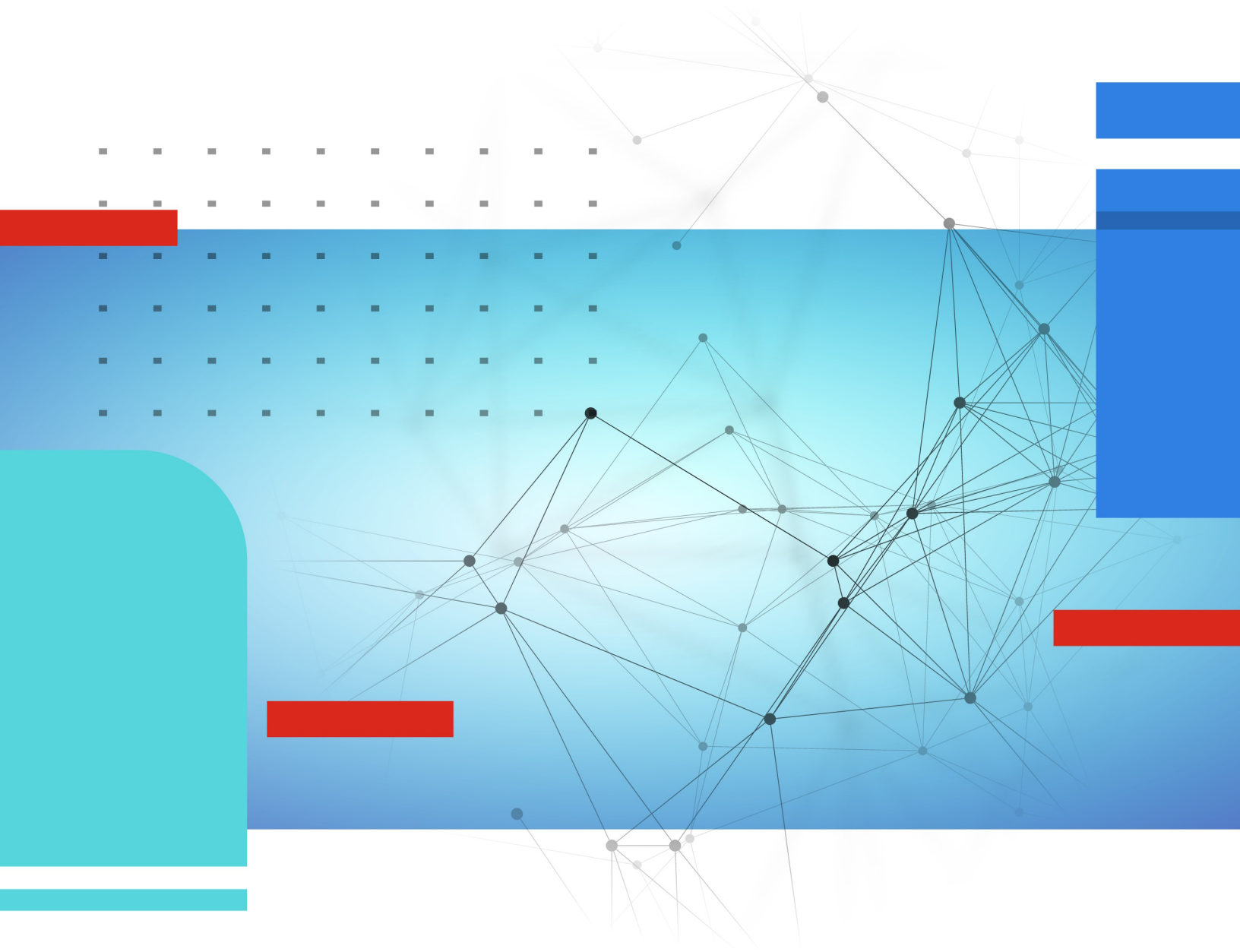
User Guide

FortiAppSec Cloud 25.4



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

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 11, 2025
FortiAppSec Cloud 25.4 User Guide

TABLE OF CONTENTS

What's New ... **8**
25.4.a released December 11, 2025 ... 8
Client-Side Protection ... 8
WAF ... 9
GSLB ... 9
Advanced Bot Protection ... 9
25.4 released November 6, 2025 ... 10
WAF ... 10
GSLB ... 11
Advanced Bot Protection ... 11
25.3.b released September 25, 2025 ... 11
25.3.a released August 28, 2025 ... 13
25.3 released July 31, 2025 ... 13
25.2.a released June 26, 2025 ... 15
25.2 released June 3, 2025 ... 15
25.1.a released March 27, 2025 ... 17
25.1 released February 27, 2025 ... 17
WAF ... 17
Advanced Bot Protection ... 18
GSLB ... 19
24.4.p1 released on January 9, 2024 ... 19
Overview ... **20**
Getting Started ... **21**
License & Contract ... 21
FortiAppSec Cloud contract options ... 22
View contract ... 28
Renew contract ... 29
Overage and expiration behavior ... 29
License Upgrade Trial ... 30
Fortinet Contracts ... 31
FortiFlex ... 32
Public Cloud Marketplace subscriptions ... 37
Onboarding ... 50
Add Application ... 50
Home ... **51**
Understanding Insights ... 51
FortiAI Assistant ... **54**
Activate FortiAI Assistant ... 54
How to use FortiAI Assistant ... 54
Chatbot Limitations ... 59
Token usage ... 60
WAF ... **61**
WAF Concepts ... 61

WAF setup ... 63
Onboard WAF applications ... 65
Change DNS record ... 73
Changing IP addresses of origin servers ... 76
Restricting direct traffic & allowing FortiAppSec Cloud IP addresses ... 76
How does WAF choose regions? ... 78
Understanding block mode and action ... 81
WAF Workflow and Dashboard Overview ... 82
WAF Applications ... 86
Viewing application information ... 87
Onboarding applications ... 89
Cloning the application configurations ... 89
Enabling/disabling CDN ... 89
Changing FortiAppSec Cloud scrubbing center ... 89
WAF Application Dashboard ... 90
FortiView ... 92
Network ... 95
Endpoints ... 95
Origin Servers ... 103
Content Routing ... 110
Supported cipher suites & protocol versions ... 116
Diagnostics ... 117
Log Settings ... 120
Attack Log Alerts ... 120
Exporting traffic logs ... 122
Sensitive Data Masking ... 125
Retention and Periodic clean ... 125
WAF modules ... 127
Add and Remove Modules ... 128
Security Rules ... 130
Client Security ... 146
Access Rules ... 150
Bot Mitigation ... 161
DDoS prevention ... 172
Connection Limits ... 172
Advanced Applications ... 174
API Protection ... 180
Account Takeover ... 191
Application Delivery ... 192
Global Trustlist ... 200
Vulnerability Scan ... 201
Templates ... 202
System Settings ... 204
WAF Settings ... 204
Cloud Connectors ... 205
Custom Pages ... 207
Use cases ... 214
DevOps tools ... 215

Using WAF behind a Content Distribution Service 233
Network settings for applications serving different content over HTTP and HTTPS 241
Multiple domains sharing the same IP address 241
Connecting WAF to the Fortinet Security Fabric 242
Managing External IdP roles in FortiCloud IAM 243
Frequently used regular expressions 243
Operational Guidelines 245
Maximum configuration values 245
Sequence of scans 247
Advanced Bot Protection 254
Overview 255
Security Fabric Integration 255
ABP Workflow and Dashboard Overview 256
ABP Setup 264
Onboarding ABP Applications 264
Integrate ABP on an on-premises device 276
ABP Application 284
Usage 289
Traffic Insights 290
Dashboard 291
Transactions 295
Attack Query 298
Account Monitor 300
Bot Monitor 302
Exploration 305
General 307
Configurations 307
Signals 310
Connectors 311
GSLB 313
GSLB Dashboard 314
Onboarding GSLB Applications 316
Configuring GSLB Objects 316
Linking GSLB to domain register 318
Maintenance 324
Anycast Migration for global DNS service 324
Migrate Legacy GSLB Organizations to FortiCloud Organizational Units (OU) 328
Topology 334
Service 337
FQDN 338
Virtual Server Pool 348
Location 351
Address group 353
Virtual Server 353
Fabric connector 353
Data center 357
DNS service 358

DNS Resource Types 362
How to create a DNS record 366
How to enable DNSSEC on GSLB 366
How to add GSLB as sub-domain 369
Synthetic testing 371
How to set up synthetic testing for multisite applications 372
Health check 373
Before you begin 374
Configure health check 374
Add Health Check to a Virtual Server 376
Integrating GSLB into the Fortinet Security Fabric 378
Setting up an FQDN with Generic-Host connector 379
FortiADC Integration with One-Click GSLB 380
FortiGate Integration 385
Fabric connectors with AWS and Azure 395
GSLB Settings 398
Email Notification Subscription 398
Threat Analytics 400
Threat Analytics Dashboard 400
Filter 401
Widgets 401
Incidents 402
Incident Organization 403
Additional Incident Details 405
Analyze with AI 406
Insights 407
Settings 408
Attack logs Export 408
Attack logs 412
Forwarding FortiADC attack logs to Threat Analytics 416
Forwarding FortiWeb attack logs to Threat Analytics 421
Gateways 423
Security Operations Center-as-a-Service (SOCaaS) 423
General 425
Settings 426
Audit Logs Export 426
Contract Sharing Mode 428
API Key 428
Asset Groups 429
Audit Logs 431
Contracts 433
Usage 436
Contract-based usage 436
Points-based usage 438
Reports 440
Notifications 441

Organization 445
FortiCloud IAM 445
FortiCloud Organizational Units 453
Best Practices 456
Compliance 456
WAF Best practices 459
Support 463
FAQs 465
General 465
Overview 465
FortiAppSec contracts 467
Notifications and Communication 470
Miscellaneous 471
WAF FAQ 472
Application Onboarding 472
Network 474
Usage 478
Miscellaneous 478
ABP FAQ 479
Onboarding 480
Integration (deployment mode) 480
Miscellaneous 481
GSLB FAQ 481
GSLB and DNS Services 482
Health check 484
One-click GSLB 485
DevOps 486
Synthetic testing 486
Miscellaneous 488
Threat Analytics FAQ 488
Onboarding 488
Log Management 489
Migration 491
Migrating from preceding Fortinet services 493

What's New

25.4.a released December 11, 2025

FortiAI Assistant Audit Logs Support

FortiAI Assistant now supports analyzing Audit Logs through natural language queries.

For more information, please refer to FortiAI Assistant.

Region IP Update

Additional scrubbing centers have deployed in the following regions. Please make sure to allow access to your application from the IP addresses listed below.

AWS me-central-1: Middle East (Abu Dhabi)

- 51.112.103.160
  2406:da17:467:6301:dd8e:37a:ecc0:6c27
- 3.29.150.238
  2406:da17:467:6301:8238:4a75:d770:efba
- 40.172.37.225
  2406:da17:467:6301:5574:fa67:6b36:bf01
- 40.172.219.217
  2406:da17:467:6302:bc1c:6849:e592:f869
- 51.112.133.247
  2406:da17:467:6302:cf79:1143:c4f7:eabc
- 158.252.80.239
  2406:da17:467:6302:f2d1:d1ec:4e63:b14b

GCP me-central2: Middle East (Dammam)

- 34.166.213.46
- 34.166.73.8
- 34.166.152.210
- 34.166.140.221
- 34.166.234.73
- 34.166.152.78

Client-Side Protection

The Client-Side Protection feature is currently on hold for a future release.

WAF

Customized Waiting Room Page

Waiting Room pages are now customizable. Configure this under **WAF > System Settings > Custom Pages**.

For more information, please refer to Custom Pages.

Trusted IP Enhancements

A new link on the IP List page has been added allowing to quickly review existing blocked IPs when setting up IP rules. From there, you can manually unblock any IPs if required.

For more information, please refer to IP Protection.

Exceptions for ML Based Bot Detection

ML Based Bot Detection now supports adding **Exceptions** for more granular control.

For more information, please refer to ML Based Bot Detection.

Geo IP Filtering in Custom Rules

Custom Rule now supports Geo IP filtering for precise, location-based traffic control.

For more information, please refer to Custom Rule.

