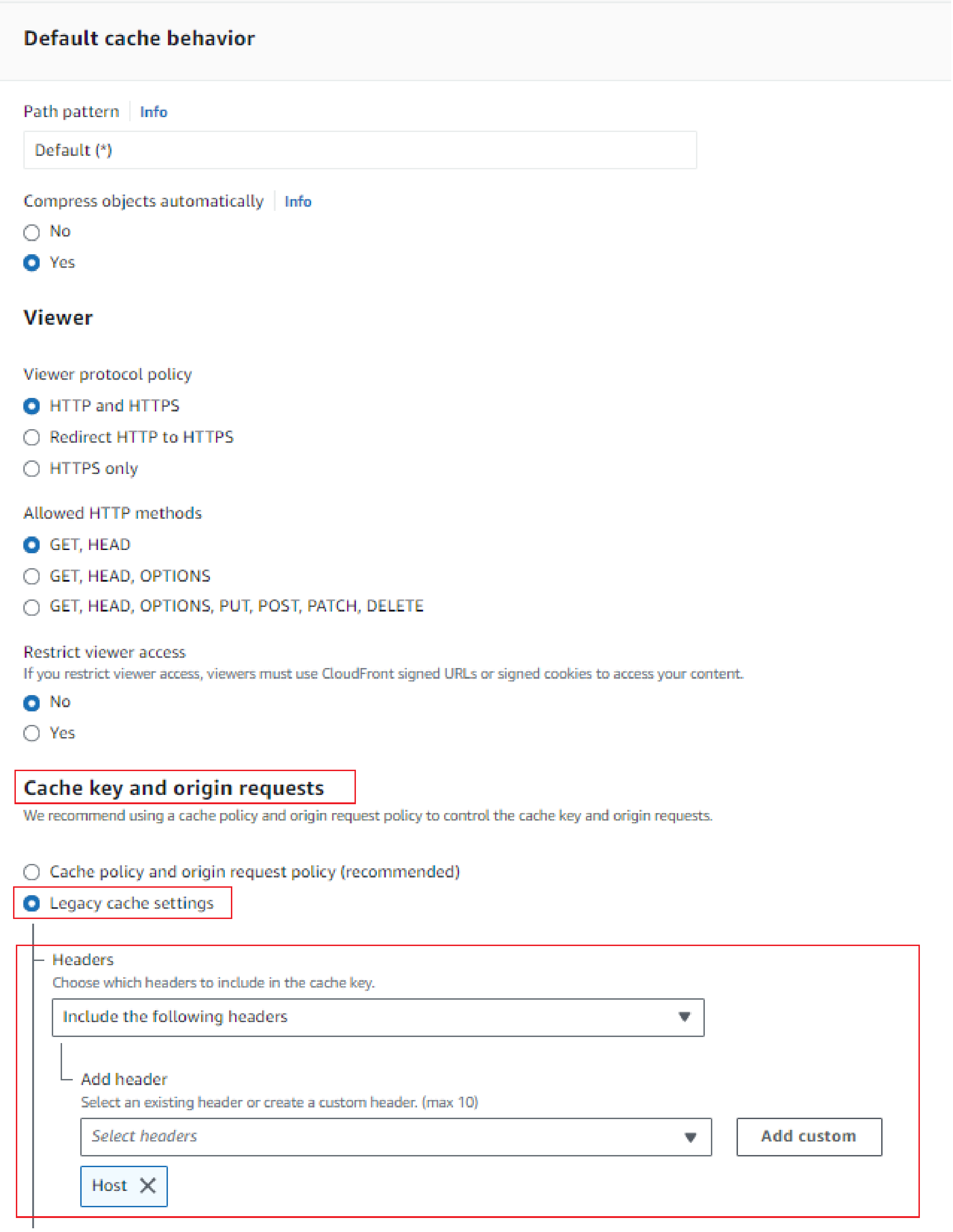
Name

Enter a name for this origin.

[redacted]

Default Cache Behavior	
Path Pattern	This field specifies to which requests you want this cache behavior to apply. For example, a path pattern of **images/*.jpg** would apply the cache behavior to .jpg images.
Compress objects automatically	Select "Yes" if you want CloudFront to automatically compress specific file types when viewers support compressed content. This accelerates downloads by reducing file sizes, resulting in faster rendering of web pages for your users.

Viewer Protocol Policy	You can set this option as you want, but, if you select **Redirect HTTP to HTTPS**, it's suggested to turn off **Redirect all HTTP traffic to HTTPS** in **Network > Endpoint** in FortiWeb Cloud. See Endpoints on page 118.
Allowed HTTP methods	Select the HTTP methods that you want CloudFront to process and forward to your origin
Restrict viewer access	Choose **No** for public URLs or **Yes** for signed URLs when configuring the cache behavior's PathPattern. If selecting **Yes**, specify trusted signers, which are the AWS accounts authorized to create signed URLs.
Cache key and origin requests	Select **Legacy cache settings** from the list, then add header **Host**. CloudFront will directly forward the host header to FortiWeb Cloud.



Default cache behavior

Path pattern | Info

Default (*)

Compress objects automatically | Info

○ No

● Yes

Viewer

Viewer protocol policy

● HTTP and HTTPS

○ Redirect HTTP to HTTPS

○ HTTPS only

Allowed HTTP methods

● GET, HEAD

○ GET, HEAD, OPTIONS

○ GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

● No

○ Yes

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

○ Cache policy and origin request policy (recommended)

● Legacy cache settings

Headers

Choose which headers to include in the cache key.

Include the following headers ▼

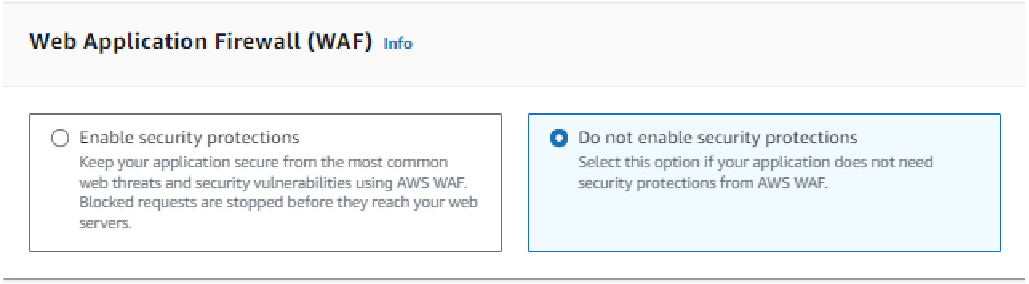
Add header

Select an existing header or create a custom header. (max 10)

Select headers ▼ | Add custom

Host ✕

4. You can choose either WAF option.



Web Application Firewall (WAF) Info

○ Enable security protections

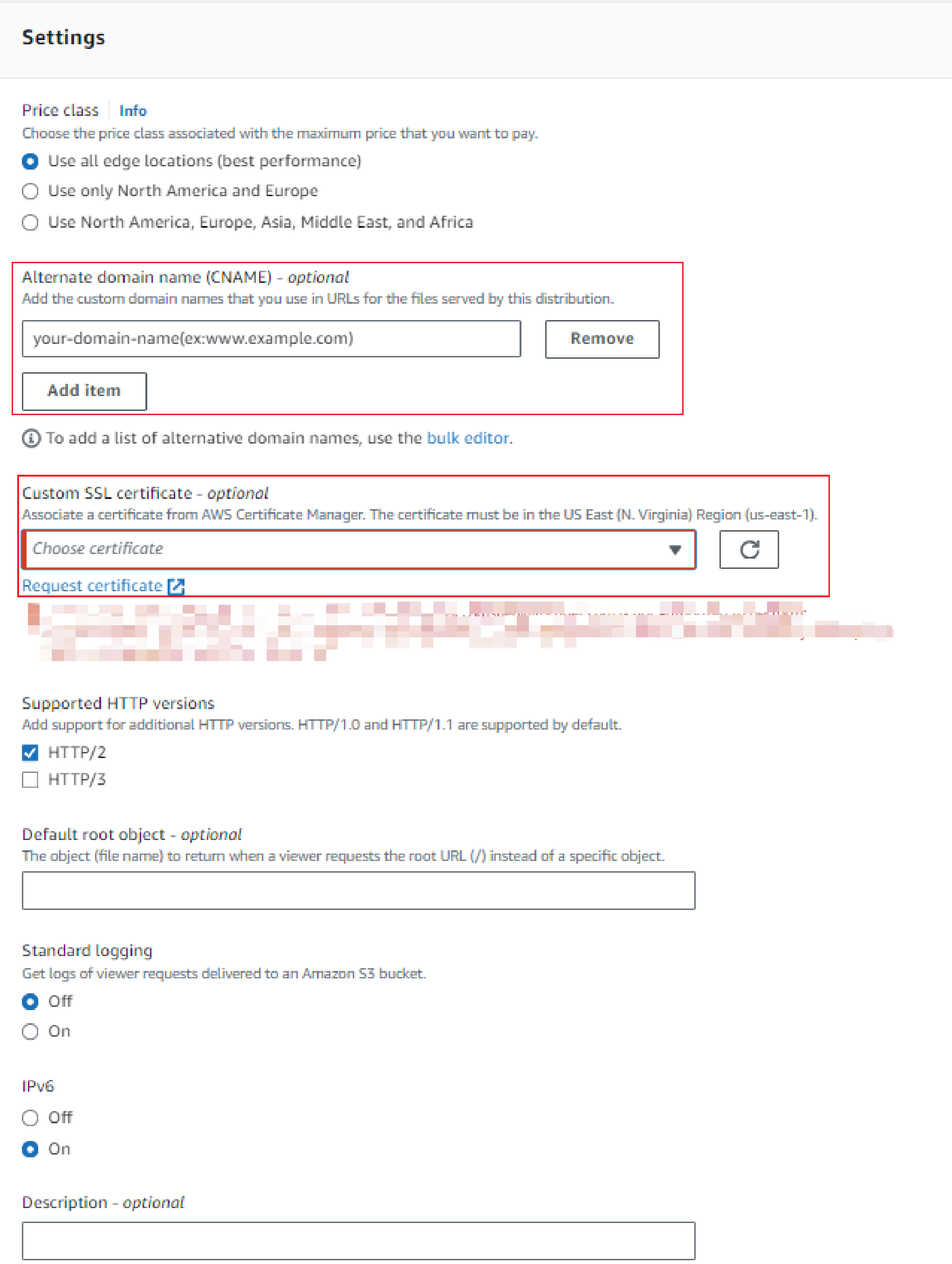
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

● Do not enable security protections

Select this option if your application does not need security protections from AWS WAF.

5. Configure the following options as described. You can set any option not specified here according to your preference. Refer to AWS online help for more information.

Settings	
Alternate Domain Names (CNAMEs)	Enter an additional domain name (e.g., www.example.com) that users use to access your application. FortiWeb Cloud supports multiple domain names for a single application.
SSL Certificate	Select Custom SSL Certificate to upload the SSL certificate.



Settings

Price class | Info

Choose the price class associated with the maximum price that you want to pay.

● Use all edge locations (best performance)

○ Use only North America and Europe

○ Use North America, Europe, Asia, Middle East, and Africa

Alternate domain name (CNAME) - *optional*

Add the custom domain names that you use in URLs for the files served by this distribution.

ⓘ To add a list of alternative domain names, use the bulk editor.

Custom SSL certificate - *optional*

Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

[redacted]

Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

☑ HTTP/2

□ HTTP/3

Default root object - *optional*

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

Standard logging

Get logs of viewer requests delivered to an Amazon S3 bucket.

● Off

○ On

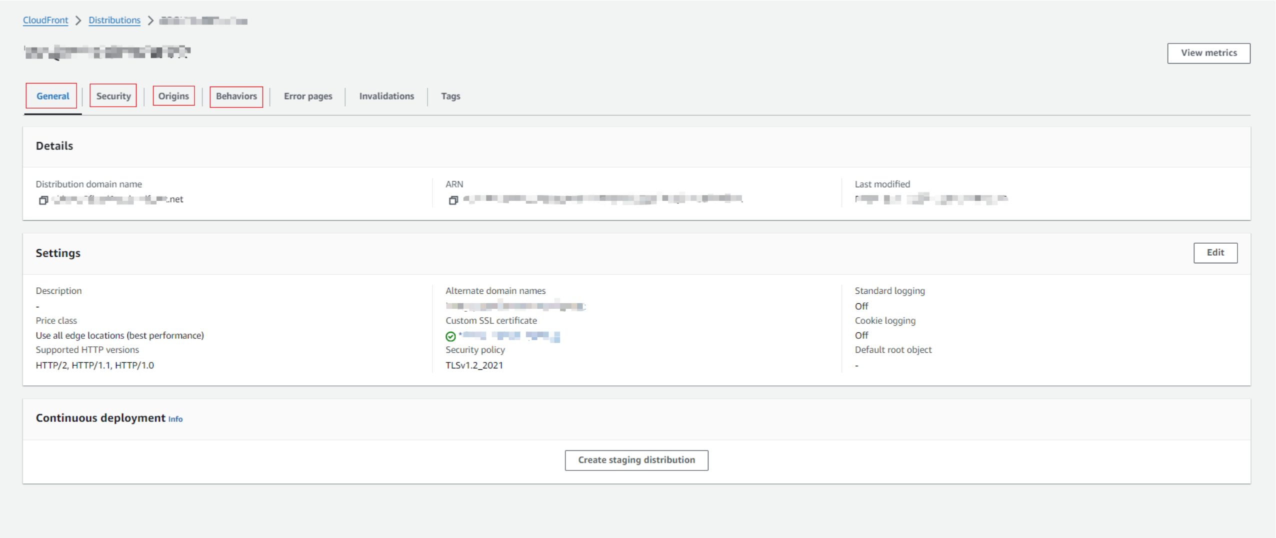
IPv6

○ Off

● On

Description - *optional*

6. Modify your existing CloudWatch distributions by clicking into the tabs outlined below. Additionally, you can consult the configuration details provided in steps 3-5 above.
   - **General**: Settings configurations (details in Settings on page 224).
   - **Security**: WAF configurations (details in WAF options).
   - **Origins**: Origin configurations (details in Origin on page 220).
   - **Behaviors**: Default Cache Behaviors Configurations (details in Default Cache Behavior on page 221).



CloudFront > Distributions > [redacted]

[redacted]

Details

Distribution domain name
[redacted].net

ARN
[redacted]

Last modified
[redacted]

Settings

Description
-
Price class
Use all edge locations (best performance)
Supported HTTP versions
HTTP/2, HTTP/1.1, HTTP/1.0

Alternate domain names
[redacted]
Custom SSL certificate
✓ [redacted]
Security policy
TLSv1.2_2021

Standard logging
Off
Cookie logging
Off
Default root object
-

Continuous deployment Info

Modifying DNS record to use the domain name provided by CloudFront

Go to your DNS service to modify the DNS record to route queries for the your application's domain name (e.g. www.example.com) to the CloudFront domain name (e.g. d1234.cloudfront.net).

If you use AWS Route 53, refer to Working with Records on how to create or change the DNS records.

At this point, the queries to your application's domain name should successfully be forwarded to CloudFront first, then reach FortiWeb Cloud.

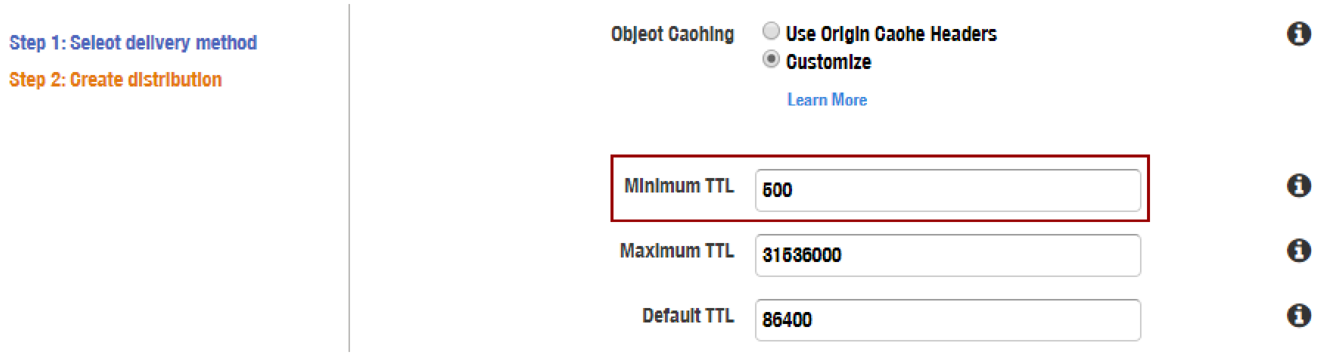
Configuring Error Pages

When FortiWeb Cloud detects a violation to its security rules, it takes appropriate actions, such as blocking the request and returning an error code to the client who initiated this request. The error code is cached in CloudFront, so that when the same client initiates the same request next time, CloudFront can directly return this error code to the client.

However, the request might be falsely detected as a violation. You can add the request as an exception in FortiWeb Cloud so that it will not be detected as a violation next time, but, if you have set a long Minimum TTL, the client may keep receiving the cached error code until the minimum TTL passes. During this period, CloudFront uses the cached error code to respond to the subsequent requests instead of forwarding them to FortiWeb Cloud for re-processing.

In most cases, the minimum TTL in the distribution settings is set to a long time value because for efficiency considerations you may not want CloudFront to renew its caches too frequently, so, the optimal solution for the above mentioned error code caching problem is to set a comparatively shorter Minimum TTL specially for error codes.

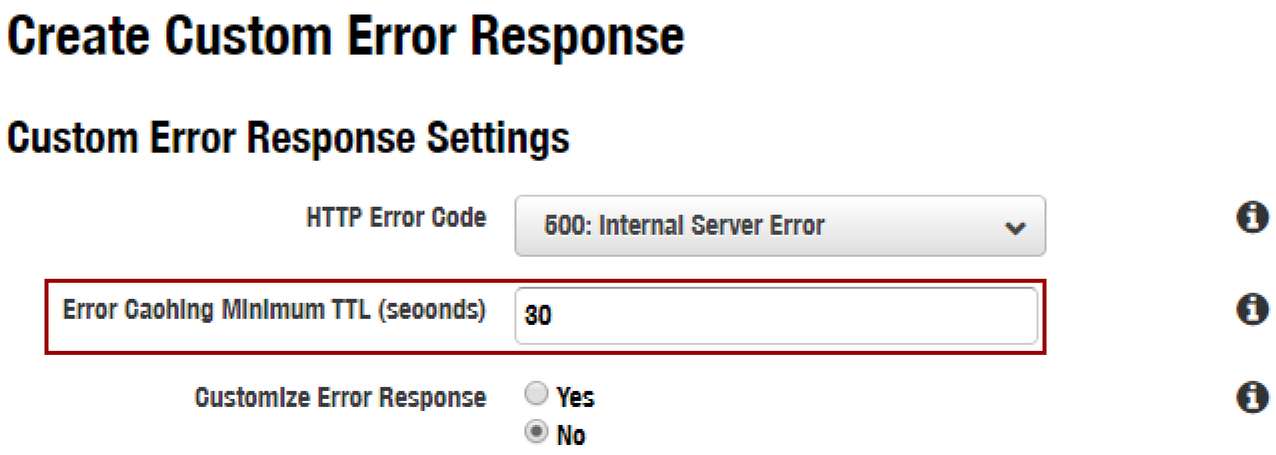
In the following example shown in the screenshots, the Minimum TTL in the distribution is set to 500s, while the Minimum TTL for the error code is set much shortely to 30s. This distinguishes the minimum TTL time for error codes and the rest content. The objects such as the rarely changing icons and background images stay in cache for a long time, while the error codes frequently renews.



Step 1: Select delivery method
Step 2: Create distribution

Object Caching ○ Use Origin Cache Headers ● Customize
Learn More

Minimum TTL: 500
Maximum TTL: 31536000
Default TTL: 86400



Create Custom Error Response

Custom Error Response Settings

HTTP Error Code: 500: Internal Server Error
Error Caching Minimum TTL (seconds): 30
Customize Error Response: ○ Yes ● No

To set the Minimum TTL for error pages:

1. In the distribution list, find the distribution you just created. Click its ID to open the distribution details page.
2. Select **Error Pages** tab.
3. Click **Create Custom Error Response** to create a new error page, or click an existing error page to edit its Minimum TTL.
4. Set **Error Caching Minimum TTL (Seconds)**.
5. Configure other options as desired.
6. Click **Create**.

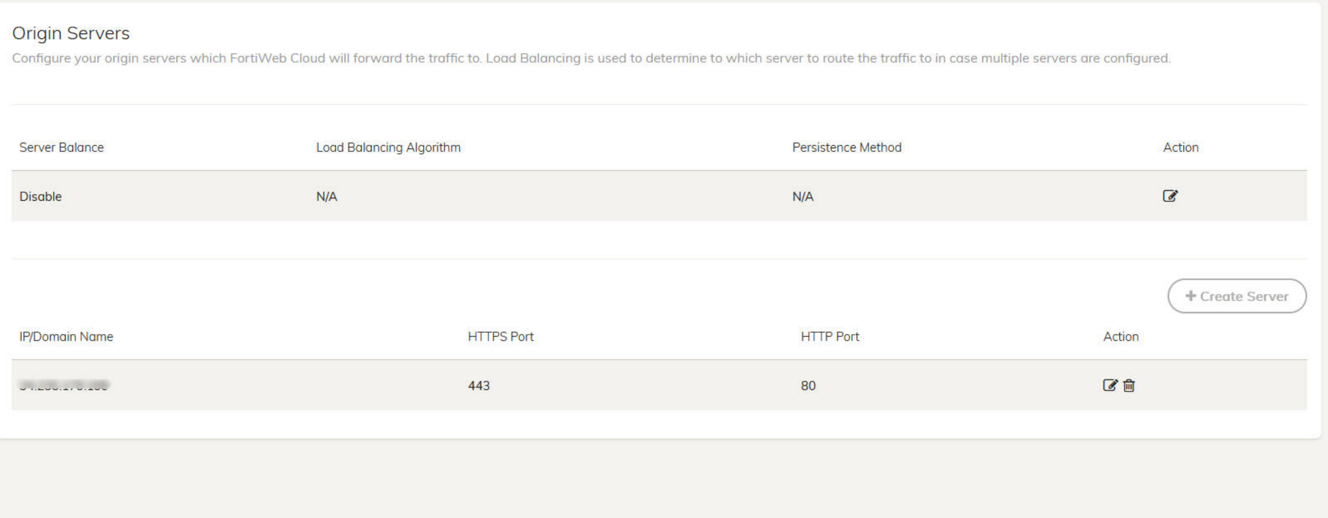
After you complete the settings above, you can go ahead configure security rules in FortiWeb Cloud to protect your application.

FortiWeb Cloud has a security module called Caching and Compression. It allows you to cache and compress objects that rarely change, such as icons, background images, movies. If you have configured CloudFront to cache such objects, you can disable this module in FortiWeb Cloud.

Network settings for applications serving different content over HTTP and HTTPS

In most cases, when users enter the application's domain name over either HTTP or HTTPS, the same content is returned. However, if you have configured your application server to serve different content over HTTP and HTTPS protocols, you should configure the network settings in FortiWeb Cloud as described below.

In the following example, Server Balance is turned off, causing all HTTP traffic to route through Port 80, while HTTPS traffic is routed through Port 443.



Origin Servers

Configure your origin servers which FortiWeb Cloud will forward the traffic to. Load Balancing is used to determine to which server to route the traffic to in case multiple servers are configured.

Server Balance	Load Balancing Algorithm	Persistence Method	Action
Disable	N/A	N/A	✎

+ Create Server

IP/Domain Name	HTTPS Port	HTTP Port	Action
[redacted]	443	80	✎ 🗑

Endpoints

In **Network > Endpoints**, or in the **Network Settings** step of the **Add Application wizard**, enable **HTTP** and **HTTPS**. Disable **Redirect all HTTP traffic to HTTPS**.