GSLB

DNS Traffic Logs

DNS traffic logs are now available, providing enhanced visibility and a more complete analytics dashboard for GSLB.

Administrators can set the log storage region (US or EU) at both the FQDN and DNS Service levels. Existing FQDNs and DNS Services default to the EU region. To switch storage to the US, follow the configuration steps under FQDN or DNS Service.

GSLB Interface Enhancements

The GSLB dashboard now displays DNS traffic log data, with new FortiView pages to display detailed **FQDN**, **Zone**, and **Resource** analytics.

For more information, please refer to GSLB FortiView.

Advanced Bot Protection

SSL Certificate Verification

When adding or editing **Entry Points**, enabling **SSL Certificate Verification** ensures that the server's SSL certificate is validated when Auto Discovery connects to the Entry Point.

This option is enabled by default. Disable it only when using self-signed or staging/test certificates that are not trusted by standard browsers.

For more information, please refer to Onboarding ABP Applications.

25.4 released November 6, 2025

FortiAI Assistant Enhancements

The FortiAI Assistant now supports analyzing Threat Analytics Incidents and Attack Logs from on-premises devices. enable directly from the log by clicking Analyze with AI, or by clicking the FortiAI icon in the top-right corner of the page.

For more information, please refer to FortiAI Assistant.

New 30-day License Upgrade Trial

If you have an active license, you can now explore more advanced features available in other FortiAppSec Cloud Plans with a free 30-day upgrade trial.

To enable, please contact Fortinet Sales.

Contract and Usage Status Alert

The **Home** page now displays alerts for contract and usage updates, such as license expirations, overages, and other critical notices.

Scheduled System Upgrade Notifications

FortiAppSec Cloud now displays banners notifying users of upcoming system upgrades and maintenance windows, improving visibility of potential feature unavailability and service delays.

WAF

Role-based Permissions Granularity Enhancement

To provide additional granularity for role-based access control, the **WAF- Application** permission profile in **FortiCloud** is now divided into **WAF- Application Management**, **WAF- Application Networking**, and **WAF- Application Security**. This allows for more precise control over permissions in the **WAF** module. For more details, please refer to the FortiAppSec Cloud User Guide.

For details on how this affects your applications, please refer to FortiCloud IAM.

API Gateway Template backend enhancements

The API Gateway feature has been restructured to improve security and fix permission issues.

Changing an API Gateway's template inheritance now automatically regenerates API keys. Replace any existing keys in use with the new ones to avoid service interruptions.

For more information, please refer to API Gateways.

GSLB

New outbound connections IP address

If you have connected a FortiGate server to a FortiAppSec Cloud GSLB application, you have received an email from **no-reply-appsec@fortinet.com** requesting you to update your allowlist.

To ensure uninterrupted connectivity, update your configuration to redirect all outbound connections to 44.241.230.143。

Backend enhancements

GSLB now provides improved Security Fabric connectivity.

Advanced Bot Protection

New self-service onboarding Capability

To improve efficiency, a new Advanced Bot Protection self-service Auto-Discovery capability has been added to replace manual Pre-Provisioning in application onboarding.

For details on the new concepts introduced in the onboarding system and configuration instructions, refer to Creating ABP Applications.

25.3.b released September 25, 2025

Audit Log Notifications

Stay informed with email alerts for important log events.

Go to **General > Notification** and enable Notification Emails to receive alerts based on your configured criteria.

For more information, please refer to Notifications.

Removed Support for OCI Platform

FortiAppSec Cloud no longer supports the OCI platform. All WAF scrubbing centers operating on OCI have been permanently removed.

If you have any questions or need assistance, please contact **Support** by submitting a support ticket.

WAF

Application Diagnostics Agent

Get AI-powered insights into application connectivity and troubleshooting.

Go to **WAF > Network > Diagnostics**, and activate FortiAI Assistant under Actions.

For more information, please refer to Diagnostics.

Client Certificate security enhancements

Strengthen authentication security by enabling **Client Certificate Authentication** to verify connecting clients. Once enabled, you can optionally activate:

- **Strictly Require Client Certificate**: only clients presenting a valid certificate are allowed.
- **Client Certificate Forwarding**: forward the certificate to your backend server for authentication, user-specific permissions, and access control.

For more information, please refer to Endpoints.

Origin Server Lock

Lock your origin server's IP to ensure it can only be used by your account. This prevents other FortiAppSec Cloud accounts from targeting your server with malicious traffic. To enable, go to **WAF > Applications**, edit the desired server pool, and turn on Lock Server.

For more information, please refer to WAF Applications.

Threat Analytics

Centralized Log Export Configuration

You can now configure attack log export servers globally under **Threat Analytics > Settings**, rather than per application. This allows multiple applications to share the same export server configuration, reducing repetitive setup and improving export efficiency.

For more information, please refer to Threat Analytics Settings.

Attack Logs Signature Exceptions

Allow events when specific values match criteria such as **Request Host**, **Request URL**, **Parameter Name and Value**, **Cookie Name**, or **JSON Element Name and Value**.

Navigate to **Threat Analytics > Attack Log**, select the desired event, and click **Add Exception**.

For more information, please refer to Attack Logs.

Exception Rules Support Matching by Request Host

Exception Rules under Known Attacks, Information Leakage, and Attack Logs now support matching by **Request Host**, providing greater flexibility when defining exceptions.

Blocked Status Tag in Attack Logs

Attack logs now display a **Blocked** tag under **Client Information** when a source IP is blocked for a period of time.
You can hover over the tag to view the block duration and reason, or click **Unblock** to unblock the IP directly.

For more information, please refer to Attack Logs.

25.3.a released August 28, 2025

WAF

GEO IP Allow list

Under **WAF > Access Rules > IP Protection**, you can now also allow traffic based on specific countries for finer geo-based access control.

For more information, please refer to IP Protection.

Advanced Bot Protection

Backend Enhancements

Advanced Bot Protection now provides improved detection and defense against naive bots.

25.3 released July 31, 2025

FortiAI Chatbot

FortiAppSec Cloud is now integrated with FortiAI, Fortinet's advanced artificial intelligence platform that enhances cybersecurity and network operations across the Fortinet Security Fabric. FortiAI uses generative AI (GenAI), machine learning, and automation to help security and network teams respond faster and more effectively.

You can ask the FortiAI chatbot questions by clicking its icon in the top right corner.

For more information, please refer to FortiAI Assistant on page 54

Asset Groups

You can now manage role-based permissions at a more granular, application-specific level and assign user access permissions at the application level. To access this page, go to **General > Settings** and enable **Asset Groups**.

For more information, please refer to Asset Groups on page 429.

In-Portal Public Marketplace license downgrade

You can now downgrade your FortiAppSec Cloud subscription plan to reduce supported features and contract capacity directly through the FortiAppSec portal.

For more information, please refer to Contracts on page 433.

WAF

Support for HTTP Header Insertion and Removal in Server Responses

You can now configure HTTP header insertion and removal for server response types under URL Rewriting.

For more information, please refer to Rewriting Requests on page 193.

Support for HTTP Header Referrer Policy

You can now control how much referrer information is shared in HTTP requests by enabling the **Referrer-Policy** option and selecting your desired policy value.

For more information, please refer to HTTP Header Security on page 146.

Support for Content Routing Based on Client Certificate X509

When configuring Content Routing, you can now set the match object to **X509 Certificate subject** and **X509 Certificate extension** fields.

For more information, please refer to Content Routing on page 110.

GSLB

DNS Validation

You can now check the DNS Status to view the resolution status of configured FQDNs. This helps identify DNS issues and assists with proper DNS zone configuration.

For more information, please refer to FQDN on page 338.

Geolocation Enhancements with EDNS Client Subnet (ECS)

GSLB now supports EDNS Client Subnet (ECS), enabling more accurate client geolocation during DNS resolution. With ECS enabled, the authoritative DNS server can consider the client's subnet when making load-balancing decisions. This improves DNS-based traffic steering, especially for users behind public DNS resolvers, by routing them to the nearest or most optimal data center based on their actual location.

DNS Security Improvements

The DNS Security feature has been enhanced to protect against a wide range of potential attacks, including denial-of-service (DoS), cache poisoning, and memory corruption exploits. This also includes detection and mitigation of malformed queries, such as those with invalid label lengths or malformed headers.

25.2.a released June 26, 2025

WAF

SOCaaS Integration

You can now enable Security Operations Center-as-a-Service (SOCaaS) for your WAF applications by clicking the **Enable SOCaaS** button on the **WAF > System Settings > Settings** page. This opens the SOCaaS portal to complete onboarding. SOCaaS is available for customers with the **Enterprise** bundle or customers that purchased the SOCaaS SKU.

Once onboarding is successful, you should see the updated SOCaaS status on the same **Settings** page.

For more information, please refer to WAF Settings on page 204

GSLB

Enhanced Diagnostics for GSLB Topology (VS/HC) and Fabric Connectors

You can now run diagnostics on Virtual Servers, Fabric Connectors, and Health Checks directly from the GSLB Topology view by selecting the item and clicking **Diagnose**. This provides quick visibility into connection and health check issues.

For more information, please refer to Topology on page 334.

25.2 released June 3, 2025

Contract and License Update

FortiAppSec Cloud has expanded supported contract and license offerings, and restructured license offerings for some products.

Enterprise Plan Support

FortiAppSec Cloud introduces the Enterprise plan, an all-inclusive annual subscription that bundles Advanced WAF features, Advanced Bot Protection, DAST, and GSLB services into one plan. Pricing is simplified to a predictable bandwidth-only model.

For more information, please refer to License & Contract.

AWS, Azure, and GCP Marketplace License Support

You can now purchase and manage FortiAppSec Cloud contracts through AWS, Azure, and GCP marketplaces.

For more information on the new license options, please refer to Public Cloud Marketplace subscriptions.

If you are looking to transfer a legacy FortiWeb Cloud Marketplace License to the FortiAppSec Cloud AWS, Azure, or GCP license, please refer to Migrating from existing Fortinet services.

FortiFlex License Support

FortiAppSec Cloud now supports FortiFlex, a flexible, usage-based security licensing program from Fortinet that allows organizations to provision FortiAppSec Cloud on-demand, paying only for what you consume. It eliminates the need for pre-planning, over-provisioning, or under-provisioning, offering a simplified and flexible licensing model.

For more information on this new license option, please refer to FortiFlex on page 32.

If you are looking to transfer a legacy FortiFlex entitlement to the FortiAppSec Cloud Fortiflex entitlement, please refer to Migrating from existing Fortinet services.

Advanced Bot Protection and DAST Contract Model Update

Dynamic Application Security Testing (DAST) and Advanced Bot Protection (ABP) are now included in the Advanced and Enterprise subscription plans respectively. These services are no longer available as standalone contracts. For more information, please refer to License & Contract.

GSLB

DNSSEC Enhancement

The DNSSEC feature in GSLB been enhanced with advanced cryptographic algorithms, providing stronger protection against DNS spoofing and related threats.

For more information on how to enable this feature, please refer to How to enable DNSSEC on GSLB.

Multi-Region Health Check Support

FortiAppSec Cloud GSLB now supports health checks from additional areas: **Europe** and **Asia Pacific**, alongside the existing **North America** option.

When configuring a health check, you can select its **area** of origin. Multiple health checks from different areas can be assigned to the same virtual server. GSLB aggregates results from all selected areas to determine server health, improving the accuracy of global availability monitoring.

For the list of IP addresses to add to your application's allowlist, please refer to Health check on page 373.

Enhanced Server Status Descriptions

When a server or virtual server is marked as down, the web portal now displays the specific reason.

Hovering over the **server status** icons on the Topology and FQDN pages reveals detailed messages with clear diagnostic information.

AWS Connector Load Balancing Support

GSLB now supports load balancing with AWS connectors using CNAME record types and single-record responses. This enhancement enables AWS-based applications to participate in traffic distribution. Only CNAME records are supported when using AWS connectors.

For more information, please refer to Fabric connectors with AWS and Azure.

Topology Page Filtering

The Topology page now includes a **filter** option, allowing you to quickly locate specific servers or virtual servers by name or status.

Advanced Bot Protection

FortiWeb Version Requirement Update

Advanced Bot Protection integration with FortiWeb now requires FortiWeb version 7.4.8 or later for continued compatibility.

25.1.a released March 27, 2025

Bug Fixes

This release fixes several bugs for improved stability and experience.

25.1 released February 27, 2025

WAF

Enhanced Known Attacks

Known Attacks has been enhanced with Extended Mode. This adds additional signatures to every Sensitivity Level but should be used with caution as it may result in higher false positive rates. For more information, please see Known Attacks.

Bot Mitigation Exception Policies

Exceptions (whitelisting) are now supported for Bot mitigation policies. Build granular exceptions based on elements such as client IPs, hostnames and URLs. For more information, please see Exception Policy.

Cloud Deployment Granularity

Application onboarding now allows choosing the Cloud platform and region during WAF onboarding. For more information, please refer to Onboard WAF applications on page 65.

View Server Health Check Status on Applications Page

You can now view the status of all origin servers for an application under the **Health Check** column on the **WAF > Applications** page. For more information, please refer to WAF Applications on page 86.

Log Format for Attack Logs

Attack Logs now support the **Template Name** and **Destination IP** field when **Log Format** is set to **Custom**. For more information on **Attack Log Server** options, please refer to Log Settings on page 120.

Splunk URL change

The **FortiAppSec Cloud Splunk Add-On** has been updated with new URLs. For more information, please refer to Using WAF with Splunk on page 225.

Region IP Update

Additional scrubbing centers have deployed in the following regions. Please make sure to allow access to your application from the IP addresses listed below.

- AWS ap-southeast-3: Asia Pacific (Jakarta)
  - 16.78.99.255
    2406:da19:4a2:1f01:4bfd:3d35:eeea:9960
  - 16.78.217.33
    2406:da19:4a2:1f02:f4ff:d71d:bc20:34fe
  - 16.78.170.51
    2406:da19:4a2:1f01:a2d8:6f29:242:b8d3
  - 43.218.33.190
    2406:da19:4a2:1f02:621a:ed16:4cea:df5d
  - 16.78.206.248
    2406:da19:4a2:1f01:4e37:3198:afa2:103f
  - 108.137.179.56
    2406:da19:4a2:1f02:e03c:7d81:aa91:7c29
- Azure South Africa North (Johannesburg)
  - 4.221.199.162
  - 4.221.192.56
  - 4.221.113.144
  - 4.222.21.210
  - 4.222.18.196
  - 4.222.21.170
  - 10.40.1.10
  - 4.221.143.107

Advanced Bot Protection

Web Portal Improvements

Several pages under **Advanced Bot Protection > [Application name] > Traffic Insights** have been enhanced with additional graphs and navigation elements. For more information on the updated pages, please see Dashboard on page 291, Transactions on page 295, Bot Monitor on page 302, and Exploration on page 305.

Attack Query Enhancement

The web portal now includes a page with historical charts and statistics for Attack Query insights. For more information, please refer to Attack Query on page 298.

GSLB

Support DNS CAA Record in GSLB

GSLB now supports Certificate Authority Authorization (CAA) records, enabling administrators to specify authorized CAs for their domains. This ensures secure and compliant certificate issuance while maintaining GSLB's high availability and performance. For more information, please refer to DNS service on page 358.

24.4.p1 released on January 9, 2024

Bug Fixes

This release fixes several bugs for improved stability and experience.

Overview

FortiAppSec Cloud provides an all-in-one dashboard for accessing the following four subservices:

- **Web Application Firewall (WAF)**

  Protects public cloud hosted web applications from the OWASP Top 10, zero day threats, and sophisticated Layer 7 attacks with adaptive security policies and real-time threat intelligence. It also integrates FortiDAST's web vulnerability scanner (WVS) in its Vulnerability Scan feature.
- **Advanced Bot Protection**

  Detects and mitigates malicious automated traffic, preventing attacks such as bot-driven scraping, credential stuffing, account takeovers, and API abuse through behavioral analysis and machine learning.
- **Global Server Load Balancer (GSLB)**

  Enhances application availability and resilience by distributing traffic across multiple data centers or cloud environments, reducing latency and ensuring business continuity.
- **Threat Analytics**

  Leverages AI-powered analytics to correlate security events across your application stack, filtering out false positives and highlighting critical incidents that require immediate attention.

Getting Started

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

- License & Contract on page 21
- Onboarding on page 50

License & Contract

- FortiAppSec Cloud contract options on page 22
  - Annual contract or pay-as-you-go on page 22
  - Where to purchase FortiAppSec Cloud contracts on page 22
  - Contract comparison table on page 23
  - Standard, Advanced, and Enterprise plans on page 25
- View contract on page 28
- Renew contract on page 29
- Overage and expiration behavior on page 29
- License Upgrade Trial on page 30

FortiAppSec Cloud offers several licensing options. Review the information below to determine the most suitable contract type for you.



If you are using a legacy FortiWeb Cloud/ FortiGSLB/ FortiABP contract, you will be required to transition fully to a FortiAppSec Cloud contract to continue service past its expiry date. For information on the transition, please refer to Contract Migration on page 495.



Only one primary contract type can be active at a time within a single account. While a contract type is active, any other contract types remain inactive and cannot be used.

An inactive contract's specified seat quantity is not available and does not count toward the total number of available seats.

Gateway licenses are not subject to this restriction.

FortiAppSec Cloud contract options

Annual contract or pay-as-you-go

Annual contracts:

- Billing: Single upfront charge for agreed-upon usage.
  - With a Fortinet Contract, bandwidth and application can be purchased under separate contracts.
  - With Marketplace (AWS/Azure), you pre-pay for a set number of usage points (for example, 10,000). Any usage beyond this is billed as overage.
- Cost: More cost-effective for consistent, long-term usage. Discounts may apply for multi-year terms (24 or 36 months).
- Renewal: Service access expires if the contract is not renewed.
- Enterprise Support: Supported for all annual contract types.

Pay-as-you-go:

- Billing: Monthly charges based on actual usage, ideal for variable workloads.



Some services have a minimum billable usage, regardless of actual traffic.

For example, if a WAF application is deployed, a minimum of 25 Mbps per day of WAF bandwidth will be billed, even if the application receives no traffic.

- Cost: Flexible, no upfront commitment.
- Enterprise Support: Supported through FortiFlex, but not available on public marketplaces (AWS, Azure, GCP).

For more information, please see the Contract comparison table on page 23.

Where to purchase FortiAppSec Cloud contracts

FortiAppSec Cloud contracts are available through three different purchasing avenues.

- **Fortinet Sales** offers contracts priced based on bandwidth usage, with the following features available to different tiers: Web Application Firewall (WAF), bandwidth management, Dynamic Application Security Testing (DAST), Global Server Load Balancing (GSLB) with query-per-second (QPS) limits and health checks, Advanced Bot Protection (ABP), and Security Operations Center (SOC) services.
  - WAF: Requires both an Application contract and a Bandwidth contract. The number of applications and bandwidth limits are fixed at purchase.

    Plan tiers cannot be mixed. For example, if you register a Standard plan for Application and an Advanced plan for Bandwidth, both contracts will be invalid.
  - GSLB: Can be purchased as a standalone contract or together with other services.
  - ABP: Available in the Enterprise contract tier

  To purchase a new contract or make changes to an existing one, contact Fortinet Sales.
- **FortiFlex** offers a pay-as-you-go billing model where FortiFlex points are consumed based on your usage.

To purchase a new contract that includes FortiFlex points, contact Fortinet Sales. To manage changes to an existing account, log into the FortiFlex portal.

- **AWS/Azure/GCP Marketplace** offers tailored subscriptions for AWS, Azure, and Google Cloud Platform, including usage-based pricing, contract-based pricing, and contracts with consumption-based billing.

  New contracts can be purchased by logging into the portals for AWS, Azure, or Google Cloud Platform. To upgrade or downgrade your existing plan, navigate to the General > Contracts page

Contract comparison table

The following table lists the FortiAppSec Cloud contracts available for purchase. Usage limits vary by contract.

For additional details on the supported features of the Standard, Advanced, and Enterprise plans, please see Standard, Advanced, and Enterprise plans on page 25

Payment type	Contract type	Plan	Support
Annual Contract	Fortinet Contract	Standard	Included: • WAF Add-on options: • SOCaaS
		Advanced	Included: • WAF • DAST Add-on options: • SOCaaS
		Enterprise	Included: • WAF • DAST • GSLB • ABP • SOCaaS
	AWS Annual contract	Standard	Included: • WAF • GSLB
		Advanced	Included: • WAF • GSLB • DAST
		Enterprise	Included: • WAF • GSLB • DAST • ABP

Payment type	Contract type	Plan	Support
			Please note, SOCaaS is not supported as an add-on.
	Azure Annual Contract	Standard	Included: • WAF • GSLB
		Advanced	Included: • WAF • GSLB • DAST
		Enterprise	Included: • WAF • GSLB • DAST • ABP Please note, SOCaaS is not supported as an add-on.
Pay-As-You-Go	FortiFlex	Standard	Included: • WAF Add-on options: • SOCaaS • GSLB
		Advanced	Included: • WAF Add-on options: • SOCaaS • GSLB
		Enterprise	Included: • WAF • DAST • GSLB • ABP • SOCaaS
	AWS/ Azure/ GCP Pay-As-You-Go (PAYG)	Standard	Included: • WAF • GSLB
		Advanced	Included: • WAF • GSLB

Payment type	Contract type	Plan	Support
			• DAST

Standard, Advanced, and Enterprise plans

FortiAppSec Cloud contracts are available in 3 tiers:

- **Standard**: Focuses on core protections, including negative security model policies, default configurations such as signatures, request limits, and more.
- **Advanced**: Includes all features of the **Standard** plan and adds advanced capabilities, such as machine learning for web/API/bot protection, Threat Analytics, and additional security enhancements.
- **Enterprise:** Includes all features of the **Advanced** plan, and also bundles services that are billed separately in the **Standard** and **Advanced** plans, such as Advanced Bot Protection, GSLB, and SOCaaS.
  - Each GSLB application includes a lifetime allocation of 10 GSLB health checks (HC).
  - For every 5 Mbps of licensed bandwidth, the system allows a monthly average of up to 20 queries per second (QPS).

Review plan feature differences here:

Feature Category	Standard	Advanced	Enterprise
Web Application Protection			
Signature based Protection	✓	✓	✓
IP Threat Intelligence	✓	✓	✓
GEO-IP Intelligence	✓	✓	✓
Custom Security Rules	✓	✓	✓
HTTP Compliance	✓	✓	✓
URL, Parameter and CORS Protection	✓	✓	✓
Cookie Protection	✓	✓	✓
Information Leakage	✓	✓	✓
AV for File Uploads	✓	✓	✓
Sandboxing for File Uploads		✓	✓

Feature Category	Standard	Advanced	Enterprise
Zero Day Attack Protection - Machine Learning based Anomaly Detection		✓	✓
API Security			
Schema Enforcement (OpenAPI, XML, JSON)	✓	✓	✓
API Gateway		✓	✓
Mobile API Protection		✓	✓
Machine Learning based - Discovery, PII Catalog, Protection		✓	✓
Client Security			
HTTP Header Protection	✓	✓	✓
CSRF and MiTB Protection	✓	✓	✓
Bot Defense			
Signature, Threshold, Biometric and Deception	✓	✓	✓
Machine Learning based Bot Defense		✓	✓
Advanced Bot Protection			✓
Account Takeover			
User Tracking		✓	✓
Session Fixation Protection		✓	✓
Credential Stuffing Defense		✓	✓
DDoS			
Layer 3-4 DDoS Mitigation	✓	✓	✓

Feature Category	Standard	Advanced	Enterprise
Layer 7 DDoS Mitigation	✓	✓	✓
Application Delivery			
SSL Certificates - Automatic and Custom	✓	✓	✓
Client Authentication / Mutual TLS		✓	✓
Content Delivery Network (CDN)	✓	✓	✓
Limited GEO CDN	✓	✓	✓
Load Balancing and Server Health Monitoring	✓	✓	✓
Origin Server Content Routing		✓	✓
Waiting Room		✓	✓
Global Server Load Balancing (GSLB)			
DNS Load Balancing	Available Separately	Available Separately	✓
DNS Services + DNSSEC	Available Separately	Available Separately	✓
Health Check (Synthetic Testing)	Available Separately	Available Separately	✓
DAST Scanning			
Vulnerability Assessment		✓	✓
API Scanning		✓	✓
Reporting and Analytics			
Attack Logs	✓	✓	✓
Alert Notifications	✓	✓	✓
SIEM Integration	✓	✓	✓

Feature Category	Standard	Advanced	Enterprise
Log Sensitive Data Masking	✓	✓	✓
FortiView - Realtime and historical log Analysis	✓	✓	✓
Security and Network Dashboards and Reports	✓	✓	✓
Traffic Logs (Cloud native storage integration)		✓	✓
Threat Analytics AI		✓	✓
Management			
Role Based Access Control	✓	✓	✓
Single-Sign-On Support	✓	✓	✓
API Support	✓	✓	✓
Services			
24/7 Support	✓	✓	✓
SOCaaS - log monitoring, incident triage and SOC escalation service	Available Separately	Available Separately	✓ *Available with Fortinet and FortiFlex contracts. Not available via marketplace subscriptions.