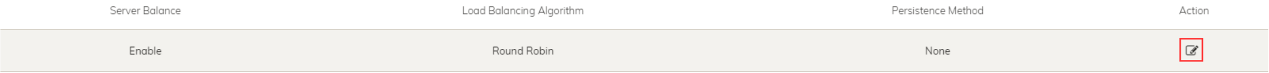
Servers

FortiWeb Cloud communicates with your application server over both HTTP and HTTPS protocols when there is only one origin server.

Step 1 - Disabling server balance

After the application is onboarded, **Server Balance** is enabled by default to apply load balancing algorithm to multiple servers. As only one server is allowed if you want FortiWeb Cloud to communicate with the origin server over both HTTP and HTTPS, you need to disable **Server Balance**.

1. In **Network > Origin Servers**, click the **Edit** icon.



Server Balance	Load Balancing Algorithm	Persistence Method	Action
Enable	Round Robin	None	✎

2. Turn off **Server Balance**. Please note the existing origin servers will all be deleted. You can add one server later.
3. Click **OK**.

Step 2 - Creating server

Add a single server and specify the HTTP and HTTPS ports.

1. In **Network > Origin Servers**, click **Create Server**.
2. Refer to Origin Servers on page 114 to configure server settings. Make sure to specify both HTTP and HTTPS port numbers. If you haven't disabled **Server Balance**, only one port is allowed to be configured on this page.
3. Click **OK**.

FortiWeb Cloud and Splunk

About Splunk

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.

FortiWeb Cloud App for Splunk

The Fortinet FortiWeb Cloud App provides real-time and historical dashboard on threats, performance metrics and audit information for FortiWeb Cloud.

With the massive set of logs and big data aggregation through Splunk, the FortiWeb Cloud App for Splunk is certified with pre-defined threat monitoring and performance indicators that help guide network security . As the de facto trending dashboard for many enterprises or service providers, IT administrators can also modify the regular expression query to custom fit views for advanced security reporting and compliance mandates.
FortiWeb Cloud App for Splunk: https://splunkbase.splunk.com/app/4627/

Fortinet FortiWeb Cloud App depends on the Add-on to work properly. Make sure Fortinet FortiWeb Cloud Add-on for Splunk has been installed before you proceed.

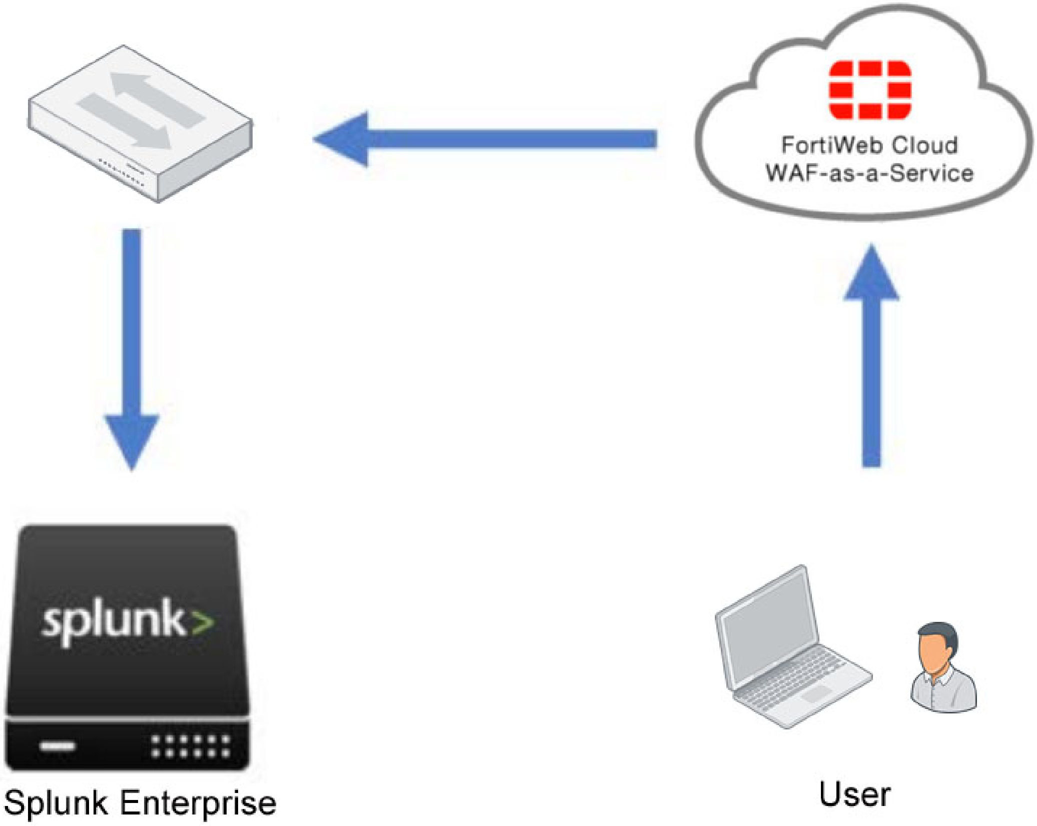
FortiWeb Cloud Add-on for Splunk

Fortinet FortiWeb Cloud Add-On for Splunk is the technical add-on (TA) developed by Fortinet, Inc. The add-on enables Splunk Enterprise to ingest or map security and audit data collected from FortiWeb Cloud, which includes attack and audit logs.

Fortinet FortiWebCloud Add-on for Splunk: https://splunkbase.splunk.com/app/4626/

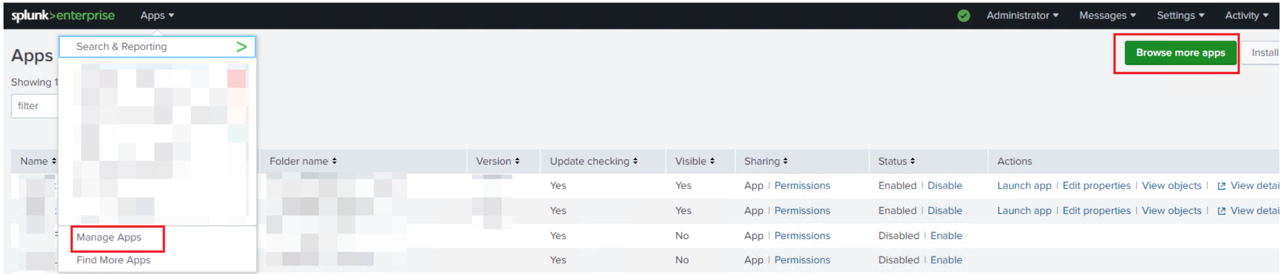
Deployment prerequisites

1. Splunk version 8.1.0 or later
2. FortiWeb Cloud Add-On for Splunk (https://splunkbase.splunk.com/app/4626)
3. FortiWeb Cloud App for Splunk (https://splunkbase.splunk.com/app/4627)
4. A Splunk.com username and password



Splunk configuration

1. Click the gear (Manage Apps) from Splunk Enterprise.
2. Click **Browse more apps**, and search for **FortiWebCloud**.



Apps

Showing 1

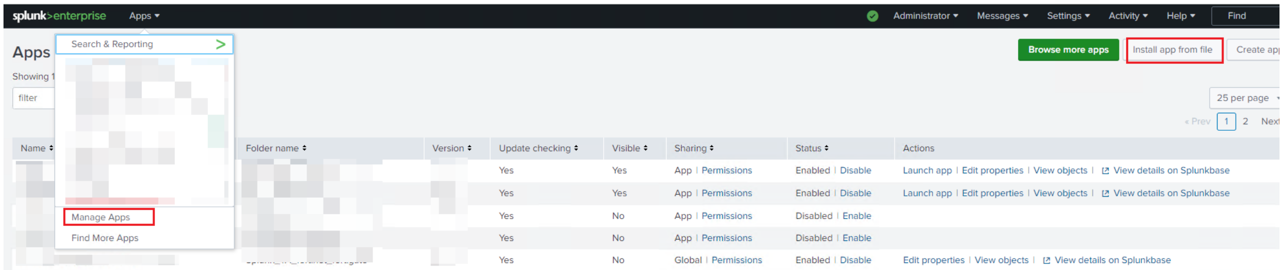
filter

Name ⬍	Folder name ⬍	Version ⬍	Update checking ⬍	Visible ⬍	Sharing ⬍	Status ⬍	Actions
[redacted]	[redacted]	[redacted]	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View detai
[redacted]	[redacted]	[redacted]	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View detai
[redacted]	[redacted]		Yes	No	App | Permissions	Disabled | Enable	
[redacted]	[redacted]		Yes	No	App | Permissions	Disabled | Enable	

3. Install **Fortinet FortiWebCloud Add-on for Splunk**.

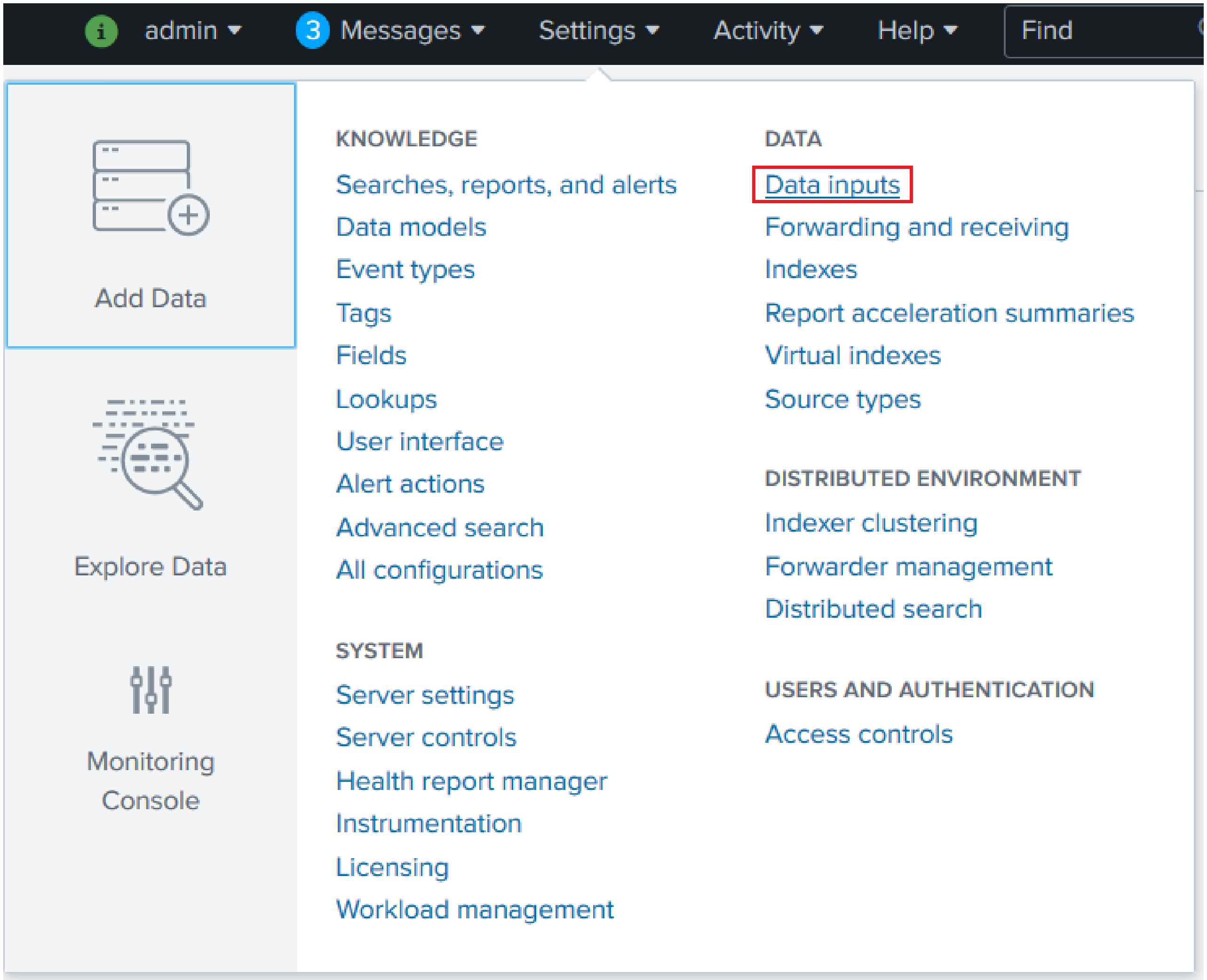
4. Install **Fortinet FortiWebCloud App for Splunk** .

   Note: If the **Fortinet FortiWebCloud App for Splunk** and **Fortinet FortiWebCloud Add-on for Splunk** cannot be installed from **Browse more apps**, please go to Splunkbase, download the Add-on and App (two .tgz files), then install them by clicking the gear (Manage Apps) > **Install app from file**

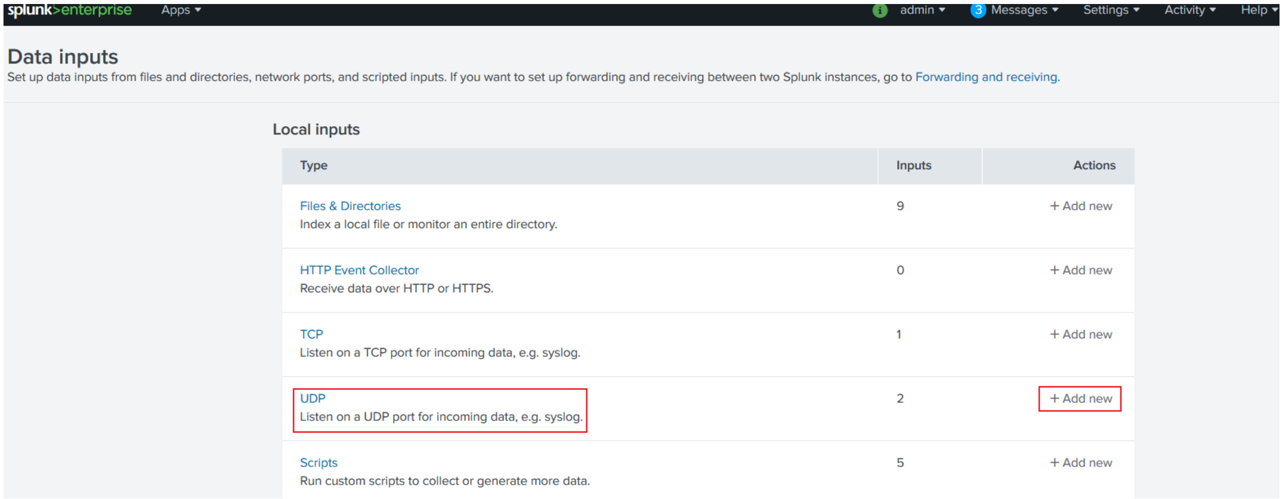


Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
[redacted]	[redacted]	[redacted]	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
[redacted]	[redacted]	[redacted]	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on Splunkbase
[redacted]	[redacted]	[redacted]	Yes	No	App | Permissions	Disabled | Enable	
[redacted]	[redacted]	[redacted]	Yes	No	App | Permissions	Disabled | Enable	
[redacted]	[redacted]	[redacted]	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase

5. Restart Splunk Enterprise.
6. From **Settings**, click **Data Inputs** under **Data**.



7. Click **Add new** in the UDP or TCP line to create a new input rule with corresponding protocol. See the UDP protocol example below.



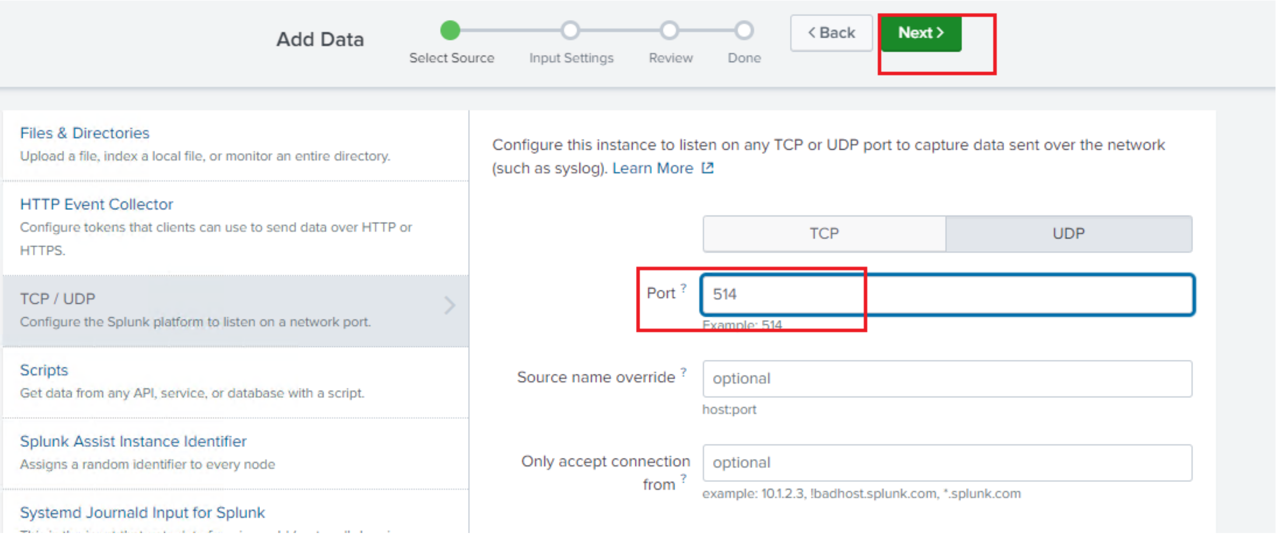
Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	9	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	2	+ Add new
Scripts Run custom scripts to collect or generate more data.	5	+ Add new

8. Create a UDP data source. In the example below, we have used Port 514. Afterwards, click **Next**.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journald Input for Splunk

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

TCP | UDP

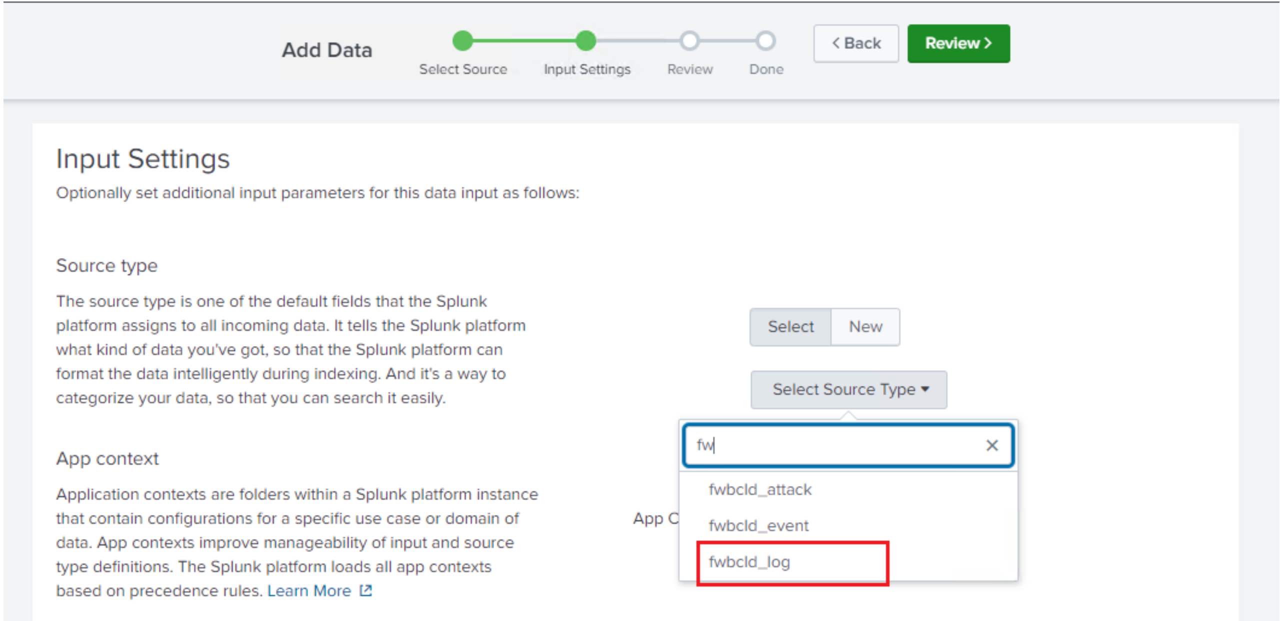
Port ? 514
Example: 514

Source name override ? optional
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

9. For **Source type**, click the **Select** tab then click **Select Source Type**. Enter "fwbcld" in the filter box, and select **fwbcld_log**.
By default, **Fortinet FortiWebCloud App for Splunk** will automatically extract FortiWebCloud log data from inputs

with source type 'fwbcld_log'.