View contract

To view your contract type for an active service, log into the FortiAppSec Cloud web portal and go to **General > Contracts**.

For details on what you can do on this page, please see Contracts on page 433

Renew contract



If you have an active contract, your new contract will automatically begin when your existing contract ends.

If you need to increase the number of applications, bandwidth, or seats before your current contract ends, please upgrade your contract. For detailed instructions specific to your contract type, see Contracts.

To renew your annual contract, purchase a new FortiAppSec Cloud license by contacting your Fortinet sales representative directly or from your public cloud marketplace platform (AWS or Azure).

For service continuity and correct licensing, ensure to register the new FortiAppSec Cloud contract under the same Fortinet (FortiCloud/FortiCare) account as your existing service.

Overage and expiration behavior

FortiAppSec Cloud may enter read-only mode due to contract violation or expiration. If your license has expired or your usage exceeds the license contract, please buy or upgrade your existing contract immediately.

- **Bandwidth Overage**

  If your bandwidth usage exceeds your quota limits for two consecutive months, your account will enter **read-only** mode.

  To regain full access:

  - *Register a new or upgraded license*

    Contact your sales representative to adjust the quantity on your existing contract.

    The 95th percentile bandwidth quota resets on the 1st of each month. When the new cycle begins, access will automatically be restored as long as your usage remains within quota for that cycle. Because read-only mode limits service functionality, we do not recommend waiting for the next billing cycle in place of increasing your bandwidth limit. Consider it only if you are very close to the start of the next cycle and do not expect to exceed your bandwidth quota again.

- **Application Overage**

  If you have more applications than is supported by your contract, your account will enter **read-only** mode.

  To regain full access:

  - *Increase your application limit*

    Contact your sales representative to adjust the quantity on your existing contract.
  - *Decrease number of applications*

    Delete applications until the number of applications falls under your contract quota.
- **Expired Contract**

  When your contract expires, your account enters a 21-day grace period during which it remains in **read-only** mode.

  To regain full access:

  - *Purchase additional contracts*

    You can purchase additional FortiAppSec Cloud contracts through any supported platform.

- *Extend expiration date*

  Contact your sales representative to extend your current contract.

Once the 21 day grace period ends, your applications will be deleted from your FortiAppSec Cloud account.

If the license is managed via FortiFlex, a 7-day FortiFlex grace period begins first. The entitlement may show as “Expired” but remains active during this time. The 7-day FortiAppSec Cloud grace period starts after the FortiFlex period ends.

Changing license types (e.g., from legacy FortiWeb Cloud to FortiAppSec UC contract) may result in a change to the serial number.

License Upgrade Trial

If you have an active Fortinet Contract, you can now explore more advanced features available in other FortiAppSec Cloud Plans with a free 30-day trial. To enable, contact Fortinet Sales.

The trial license operates independently from your existing FortiAppSec Cloud contract.

Once activated:

- Any changes made to your original contract license will not affect the trial license.
- Any updates to the trial license itself (for example, changing plans or the number of seats) must be requested through Fortinet Sales, and require Product Management approval before changes are applied.

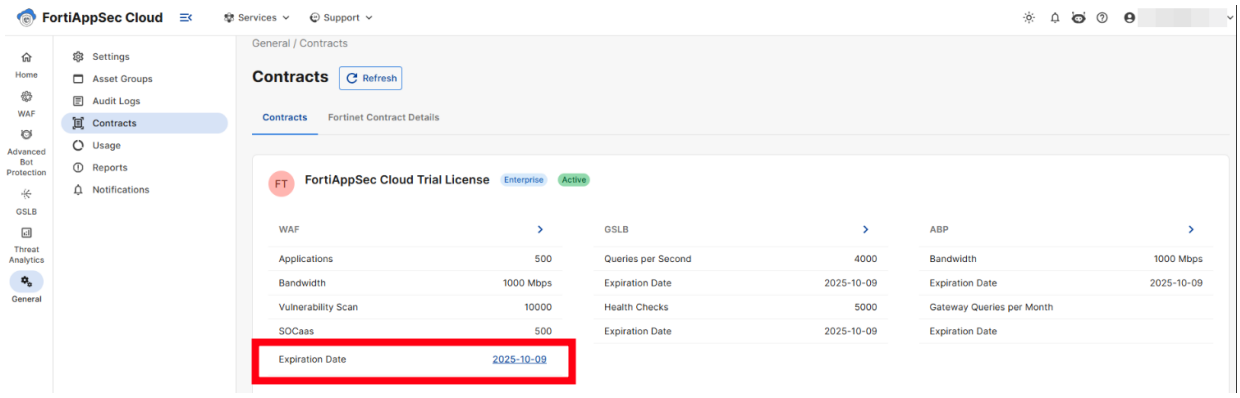
Service Impact on Plan Downgrade

When the trial expires, your license enters a 7-day grace period. After the grace period ends, the system automatically reverts to your original contract license.

If this involves a plan downgrade (for example, from Enterprise to Standard), certain modules may be disabled automatically.

For instance, features such as Content Routing may stop functioning after downgrade, which can result in service interruption.

You can check your trial license **expiration date** on the **General > Contracts** page.



Fortinet Contracts

Fortinet Sales offers a range of licenses, each priced based on the maximum bandwidth limit, with varying features and pricing structures across the different tiers.

Licenses are available in Standard, Advanced, and Enterprise plans. For full details on the differences between the various plans, please refer to Standard, Advanced, and Enterprise plans on page 25

- Bandwidth Calculation on page 31
- Purchasing and Activating FortiAppSec Cloud contracts on page 31

Bandwidth Calculation

Each account is measured using a burstable model for bandwidth calculation, which is based on the 95th percentile of clean traffic usage.

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 top 5% of buckets with the highest Mbps are discarded. The highest Mbps rate from the remaining buckets represents the 95th percentile value for the account.

At the beginning of each month, the 95th percentile bandwidth displayed in FortiWeb Cloud may appear very low, or even as 0. This is because not enough 5-minute data intervals (buckets) have been collected to calculate an accurate value. As more buckets are generated throughout the month, the value becomes more accurate.

Purchasing and Activating FortiAppSec Cloud contracts

To purchase a FortiAppSec Cloud Contract from Fortinet, please contact our sales team.

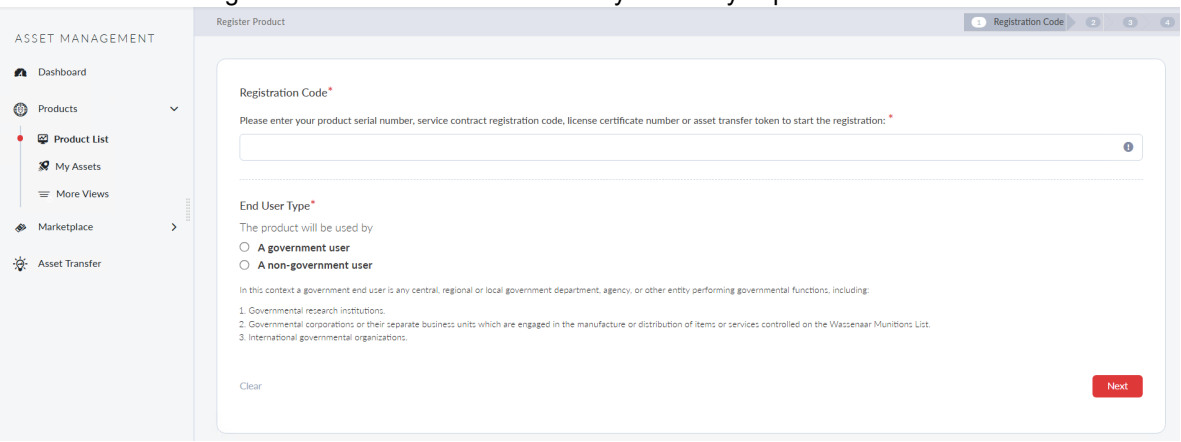


Please note that the Standard and Advanced plans require separate licenses for applications and bandwidth. These licenses respectively determine how many applications you can add to your account and the maximum bandwidth allowed. **Both licenses are required to activate the service contract.**

Once you receive your contract registration codes, activate your service by doing the following:

1. Create a FortiCloud account. It can be used to log in to all Fortinet products. Skip this step if you already have an account.
2. Log in to Fortinet Support.
3. Register a new product. You can do this from the **Asset Management Dashboard** page, or navigate to **Products > Product List** and click **Register More**.

4. Enter the contract registration code that was emailed to you when you purchased the contract.



5. Select the **End User Type**. Click **Next**.
6. 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**.
7. Read *Fortinet Product Registration Agreement*. Check the box if you agree. Click **Next**.
8. Carefully review the verification page. Once you are done, check the box to acknowledge the activation of the contract. Please note, the **activation date cannot be changed** once you confirm.
9. Click **Confirm**.
10. Repeat the registration steps if you have multiple contracts.
11. Log in to FortiAppSec Cloud with your FortiCloud account.
12. The contract information will be displayed in **General > Contracts**.



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

FortiFlex

FortiAppSec Cloud now supports FortiFlex, a flexible contract management system that lets you purchase points and apply them to specific Application and Bandwidth needs, rather than being limited to fixed contract types.

These contracts are billed on a pay-as-you-go basis. Use the FortiFlex Calculator to estimate point consumption based on your projected usage parameters.

If you are looking to transfer a legacy FortiFlex entitlement to the FortiAppSec Cloud Fortiflex entitlement, please refer to Migrating from existing Fortinet services.

If you are purchasing a contract for an existing account, please use the same email address associated with that account when completing the purchase. This ensures the new contract is correctly linked to your existing FortiCloud account.

Flex Entitlement Rules

- Each account may create only one FortiAppSec Cloud Flex entitlement.
- A new entitlement must have an expiration date at least 90 days from the creation date.

- Entitlements cannot be stopped during the first 90 days.

Prerequisites

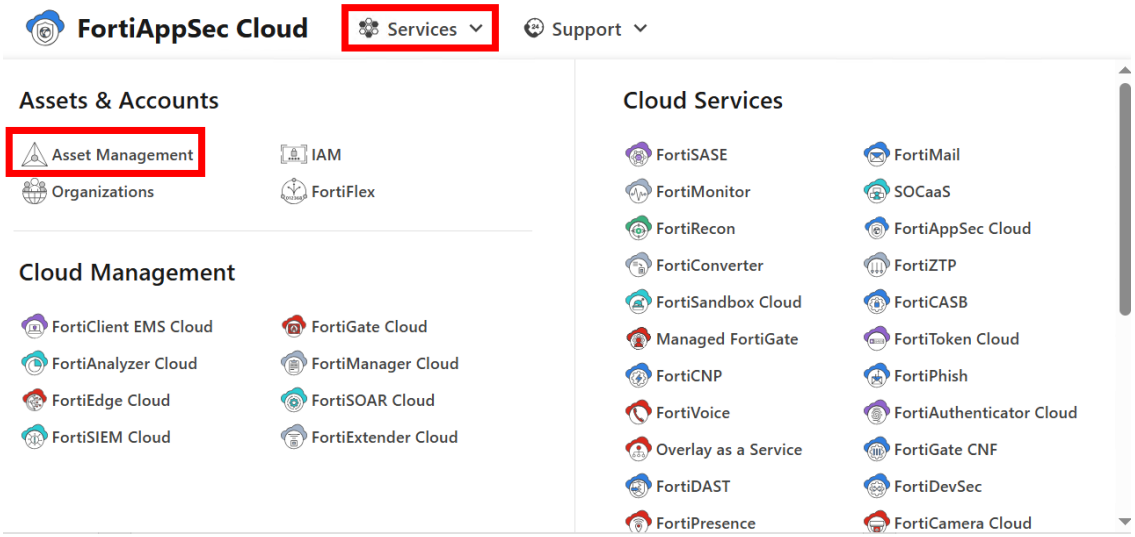
To use FortiFlex, you must have the following:

- 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.