Input Settings

Optionally set additional input parameters for this data input as follows:

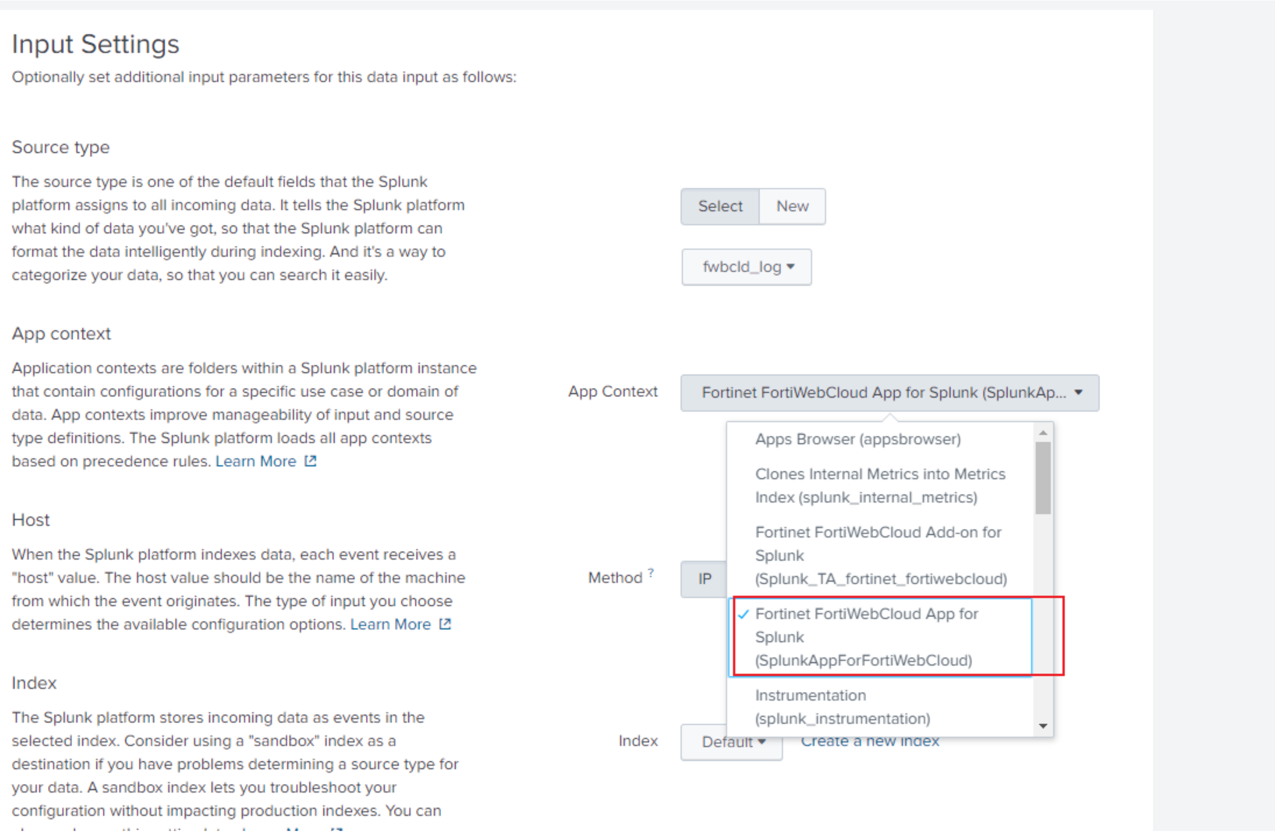
Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

10. For **App context**, select Fortinet FortiWebCloud App for Splunk .


Select
New
fwbcld_log ▾
App Context
Fortinet FortiWebCloud App for Splunk (SplunkAp... ▾
Apps Browser (appsbrowser)
Clones Internal Metrics into Metrics Index (splunk_internal_metrics)
Fortinet FortiWebCloud Add-on for Splunk (Splunk_TA_fortinet_fortiwebcloud)
✓ Fortinet FortiWebCloud App for Splunk (SplunkAppForFortiWebCloud)
Instrumentation (splunk_instrumentation)
Method ?
IP
Index
Default ▾
Create a new index

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can

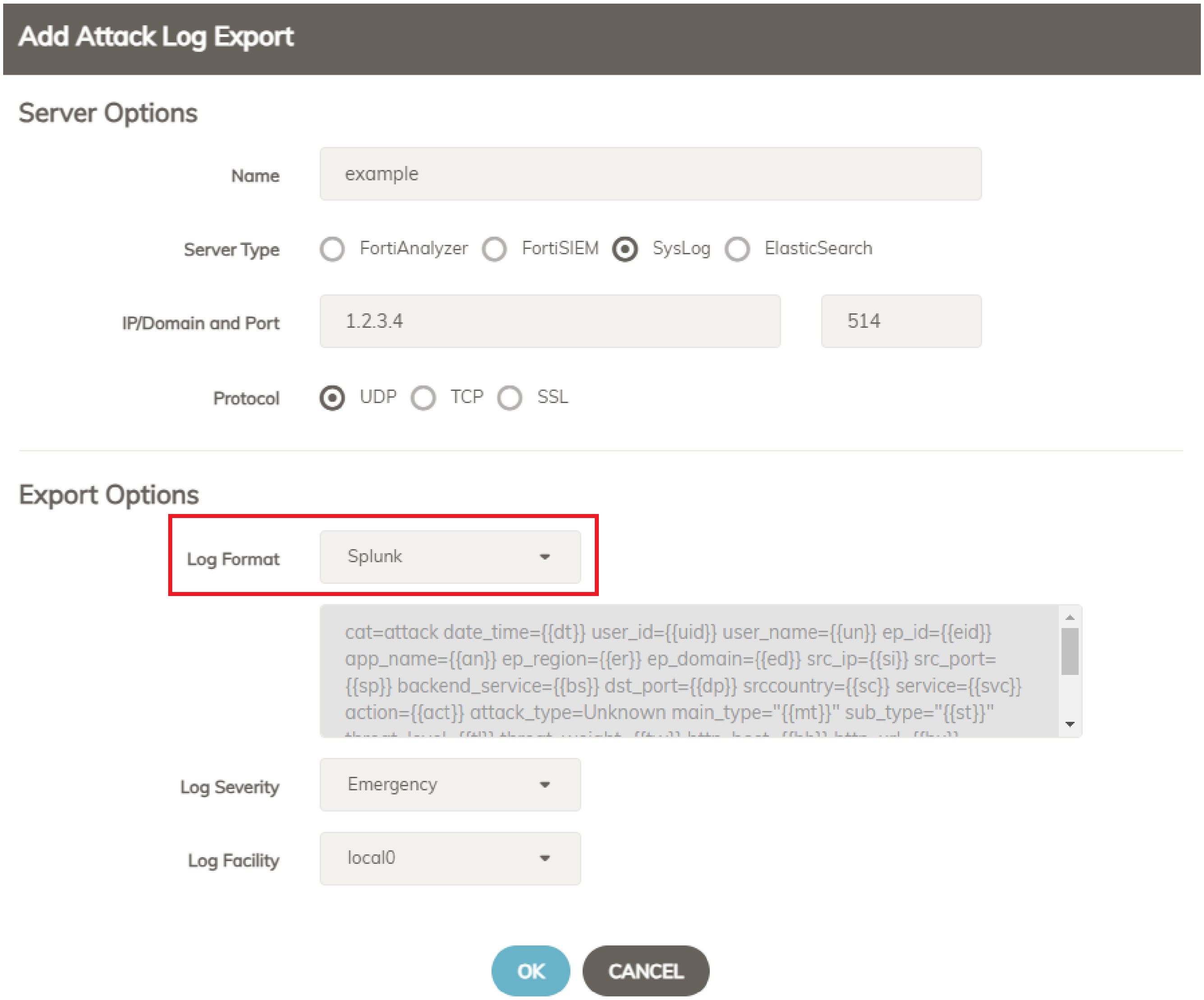
11. Click **Review** to check the items.
12. Click **Submit**.

FortiWeb Cloud configuration

Configure FortiWeb Cloud to send logs to Splunk server.

Attack logs

1. Go to **Log Settings**, enable **Attack Log Export**.
2. Click **Add Log Server**.
3. Configure the server and export options. See Exporting attack logs on page 105 for details.
   For Log Format, select **Splunk**.



Add Attack Log Export

Server Options

Name: example

Server Type: ○ FortiAnalyzer ○ FortiSIEM ● SysLog ○ ElasticSearch

IP/Domain and Port: 1.2.3.4 514

Protocol: ● UDP ○ TCP ○ SSL

Export Options

Log Format: Splunk

```
cat=attack date_time={{dt}} user_id={{uid}} user_name={{un}} ep_id={{eid}}
app_name={{an}} ep_region={{er}} ep_domain={{ed}} src_ip={{si}} src_port=
{{sp}} backend_service={{bs}} dst_port={{dp}} srccountry={{sc}} service={{svc}}
action={{act}} attack_type=Unknown main_type="{{mt}}" sub_type="{{st}}"
```

Log Severity: Emergency

Log Facility: local0

Audit logs

1. Go to **Global > System Settings > Settings**.
2. Enable **Audit Logs Export**.
3. Configure these settings. See Audit logs on page 83 for details.
   For Log Format, select **Splunk**.

Logs verification on Splunk server

To verify whether logs have been received by Splunk server

1. On Splunk web UI, go to **Apps > Search & Reporting**.
2. If attack logs have been sent to Splunk, enter **'sourcetype="fwbcld_attack"'** in the search box. Change the time range if necessary. The attack logs will be listed below.
3. If audit logs have been sent to Splunk, enter **'sourcetype="fwbcld_event"'** in the search box. Change the time range if necessary. The audit logs will be listed below.
4. Go to the dashboard of Fortinet FortiWebCloud App for Splunk , from the **Security Overview**, **Attack**, and **Event** tabs, you can see data parsed and presented.

Troubleshooting

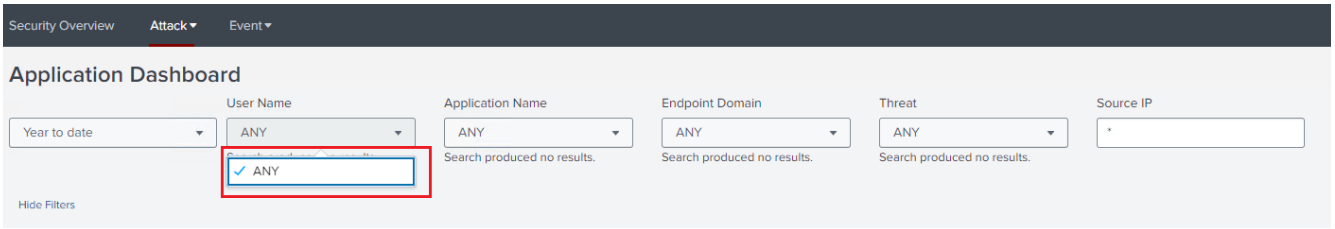
If data is not showing up in the Dashboards:

- Go to **Settings > Data Inputs.** Verify that you have a UDP data input enabled on port ,for example, 514.
- Go to **Settings > Indexes.** Verify that your Index (typically main) is receiving data and that the Latest Event is recent. If not, verify the FortiWeb Cloud Syslog settings are correct and that it can reach the Splunk server.
- Verify that the port used for data input is accessible in your security group of the Splunk server.
- Ensure that the FortiWeb Cloud service Management IP addresses are in the white list of your Splunk server.
- Verify the Splunk server is listening to the correct port.

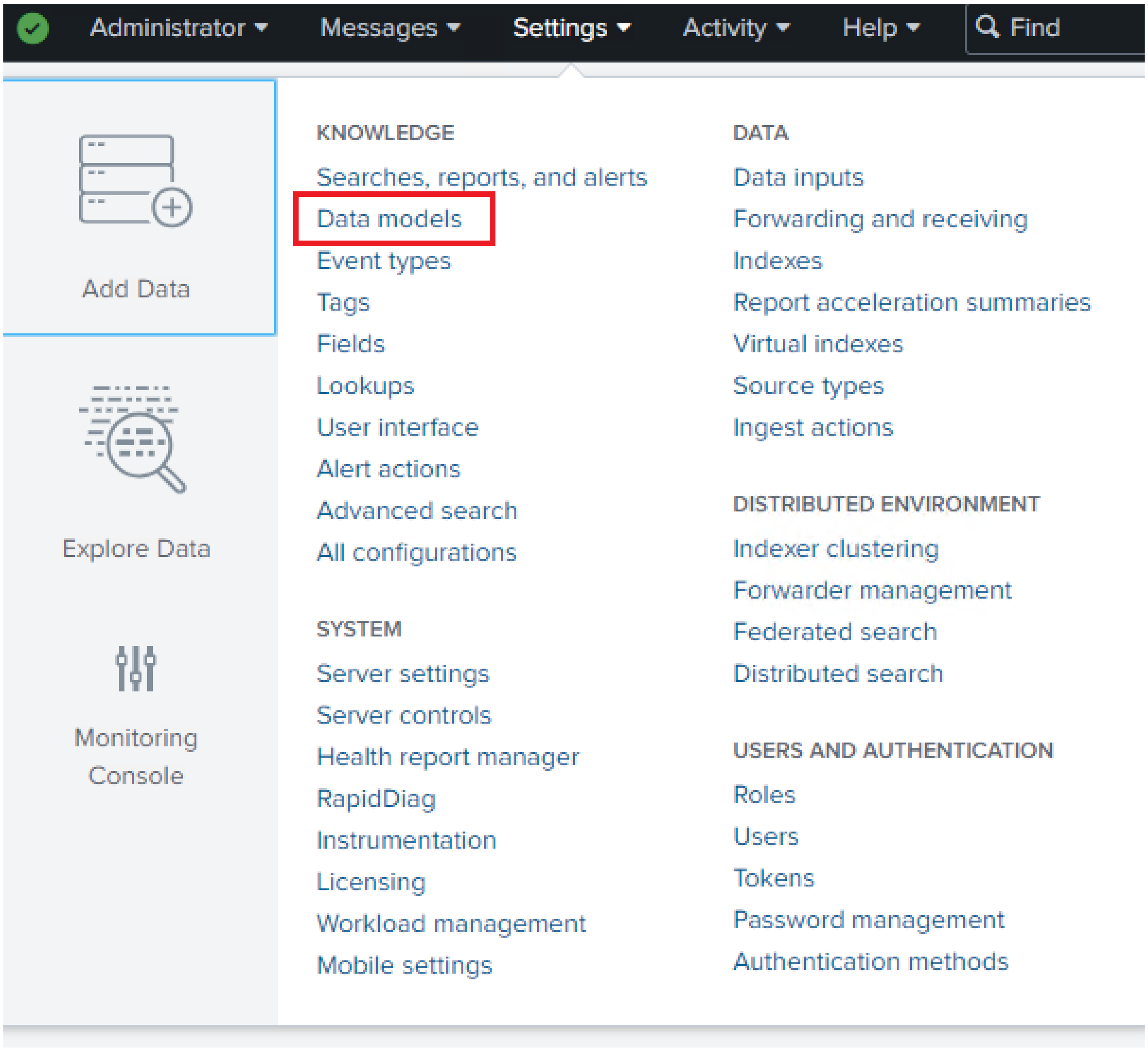
If the App and Add-on cannot be installed from **Browse more**:

- Go to Splunkbase, download the Add-on and App (two .tgz files), then install them by clicking the gear (Manage Apps) > **Install app from file.**

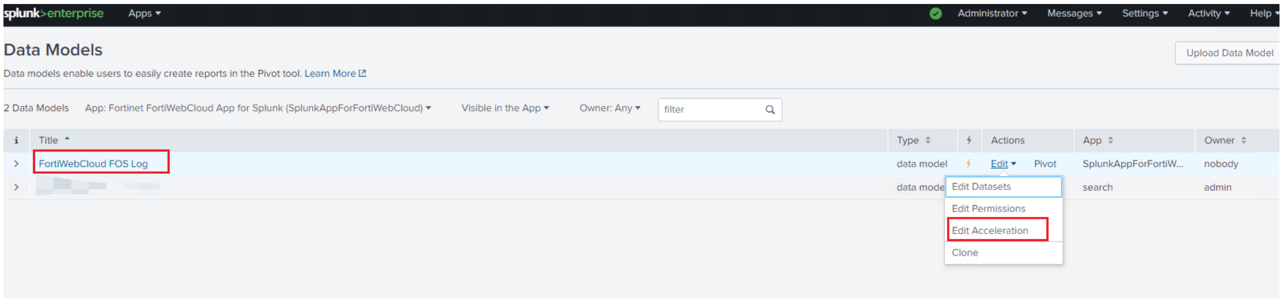
If the dropdown in Attack or Event dashboards does not have value:



a. Go to **Settings > Data models**



b. Find **FortiWebCloud FOS** Log, click **Edit > Edit Acceleration**



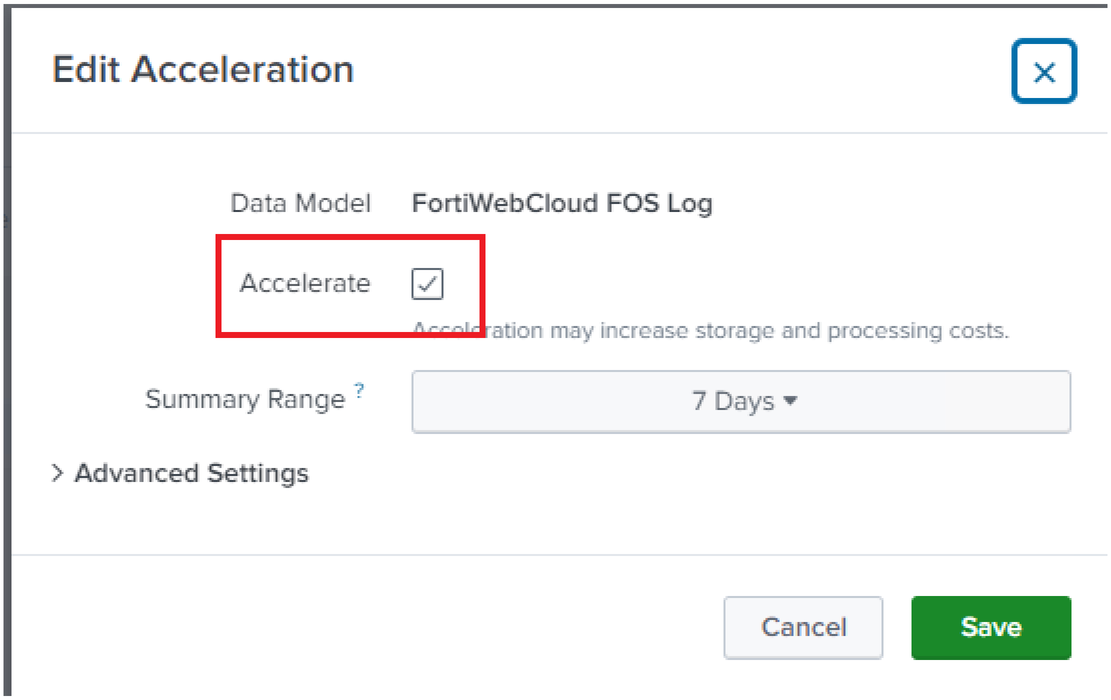
Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

2 Data Models App: Fortinet FortiWebCloud App for Splunk (SplunkAppForFortiWebCloud) ▾ Visible in the App ▾ Owner: Any ▾ filter

i	Title	Type	⚡	Actions		App	Owner
>	FortiWebCloud FOS Log	data model	⚡	Edit ▾	Pivot	SplunkAppForFortiW...	nobody
>	[redacted]	data mode				search	admin

c. Enable **Accelerate**, then wait for 5 mins or restart Splunk. You will see the dropdown in App.



Edit Acceleration

Data Model FortiWebCloud FOS Log

Accelerate ☑

Acceleration may increase storage and processing costs.

Summary Range ? 7 Days ▾

> Advanced Settings

Fortinet Security Fabric

FortiWeb Cloud supports Fortinet Security Fabric. You can configure FortiGate to view statistics of sites secured by FortiWeb Cloud from the FortiGate Dashboard page.

Add FortiWeb Cloud device to the Security Fabric

1. Ensure your FortiGate is running version 7.0.0 or newer, as older versions are no longer supported.

   Check your FortiGate version in the GUI by going to **Dashboard > Status**. The **Firmware** field in the **System Information** widget shows the version along with the build number.
2. Configure your FortiGate firewall or security group to allow access for the fabric connector's IPs: 3.226.2.163 and 3.123.68.65.
3. Ensure that the Security Fabric is enabled on FortiGate. See the FortiGate Administration Guide for more information.
4. On the root FortiGate of the Security Fabric, make sure **Allow other Security Fabric devices to join** is enabled.
5. On the root FortiGate, ensure that the appropriate interface is enabled to listen for supported Fabric devices.
6. Configure the FortiGate information on the FortiWeb Cloud GUI.
   1. Login to your FortiWeb Cloud account, and go to **Global> System Settings > settings**.
   2. Scroll down to Fabric Connector and click **Create**. The **Add FortiGate Information** pane opens.
   3. Enter the management IP of your fabric connector. The Port number is set to 8013 by default.
7. Access the FortiGate GUI and wait for the connection request to appear, typically within a minute after completing the previous step.
8. After approving the connection request, you can access the dashboard of the newly added fabric connector, which is customizable with widgets. For further details, see Dashboards and Monitors.

Add dashboard widget for the FortiWeb Cloud device

1. Select a dashboard in the tree menu of the FortiGate GUI.
2. In the banner, click **Add Widget**. The **Add Dashboard Widget** pane opens.
3. Select **Fabric Device** in Security Fabric.
4. Select the desired device and the widget name.
5. Click **Add Widget**.
   You can add multiple widget names.

View statistics of sites secured by FortiWeb Cloud

1. Go to **Dashboard**.
2. Click the dashboard's name.
   You can now see the incoming requests, server status, threats, and throughput, etc. of the sites.

Managing External IdP roles in FortiCloud IAM

FortiCloud enables you to access and manage all of Fortinet's Cloud Services, including FortiWeb Cloud, through a single account. When you access FortiWeb Cloud, the login is authenticated through your FortiCloud account.

FortiCloud offers the IAM feature that enables you to create and manage External IdP roles that allow users from your organization to log in to the FortiWeb Cloud portal using the user credentials with your organization's ID provider. External IdP users are authenticated by your organization's ID provider. After the user is authenticated, they can access FortiWeb Cloud based on their role.

This feature is only available for certain accounts upon request. Contact the FortiCare team to request setup.

When an IdP user clicks **Logout**, they are only logging out of the FortiWeb Cloud portal, not your organization's ID provider.

Please see FortiCloud documentation for detailed instructions on Adding external IdP roles.

Frequently used regular expressions

Some elements occur often in FortiWeb Cloud regular expressions, such as expressions to match domain names, URLs, parameters, and HTML tags. You can use these as building blocks for your own regular expressions.

To match...	You can use...
Line endings (platform-independent)	(\r\n)|\n|\r

To match...	You can use...
Any alphanumeric character (ASCII only; e.g. does not match é or É)	[a-zA-Z0-9]
Specific domain name (e.g. www.example.com; case insensitive)	(?i)\bwww\.example\.com\b
Any domain name (valid non-internationalized TLDs only; does **not** match domain names surrounded by letters or numbers)	(?i)\b.*\.(a(c|d|e(ro)?|f|g|i|m|n|o|q|r|s(ia)?|t|y|w|x|z)|b(a|b|d|e|f|g|h|i(z)?|j|m|n|o|r|s|t|v|w|y|z)|c(a(t)?|c|d|f|g|h|i|k|l|m|n|o((m)?(op)?)|r|s|u|v|x|y|z)|d(e|j|k|m|o|z)|e(c|du|e|g|h|r|s|t|u)|f(i|j|k|m|o|r)|g(a|b|d|e|f|g|h|i|l|m|n|ov|p|q|r|s|t|u|w|y)|h(k|m|n|r|t|u)|i(d|e|l|m|n(fo)?(t)?|o|q|r|s|t)|j(e|m|o(bs)?|p)|k(e|g|h|i|m|n|p|r|w|y|z)|l(a|b|c|i|k|r|s|t|u|vy)|m(a|c|d|e|g|h|il|k|l|m|n|o(bi)?|p|q|r|s|t|u(seum)?|v|w|x|y|z)|n(a(me)?|c|e(t)?|f|g|i|l|o|p|r|u|z)|o(m|rg)|p(a|e|f|g|h|k|l|m|n|r(o)?|s|t|w|y)|qa|r(e|o|s|u|w)|s(a|b|c|d|e|g|h|i|j|k|l|m|n|o|r|s|t|u|v|y|z)|t(c|d|el|f|g|h|j|k|l|m|n|o|p|r(avel)?|t|v|w|z)|u(a|g|k|s|y|z)|v(a|c|e|g|i|n|u)|w(f|s)|xxx|y(e|t|u)|z(a|m|w))\b
Any sub-domain name	(?i)\b(.*)\.example\.com\b
Specific IPv4 address	\b10\.1\.1\.1\b
Any IPv4 address	\b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b
Specific HTML tag (well-formed HTML only, e.g. `<br>` or `<img src="1.gif" />`; does **not** match the element's contents between a tag pair; does **not** match the closing tag)	(?i)<\s*TAG\s*[^>]*>
Specific HTML tag pair and contained text/tags, if any (well-formed HTML only; expression does **not** validate by DTD/Schema)	(?i)<\s*(TAG)\s*[^>]*>[^<]*</\1>
Any HTML tag pair and contained text/tags, if any (well-formed HTML only; expression does **not** validate by DTD/Schema)	(?i)<\s*([A-Z][A-Z0-9]*)\b[^>]*>(.*?)</\1>
Any HTML comment	(?:<|<)!--[\s\S]*?--[\t\n\r]*(?:>|>)
Any HTML entity (well-formed entities only; expression does **not** validate by DTD/Schema)	&(?i)(#((x([\dA-F]){1,5})|(104857[0-5]|10485[0-6]\d|1048[0-4]\d\d|104[0-7]\d{3}|10[0-3]\d{4}|0?\d{1,6}))|([A-Za-z\d.]{2,31}));
JavaScript UI events (`onClick()`, `onMouseOver()`, etc.)	(?i):on(blur|c(hange|lick)|dblclick|focus|keypress|(key|mouse)(down|up)|(un)?load|mouse(move|o(ut|ver))|reset|s(elect|ubmit))

To match...	You can use...
All parameters that follow a question mark or hash mark in the URL (e.g. `#pageView` or `?param1=valueA&param2=valueB`...; back-reference to this match does not include the question/hash mark itself)	[#\?](.*)

Best practices

The following topics introduce the best practices when using FortiWeb Cloud.

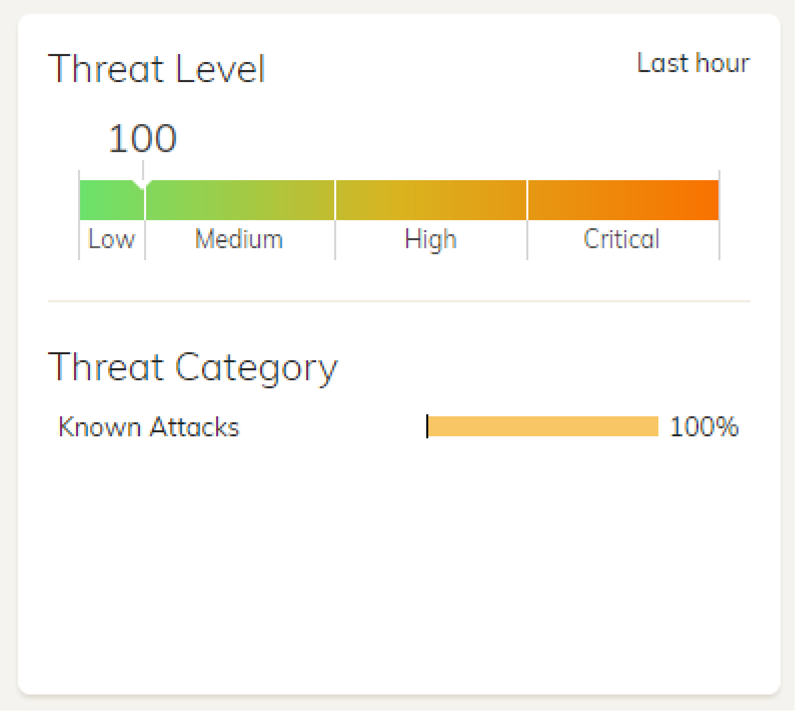
- Using Dashboard to monitor important notices
- Utilizing FortiView to reduce false positives
- Setting up a secure environment

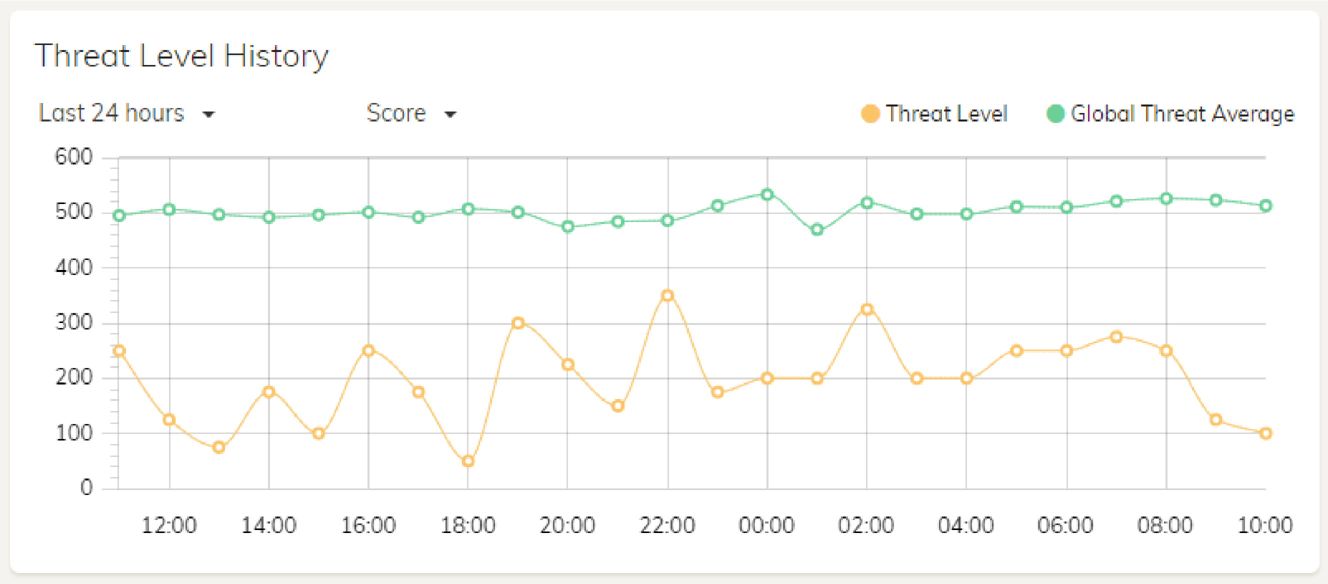
Using Dashboard to monitor important notices

The Dashboard page displays the application's request and threat data, and other important statistics.

Threat data

The Threat Level and Threat Level History widgets display the threat scores of the application over a certain time range. FortiWeb Cloud can send alerts to the specified email addresses if the threat score exceeds a certain level. For how to configure the alert email settings, see Configuring attack log alert.

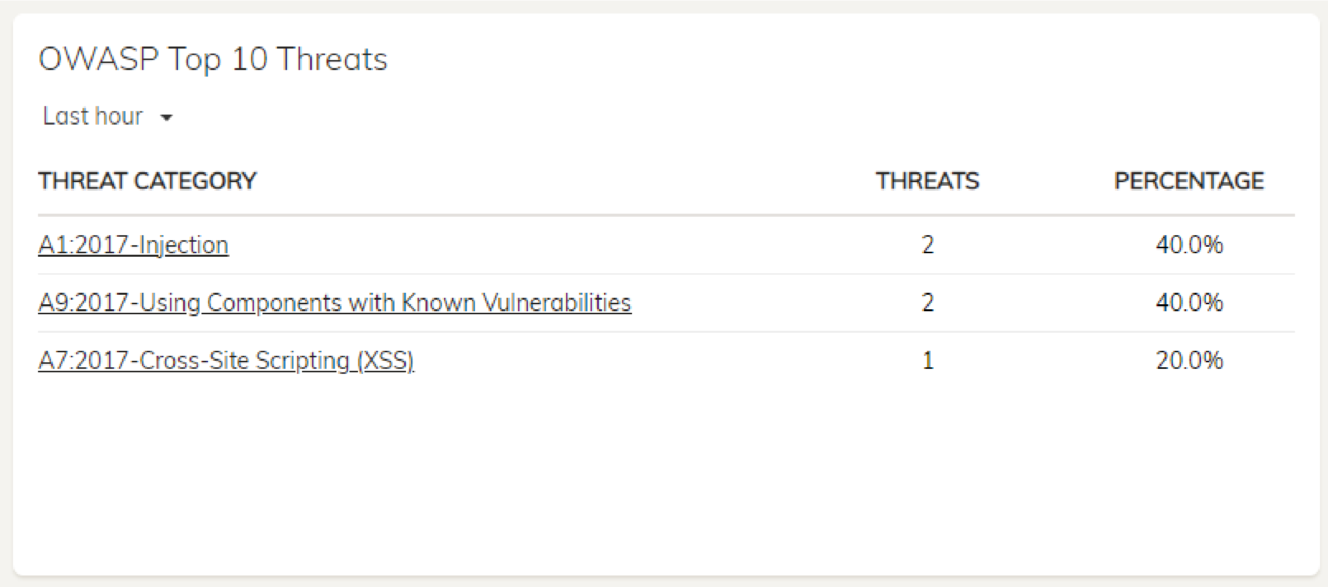




Threat Level History

Last 24 hours ▾ Score ▾

Use the OWASP Top 10 Threats widget to investigate into the most critical attacks to your application. Click the threat category links to check the details such as the source IP and affected URLs.



OWASP Top 10 Threats

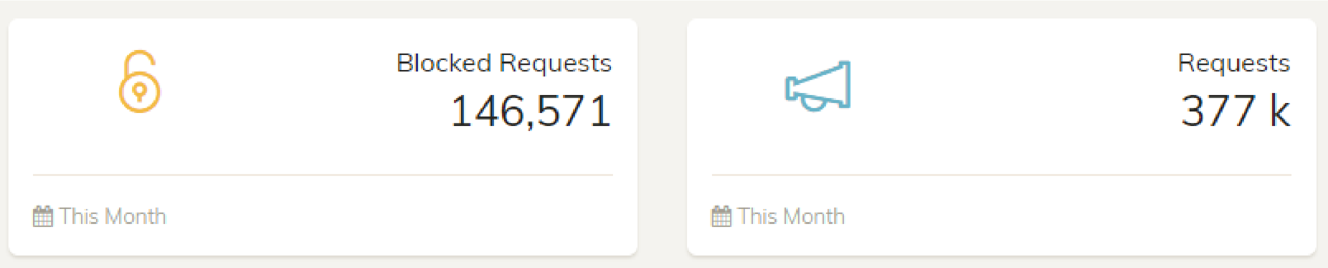
Last hour ▾

THREAT CATEGORY	THREATS	PERCENTAGE
A1:2017-Injection	2	40.0%
A9:2017-Using Components with Known Vulnerabilities	2	40.0%
A7:2017-Cross-Site Scripting (XSS)	1	20.0%

Statistics on requests

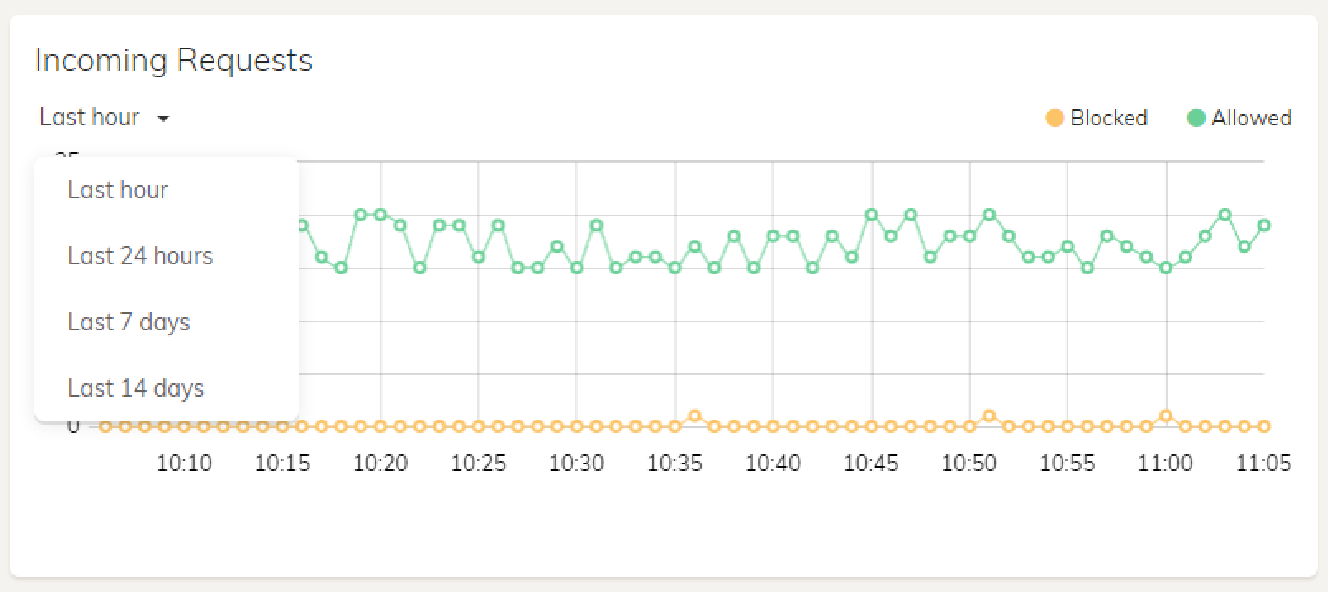
The following widgets display the number of requests to the application, and how many requests are blocked by FortiWeb Cloud.

You can use the time range selector in the Incoming Requests widget to view the number of allowed and blocked requests over the last hour, 24 hours, 7 days, and 14 days.



Blocked Requests
146,571
This Month

Requests
377 k
This Month



Incoming Requests

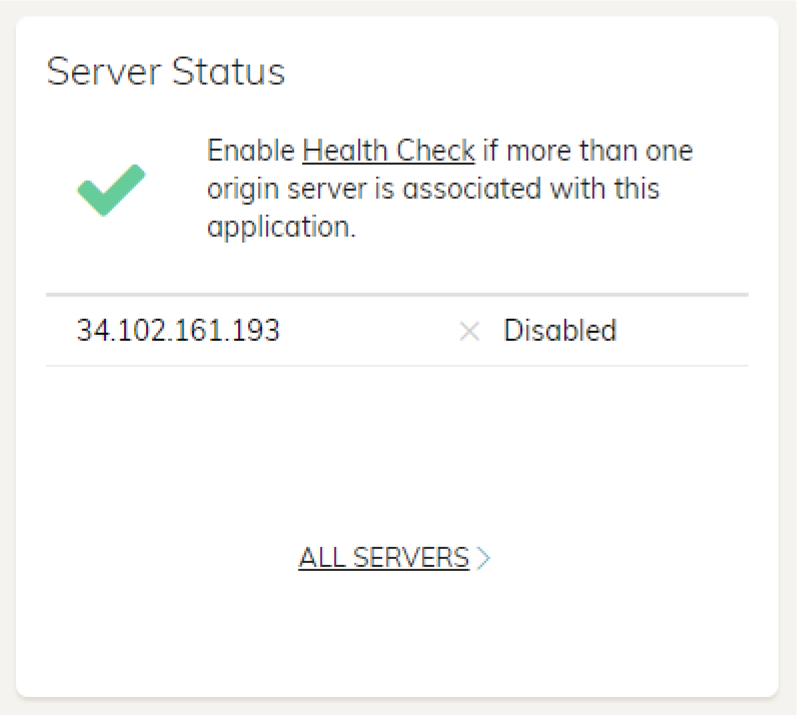
Last hour

- Last hour
- Last 24 hours
- Last 7 days
- Last 14 days

Monitoring server status

The Server Status widget displays whether the origin server is available. In the following example, the server is available (✓), while the health check is disabled (✕ Disabled).

If you have multiple origin servers, it's recommended to enable Health Check, so that when a server becomes unavailable FortiWeb Cloud can distribute its traffic to other servers.



Server Status

✓ Enable Health Check if more than one origin server is associated with this application.

34.102.161.193	× Disabled

Utilizing FortiView to reduce false positives

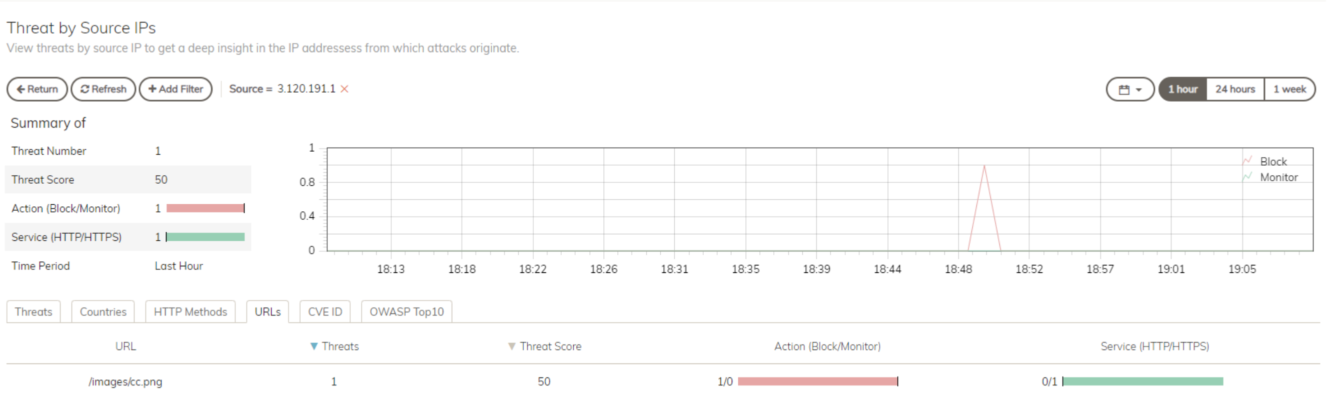
Sometimes legitimate traffic may be detected as attacks if inappropriate thresholds are set in the security rules. Moreover, even regular users may violate the rules due to the nature of some web pages, such as the stock list web page, where users can be identified as bots because they tend to frequently refresh the pages.

To avoid legitimate traffic being blocked, it's recommended to regularly check the attack statistics in FortiView. It provides deep insights in the attack information and helps you figure out the false positives.

For example, if the attacks are originated from many different source IPs, but they affect the same URL, this might be false positives. It can be caused by the nature of the web page itself that the regular traffic behaves like attacks. You can investigate the issue by clicking source IPs on the **Threat by Source IPs** page. If the **URLs** tab of many source IPs shows the same URL, you may consider whether they are false positives.

If the false positives are of the **Known Attacks** type, you can click **Add Exception** beside the signature ID. The traffic to that URL will no longer be treated as an attack even if it matches the signatures.

If the false positives are of other types, you can edit the corresponding security rules to add this URL as an exception.



Threat by Source IPs

View threats by source IP to get a deep insight in the IP addressess from which attacks originate.

Source = 3.120.191.1

Summary of

Threat Number	1
Threat Score	50
Action (Block/Monitor)	1
Service (HTTP/HTTPS)	1
Time Period	Last Hour

URL	Threats	Threat Score	Action (Block/Monitor)	Service (HTTP/HTTPS)
/images/cc.png	1	50	1/0	0/1

The method mentioned above is just an example. Go ahead explore more ways to utilize FortiView for false positive investigation.

Setting up a secure environment

FortiWeb Cloud provides features such as Two-Factor Authentication (2FA), Role Management, etc. for you to secure your account and restrict permissions for the administrators.

With 2FA enabled, your account will be secured not only by the account credential, but also by a dynamic code generated on the 2FA device. See Two-Factor Authentication.

If you have multiple administrators managing your account, it's a good practice to create roles for them to access different applications in your account or distinguish them with read-only or read-write permissions. See Role management on page 77

How to block the ongoing DDoS attack

To identify the characteristics of HTTP requests in a DDoS attack and add security rules to defend against it, the following methods can be used to analyze the attack and set up rules to block it:

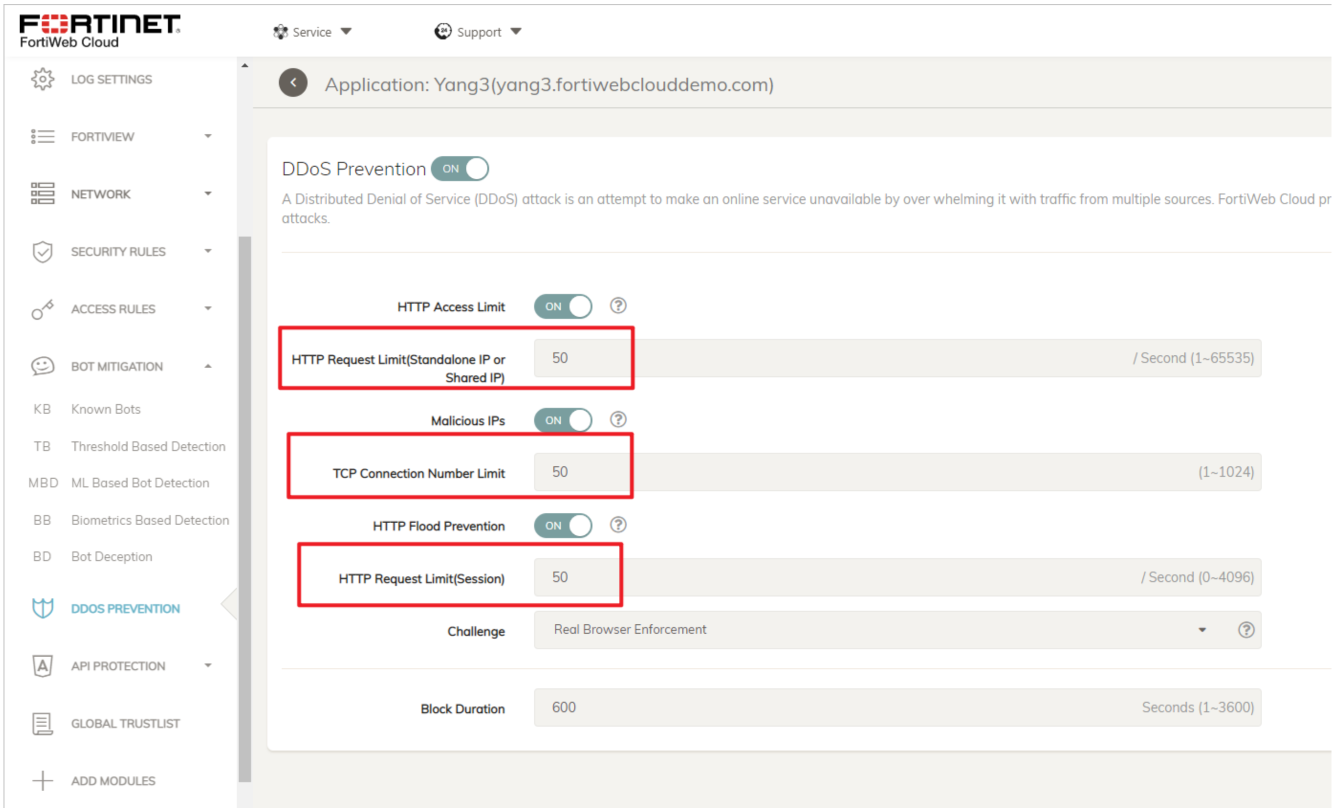
- STEP 1: Limiting the frequency and blocking source IP addresses
- STEP 2: Blocking requests based on user-agent, parameters, HTTP headers, etc.
- STEP 3: Blocking bots

STEP 1: Limiting the frequency and blocking source IP addresses

Check the server's HTTP access logs to examine the frequency and source IP address of requests. Attackers often flood the server with a large number of fake requests, so it is possible to identify malicious requests based on their frequency and source IP address.

The following rules can be set on FortiWeb Cloud to limit the frequency and block the source IPs:

- **DDoS Prevention**
  Set up rules to limit the frequency of HTTP requests and TCP connections (e.g., set the limit to 50).
  For more information, see DDoS prevention



Application: Yang3(yang3.fortiwebclouddemo.com)

DDoS Prevention ON

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by over whelming it with traffic from multiple sources. FortiWeb Cloud pr
attacks.

HTTP Access Limit ON

HTTP Request Limit(Standalone IP or Shared IP) 50 / Second (1~65535)

Malicious IPs ON

TCP Connection Number Limit 50 (1~1024)

HTTP Flood Prevention ON

HTTP Request Limit(Session) 50 / Second (0~4096)

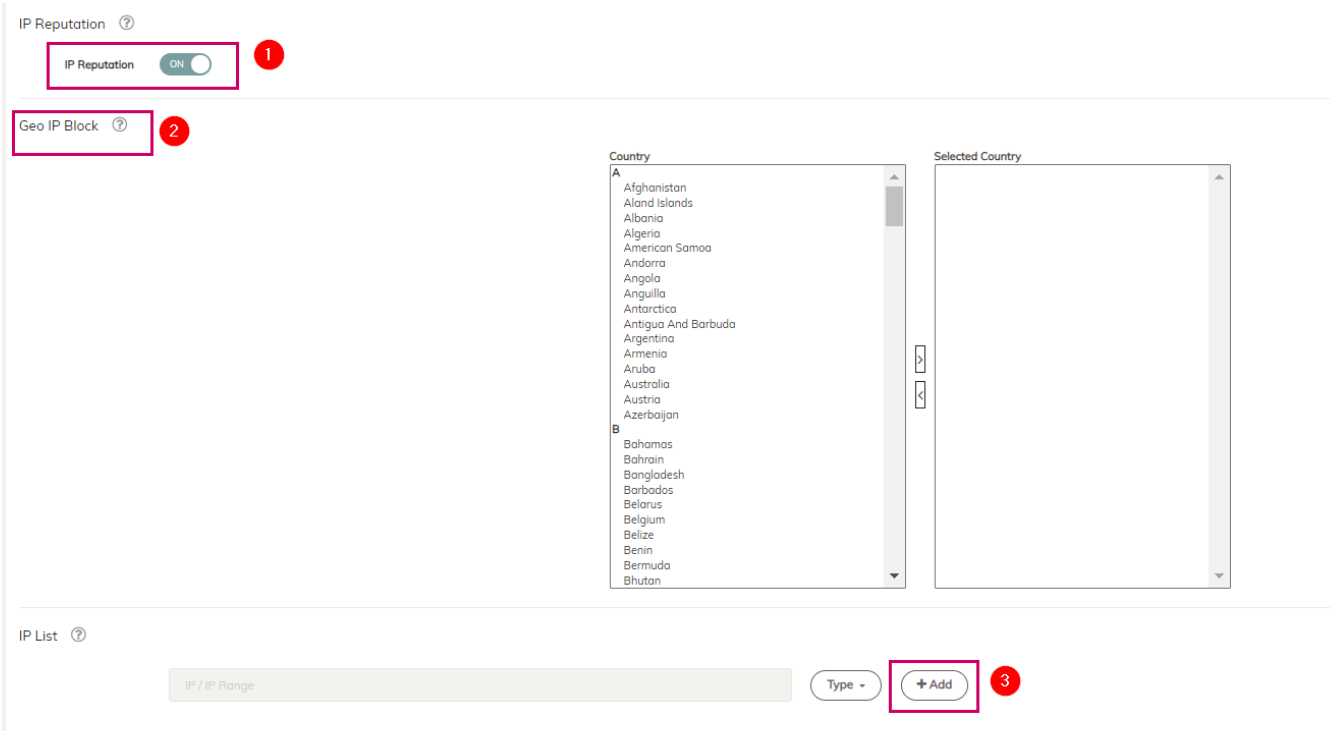
Challenge Real Browser Enforcement

Block Duration 600 Seconds (1~3600)

- **Access Rules > IP Protection**

1. Enable **IP Reputation** to block client access based on up-to-date threat intelligence.
2. Select the countries of origin for the attacks.
3. Add the source IP addresses of the attacks in the **IP List**.
   Please note that source IP blocking can also be set in **Advanced Applications > Custom Rule**.