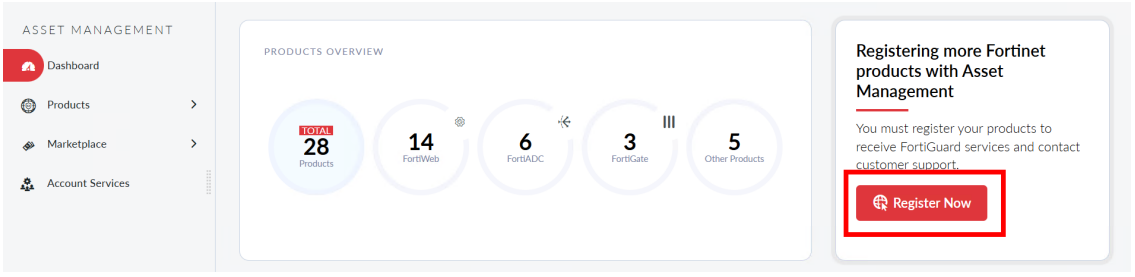
For more information, please see FortiFlex documentation on registration:
https://docs.fortinet.com/document/flex-vm/latest/administration-guide/791307/registering-fortiflex.

Register FortiAppSec Cloud with FortiFlex

1. Register FortiAppSec Cloud Product
   a. Log into either FortiAppSec Cloud or FortiCloud, and navigate to Asset Management from the **Services** menu in the top navigation bar.



   b. Register your FortiAppSec Cloud product by clicking **Register Now**.

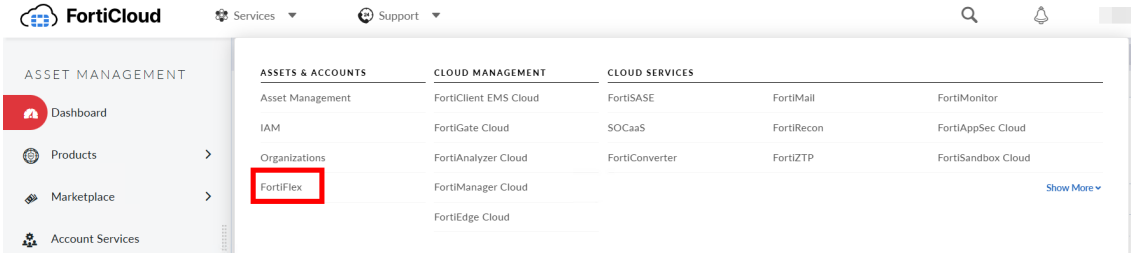


   c. Enter the **Registration Code** you received upon purchase of your FortiFlex License.
      - For **prepaid** programs, you must register an additional license to activate and allocate points.
      - For **postpaid (pay-as-you-go)** programs, only the initial license needs to be activated—no

additional point license registration is required.



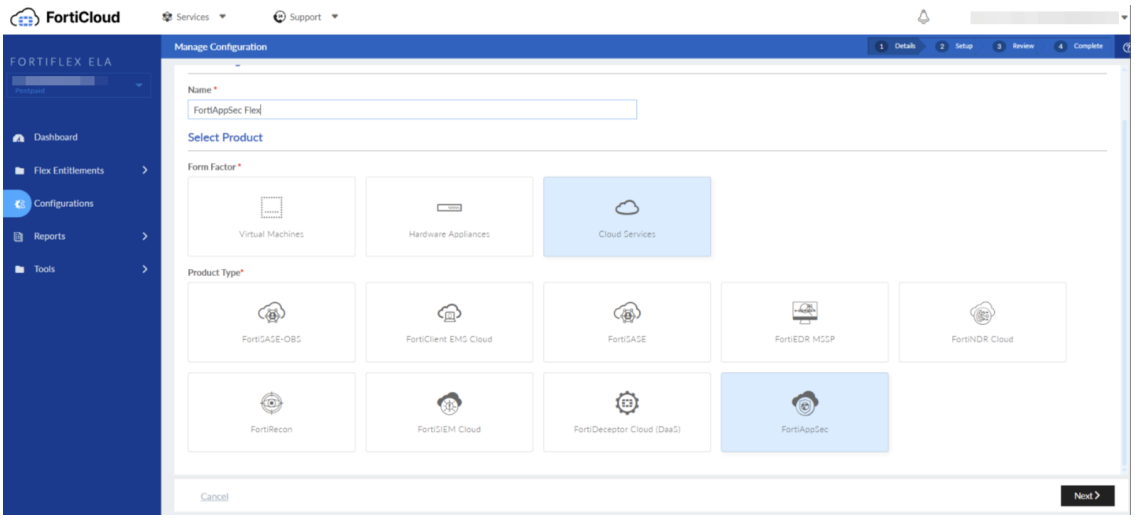
2. Add configuration in FortiFlex
   a. Navigate to **FortiFlex** from the **Services** menu in the top navigation bar.



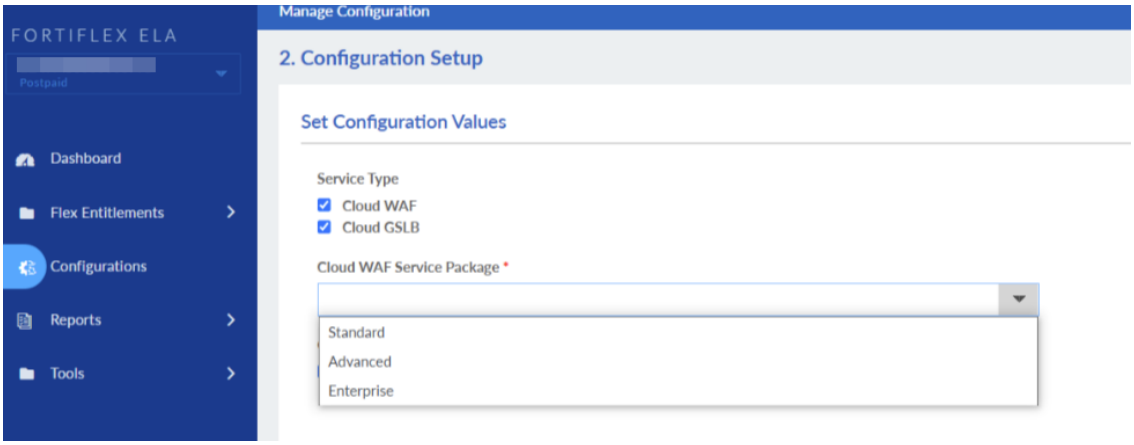
   b. Navigate to **Configurations**, and click **New Configuration**.

   Enter a name for your FortiAppSec Cloud FortiFlex service, and select **Cloud Services** and **FortiAppSec**.

   Click **Next** to continue.



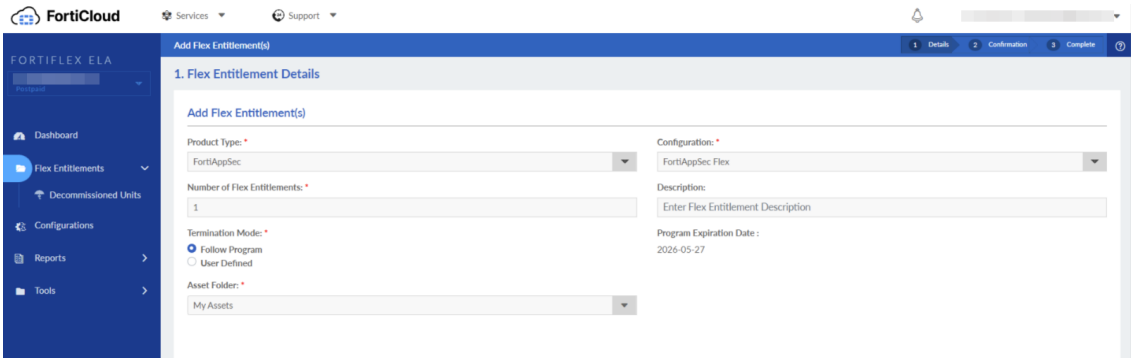
   c. Select your desired **Service Type**
      - If you select **Cloud WAF**, you must also choose the desired service package. For details on the differences between Standard, Advanced, and Enterprise, please refer to License & Contract on page 21.



d. Click **Next** to review changes, then **Submit** when you are ready.

3. Add **Flex Entitlement**

a. Navigate to **Flex Entitlements** and click **New Flex Entitlement**.



b. From the **Product Type** dropdown, select **FortiAppSec**.

c. From the **Configuration** dropdown, select the configuration you just created in step 2.

d. Set the **Program Expiration Date** to at least 90 days from today.

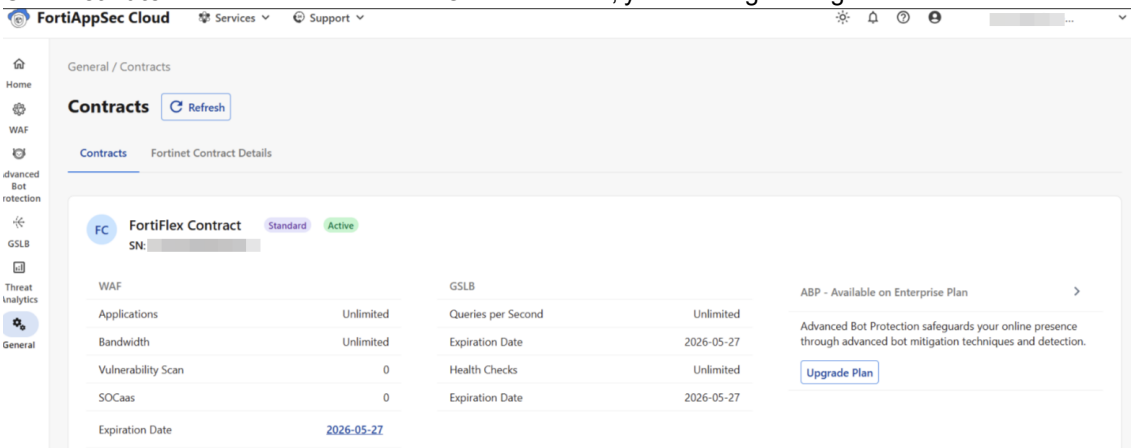
e. For more information on the other settings on this page, please refer to Creating Cloud service entitlements.

f. Click **Next** to review changes, then **Submit** when you are ready.

4. Activate Contract

a. Return to the FortiAppSec Cloud web portal, and navigate to **General > Contracts**.

b. Click **Activate** next to the new contract. Once activated, you can begin using the new service.



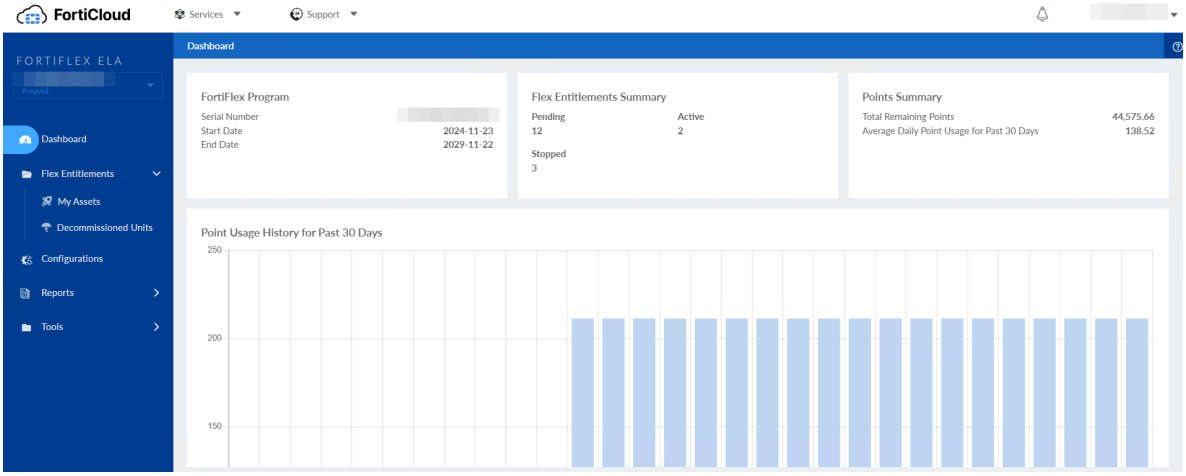
View FortiFlex points and Usage:

View in FortiAppSec Cloud:

1. Log into your FortiAppSec Cloud portal.
2. Navigate to **General** > **Usage**.

View in FortiCloud

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.