For more information, see IP Protection.



IP Reputation

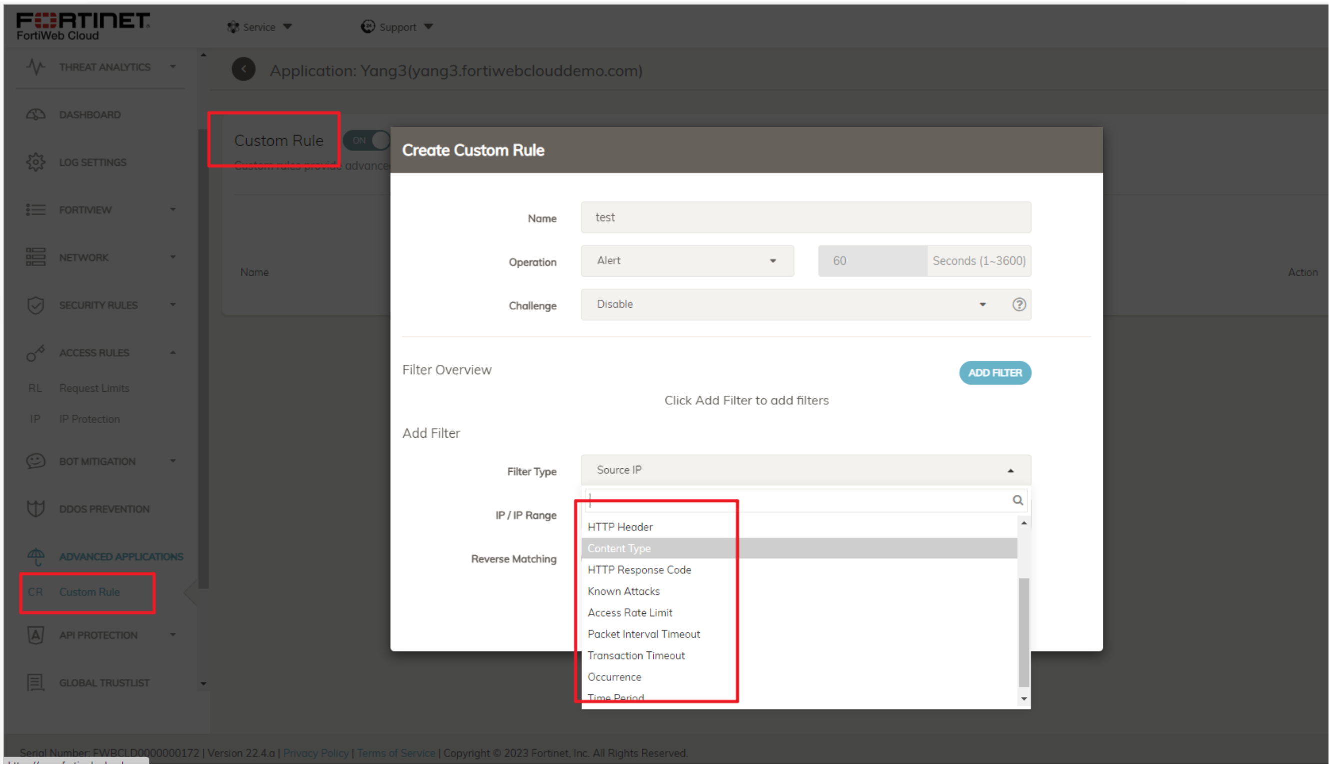
IP Reputation: ON

STEP 2: Blocking requests based on user-agent, parameters, HTTP headers, etc.

- Analyze the user-agent field in the HTTP requests as attackers often use custom user-agents to hide their identity. Identify specific user-agents that are likely malicious.
- Check the parameters in the HTTP requests as attackers may use specific parameters to try to bypass security measures (e.g., look for common attack parameters like 'wp-admin').
- Use an HTTP header analyzer to examine the HTTP request headers in the attack, such as Accept-Encoding and Content-Encoding, as attackers may use compression techniques to hide their malicious code.

To accurately target the attacks, add corresponding filters in **Advanced Applications > Custom Rule** and set the action to **Period Block**.

For more information, see Custom Rule on page 162.



Create Custom Rule

Name: test

Operation: Alert — 60 Seconds (1~3600)

Challenge: Disable

Filter Overview

Click Add Filter to add filters

Add Filter

Filter Type: Source IP

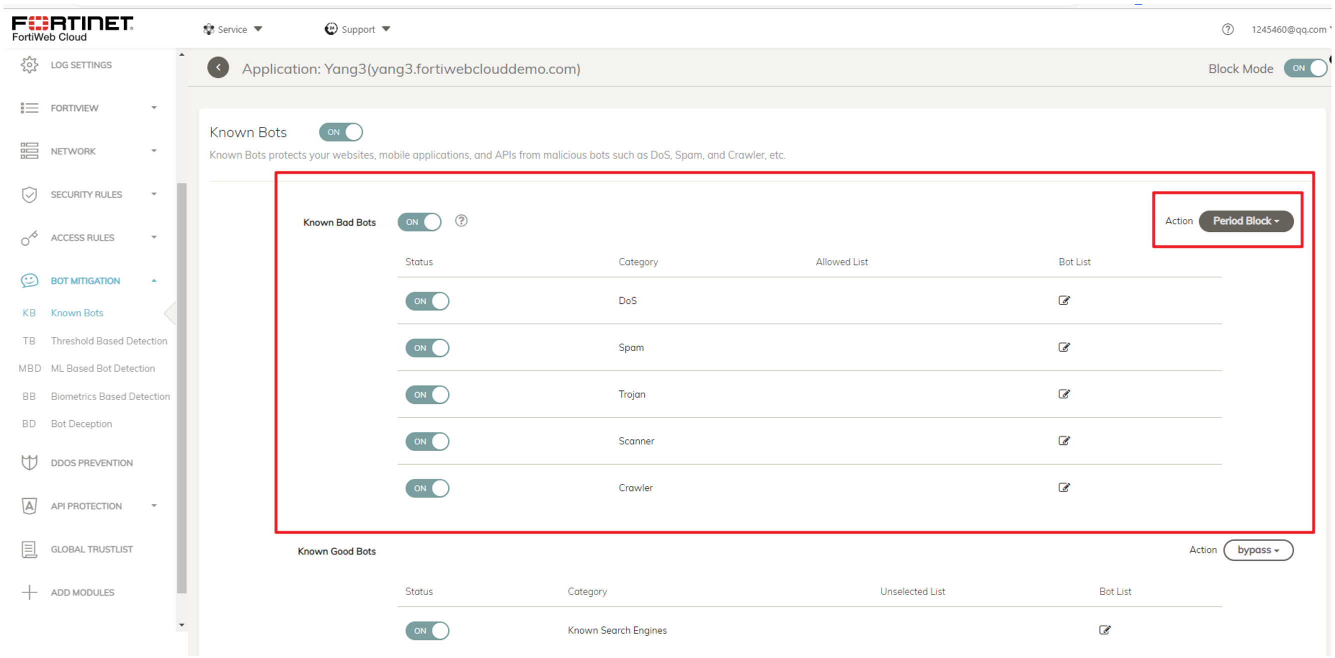
IP / IP Range

Reverse Matching

Serial Number: FWBCLD0000000172 | Version 22.4.a | Privacy Policy | Terms of Service | Copyright © 2023 Fortinet, Inc. All Rights Reserved.

STEP 3: Blocking bots

- Some DDoS attacks come from known bots. Enable the following categories in **Bot Mitigation > Known Bots** and set the action to **Period Block**. For more information, see Known Bots.



Application: Yang3(yang3.fortiwebclouddemo.com) — Block Mode: ON

Known Bots: ON

Known Bots protects your websites, mobile applications, and APIs from malicious bots such as DoS, Spam, and Crawler, etc.

Known Bad Bots: ON — Action: Period Block

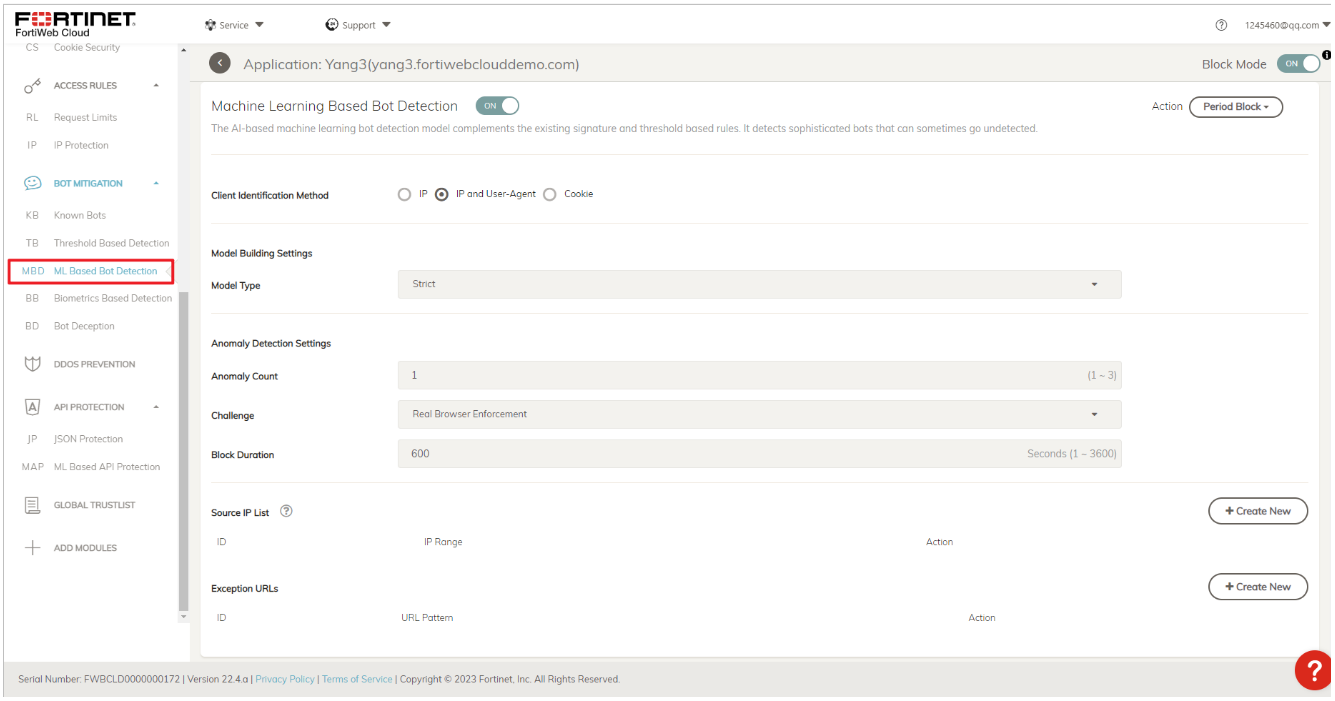
Status	Category	Allowed List	Bot List
ON	DoS		
ON	Spam		
ON	Trojan		
ON	Scanner		
ON	Crawler		

Known Good Bots — Action: bypass

Status	Category	Unselected List	Bot List
ON	Known Search Engines		

- **Bot Mitigation > ML Based Bot Detection**

Enable **Machine Learning Based Bot Detection**. This complements existing signature and threshold-based rules to detect sophisticated bots that can sometimes go undetected.For more information, see ML Based Bot Detection on page 157.



Application: Yang3(yang3.fortiwebclouddemo.com)

Block Mode ON

Machine Learning Based Bot Detection ON

Action Period Block

The AI-based machine learning bot detection model complements the existing signature and threshold based rules. It detects sophisticated bots that can sometimes go undetected.

Client Identification Method ○ IP ● IP and User-Agent ○ Cookie

Model Building Settings

Model Type: Strict

Anomaly Detection Settings

Anomaly Count: 1 (1 ~ 3)

Challenge: Real Browser Enforcement

Block Duration: 600 Seconds (1 ~ 3600)

Source IP List

ID	IP Range	Action

Exception URLs

ID	URL Pattern	Action

Serial Number: FWBCLD0000000172 | Version 22.4.a | Privacy Policy | Terms of Service | Copyright © 2023 Fortinet, Inc. All Rights Reserved.

Maximum configuration values

The following table provides the maximum number of configuration objects in each application.

Application item	Maximum value
Logs > attack log servers	5
Network > origin servers	32
Network > Endpoint > Custom Certificate	32
Network > Endpoint > Intermediate Certificate	32
Network > Endpoint > Domains	10
Security Rules > Known Attack > Exception rules	128
Security Rules > Anomaly Detection > Source IP List	No Limit
Security Rules > Information Leakage > Exception rules	128
Security Rules > Cookie Security > Except Cookies	64
Client Security > CSRF Protection > Page List	256
Client Security > CSRF Protection > URL List	256
Client Security > MITB Protection > Protected Parameter	256
Client Security > MITB Protection > Allowed External Domains for AJAX Request	256
Access rules > URL access rules	12
Bot Mitigation > Biometrics Based Detection rules	12
Bot Mitigation > Bot Deception rules	255
Advanced Applications > Custom rules	12
Advanced Applications > Web Socket Security rules	12
API Protection > Open API Validation > Validation rules	10
API Protection > API Gateway > API users	12
API Protection > API Gateway > API Gateway rules	12
API Protection > Mobile API Protection Request URL	12
API Protection > JSON Security rules	10
API Protection > XML Protection rules	10
Application Delivery > Rewriting Request rules	12
Global Trustlist	12

The following table provides the maximum number of configuration objects in **Global** tabs.

Global item	Maximum value
Global > Templates	16
Global > Report	No Limit
Global > Admin Management > Users	No Limit
Global > Administrators > Role Management > Roles	No Limit
Global > System Settings > Cloud Connectors	No Limit
Global > System Settings > Custom Block Pages	8
Global > System Settings > Settings > API Key	1

Sequence of scans

FortiWeb Cloud applies protection rules and performs scans according to orders in the table below (from the top to the bottom).

You may find that the actual scan sequence sometimes is different from that listed in the following scan sequence table. Various reasons may explain this, for example, for the scans involving the whole request or response packet, its sequence may vary depending on when the packet is fully transferred to FortiWeb Cloud. **File Protection** is one of the scan items that involve scanning the whole packet. FortiWeb Cloud scans `Content-Type:` and the body of the file for File Protection. While the `Content-Type:` is scanned instantly, the body of the file may be postponed after the subsequent scans until the whole body of the file is done uploading to FortiWeb Cloud.

Please also note that the scan sequence refers to the sequence within the same packet. For example, **TCP Connection Number Limit** precedes **HTTP Request Limit** in the scan sequence table. However, if there are two packets containing HTTP traffic and TCP traffic respectively, and the HTTP packet arrives first, FortiWeb Cloud thus checks the **HTTP Connection Number Limit** first.

To improve performance, block attackers using the earliest possible technique in the execution sequence and/or the least memory-consuming technique. The blocking style varies by feature and configuration. For example, when detecting Syntax-based SQL injection, instead of blocking the SQL injection by its syntax, you could log and block the injection by the blocklist defined in IP List. For details, see each specific feature.

Scan/action	Involves
TCP Connection Number Limit (TCP Flood Prevention)	• Source IP address of the client in the IP layer. • Source port of the client in the TCP layer.
Add X-Forwarded-For:	• `X-Forwarded-For:` • `X-Real-IP:` • `X-Forwarded-Proto:`
IP List	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • Source IP address of the client in the IP layer. **Note:** If a source IP is in allowlist, subsequent checks will be skipped.
IP Reputation	Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180.

Scan/action	Involves
Geo IP	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • Source IP address of the client in the IP layer.
WebSocket security	• `Host:` • URL in HTTP header • `Origin:` • `Upgrade:` • Frame Size/Message Size • `sec-websocket-extenstions`
HTTP Allow Method	• `Host:` • URL in HTTP header • `Request method in HTTP header`
HTTP Request Limit (HTTP Flood Prevention)	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • `Cookie:` • Session state • URL in the HTTP header • HTTP request body
TCP Connection Number Limit (Malicious IP)	• `Cookie:` • Session state • Source IP address of the client in the IP layer • Source port of the client in the TCP layer
HTTP Request Limit (HTTP Access Limit)	• `ID` field of the IP header • Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. . • HTTP request body
URL Access	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • `Host:` • URL in HTTP header • Source IP of the client in the IP header
Mobile API Protection	• `Host:`

Scan/action	Involves
	- URL in HTTP header - Token header
Protocol Limits	- Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. - `Content-Length:` - Parameter length - Body length - Header length - Header line length - Count of `Range:` header lines - Count of cookies
File Protection	- Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. - `Content-Type:` in `PUT` and `POST` requests - URL in HTTP header - The body of the file
Bot Deception	- `Host:` - URL in the HTTP header
Cross-site request forgery (CSRF) attacks	- `<a href>` - `<form>`
Protection for Man-in-the-Browser (MITB) attacks	- `Host:` - URL in HTTP header - Request method in HTTP header - Parameters in URL - `Content-Type:`
Biometrics Based Detection	- Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. - URL - `Host:` - `X-Forwarded-For:`
XML Protection	- URL - HTTP header - Body
JSON Protection	- URL - HTTP header

Scan/action	Involves
	• Body
Signature Based Detection	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • HTTP headers • HTML Body • URL in HTTP header • Parameters in URL and request body
SQL Syntax Based Detection	• `Host:` • `Cookie:` • URL in HTTP header • Parameters in URL and request body
Custom Rule	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • URL in the HTTP header • HTTP header • Parameter in the URL
Threshold Based Detection	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 180. • URL • `Host:` • `X-Forwarded-For:`
Account Takeover	• `Host:` • `Cookie:` • Parameters in the URL • URL in HTTP header • HTTP body • Client's certificate
API Gateway	• `Host:` • URL in HTTP header • API Key as HTTP parameter in URL • API Key as HTTP header • Source IP address of the client depending on your configuration of API user • Request methods in HTTP header • HTTP Referer depending on your configuration of API user

Scan/action	Involves
OpenAPI Validation	• Host: • HTTP headers, especially the content-type: headers • URL in HTTP header • Request method in HTTP header • Parameters in URL • Multipart filename
URL Rewriting (rewriting & redirection)	• Host: • Referer: • Location: • URL in HTTP header • HTML body
Machine Learning - Anomaly Detection	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the SRC field in the IP header, or the X-Forwarded-For: and X-Real-IP: HTTP headers. For details, see "Defining your proxies, clients, & X-headers" on page 1. • URL in the HTTP header • Request method in HTTP header • Parameter in the URL, or the HTTP header or body • Content-Type:
Compression	Accept-Encoding:
Cookie Security	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the SRC field in the IP header, or the X-Forwarded-For: and X-Real-IP: HTTP headers. For details, see Request Limits on page 144 • Cookie:
Reply from server to client	
Web Socket Protocol	• Upgrade:
Caching	• Host: • HTTP method • Return code • URL in the HTTP header • Content-Type: • HTTP headers • Size in kilobytes (KB) of each URL to cache
Bot Deception	• Host: • URL in the HTTP header
Protection for Man-in-the-Browser (MiTB) attacks	• Status code • Response body
Biometrics Based Detection	• Source IP address of the client depending on your configuration of

Scan/action	Involves
	X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Request Limits on page 144 • URL • `Host:` • `X-Forwarded-For:` • HTTP header • Custom signature • Body • The latest HTTP transaction time • The response content type • Status code
Signature Based Detection (Information Leakage)	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Request Limits on page 144 • HTTP headers • HTML Body • URL in HTTP header • Parameters in URL and body • XML in the body of HTTP POST requests • Cookies • Headers • JSON Protocol Detection • Uploaded filename (MULTIPART_FORM_DATA_FILENAME)
Custom Rule	• HTTP response code • `Content-Type:`
Account Takeover	• Status code • HTTP headers • HTML body
URL Rewriting (rewriting)	• `Host:` • `Referer:` • `Location:` • URL in HTTP header • HTML body
HTTP Header Security	• HTTP headers

Supported cipher suites & protocol versions

A secure connection’s protocol version and cipher suite, including encryption bit strength and encryption algorithms, is negotiated between the client and the SSL/TLS terminator during the handshake.

The **SSL/TLS Encryption Level** controls how many ciphers are supported and the settings provides the following options:

- **Mozilla-Modern:** For services with clients that support TLS 1.3 and don't need backward compatibility, Mozilla-Modern is the recommended configuration as it provides an extremely high level of security.
- **Mozilla-Intermediate:** For services that don't need compatibility with legacy clients such as Windows XP or old versions of OpenSSL, Mozilla-Intermediate is the recommended configuration as it is highly secure and in the meanwhile compatible with nearly every client released in the last five (or more) years.
- **Mozilla-Old:** For services accessed by very old clients or libraries, such as Internet Explorer 8 (Windows XP), Java 6, or OpenSSL 0.9.8. Mozilla-old is the recommended configuration as it is compatible with most of the clients.
- **Customized** – Supports a customizable list of all ciphers.

Ciphers supported by Mozilla-Modern/Intermediate/Old levels

Cipher	Mozilla Modern	Mozilla Intermediate	Mozilla Old
TLS_AES_256_GCM_SHA384	Yes	Yes	Yes
TLS_CHACHA20_POLY1305_SHA256	Yes	Yes	Yes
TLS_AES_128_GCM_SHA256	Yes	Yes	Yes
ECDHE-ECDSA-AES128-GCM-SHA256		Yes	Yes
ECDHE-RSA-AES128-GCM-SHA256		Yes	Yes
ECDHE-ECDSA-AES256-GCM-SHA384		Yes	Yes
ECDHE-RSA-AES256-GCM-SHA384		Yes	Yes
ECDHE-ECDSA-CHACHA20-POLY1305		Yes	Yes
ECDHE-RSA-CHACHA20-POLY1305		Yes	Yes
DHE-RSA-AES128-GCM-SHA256		Yes	Yes
DHE-RSA-AES256-GCM-SHA384		Yes	Yes
DHE-RSA-CHACHA20-POLY1305			Yes

Cipher	Mozilla Modern	Mozilla Intermediate	Mozilla Old
ECDHE-ECDSA-AES128-SHA256			Yes
ECDHE-RSA-AES128-SHA256			Yes
ECDHE-ECDSA-AES128-SHA			Yes
ECDHE-RSA-AES128-SHA			Yes
ECDHE-ECDSA-AES256-SHA384			Yes
ECDHE-RSA-AES256-SHA384			Yes
ECDHE-ECDSA-AES256-SHA			Yes
ECDHE-RSA-AES256-SHA			Yes
DHE-RSA-AES128-SHA256			Yes
DHE-RSA-AES256-SHA256			Yes
AES128-GCM-SHA256			Yes
AES256-GCM-SHA384			Yes
AES128-SHA256			Yes
AES256-SHA256			Yes
AES128-SHA			Yes
AES256-SHA			Yes
DES-CBC3-SHA			Yes

FAQs

Onboarding applications

For how to onboard applications, please refer to Getting Started in our online help.

It's suggested to perform the following actions after an application is onboarded:

Required actions

- Change the DNS record at your DNS service using the CNAME provided by FortiWeb Cloud.
- Configure your origin servers to only accept traffic from FortiWeb Cloud IP addresses. See this article for a list of FortiWeb Cloud IP addresses.
- Configure security rules and observe the attack logs in FortiView or Attack Logs. If legitimate traffic is falsely detected as attacks, add exceptions or modify the security rules to avoid false positives in the future. See Log Settings on page 105 for how to add exceptions.
- Enable **Block Mode** in **Global > Applications** if you have continuously observed the attack logs for several days and there aren't any false positives recorded in the logs.

Optional actions

- Whitelist FortiWeb Cloud IP addresses to make sure access from FortiWeb Cloud to your web application is uninterrupted. See this article for a list of FortiWeb Cloud IP addresses.

In FortiWeb Cloud, an application is a declared domain name and up to 9 other domain names attaching to it, which all belong to the same root domain and all point to the same origin server(s). For example, "example.com" and "test.example.com" can be part of the same application "example.com", while "test.com" is a different application.

A CNAME record is a part of the DNS zone records (that may or may not be present) that is used to essentially redirect from one URL to another. The CNAME record for a DNS zone will have a URL for the record NAME, it will be of record TYPE “CNAME”, and it will have a VALUE of another URL. The VALUE field of a CNAME record is often called the CNAME, or canonical (true) name.

When you complete onboarding an application, FortiWeb Cloud provides you with a CNAME. You need to go to your DNS service and pair this CNAME with your application's domain name.

If your DNS service does not support CNAME, the workaround is to pair your application's domain name with the IP addresses of the FortiWeb Cloud scrubbing center which is deployed in the same region with your origin server. See this article for a list of FortiWeb Cloud IP addresses.

Please note the CDN feature won't be available in this scenario because all the traffic will be forwarded to a fixed scrubbing center.

FortiWeb Cloud supports most of the regions on AWS, Azure, and Google Cloud. See this article for a detailed list of supported regions.

By enabling **CDN**, the data on your origin servers can be cached in FortiWeb Cloud scrubbing centers distributed around the world. When users request data from your application, they can be directed to the nearest scrubbing center and rendered with the requested data. See this article for a list of FortiWeb Cloud IP addresses.

You can enable CDN when onboarding an application, or set this option in the **Application Settings** dialog (**Global > Applications**).
Please check with your certificate provider to confirm whether an intermediate certificate is required. If so, you will need to upload it as well.

Network

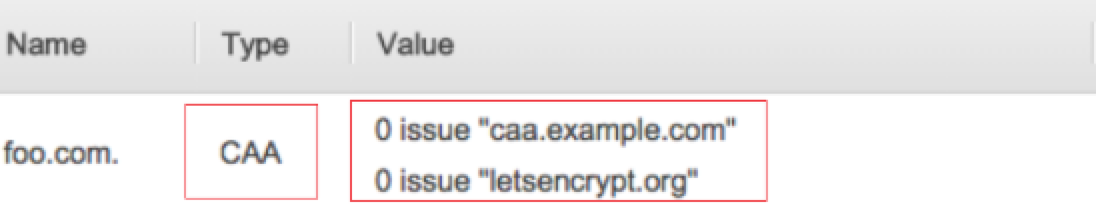
FortiWeb Cloud by default uses port 80 for HTTP protocol and 443 for HTTPS protocol. Non-standard ports are also available. You can select them when you onboard applications. Please note if non-standard port is selected for HTTPS, you will not be allowed to configure HTTPS redirection.

If you need to use different ports, please contact Fortinet Support or your sales engineer for further help. Notice not all non-standard ports can be used, and HTTP and HTTPS services must use different ports.
Up to 100 domains are supported in one single application. They should all belong to the same root domain and point to the same origin server(s).
Yes, all the domains should belong to the same root domain, such as www.example.com and mail.example.com.

After the application is onboarded, you can go to **Network > Endpoints** to change or add domains, but you are not allowed to change the first domain in the list. Highly recommend to use root domain as the first domain.
You can add at most 128 origin servers to the server pool of an application.
FortiWeb Cloud automatically obtains an SSL certificate on your behalf from Let’s Encrypt within two minutes of the DNS CNAME record change. It will be used in HTTPS connections to encrypt or decrypt the traffic. If FortiWeb Cloud fails to obtain the certificate, it will try again 12 minutes later.

Thirty days before your certificate expires, FortiWeb Cloud verifies again that your DNS CNAME record is still correct. If it is, FortiWeb Cloud renews your certificate for another 90 days, so it never expires. For more information, see Automatic Certificate on page 119.
FortiWeb Cloud automatically retrieves SSL certificates from the Certificate Authority Let's Encrypt. See Automatic Certificate for the things you should pay attention to if automatic certificate is used.
DNS Certification Authority Authorization (CAA) is an Internet security policy mechanism which allows domain name holders to indicate to certificate authorities whether they are authorized to issue digital certificates for a particular domain name. It does this by means of a new "CAA" Domain Name System (DNS) resource record.

If you have configured a CAA record at your DNS service and want to use automatic certificate in FortiWeb Cloud, make sure to add "letsencrypt.org" in the CAA value. This allows Let's Encrypt to issue certificates for your domain name.



Name	Type	Value
foo.com.	CAA	0 issue "caa.example.com" 0 issue "letsencrypt.org"

No. We now support TLS 1.1, 1.2, and 1.3.
Check the following if “connection is not secure” displays in the browser when users visit your application:

- If HTTP protocol is used in this connection, it's suggested to enable **HTTPS** service and **Redirect all HTTP traffic to HTTPS** in **Network > Endpoints** in FortiWeb Cloud, so that the HTTP access can be redirected to HTTPS, which is secured by SSL/TSL certificates.
- If HTTPS protocol is used in this connection, check whether the certificates are valid:
  - If **Custom Certificate** is selected in **Network > Endpoints**, make sure the SNI certificates or intermediate certificates you imported are valid.
  - If **Automatic Certificate** is selected, see the following FAQs to trouble-shoot:
    - Network on page 260
    - Network on page 260

To troubleshoot network connectivity when traffic doesn't go through, follow these steps:

1. Ensure that you are using a supported web browser. FortiWeb Cloud supports Mozilla Firefox version 59 or higher, and Google Chrome version 65 or higher. While other browsers may also display well but we cannot guarantee compatibility.
2. Check the error message displayed. If it shows server connectivity issue, perform either one of the following actions:
   a. Modify the local host file on your computer to map your application's domain name to the IP address of the origin server. Then, enter the domain name of your application in the browser to verify the traffic can go through when FortiWeb Cloud is bypassed.
   b. If there are more than one origin servers, FortiWeb Cloud performs health check and displays the server status in the **Server Status** widget on **Dashboard** page, as well as in the **Server Status** column of the **Origin Server** page. Make sure the **Health Check** option is turned on and the **URL Path** on the **Origin Server** page is configured correctly, as FortiWeb Cloud relies on it to verify server responsiveness.
   If the origin server is accessible, proceed to the following steps to identify the specific configuration on FortiWeb Cloud causing the error.
   If the origin server is not accessible, it suggests that the connectivity issue is unrelated to FortiWeb Cloud and you should troubleshoot the origin server.
3. Verify the **SSL Encryption Level** configuration on the **Origin Server** page and ensure that your origin server supports the specified SSL Encryption Level.
4. Disable **HTTP/2** on the **Origin Server** page and check if the traffic goes through. If it does, it indicates that your origin server doesn't support HTTP/2, and therefore, the HTTP/2 option on FortiWeb Cloud should be disabled.
5. Analyze attack logs in **Threat Analytics > Attack Logs** to identify any WAF modules that may be blocking traffic.

FortiWeb Cloud support sending logs to your syslog or ElasticSearch server to notify the origin server status change.

1. Enable **Health Check** for the origin server in the Load Balancing rule in **Network > Origin Server**. Please note this setting is only available when the **Server Balance** is turned on.
2. Refer to Audit logs to export logs to your syslog server.

When using FortiWeb Cloud, the client's requests from the Internet are forwarded to FortiWeb Cloud first before they reach the ALB/ELB.

When you onboard an application, for **Origin Server** settings in **Step 2- Network**, select **Customize**, then enter the ALB/ELB's domain name in **IP Address or FQDN**. Make sure to enter the domain name, not the IP address.

In the DNS record that pairs the dynamic domain name and IP address, you will find a TTL (Time to Live) value. FortiWeb Cloud updates the IP address according to this TTL value. If the TTL indicates the IP address expires, FortiWeb Cloud will resolve the domain name to obtain the latest IP address.

You can use **Cloud Connectors** to obtain the IP addresses if your origin servers are deployed on AWS, Azure, or GCP.

1. Create a Cloud Connector to authorize FortiWeb Cloud to access the resources in your public cloud account. See Cloud Connectors on page 80.
2. In **Network > Origin Servers**, select **Dynamic** for **Server Type**, then configure **Cloud Connector** and **Filter** as instructed in Origin Servers on page 114.

See Using FortiWeb Cloud behind a Content Distribution Service on page 218 for detailed information.

See Network settings for applications serving different content over HTTP and HTTPS on page 227 for more information.

- Check the inbox of your account email. Search for keywords "new WAF cluster" from "noreply@fortiweb-cloud.com".
- Check the What's New part in Online help.
- Use the following APIs to retrieve the IP lists:
  - IPv4: https://www.fortiweb-cloud.com/ips-v4
  - IPv6: https://www.fortiweb-cloud.com/ips-v6

Security

The following security features are provided by FortiWeb Cloud:

- Security Rules
- Client Security
- Access Rules
- Bot Mitigation
- DDoS Prevention
- Advanced Applications
- API Protection
- Account Takeover
- Application Delivery
- When Block Mode is enabled, FortiWeb Cloud blocks requests if they trigger violations. Your application server does not receive these requests.
- When Block Mode is disabled (that is, the Monitor mode), FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. You can view the attack logs in FortiView or Attack Logs.

You can add exceptions in **Attack Logs** so that the requests from the specified URL or parameter will not be detected as attack again. See Log Settings on page 105 for more information.

You can also add exceptions in the following three security modules:

- Known Attacks on page 128
- Threshold Based Detection on page 154
- Information Leakage on page 135

You can use the **URL Access** in **Access Rules** to define which HTTP requests FortiWeb Cloud accepts or denies based on their `Host:` name and URL, as well as the origin of the request. See URL Access for more information.

You can also add **URL filters** in **Custom Rules** to match the requests with specified URLs. See Custom Rule for more information.

No. FortiWeb Cloud does not charge for inbound traffic, so additional charges will not be incurred related to DDoS attacks. An advantage of deploying FortiWeb Cloud in public cloud (AWS, Azure, and Google Cloud) is that FortiWeb Cloud enjoys the protection of the volumetric DDoS protections provided by those platforms. FortiWeb Cloud also provides additional DDoS protections for Network and transport layer (TCP/IP) and Application layer (HTTP or HTTPS) DDoS attacks (see DDoS prevention).

FortiWeb Cloud provides **Templates** for you to create configuration templates and apply them to multiple applications. For more information, see Templates on page 67.

FortiWeb Cloud executes the security rules in a certain sequence. See Sequence of scans on page 251.

The MITB Protection restricts AJAX requests to external domains. If you come across this warning, it could be because the request has triggered the MITB rules. If you are confident in its safety, you have the option to add this link to the External Domain allowlist in MITB Protection. For more information, see MITB Protection.

DDoS attacks can be prevented at Application layer (HTTP or HTTPS) and Network layer (TCP/IP).

As public cloud platforms already execute basic Network layer TCP Flood Prevention checks affront, when traffic comes into FortiWeb Cloud, it only detects DDoS attacks at Application layer (HTTP or HTTPS).

Please verify if the Block Mode is currently enabled.

By default, after an application is onboarded, the Block Mode is in Disabled status. You need to enable it first for the WAF modules to take effect.

On **Applications** page, you can turn on/off the Block Mode for each application. However, before enabling Block Mode, it is important to perform several checks. For more detailed information on Block Mode, see Understanding block mode and action.

The website (https://www.fortiguard.com/services/ws) maintains an up-to-date database of IP reputation. However, it's important to note that FortiWeb Cloud may still be using data from a few days ago, resulting in a latency in the database update.

Therefore, when the database in FortiWeb Cloud is updated, this IP address will be removed from the Bad Reputation IP list. If you have confidence in the trustworthiness of this IP address and don't wish to wait for the database update, you have the option to manually add this IP address to the **Trust IP** list in the **IP Protection** settings.
Turn on **Advanced Threat Protection** in **File Protection**, then FortiWeb Cloud will send files that meet the configured conditions to FortiSandbox for evaluation.

This option works only if your application is hosted on AWS or Azure. Refer to https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/748121/file-protection.
IPs in Trust IP list will be fully trusted by FortiWeb Cloud without undergoing any additional scanning, while the IPs in Allow-Only list is only trusted by the IP Protection module and will be forwarded to other modules for security checks.

It is important to note that there are other considerations regarding these lists. For more comprehensive details, refer to the description of the "Type" option in IP Protection.
To allow certain IPs from a restricted country, you can configure the following steps in **Access Rules > IP Protection**:

1. Block the country through **GEO IP Block**. This will prevent access from IP addresses originating from the specified country.
2. Add IPs to **Allow-Only** IP List. This ensures that the IP Protection module will trust and forward these IPs to other modules for additional security checks. If you have complete trust in these IP addresses, you can include them in the **Trust** IP list, so these IPs will bypass any further security checks and be directly permitted.

By combining these steps, you can effectively block access from the restricted country while allow specific IPs.

For more comprehensive details, refer to IP Protection.

Logs

FortiWeb Cloud saves the attack logs for two months and the audit logs for three months. After that, they will be deleted.
Exceptions are added in Attack Logs. It can't be reversed once being added.

If you believe that the Anomaly Detection model is inaccurate with certain exceptions, you have the option to access the TreeView page of the Anomaly Detection module. From there, you can locate the parameter to which the exception is applied and rebuild the model specifically for that parameter. When the new model is rebuilt, the exceptions added to the Anomaly Detection attack logs corresponding to that parameter will be cleared.
In the scanning process, when a request passes through different modules in sequence, the configured action for certain modules can be set to "Alert" or "Monitor". In this case, if an attack is detected by a module with such an action, it will allow the request to continue to the next module for further scanning. However, an attack log will be generated by the module that identified the attack.

As the request progresses through subsequent modules, it is possible for the attack to be logged multiple times by different preceding modules before it is blocked by a module with a different action, such as "Block Period" or "Deny".

As for the scan sequence, please refer to https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/234292/sequence-of-scans.
If the `https_host` in GEO IP attack logs shows `none`, it can be solved by enabling **Use X-Header to Identify Original Clients' IP** and **Add X-Forwarded-For** in the **Rewriting Requests** module.
To observe the client's original source IP, it is advised to enable the **Rewriting Requests** module, turning on **X-Forwarded-For**, **X-Real-IP**, and **Use X-Header to Identify Original Clients' IP** options.
Logs are sent from FortiWeb Cloud to the origin server, so the `IP:` header (layer 3) of the logs is supposed to be FortiWeb Cloud's IP address. This is expected behavior.

To check the client real IP, you need to find it in the `X-Forwarded-For`: or `X-Real-IP:` header in the packets forwarded from FortiWeb Cloud to your server. Be aware that to record the client real IP it's required to enable both **Add X-Forwarded-For** and **Use X-Header to Identify Original Client's IP** in the **Rewriting Requests** module.
The signatures used in Known Attacks are primarily designed to detect known patterns of malicious code. However, they may not cover all variants or newly emerging forms of attacks.

In cases where an attack is logged under the Anomaly Detection threat type instead of being matched with a signature, it in fact indicates the successful functioning of the machine learning model in Anomaly Detection. It effectively screened out unknown or new variant attacks that do not align with existing signatures.
You can view the blocked requests in three places: 1) Attack Logs; 2) FortiView ; 3) Blocked Requests widget on Dashboard. The ways they count the blocked requests are slightly different.

- To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such item are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget.
- If you have set FortiWeb Cloud to block attacks but do not generate a log when certain violation occurs, such as Alert & Deny (no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget.
- The invalid requests to the host header HOST will be blocked without generating any log.
- When the Block Mode is in disabled state, attacks won't be blocked but logs are generated.

If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as 'Alert & Deny (no log)', then the attacks will not be logged in Attack Logs and FortiView but will be counted in the Blocked Requests widget.

If you need to have detailed logs for auditing or analysis purposes, you may consider using a different action, such as 'Alert & Deny' or 'Block Period', which will not only block the request but also generate a log entry.

To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below.

Attack ID	Security Rule
20000001	Allow Method
20000002	Protected Hostnames
20000003	Page Access
20000004	Start Pages
20000005	Parameter Validation
20000006	Black IP List
20000007	URL Access
20000008	Signature Detection
20000009	Custom Signature Detection
20000011	Hidden Fields
20000012	Site Publish
20000013	HTTP Parsing Error
20000014	DoS Protection
20000015	SYN Flood Protection
20000016	HTTPS Connection Failure

Attack ID	Security Rule
20000017	File Upload Restriction
20000018	GEO IP
20000019	Illegal XML Format
20000020	Illegal JSON Format
20000021	Custom Access
20000022	IP Reputation
20000023	Padding Oracle
20000024	CSRF Protection
20000025	Quarantined IPs
20000026	HTTP Protocol Constraints
20000027	Credential Stuffing Defense
20000028	User Tracking
20000029	XML Validation Violation
20000030	Cookie Security
20000031	FTP Command Restriction
20000032	FTP Parsing Error
20000033	Timeout Session
20000034	Other Attacks
20000035	FTP File Security
20000036	FTPS Connection Failure
20000037	Anomaly Detection
20000038	OpenAPI Validation Violation
20000039	WebSocket Security
20000040	MITB AJAX Security
20000041	Bot Detection
20000042	CORS Check Security
20000043	JSON Validation Security
20000044	Mobile API Protection
20000045	Bot Deception
20000046	Biometrics Based Detection
20000047	Threshold Based Detection

Attack ID	Security Rule
20000048	API Gateway
20000049	URL Encryption
20000050	SQL/XSS Syntax Based Detection
20000051	Known Bots Detection
20000053	Allow Only IP List
20000200	Known Attacks
20000201	Information Leakage
20000202	Cookie Security
20000203	File Protection
20000204	Client Security
20000205	Request Limits
20000206	URL Access
20000207	IP Protection
20000208	Bot Mitigation
20000209	DDoS Prevention
20000210	XML Security
20000211	OpenAPI Validation
20000212	WebSocket Security
20000213	Known Bots Detection
20000214	API Gateway
20000215	Mobile API
20000216	JSON Security

You may need to authorize the devices of FortiWeb Cloud in your FortiAnalyzer.

Check if your FortiWeb Cloud's application serial number shows up under **FAZ > Device Manager > Unauthorized Devices**, if so, authorize it to send attack logs to FortiAnalyzer.

Subscriptions and Contracts

If your application is deployed on AWS, we will select a FortiWeb Cloud scrubbing center that is also hosted on AWS, regardless of where you have subscribed to FortiWeb Cloud. This ensures optimal performance, minimizing network latency and providing a seamless experience for securing your application.

The subscription platform primarily serves billing purposes, enabling you to pay for the traffic processed by FortiWeb Cloud. It takes care of the financial aspects related to the FortiWeb Cloud service.
We have updated our FortiWeb Cloud PAYG listing on Azure to include the Vulnerability Scan service. To change your old plan to the new one, you must unsubscribe from your current plan and then re-subscribe to the new plan within 7 days of unsubscribing.

Your existing applications and resources are attached to the account, not the subscription. When you unsubscribe from your plan, your onboarded applications will continue to function normally, but with reduced UI access in "read-only" mode. FortiWeb Cloud will continue to protect your applications during this period.

After successfully subscribing to the new plan, your UI access will be fully restored to "read/write," allowing you to resume your work without any interruptions.

- For subscriptions on AWS, Azure, and Google Cloud: You can unsubscribe from FortiWeb Cloud anytime, while the data in your FortiWeb Cloud account will be kept for an additional week.
- For FortiWeb Cloud contract: After the contract expires, FortiWeb Cloud continues protecting your applications for 21 days. During this period, you are not allowed to edit configuration for your applications unless the contract is renewed. After the 21-day extension, your applications will be deleted from your FortiWeb Cloud account.

After you unsubscribe from FortiWeb Cloud, remember to replace CNAME with the right IP address in the DNS record so your web application does not experience service interruption.

Please note that the Vulnerability Scan feature follows a different billing structure; for more information, please look under vulnerability scan.
After your contracts expire, FortiWeb Cloud initiates a grace period, during which you have read-only access to all of your applications until the contracts are renewed.

For public cloud subscription customers, this grace period is 7 days. For all other customers, this grace period is 21 days.

Once the grace period ends, all of your applications will be deleted from FortiWeb Cloud.
No. Due to security and privacy considerations, FortiWeb Cloud does not retain any customer configurations once the application has been deleted.

However, several days before the licenses become invalid, you should receive a warning email specifying the expiration date of the licenses. During this period, you have the option to extend the licenses if you intend to continue using the service.
The data for this application will be deleted and can't be restored.
After your contracts expire, FortiWeb Cloud initiates a grace period, during which you have read-only access to all of your applications until the contracts are renewed.

For public cloud subscription customers, this grace period is 7 days. For all other customers, this grace period is 21 days.

Once the grace period ends, all of your applications will be deleted from FortiWeb Cloud. Make sure to keep at least one valid contract to avoid activating this grace period.
You can contact the FortiWeb Cloud Team for help with migrating applications between accounts. In your inquiry, please include account details for both accounts, including the Serial Number and associated email for each account, along with platform information (e.g., AWS, Azure, GCP). For additional guidance on how to contact our Customer Service, please refer to the Contacting Customer Service section.
When an account has onboarded more applications than their contract allows, FortiWeb Cloud will immediately lock the UI and move it to read-only. Customers will not be able to make any changes until additional contracts are purchased.

For example: A customer purchases two contracts; the first one is purchased on January 1 for a single web application. On April 1, the customer purchases another contract for five more applications. On January 1 of the next year, the first contract for the single web app expires leaving the customer with a 5 web app contract. The customer now has 6 applications onboarded while the license only allows 5 applications. The customer will have read-only access for all of their applications until they purchase another contract.

When a customer uses more bandwidth than their contract allows (bandwidth usage is measured monthly at the 95th percentile), FortiWeb Cloud triggers an internal notification. However, it does not block nor throttle access to customer applications. The account team will contact affected customers and inform them of the need to purchase new contracts immediately. Currently, as of February 2023, this notification process is manual. However, we are working on automating it, and in the future, restrictions like those mentioned above will be deployed automatically when there are bandwidth contract violations.
Fortiweb Cloud WAF is primarily focused on protecting web applications from various security threats and does not validate or manage server certificates.

The WAF processes the request as if it were in transparent mode, potentially allowing the user to reach the backend server.

Cost and Billing

FortiWeb Cloud offers 14-day free trial on public cloud platforms. After the free trial, you can subscribe to FortiWeb Cloud or purchase service contracts from Fortinet to continue using it.