Usage Reporting

Usage data is updated daily and shown on the **General > Usage** page and in **FortiCloud**.

Bandwidth is measured daily using the 95th percentile.

Grace Period

When an entitlement transitions to the **Expired** state in FortiAppSec Cloud, a new 7-day grace period begins—regardless of whether a grace period was already used in FortiFlex.



During the FortiFlex grace period, an entitlement may display as **Expired** but still remain active. Once the FortiFlex grace period ends, the entitlement is considered fully expired, and FortiAppSec Cloud's 7-day grace period begins.

For full details on FortiFlex grace period behavior, see the FortiFlex documentation.

Public Cloud Marketplace subscriptions

FortiAppSec Cloud offers a 30-day free trial, with bandwidth limits on public cloud platforms. After the trial, continue usage by subscribing on the public cloud marketplace platforms or purchasing service contracts from Fortinet.

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

Regardless of the subscription channel, you can use FortiAppSec Cloud to protect applications located on any cloud platform or in your own network. For example, a subscription through AWS still allows protection for applications hosted on Azure. The subscription channel only affects where your FortiAppSec Cloud usage is billed.

If you are purchasing a contract for an existing account, please use the same email address associated with that account when completing the purchase. This ensures the new contract is correctly linked to your existing FortiCloud account.



For a cost estimate of your public cloud marketplace subscription license, please visit the FortiAppSec Cost Calculator.

Billing

The billing rates are the same across all supported public cloud marketplaces (Azure, AWS, and GCP).

- Annual subscription customers prepay for a set number of usage points (e.g., 10,000 points) at the time of subscription. They are only charged extra if their monthly usage exceeds the pre-purchased amount.
- PAYG (Pay-As-You-Go) subscription customers subscribe at no upfront cost and are billed monthly based on the number of points they actually use.



- **FortiAppSec WAF Minimum Charge:** A daily charge for 5 Mbps of bandwidth applies whenever a WAF application exists.
- **FortiAppSec GSLB DNS Query Minimum Charge:** A daily charge for 20 QPS applies when GSLB DNS is enabled.

WAF

Standard

Includes core WAF and API security features to protect against common threats.

- 0.14 points per application per hour
- 4.38 points per 5 Mbps per day

Advanced

Adds machine learning-based WAF and API protection, Web Vulnerability Scanning (DAST), and Threat Analytics.

- 0.21 points per application per hour
- 6.56 points per 5 Mbps per day

Enterprise

Includes all Advanced features plus Advanced Bot Protection, Global Server Load Balancing (GSLB), and additional custom rules.

• 0.27 points per application per hour

• 8.77 points per 5 Mbps per day

GSLB

Global Server Load Balancing (GSLB) can also be purchased separately:

- Health Checks – 0.02 points per 10 checks per hour
- Query Capacity – 0.99 points per 20 QPS per day

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

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

Subscribing on AWS Marketplace

FortiAppSec Cloud on AWS supports an annual subscription and a pay-as-you-go billing model.

For usage details and consumption rates, please visit the **Fortinet FortiAppSec Cloud Web Application and API Protection** page on AWS Marketplace.

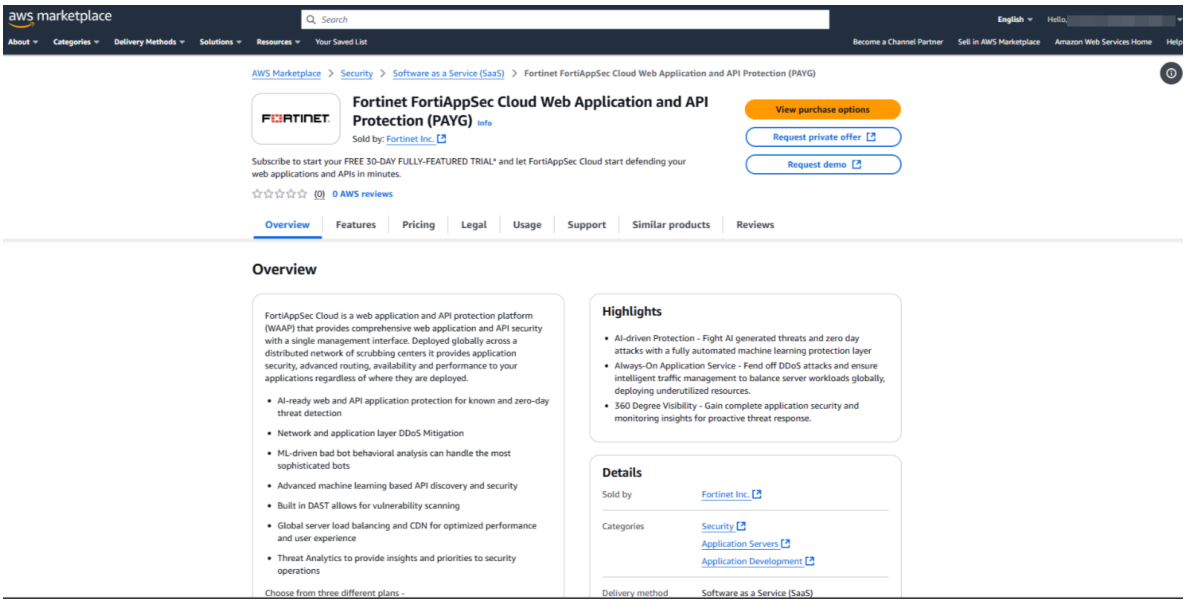
If you are purchasing a contract for an existing account, please use the same email address associated with that account when completing the purchase. This ensures the new contract is correctly linked to your existing FortiCloud account.

Subscription Steps

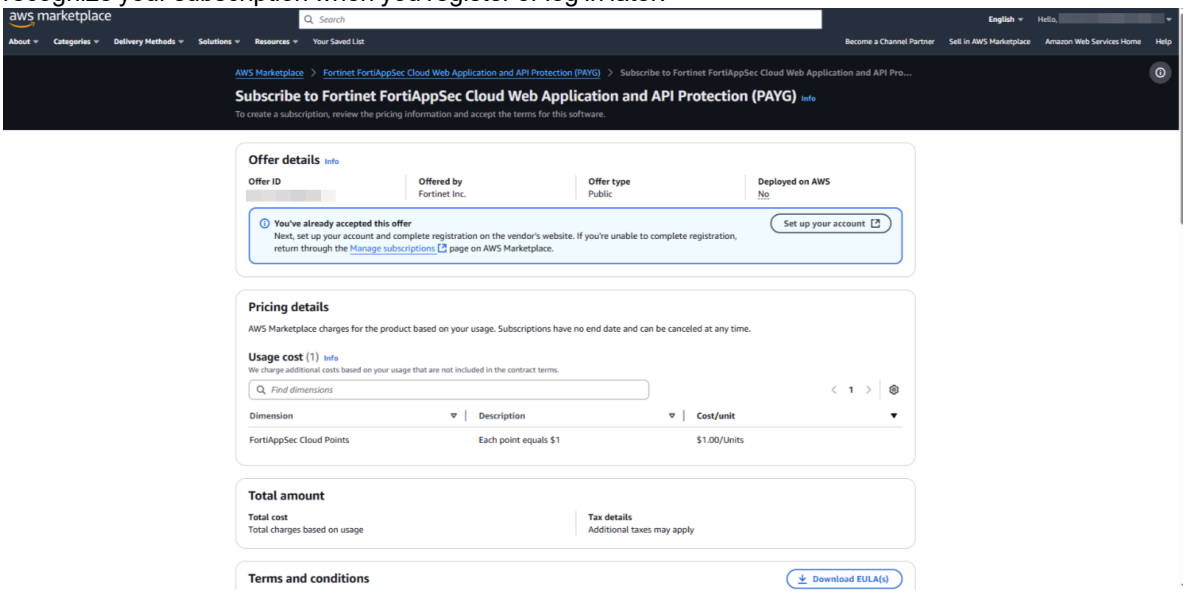
Follow the steps below to subscribe FortiAppSec Cloud on AWS and associate your AWS subscription with your FortiCloud account.

1. Log in to AWS. Search for **Fortinet FortiAppSec Cloud Web Application and API Protection**. You will see both Pay-As-You-Go (PAYG) and Annual Contract options.

2. On the **FortiAppSec Cloud** page, click **View purchase options** and carefully read contract details, as well as the **Terms and Conditions**.

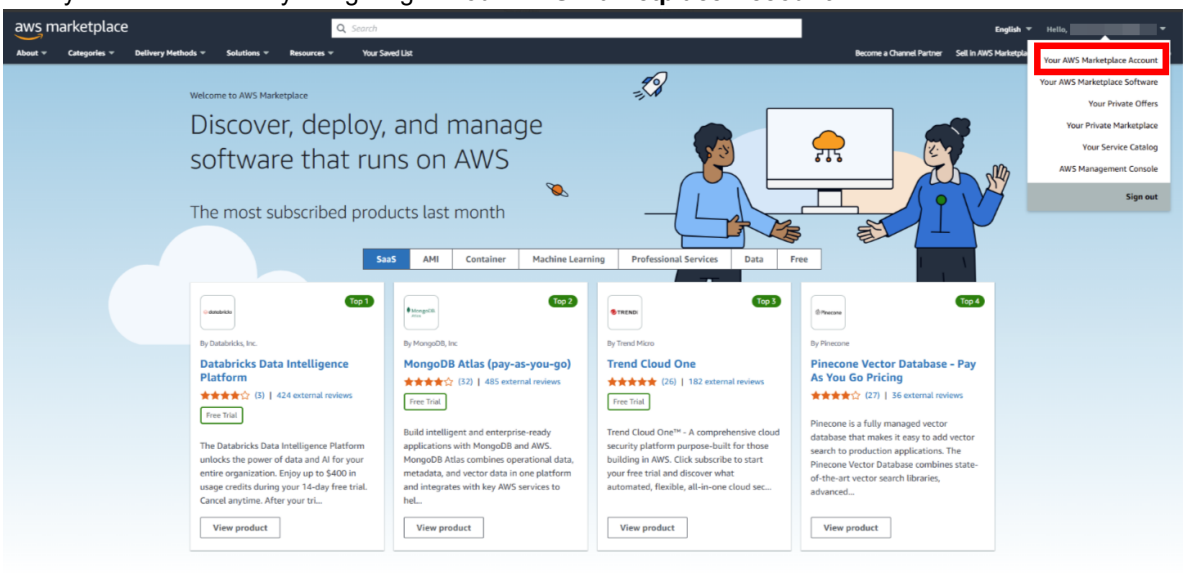


3. Click **Subscribe**. Wait for a few minutes for the subscription to be created.
Do not clear your browser cookies after creating the subscription. Otherwise FortiAppSec Cloud will not recognize your subscription when you register or log in later.



4. Click **Set Up Your Account**. You will be redirected to the FortiAppSec Cloud landing page.
5. 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 FortiAppSec Cloud will be automatically associated once you log in to your FortiCloud account.
Make sure you are using the same popup browser tab when subscribing to FortiAppSec Cloud and logging in to FortiCloud account.

6. View your new contract by navigating to **Your AWS Marketplace Account**.



Please note that even if you subscribed through AWS, you can use FortiAppSec 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 FortiAppSec Cloud usage.

Billing

The billing rates are the same across all supported public cloud marketplaces (Azure, AWS, and GCP).