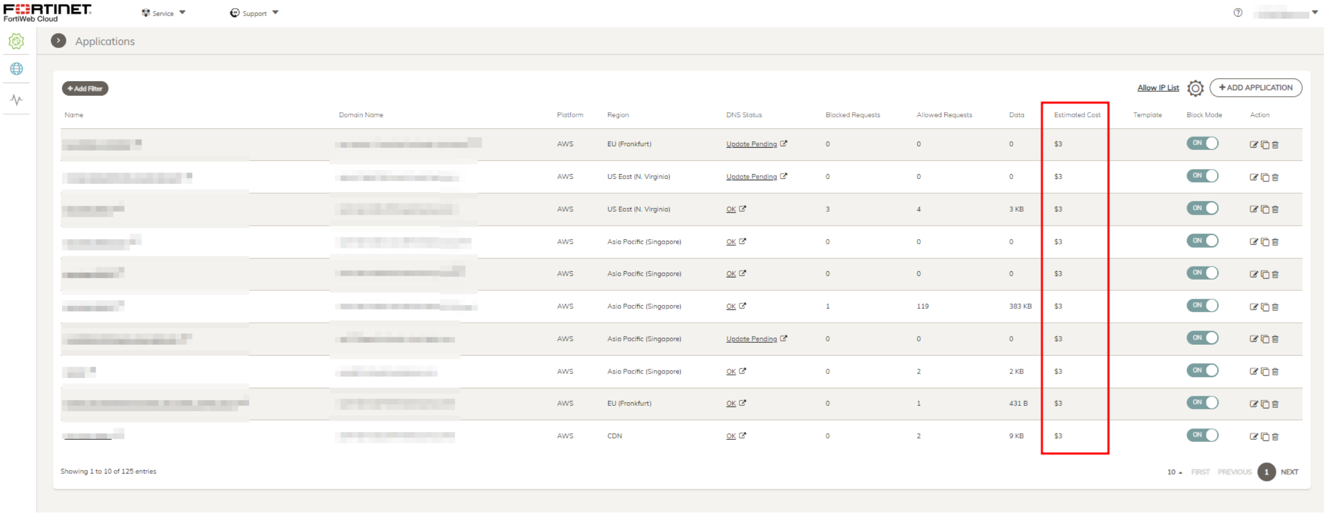
- Subscribing through AWS Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Subscribing through Azure Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Subscribing through Google Cloud Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Using FortiWeb Cloud license purchased from your Fortinet reseller. The license allows you to protect certain number of applications and specifies the maximum bandwidth.

Please note that if you have subscribed to FortiWeb Cloud on public cloud platforms and also imported a FortiWeb Cloud license in your account, it's recommended to unsubscribe from FortiWeb Cloud, otherwise you will be charged simultaneously through both channels.
If you purchase FortiWeb Cloud service from Fortinet sales team, you will be charged for the Bandwidth contract and Applications contract, which respectively control how many applications you can add in your account and the maximum bandwidth.

For those with or interested in a FortiFlex contract, use our FortiFlex Calculator to estimate service costs conveniently.

When subscribing through AWS, Azure, or Google Cloud, charges are based on data sent to your app users with a pay-as-you-go model. There's no limit on the number of apps in your account. You're charged $0.03 per hour per web app and $0.4 per GB of traffic. Hourly charges start when you onboard an app onto FortiWeb Cloud, regardless of DNS status. Traffic charges begin when data actively flows through FortiWeb Cloud to your app. Regardless of the third-party platform you use to subscribe, you can use FortiWeb Cloud to protect applications located on any other cloud platform or in your own network. The subscription channel only determines the billing places for your FortiWeb Cloud usage.

Please note, the estimated cost shown in your FortiWeb Cloud account may not be accurate, as it is estimated by FortiWeb Cloud based on the amount of data transferred in your account.



Name	Domain Name	Platform	Region	DNS Status	Blocked Requests	Allowed Requests	Data	Estimated Cost	Template	Block Mode	Action
[redacted]	[redacted]	AWS	EU (Frankfurt)	Update Pending	0	0	0	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	US East (N. Virginia)	Update Pending	0	0	0	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	US East (N. Virginia)	OK	3	4	3 KB	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	0	0	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	0	0	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	1	119	383 KB	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	Update Pending	0	0	0	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	2	2 KB	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	EU (Frankfurt)	OK	0	1	431 B	$3		ON	✎ ⧉ 🗑
[redacted]	[redacted]	AWS	CDN	OK	0	2	9 KB	$3		ON	✎ ⧉ 🗑

Showing 1 to 10 of 125 entries

The final cost is billed in your AWS/Azure/Google Cloud account, depending on where you subscribe.
FortiWeb Cloud measures each account using a burstable model for overall account bandwidth calculation. The model is based on calculating the 95th percentile of bandwidth usage of clean traffic and is also common with other CDNs and Cloud solutions.

The 95th percentile bandwidth is calculated in the following way:

- Traffic for the entire month is measured in 5 minute buckets.
- At the end of the month, the 5% of buckets with the most Mbps are dropped, and the highest Mbps rate of the remaining buckets represents the 95th percentile value for the account.

At the beginning of every month, the 95th percentile bandwidth shown in FortiWeb Cloud might be very low, or even shown as 0. This is because there aren't enough 5-minute buckets collected to calculate a valid value. At the end of the month with more buckets generated, the value becomes more accurate.

Accounts

The account management for FortiWeb Cloud is handled through FortiCloud. You can log in to FortiCloud, then select **My Account > Change Account ID (Email)** .For a step-to-step instructions, please refer to the following article: https://docs.fortinet.com/document/forticloud/latest/identity-access-management-iam/588195/my-account.

Please check if any VPN or Secure Access Service Edge (SASE) is used on your computer. If yes, please turn it off and try again. Some VPN will break the SAML response from FortiCloud and cause the failure of login.

From 21.3.b (09/03/2021), FortiWeb Cloud automatically synchronizes sub-users with the ones in your FortiCloud account and assign them with a "None" role. The role of the existing sub-users in your FortiWeb Cloud account will be restored to "None". To grant more permissions to the sub-user, go to **Global > Admin Management**, click the edit icon for this user, then assign it with a different role. See Admin management.

1. Go to **Admin Management**, and find the IAM user whose permissions you want to change in the table.
2. In the **Role Name** column, you should see "Managed by FortiCloud" for this user. Click it to go to **IAM > Users** in FortiCloud.
3. Go to **Permission Profiles** in the left navigation bar and edit the widget for FortiWeb Cloud under **Permission Profile > Permission Details**.

Miscellaneous

FortiWeb Cloud offers Two-Factor Authentication to secure your FortiWeb Cloud account by an additional security token sent through email or the FortiToken Mobile application. See Two-Factor Authentication on page 45.

FortiWeb Cloud supports the following web browsers:

- Mozilla Firefox version 59 or higher
- Google Chrome version 65 or higher

You can submit a support ticket to the support team. See Contacting customer service on page 286.

See Registering serial number for how to find the SN number and register it.

If the SN number has already been registered, you can find it through **Asset > Manage/View Products** on Fortinet Support site https://support.fortinet.com/.

Release 24.1 requires all Managed Security Service Providers (MSSPs) and tenants to migrate to FortiCloud Organization. FortiCloud Organizational Units (OUs) help MSSPs meet unified resource management and resource isolation requirements.

Additionally, OUs make it possible to purchase contracts with FortiFlex, a new usage-based security licensing solution that allows customers to pay only for what they use instead of buying yearly contracts. It is important to note that existing contracts will not be affected by this migration.

For instructions on migrating to FortiCloud OU, please refer to Technical Tip: MSSP Migration to OU.

FAQ

Onboarding applications

For how to onboard applications, please refer to Getting Started in our online help.

What are the recommended actions after an application is onboarded?

It's suggested to perform the following actions after an application is onboarded:

Required actions

- Change the DNS record at your DNS service using the CNAME provided by FortiWeb Cloud.
- Configure your origin servers to only accept traffic from FortiWeb Cloud IP addresses. See this article for a list of FortiWeb Cloud IP addresses.
- Configure security rules and observe the attack logs in FortiView or Attack Logs. If legitimate traffic is falsely detected as attacks, add exceptions or modify the security rules to avoid false positives in the future. See Log Settings on page 105 for how to add exceptions.
- Enable **Block Mode** in **Global > Applications** if you have continuously observed the attack logs for several days and there aren't any false positives recorded in the logs.

Optional actions

- Whitelist FortiWeb Cloud IP addresses to make sure access from FortiWeb Cloud to your web application is uninterrupted. See this article for a list of FortiWeb Cloud IP addresses.

What is an application in FortiWeb Cloud?

In FortiWeb Cloud, an application is a declared domain name and up to 9 other domain names attaching to it, which all belong to the same root domain and all point to the same origin server(s). For example, "example.com" and "test.example.com" can be part of the same application "example.com", while "test.com" is a different application.

What is a CNAME?

A CNAME record is a part of the DNS zone records (that may or may not be present) that is used to essentially redirect from one URL to another. The CNAME record for a DNS zone will have a URL for the record NAME, it will be of record TYPE “CNAME”, and it will have a VALUE of another URL. The VALUE field of a CNAME record is often called the CNAME, or canonical (true) name.

When you complete onboarding an application, FortiWeb Cloud provides you with a CNAME. You need to go to your DNS service and pair this CNAME with your application's domain name.

What if my DNS service does not support CNAMEs?

If your DNS service does not support CNAME, the workaround is to pair your application's domain name with the IP addresses of the FortiWeb Cloud scrubbing center which is deployed in the same region with your origin server. See this article for a list of FortiWeb Cloud IP addresses.

Please note the CDN feature won't be available in this scenario because all the traffic will be forwarded to a fixed scrubbing center.

Which public cloud regions host FortiWeb Cloud scrubbing centers?

FortiWeb Cloud supports most of the regions on AWS, Azure, and Google Cloud. See this article for a detailed list of supported regions.

What is a CDN?

By enabling **CDN**, the data on your origin servers can be cached in FortiWeb Cloud scrubbing centers distributed around the world. When users request data from your application, they can be directed to the nearest scrubbing center and rendered with the requested data. See this article for a list of FortiWeb Cloud IP addresses.

You can enable CDN when onboarding an application, or set this option in the **Application Settings** dialog (**Global > Applications**).

Why does my certificate display status Invalid Chain?

Please check with your certificate provider to confirm whether an intermediate certificate is required. If so, you will need to upload it as well.

Network

How can I add applications running on non-standard port?

FortiWeb Cloud by default uses port 80 for HTTP protocol and 443 for HTTPS protocol. Non-standard ports are also available. You can select them when you onboard applications. Please note if non-standard port is selected for HTTPS, you will not be allowed to configure HTTPS redirection.

If you need to use different ports, please contact Fortinet Support or your sales engineer for further help. Notice not all non-standard ports can be used, and HTTP and HTTPS services must use different ports.

Up to how many domains can I use in one single application?

Up to 10 domains are supported in one single application. They should all belong to the same root domain and point to the same origin server(s).

When onboarding an application, do all domains need to be part of the same root domain?

Yes, all the domains should belong to the same root domain, such as www.example.com and mail.example.com.

After the application is onboarded, you can go to **Network > Endpoints** to change or add domains, but you are not allowed to change the first domain in the list. Highly recommend to use root domain as the first domain.

Up to how many origin servers can I add for one application?

You can add at most 128 origin servers to the server pool of an application.

What is an Automatic Certificate?

FortiWeb Cloud automatically obtains an SSL certificate on your behalf from Let’s Encrypt within two minutes of the DNS CNAME record change. It will be used in HTTPS connections to encrypt or decrypt the traffic. If FortiWeb Cloud fails to obtain the certificate, it will try again 12 minutes later.

Thirty days before your certificate expires, FortiWeb Cloud verifies again that your DNS CNAME record is still correct. If it is, FortiWeb Cloud renews your certificate for another 90 days, so it never expires. For more information, see Automatic Certificate on page 119.

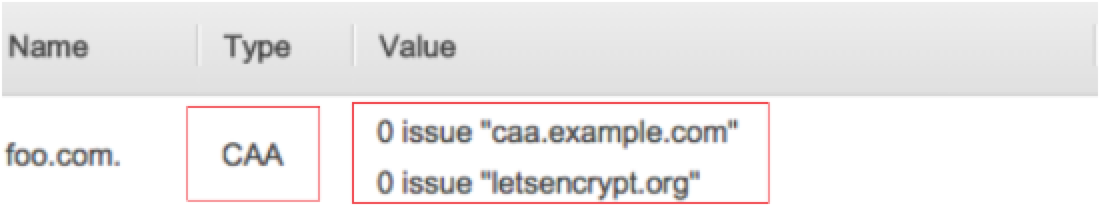
What do I need to pay attention to if I use automatic certificates?

FortiWeb Cloud automatically retrieves SSL certificates from the Certificate Authority Let's Encrypt. See Automatic Certificate for the things you should pay attention to if automatic certificate is used.

What’s a Certification Authority Authorization (CAA) record and do I need to use it? How does it affect automatic certificate?

DNS Certification Authority Authorization (CAA) is an Internet security policy mechanism which allows domain name holders to indicate to certificate authorities whether they are authorized to issue digital certificates for a particular domain name. It does this by means of a new "CAA" Domain Name System (DNS) resource record.

If you have configured a CAA record at your DNS service and want to use automatic certificate in FortiWeb Cloud, make sure to add "letsencrypt.org" in the CAA value. This allows Let's Encrypt to issue certificates for your domain name.



Name	Type	Value
foo.com.	CAA	0 issue "caa.example.com" 0 issue "letsencrypt.org"

Is TLS 1.0 still supported?

No. We now support TLS 1.1, 1.2, and 1.3.

What do I need to check if I still see “connection is not secure” in my browser?

Check the following if “connection is not secure” displays in the browser when users visit your application:

- If HTTP protocol is used in this connection, it's suggested to enable **HTTPS** service and **Redirect all HTTP traffic to HTTPS** in **Network > Endpoints** in FortiWeb Cloud, so that the HTTP access can be redirected to HTTPS, which is secured by SSL/TSL certificates.
- If HTTPS protocol is used in this connection, check whether the certificates are valid:
  - If **Custom Certificate** is selected in **Network > Endpoints**, make sure the SNI certificates or intermediate certificates you imported are valid.
  - If **Automatic Certificate** is selected, see the following FAQs to trouble-shoot:
    - What do I need to pay attention to if I use automatic certificates? on page 272
    - What’s a Certification Authority Authorization (CAA) record and do I need to use it? How does it affect automatic certificate? on page 272

How to check network connectivity when traffic does not go through?

To troubleshoot network connectivity when traffic doesn't go through, follow these steps:

1. Ensure that you are using a supported web browser. FortiWeb Cloud supports Mozilla Firefox version 59 or higher, and Google Chrome version 65 or higher. While other browsers may also display well but we cannot guarantee compatibility.
2. Check the error message displayed. If it shows server connectivity issue, perform either one of the following actions:
   a. Modify the local host file on your computer to map your application's domain name to the IP address of the origin server. Then, enter the domain name of your application in the browser to verify the traffic can go through when FortiWeb Cloud is bypassed.
   b. If there are more than one origin servers, FortiWeb Cloud performs health check and displays the server status in the **Server Status** widget on **Dashboard** page, as well as in the **Server Status** column of the **Origin Server** page. Make sure the **Health Check** option is turned on and the **URL Path** on the **Origin Server** page is configured correctly, as FortiWeb Cloud relies on it to verify server responsiveness.
   If the origin server is accessible, proceed to the following steps to identify the specific configuration on FortiWeb Cloud causing the error.
   If the origin server is not accessible, it suggests that the connectivity issue is unrelated to FortiWeb Cloud and you should troubleshoot the origin server.
3. Verify the **SSL Encryption Level** configuration on the **Origin Server** page and ensure that your origin server supports the specified SSL Encryption Level.
4. Disable **HTTP/2** on the **Origin Server** page and check if the traffic goes through. If it does, it indicates that your origin server doesn't support HTTP/2, and therefore, the HTTP/2 option on FortiWeb Cloud should be disabled.
5. Analyze attack logs in **Threat Analytics > Attack Logs** to identify any WAF modules that may be blocking traffic.

How to get notified if an origin server fails?

FortiWeb Cloud support sending logs to your syslog or ElasticSearch server to notify the origin server status change.

1. Enable **Health Check** for the origin server in the Load Balancing rule in **Network > Origin Server**. Please note this setting is only available when the **Server Balance** is turned on.
2. Refer to Audit logs to export logs to your syslog server.

How can I use FortiWeb Cloud with AWS ALB/ELB?

When using FortiWeb Cloud, the client's requests from the Internet are forwarded to FortiWeb Cloud first before they reach the ALB/ELB.

When you onboard an application, for **Origin Server** settings in **Step 2- Network**, select **Customize**, then enter the ALB/ELB's domain name in **IP Address or FQDN**. Make sure to enter the domain name, not the IP address.

I entered a dynamic domain name for my origin server's address in Network Settings. How frequently does FortiWeb Cloud update the IP address paired with this domain name?

In the DNS record that pairs the dynamic domain name and IP address, you will find a TTL (Time to Live) value. FortiWeb Cloud updates the IP address according to this TTL value. If the TTL indicates the IP address expires, FortiWeb Cloud will resolve the domain name to obtain the latest IP address.

The IP addresses of my origin servers keep changing. How can I configure FortiWeb Cloud to automatically obtain the latest IP addresses?

You can use **Cloud Connectors** to obtain the IP addresses if your origin servers are deployed on AWS, Azure, or GCP.

1. Create a Cloud Connector to authorize FortiWeb Cloud to access the resources in your public cloud account. See Cloud Connectors on page 80.
2. In **Network > Origin Servers**, select **Dynamic** for **Server Type**, then configure **Cloud Connector** and **Filter** as instructed in Origin Servers on page 114.

How can I use FortiWeb Cloud behind a Content Distribution Service?

See Using FortiWeb Cloud behind a Content Distribution Service on page 218 for detailed information.

How should I configure the network settings if my application offers different content through HTTP and HTTPS?

See Network settings for applications serving different content over HTTP and HTTPS on page 227 for more information.

How can I get notified about a new WAF IP?

- Check the inbox of your account email. Search for keywords "new WAF cluster" from "noreply@fortiweb-cloud.com".
- Check the What's New part in Online help.
- Use the following APIs to retrieve the IP lists:
  - IPv4: https://www.fortiweb-cloud.com/ips-v4
  - IPv6: https://www.fortiweb-cloud.com/ips-v6

Subscriptions and Contracts

What happens if I unsubscribe from FortiWeb Cloud?

- For subscriptions on AWS, Azure, and Google Cloud: You can unsubscribe from FortiWeb Cloud anytime, while the data in your FortiWeb Cloud account will be kept for an additional week.
- For FortiWeb Cloud contract: After the contract expires, FortiWeb Cloud continues protecting your applications for 21 days. During this period, you are not allowed to edit configuration for your applications unless the contract is

renewed.
After the 21-day extension, your applications will be deleted from your FortiWeb Cloud account.

After you unsubscribe from FortiWeb Cloud, remember to replace CNAME with the right IP address in the DNS record so your web application does not experience service interruption.

Will FortiWeb Cloud stop serving my app or degrade the service after my license expires and before the application is removed?

After the contract expires, FortiWeb Cloud continues protecting your applications for 21 days.

During this 21-day period, you can view but cannot edit configurations on FortiWeb Cloud.

For public cloud subscription customers, after canceling the subscription, FortiWeb Cloudcontinues protecting your applications for 7 days.

During this 7-day period, you can view but cannot edit configurations on FortiWeb Cloud.

Can I get the configuration backup after the app was removed due to invalid licenses?

No. Due to security and privacy considerations, FortiWeb Cloud does not retain any customer configurations once the application has been deleted.

However, several days before the licenses become invalid, you should receive a warning email specifying the expiration date of the licenses. During this period, you have the option to extend the licenses if you intend to continue using the service.

What happens if I delete an application from FortiWeb Cloud?

The data for this application will be deleted and can't be restored.

Will my applications be deleted if my contract expires?

After your contracts expire, FortiWeb Cloud initiates a grace period, during which you have read-only access to all of your applications until the contracts are renewed.

For public cloud subscription customers, this grace period is 7 days. For all other customers, this grace period is 21 days.

Once the grace period ends, all of your applications will be deleted from FortiWeb Cloud.

Can I request to migrate my applications between accounts?

You can contact the FortiWeb Cloud Team for help with migrating applications between accounts. In your inquiry, please include account details for both accounts, including the Serial Number and associated email for each account, along with platform information (e.g., AWS, Azure, GCP). For additional guidance on how to contact our Customer Service, please refer to the Contacting Customer Service section.

What happens if I exceed the usage limit for my contract?

When an account has onboarded more applications than their contract allows, FortiWeb Cloud will immediately lock the UI and move it to read-only. Customers will not be able to make any changes until additional contracts are purchased.

For example: A customer purchases two contracts; the first one is purchased on January 1 for a single web application. On April 1, the customer purchases another contract for five more applications. On January 1 of the next year, the first contract for the single web app expires leaving the customer with a 5 web app contract. The customer now has 6 applications onboarded while the license only allows 5 applications. The customer will have read-only access for all of their applications until they purchase another contract.

When a customer uses more bandwidth than their contract allows (bandwidth usage is measured monthly at the 95th percentile), FortiWeb Cloud triggers an internal notification. However, it does not block nor throttle access to customer applications. The account team will contact affected customers and inform them of the need to purchase new contracts immediately. Currently, as of February 2023, this notification process is manual. However, we are working on automating it, and in the future, restrictions like those mentioned above will be deployed automatically when there are bandwidth contract violations.

What does Fortiweb Cloud do if the certificate in the backend server is expired/self signed?

Fortiweb Cloud WAF is primarily focused on protecting web applications from various security threats and does not validate or manage server certificates.

The WAF processes the request as if it were in transparent mode, potentially allowing the user to reach the backend server.

Cost and Billing

Where can I purchase FortiWeb Cloud services?

FortiWeb Cloud offers 14-day free trial on public cloud platforms. After the free trial, you can subscribe to FortiWeb Cloud or purchase service contracts from Fortinet to continue using it.

- Subscribing through AWS Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Subscribing through Azure Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Subscribing through Google Cloud Marketplace. The cost is calculated on the Pay-as-you-go basis.
- Using FortiWeb Cloud license purchased from your Fortinet reseller. The license allows you to protect certain number of applications and specifies the maximum bandwidth.

Please note that if you have subscribed to FortiWeb Cloud on public cloud platforms and also imported a FortiWeb Cloud license in your account, it's recommended to unsubscribe from FortiWeb Cloud, otherwise you will be charged simultaneously through both channels.

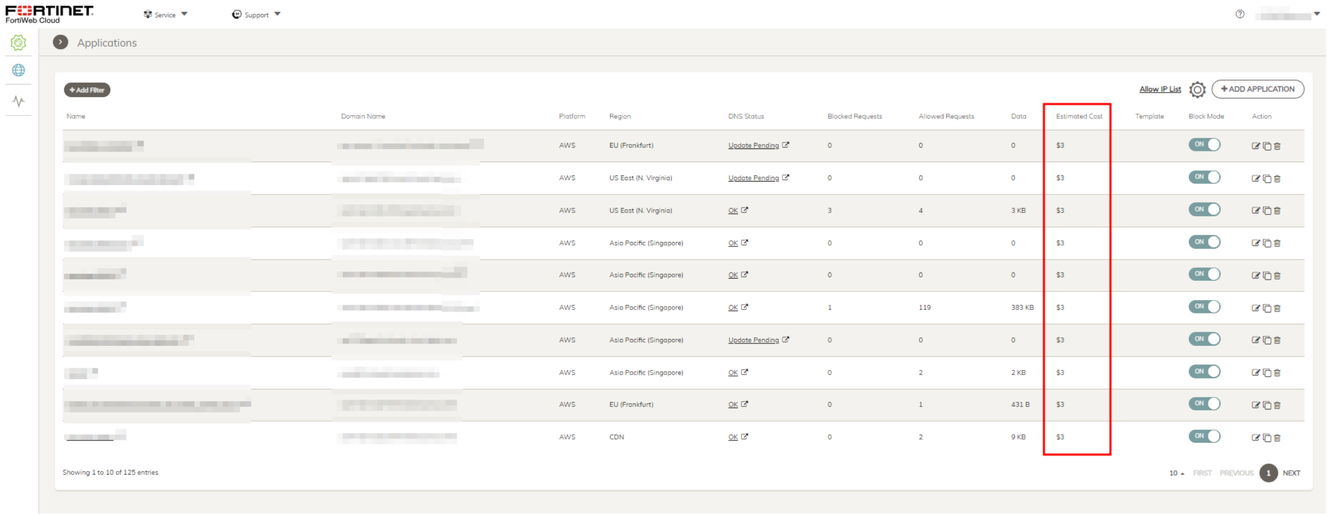
What is the billing structure of FortiWeb Cloud?

If you purchase FortiWeb Cloud service from Fortinet sales team, you will be charged for the Bandwidth contract and Applications contract, which respectively control how many applications you can add in your account and the maximum bandwidth.

For those with or interested in a FortiFlex contract, use our FortiFlex Calculator to estimate service costs conveniently.

When subscribing through AWS, Azure, or Google Cloud, charges are based on data sent to your app users with a pay-as-you-go model. There's no limit on the number of apps in your account. You're charged $0.03 per hour per web app and $0.4 per GB of traffic. Hourly charges start when you onboard an app onto FortiWeb Cloud, regardless of DNS status. Traffic charges begin when data actively flows through FortiWeb Cloud to your app. Regardless of the third-party platform you use to subscribe, you can use FortiWeb Cloud to protect applications located on any other cloud platform or in your own network. The subscription channel only determines the billing places for your FortiWeb Cloud usage.

Please note, the estimated cost shown in your FortiWeb Cloud account may not be accurate, as it is estimated by FortiWeb Cloud based on the amount of data transferred in your account.



Name	Domain Name	Platform	Region	DNS Status	Blocked Requests	Allowed Requests	Data	Estimated Cost	Template	Block Mode	Action
[redacted]	[redacted]	AWS	EU (Frankfurt)	Update Pending	0	0	0	$3		ON	
[redacted]	[redacted]	AWS	US East (N. Virginia)	Update Pending	0	0	0	$3		ON	
[redacted]	[redacted]	AWS	US East (N. Virginia)	OK	3	4	3 KB	$3		ON	
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	0	0	$3		ON	
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	0	0	$3		ON	
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	1	119	383 KB	$3		ON	
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	Update Pending	0	0	0	$3		ON	
[redacted]	[redacted]	AWS	Asia Pacific (Singapore)	OK	0	2	2 KB	$3		ON	
[redacted]	[redacted]	AWS	EU (Frankfurt)	OK	0	1	431 B	$3		ON	
[redacted]	[redacted]	AWS	CDN	OK	0	2	9 KB	$3		ON	

Showing 1 to 10 of 125 entries

10 FIRST PREVIOUS 1 NEXT

The final cost is billed in your AWS/Azure/Google Cloud account, depending on where you subscribe.

For contracts purchased via a Fortinet reseller, how does FortiWeb Cloud calculate bandwidth?

FortiWeb Cloud measures each account using a burstable model for overall account bandwidth calculation. The model is based on calculating the 95th percentile of bandwidth usage of clean traffic and is also common with other CDNs and Cloud solutions.

The 95th percentile bandwidth is calculated in the following way:

- Traffic for the entire month is measured in 5 minute buckets.
- At the end of the month, the 5% of buckets with the most Mbps are dropped, and the highest Mbps rate of the remaining buckets represents the 95th percentile value for the account.

At the beginning of every month, the 95th percentile bandwidth shown in FortiWeb Cloud might be very low, or even shown as 0. This is because there aren't enough 5-minute buckets collected to calculate a valid value. At the end of the month with more buckets generated, the value becomes more accurate.

Security

What are the security features provided by FortiWeb Cloud?

The following security features are provided by FortiWeb Cloud:

- Security Rules
- Client Security
- Access Rules
- Bot Mitigation
- DDoS Prevention
- Advanced Applications
- API Protection

- Account Takeover
- Application Delivery

What’s the difference between Monitor mode and Block mode?

- When Block Mode is enabled, FortiWeb Cloud blocks requests if they trigger violations. Your application server does not receive these requests.
- When Block Mode is disabled (that is, the Monitor mode), FortiWeb Cloud only monitors violations and generates logs for them. FortiWeb Cloud does not block the malicious requests. You can view the attack logs in FortiView or Attack Logs.

What to do if legitimate requests are blocked by FortiWeb Cloud?

You can add exceptions in **Attack Logs** so that the requests from the specified URL or parameter will not be detected as attack again. See Log Settings on page 105 for more information.

You can also add exceptions in the following three security modules:

- Known Attacks on page 128
- Threshold Based Detection on page 154
- Information Leakage on page 135

How do I block access to a particular URL or path?

You can use the **URL Access** in **Access Rules** to define which HTTP requests FortiWeb Cloud accepts or denies based on their `Host:` name and URL, as well as the origin of the request. See URL Access for more information.

You can also add **URL filters** in **Custom Rules** to match the requests with specified URLs. See Custom Rule for more information.

If a protected application is targeted by DDoS attacks, will the traffic volume generated by the attack incur additional charges?

No. FortiWeb Cloud does not charge for inbound traffic, so additional charges will not be incurred related to DDoS attacks. An advantage of deploying FortiWeb Cloud in public cloud (AWS, Azure, and Google Cloud) is that FortiWeb Cloud enjoys the protection of the volumetric DDoS protections provided by those platforms. FortiWeb Cloud also provides additional DDoS protections for Network and transport layer (TCP/IP) and Application layer (HTTP or HTTPS) DDoS attacks (see DDoS prevention).

How to quickly apply the same configuration to multiple applications?

FortiWeb Cloud provides **Templates** for you to create configuration templates and apply them to multiple applications. For more information, see Templates on page 67.

What's the sequence for FortiWeb Cloud to execute the security rules?

FortiWeb Cloud executes the security rules in a certain sequence. See Sequence of scans on page 251.

When clicking on the external link on my application, the user gets the warning "The URL xxxxxxxxxx has been denied". Why it happens?

The MITB Protection restricts AJAX requests to external domains. If you come across this warning, it could be because the request has triggered the MITB rules. If you are confident in its safety, you have the option to add this link to the External Domain allowlist in MITB Protection. For more information, see MITB Protection.

Will FortiWeb Cloud prevent from amplification attacks, UDP floods, ICMP floods, and other spoofed-packet flood?

DDoS attacks can be prevented at Application layer (HTTP or HTTPS) and Network layer (TCP/IP).

As public cloud platforms already execute basic Network layer TCP Flood Prevention checks affront, when traffic comes into FortiWeb Cloud, it only detects DDoS attacks at Application layer (HTTP or HTTPS).

I have enabled a WAF module, but why it does not take effect?

Please verify if the Block Mode is currently enabled.

By default, after an application is onboarded, the Block Mode is in Disabled status. You need to enable it first for the WAF modules to take effect.

On **Applications** page, you can turn on/off the Block Mode for each application. However, before enabling Block Mode, it is important to perform several checks. For more detailed information on Block Mode, see Understanding block mode and action.

Why is the IP address blocked due to bad reputation although it cannot be found in Bad Reputation IP list?

The website (https://www.fortiguard.com/services/ws) maintains an up-to-date database of IP reputation. However, it's important to note that FortiWeb Cloud may still be using data from a few days ago, resulting in a latency in the database update.

Therefore, when the database in FortiWeb Cloud is updated, this IP address will be removed from the Bad Reputation IP list. If you have confidence in the trustworthiness of this IP address and don't wish to wait for the database update, you have the option to manually add this IP address to the **Trust IP** list in the **IP Protection** settings.

How can I enable FortiSandbox?

Turn on **Advanced Threat Protection** in **File Protection**, then FortiWeb Cloud will send files that meet the configured conditions to FortiSandbox for evaluation.

This option works only if your application is hosted on AWS or Azure. Refer to https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/748121/file-protection.

What is the difference between "Trust IPs" and "Allow-Only IPs" in the IP Protection module?

IPs in Trust IP list will be fully trusted by FortiWeb Cloud without undergoing any additional scanning, while the IPs in Allow-Only list is only trusted by the IP Protection module and will be forwarded to other modules for security checks.

It is important to note that there are other considerations regarding these lists. For more comprehensive details, refer to the description of the "Type" option in IP Protection.

How should I configure the system to allow valid IPs from a restricted country?

To allow certain IPs from a restricted country, you can configure the following steps in **Access Rules > IP Protection**:

1. Block the country through **GEO IP Block**. This will prevent access from IP addresses originating from the specified country.
2. Add IPs to **Allow-Only** IP List. This ensures that the IP Protection module will trust and forward these IPs to other modules for additional security checks. If you have complete trust in these IP addresses, you can include them in the **Trust** IP list, so these IPs will bypass any further security checks and be directly permitted.

By combining these steps, you can effectively block access from the restricted country while allow specific IPs.

For more comprehensive details, refer to IP Protection.

Logs

How long are the logs kept in FortiWeb Cloud?

FortiWeb Cloud saves the attack logs for two months and the audit logs for three months. After that, they will be deleted.

Where to view and delete the exceptions related with Anomaly Detection?

Exceptions are added in Attack Logs. It can't be reversed once being added.

If you believe that the Anomaly Detection model is inaccurate with certain exceptions, you have the option to access the TreeView page of the Anomaly Detection module. From there, you can locate the parameter to which the exception is applied and rebuild the model specifically for that parameter. When the new model is rebuilt, the exceptions added to the Anomaly Detection attack logs corresponding to that parameter will be cleared.

Why do I find several attack logs even though there is only one attack request?

In the scanning process, when a request passes through different modules in sequence, the configured action for certain modules can be set to "Alert" or "Monitor". In this case, if an attack is detected by a module with such an action, it will allow the request to continue to the next module for further scanning. However, an attack log will be generated by the module that identified the attack.

As the request progresses through subsequent modules, it is possible for the attack to be logged multiple times by different preceding modules before it is blocked by a module with a different action, such as "Block Period" or "Deny".

As for the scan sequence, please refer to https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/234292/sequence-of-scans.

Domain name cannot be seen in GEO IP attack logs. How to solve it?

If the `https_host` in GEO IP attack logs shows `none`, it can be solved by enabling **Use X-Header to Identify Original Clients' IP** and **Add X-Forwarded-For** in the **Rewriting Requests** module.

How to show the client source IP instead of FortiWeb Cloud IP received from the server side?

To observe the client's original source IP, it is advised to enable the **Rewriting Requests** module, turning on **X-Forwarded-For**, **X-Real-IP**, and **Use X-Header to Identify Original Clients' IP** options.

Why the origin server receives logs with FortiWeb Cloud's IP rather than the client real IP even if X-Forwarded-For related options are enabled?

Logs are sent from FortiWeb Cloud to the origin server, so the `IP:` header (layer 3) of the logs is supposed to be FortiWeb Cloud's IP address. This is expected behavior.

To check the client real IP, you need to find it in the `X-Forwarded-For:` or `X-Real-IP:` header in the packets forwarded from FortiWeb Cloud to your server. Be aware that to record the client real IP it's required to enable both **Add X-Forwarded-For** and **Use X-Header to Identify Original Client's IP** in the **Rewriting Requests** module.

Why an attack log is classified as Anomaly Detection, not Known Attack?

The signatures used in Known Attacks are primarily designed to detect known patterns of malicious code. However, they may not cover all variants or newly emerging forms of attacks.

In cases where an attack is logged under the Anomaly Detection threat type instead of being matched with a signature, it in fact indicates the successful functioning of the machine learning model in Anomaly Detection. It effectively screened out unknown or new variant attacks that do not align with existing signatures.

Why is the number of blocked requests in the Attack Log and the Blocked Requests Widget inconsistent?

You can view the blocked requests in three places: 1) Attack Logs; 2) FortiView ; 3) Blocked Requests widget on Dashboard. The ways they count the blocked requests are slightly different.

- To prevent Information Leakage, FortiWeb Cloud may cloak the error pages or erase sensitive HTTP headers in response packets. Such item are logged only once per minute in Attack Logs and FortiView for you to know the Information Leakage rule took effect. In the meanwhile, the actual count is recorded in Blocked Requests Widget.
- If you have set FortiWeb Cloud to block attacks but do not generate a log when certain violation occurs, such as Deny(no log), then the attacks will not be logged in Attack Logs and FortiView , but will be counted in the Blocked Requests widget.
- The invalid requests to the host header HOST will be blocked without generating any log.
- When the Block Mode is in disabled state, attacks won't be blocked but logs are generated.

Why is there no attack log while the request is blocked?

If you have set FortiWeb Cloud to block attacks but not generate a log when certain violation occurs, such as 'Alert & Deny (no log)', then the attacks will not be logged in Attack Logs and FortiView but will be counted in the Blocked Requests widget.

If you need to have detailed logs for auditing or analysis purposes, you may consider using a different action, such as 'Alert & Deny' or 'Block Period', which will not only block the request but also generate a log entry.

To identify the security feature blocking your request, map the Attack ID value to the corresponding description in the table below.

Attack ID	Security Rule
20000001	Allow Method
20000002	Protected Hostnames
20000003	Page Access

Attack ID	Security Rule
20000004	Start Pages
20000005	Parameter Validation
20000006	Black IP List
20000007	URL Access
20000008	Signature Detection
20000009	Custom Signature Detection
20000011	Hidden Fields
20000012	Site Publish
20000013	HTTP Parsing Error
20000014	DoS Protection
20000015	SYN Flood Protection
20000016	HTTPS Connection Failure
20000017	File Upload Restriction
20000018	GEO IP
20000019	Illegal XML Format
20000020	Illegal JSON Format
20000021	Custom Access
20000022	IP Reputation
20000023	Padding Oracle
20000024	CSRF Protection
20000025	Quarantined IPs
20000026	HTTP Protocol Constraints
20000027	Credential Stuffing Defense
20000028	User Tracking
20000029	XML Validation Violation
20000030	Cookie Security
20000031	FTP Command Restriction
20000032	FTP Parsing Error
20000033	Timeout Session
20000034	Other Attacks

Attack ID	Security Rule
20000035	FTP File Security
20000036	FTPS Connection Failure
20000037	Anomaly Detection
20000038	OpenAPI Validation Violation
20000039	WebSocket Security
20000040	MITB AJAX Security
20000041	Bot Detection
20000042	CORS Check Security
20000043	JSON Validation Security
20000044	Mobile API Protection
20000045	Bot Deception
20000046	Biometrics Based Detection
20000047	Threshold Based Detection
20000048	API Gateway
20000049	URL Encryption
20000050	SQL/XSS Syntax Based Detection
20000051	Known Bots Detection
20000053	Allow Only IP List
20000200	Known Attacks
20000201	Information Leakage
20000202	Cookie Security
20000203	File Protection
20000204	Client Security
20000205	Request Limits
20000206	URL Access
20000207	IP Protection
20000208	Bot Mitigation
20000209	DDoS Prevention
20000210	XML Security
20000211	OpenAPI Validation

Attack ID	Security Rule
20000212	WebSocket Security
20000213	Known Bots Detection
20000214	API Gateway
20000215	Mobile API
20000216	JSON Security

I enabled exporting attack logs to FortiAnalyzer and passed the connectivity test. However, I cannot see any attack logs on FortiAnalyzer. Why is this happening?

You may need to authorize the devices of FortiWeb Cloud in your FortiAnalyzer.

Check if your FortiWeb Cloud's application serial number shows up under **FAZ > Device Manager > Unauthorized Devices**, if so, authorize it to send attack logs to FortiAnalyzer.

Accounts

Can I change the email address associated with the super root account, that is, the account I used when I subscribed to FortiWeb Cloud?

The account management for FortiWeb Cloud is handled through FortiCloud. You can log in to FortiCloud, then select **My Account > Change Account ID (Email)** .For a step-to-step instructions, please refer to the following article: https://docs.fortinet.com/document/forticloud/latest/identity-access-management-iam/588195/my-account.

Why I can't log in to FortiWeb Cloud?

Please check if any VPN or Secure Access Service Edge (SASE) is used on your computer. If yes, please turn it off and try again. Some VPN will break the SAML response from FortiCloud and cause the failure of login.

Sub-users could successfully log in previously, but now they encounter permission error. Why is that?

From 21.3.b (09/03/2021), FortiWeb Cloud automatically synchronizes sub-users with the ones in your FortiCloud account and assign them with a "None" role. The role of the existing sub-users in your FortiWeb Cloud account will be restored to "None". To grant more permissions to the sub-user, go to **Global > Admin Management**, click the edit icon for this user, then assign it with a different role. See Admin management.

How do I change the role/permission of an IAM user?

1. Go to **Admin Management**, and find the IAM user whose permissions you want to change in the table.
2. In the **Role Name** column, you should see "Managed by FortiCloud" for this user. Click it to go to **IAM > Users** in FortiCloud.
3. Go to **Permission Profiles** in the left navigation bar and edit the widget for FortiWeb Cloud under **Permission Profile > Permission Details**.

Miscellaneous

What's Two-Factor Authentication used for?

FortiWeb Cloud offers Two-Factor Authentication to secure your FortiWeb Cloud account by an additional security token sent through email or the FortiToken Mobile application. See Two-Factor Authentication on page 45.

What are the supported web browsers?

FortiWeb Cloud supports the following web browsers:

- Mozilla Firefox version 59 or higher
- Google Chrome version 65 or higher

Whom should I contact for help regarding FortiWeb Cloud?

You can submit a support ticket to the support team. See Contacting customer service on page 286.

How to find the serial number of my license?

See Registering serial number for how to find the SN number and register it.

If the SN number has already been registered, you can find it through **Asset > Manage/View Products** on Fortinet Support site https://support.fortinet.com/.

What are the benefits for MSSPs to migrate to FortiCloud OU?

Release 24.1 requires all Managed Security Service Providers (MSSPs) and tenants to migrate to FortiCloud Organization. FortiCloud Organizational Units (OUs) help MSSPs meet unified resource management and resource isolation requirements.

Additionally, OUs make it possible to purchase contracts with FortiFlex, a new usage-based security licensing solution that allows customers to pay only for what they use instead of buying yearly contracts. It is important to note that existing contracts will not be affected by this migration.

As an MSSP, how do I migrate to FortiCloud OU?

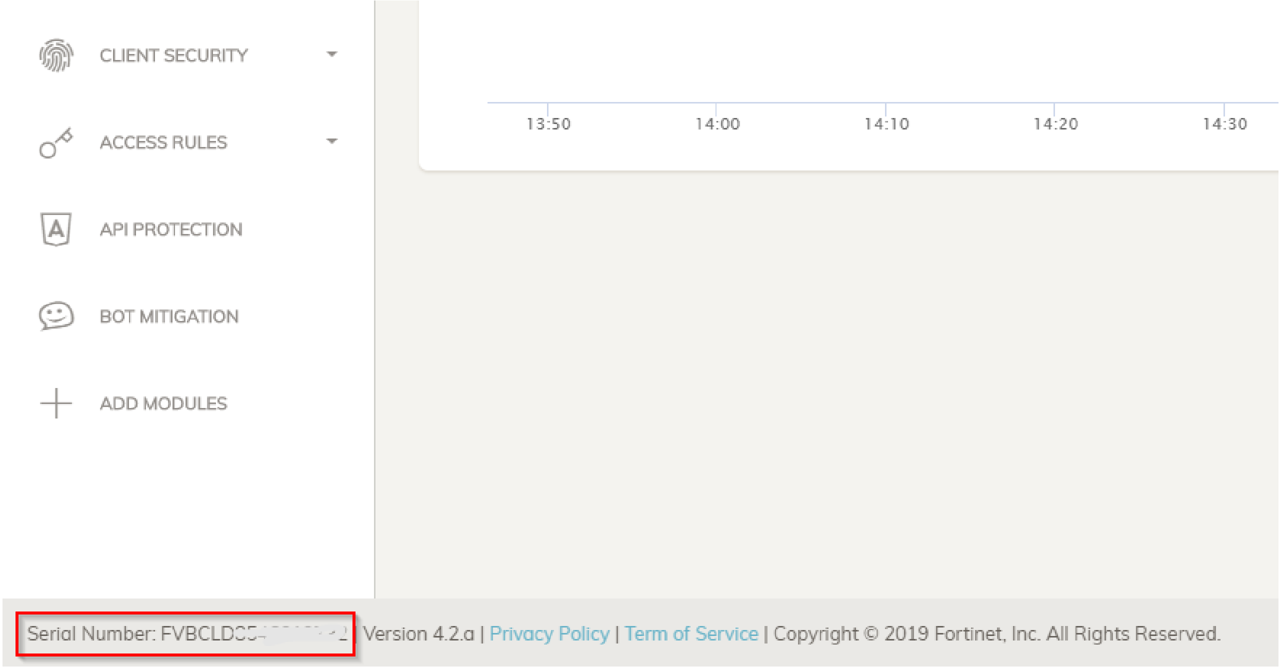
For instructions on migrating to FortiCloud OU, please refer to Technical Tip: MSSP Migration to OU.

Contacting customer service

Fortinet provides customer service and support for FortiWeb Cloud WAF-as-a-Service. To submit a support ticket, you need to first register your serial number of FortiWeb Cloud on Fortinet Support site.

Registering serial number

1. Log in to FortiWeb Cloud, take note of the Serial Number at the bottom left corner.

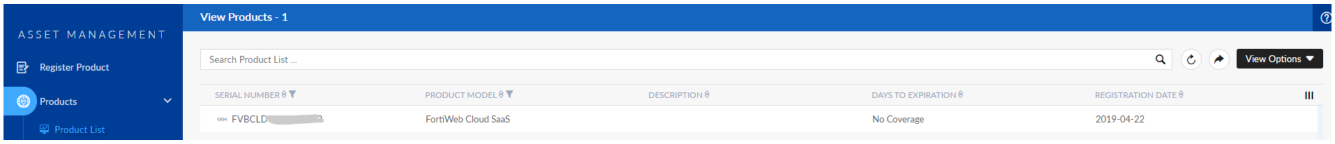


Serial Number: FVBCLD[redacted] Version 4.2.a | Privacy Policy | Term of Service | Copyright © 2019 Fortinet, Inc. All Rights Reserved.

2. Go to https://support.fortinet.com, follow the guidelines provided in the FortiCloud documentation Registering Assets to register serial numbers (assets).

Listing all your licenses

Once all of your serial numbers are registered, you can view them through **Services > Asset Management**.

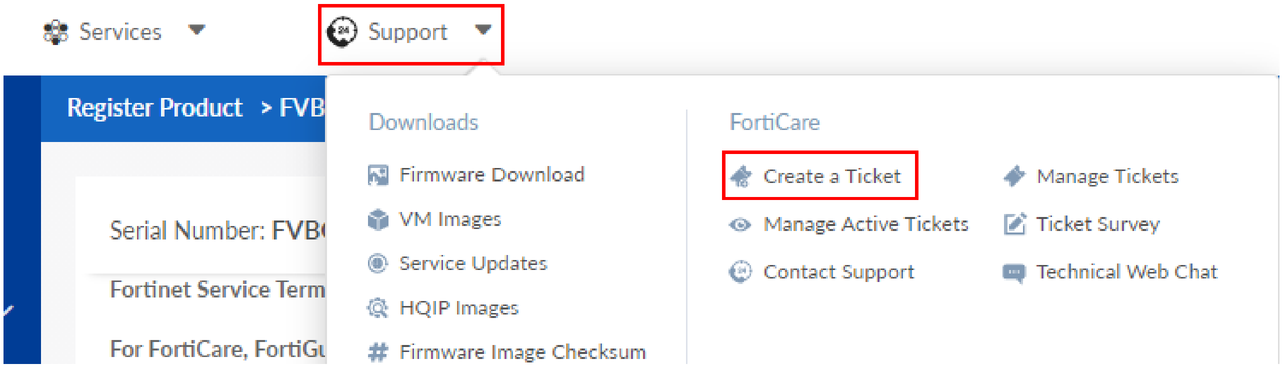


SERIAL NUMBER	PRODUCT MODEL	DESCRIPTION	DAYS TO EXPIRATION	REGISTRATION DATE
FVBCLD[redacted]	FortiWeb Cloud SaaS		No Coverage	2019-04-22

Submitting tickets

To submit a technical support tickets, you will be required to enter the serial number of an active license.

1. Select **Support > Create a Ticket**.



2. Select **Technical Support Ticket**, enter the serial number of a valid license, then click **Submit Ticket**.