- Annual subscription customers prepay for a set number of usage points (e.g., 10,000 points) at the time of subscription. They are only charged extra if their monthly usage exceeds the pre-purchased amount.
- PAYG (Pay-As-You-Go) subscription customers subscribe at no upfront cost and are billed monthly based on the number of points they actually use.



- **FortiAppSec WAF Minimum Charge:** A daily charge for 5 Mbps of bandwidth applies whenever a WAF application exists.
- **FortiAppSec GSLB DNS Query Minimum Charge:** A daily charge for 20 QPS applies when GSLB DNS is enabled.

WAF

Standard

Includes core WAF and API security features to protect against common threats.

- 0.14 points per application per hour
- 4.38 points per 5 Mbps per day

Advanced

Adds machine learning-based WAF and API protection, Web Vulnerability Scanning (DAST), and Threat Analytics.

- 0.21 points per application per hour
- 6.56 points per 5 Mbps per day

Enterprise

Includes all Advanced features plus Advanced Bot Protection, Global Server Load Balancing (GSLB), and additional custom rules.

• 0.27 points per application per hour

• 8.77 points per 5 Mbps per day

GSLB

Global Server Load Balancing (GSLB) can also be purchased separately:

- Health Checks – 0.02 points per 10 checks per hour
- Query Capacity – 0.99 points per 20 QPS per day

Unsubscribing from FortiAppSec Cloud on AWS

You can unsubscribe from FortiAppSec Cloud anytime, but keep in mind that the data in your FortiAppSec Cloud account will be cleared in one week after you unsubscribe. It can't be restored even if you subscribe to FortiAppSec Cloud again.
Before unsubscribing, to avoid service disruption to your web application, ensure that the CNAME record is replaced with the correct IP address in your DNS settings.

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. Find your **FortiAppSec Cloud** subscription, then navigate to **Manage Subscription**.
3. Under **Agreement**, expand the **Actions** menu. Click **Cancel Subscription**.
   FortiAppSec 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 FortiAppSec Cloud stops protecting your applications.

Subscribing on Azure Marketplace

FortiAppSec Cloud on Azure supports an annual subscription and a pay-as-you-go billing model.

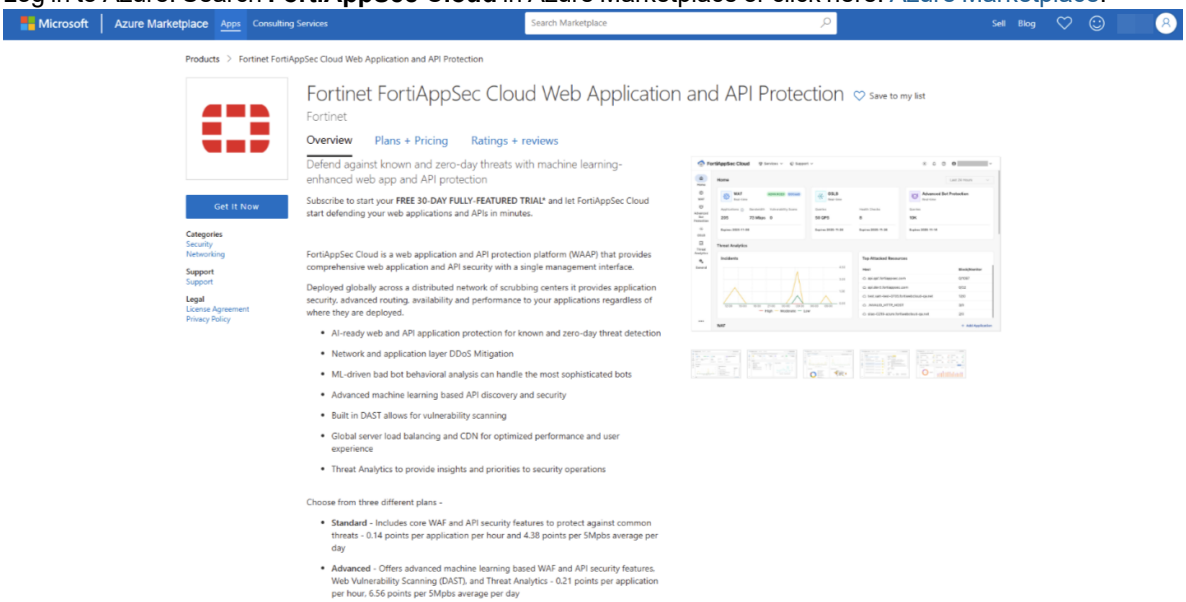
For usage details and consumption rates, please visit the **Fortinet FortiAppSec Cloud Web Application and API Protection** page on Azure Marketplace.

If you are purchasing a contract for an existing account, please use the same email address associated with that account when completing the purchase. This ensures the new contract is correctly linked to your existing FortiCloud account.

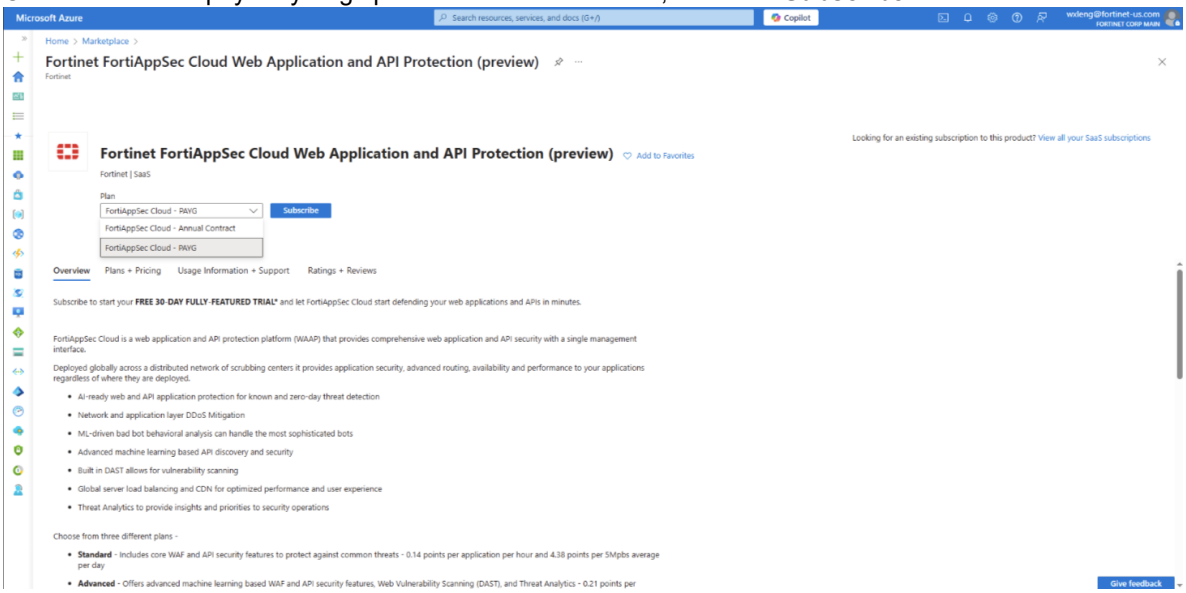
Subscription Steps

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

1. Log in to Azure. Search **FortiAppSec Cloud** in Azure Marketplace or click here: Azure Marketplace.

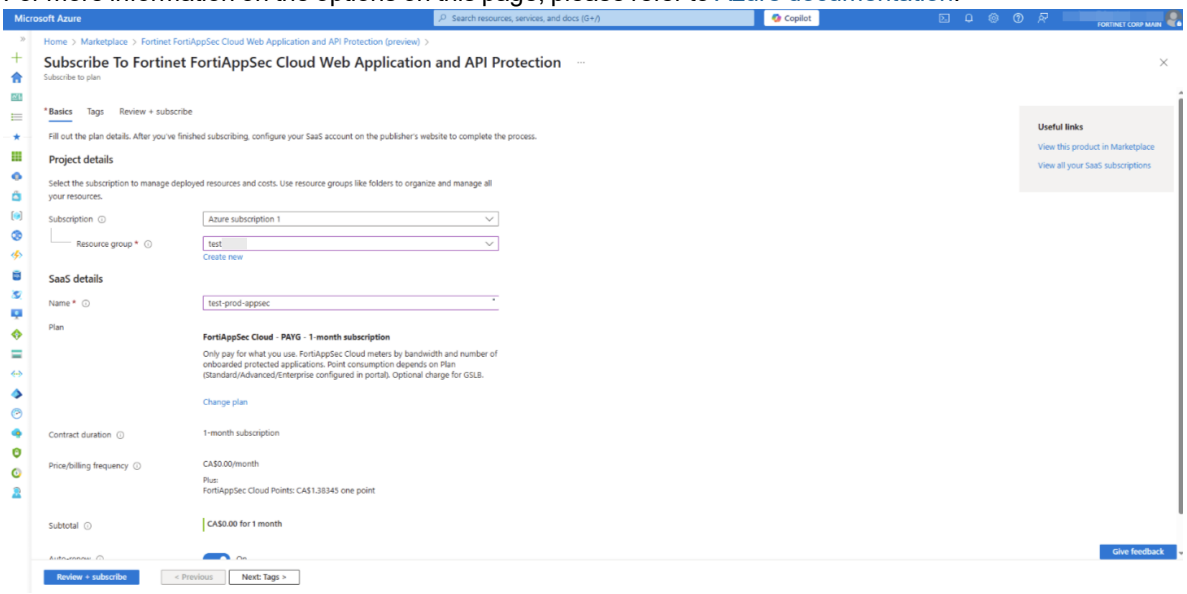


2. Choose either the pay-as-you-go plan or an annual contract, then click **Subscribe**.

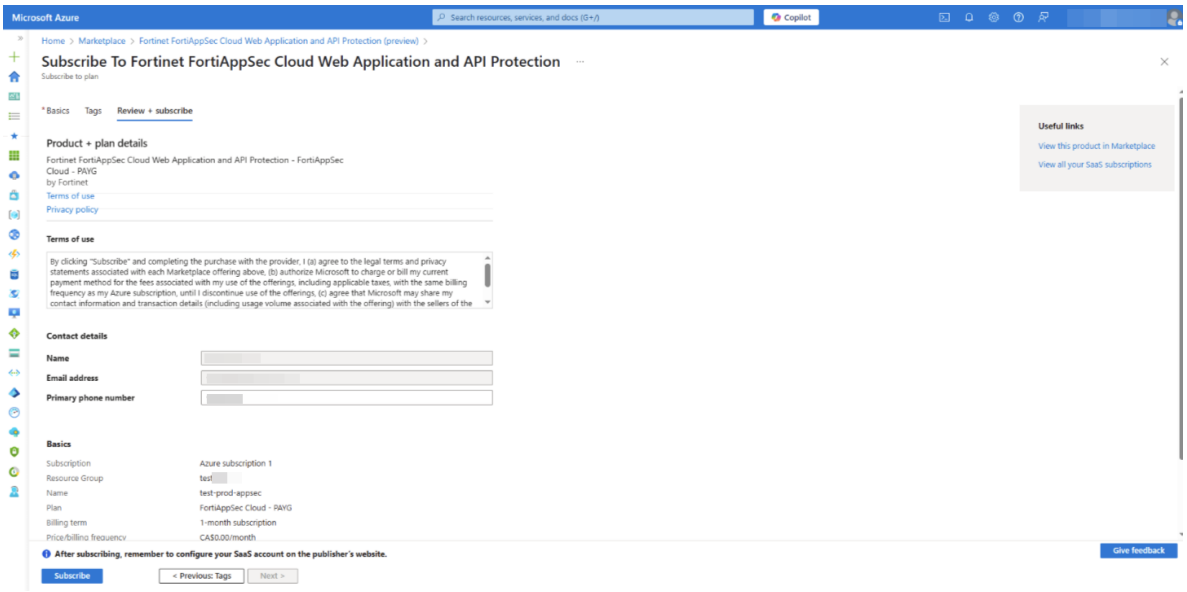


3. Basics
   a. Under **Project details**, select the desired description and resource group.
   b. Under **SaaS details**, enter the desired name, plan, and contract duration of plan.

For more information on the options on this page, please refer to Azure documentation.

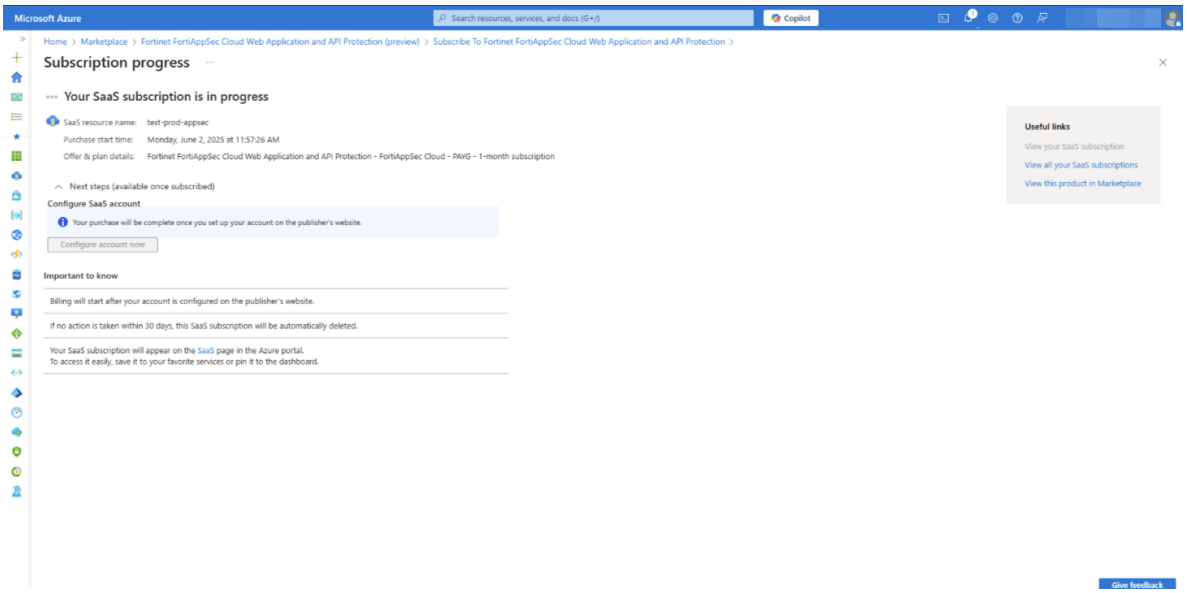


4. Configure **Tags** as needed. For more information on the options on this page, please refer to Azure documentation.
5. Continue to **Review + Subscribe** to go through the offer and plan details.

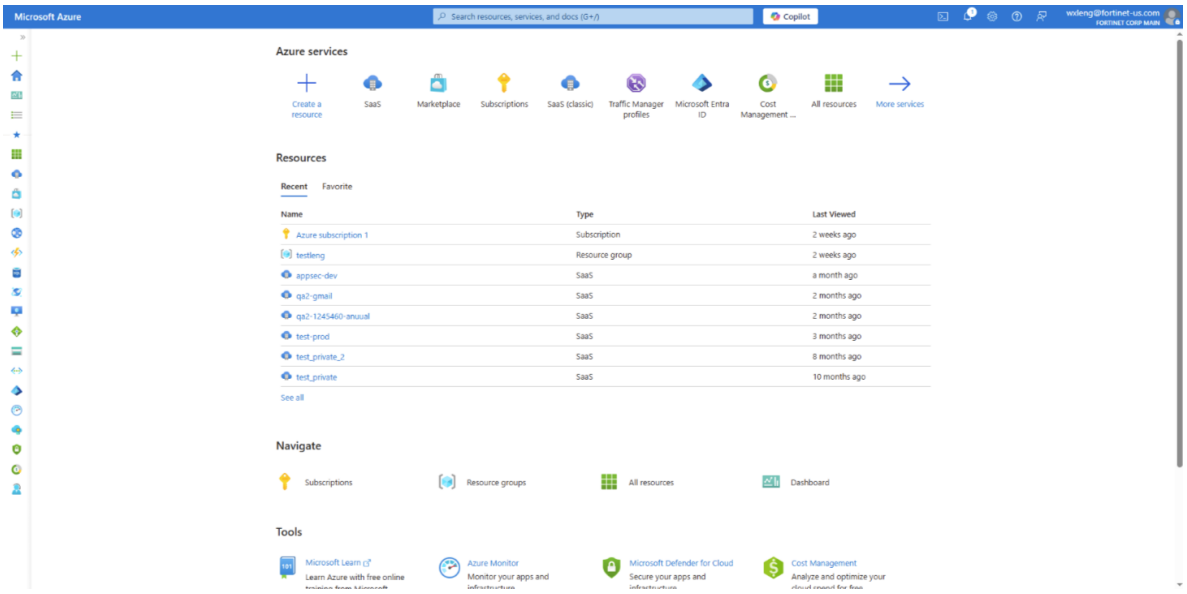


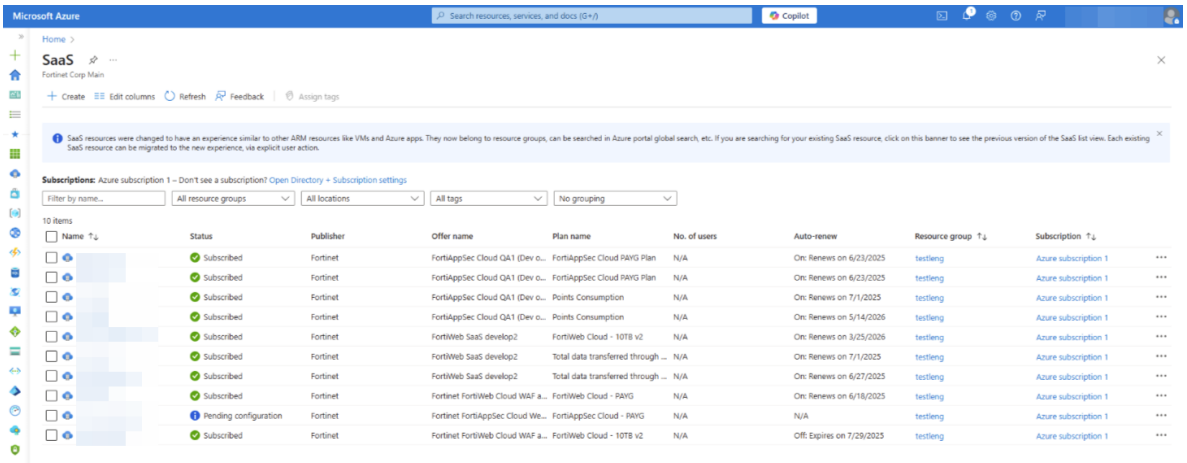
Once you have reviewed and confirmed your plan details, click **Subscribe**.

- If the **Subscription process** is successful, skip to step 7.
- If it fails, proceed to Step 6.



6. If the **Subscription process** fails:
   a. Navigate to **Software as a Service (SaaS)** in the Azure portal.
   b. Find the SaaS subscription you just created and click it to open the details page.





7. Click **Configure Account now**. You will be directed to the landing page of FortiAppSec Cloud where you can register or log in. Make sure to use the same tab when subscribing and when logging in to your account for the first time after subscribing. This ensures that your Azure subscription is automatically associated with your FortiCloud account upon login.
   You can access all of your FortiAppSec Cloud services as well as the Fortinet Support site through FortiCloud account.
8. Log in to FortiAppSec Cloud. Verify that the **Azure subscription** appears under **General > Contracts**.
   - If it does not appear, return to Azure Marketplace and search FortiAppSec Cloud WAF-as-a-Service. You should see a notice prompting you to complete the subscription process again.

Please note that even if you subscribed through Azure, you can use FortiAppSec 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 FortiAppSec Cloud usage.

Billing

The billing rates are the same across all supported public cloud marketplaces (Azure, AWS, and GCP).

- Annual subscription customers prepay for a set number of usage points (e.g., 10,000 points) at the time of subscription. They are only charged extra if their monthly usage exceeds the pre-purchased amount.
- PAYG (Pay-As-You-Go) subscription customers subscribe at no upfront cost and are billed monthly based on the number of points they actually use.



- **FortiAppSec WAF Minimum Charge:** A daily charge for 5 Mbps of bandwidth applies whenever a WAF application exists.
- **FortiAppSec GSLB DNS Query Minimum Charge:** A daily charge for 20 QPS applies when GSLB DNS is enabled.

WAF

Standard

Includes core WAF and API security features to protect against common threats.

- 0.14 points per application per hour
- 4.38 points per 5 Mbps per day

Advanced

Adds machine learning-based WAF and API protection, Web Vulnerability Scanning (DAST), and Threat Analytics.

- 0.21 points per application per hour
- 6.56 points per 5 Mbps per day

Enterprise

Includes all Advanced features plus Advanced Bot Protection, Global Server Load Balancing (GSLB), and additional custom rules.

• 0.27 points per application per hour

• 8.77 points per 5 Mbps per day

GSLB

Global Server Load Balancing (GSLB) can also be purchased separately:

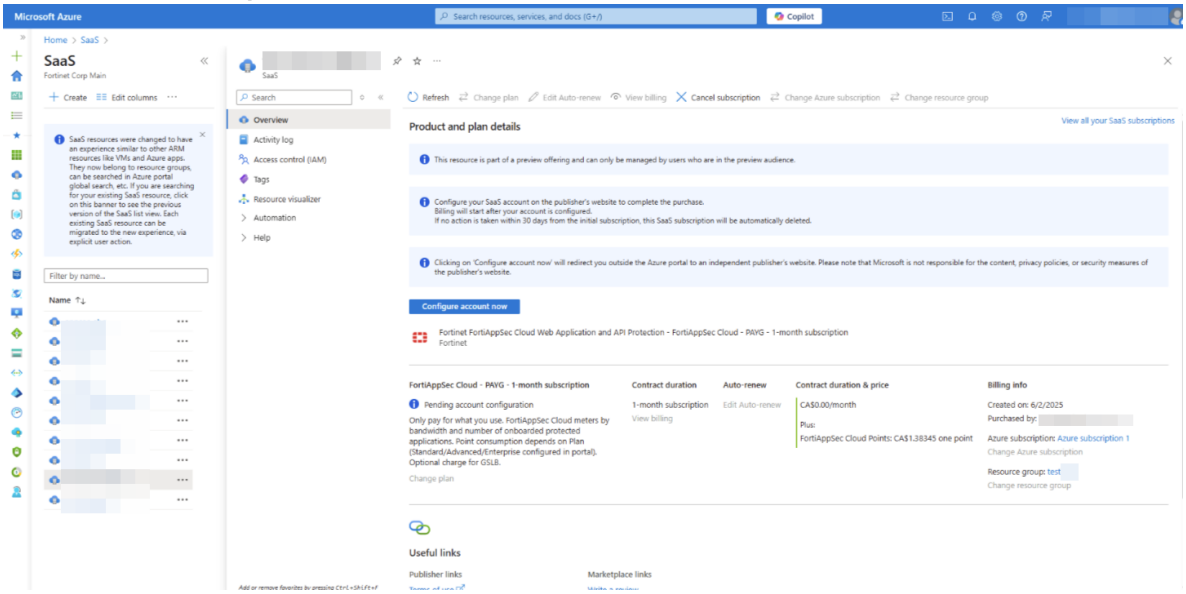
- Health Checks – 0.02 points per 10 checks per hour
- Query Capacity – 0.99 points per 20 QPS per day

Unsubscribing from FortiAppSec Cloud on Azure

You can unsubscribe from FortiAppSec Cloud anytime. However, please note that all data in your account will be permanently deleted one week after unsubscription. This data cannot be recovered, even if you resubscribe. Be sure to export any necessary information before unsubscribing.

Before unsubscribing, to avoid service disruption to your web application, ensure that the CNAME record is replaced with the correct IP address in your DNS settings.

1. Locate your newly subscribed FortiAppSec Cloud resource in the Azure portal.
   a. Navigate to **Software as a Service (SaaS)**.
2. Select the FortiAppSec Cloud subscription you just created.
3. Click **Cancel Subscription**.



Subscribing on Google Cloud Marketplace

FortiAppSec Cloud on Google Cloud Marketplace supports only the pay-as-you-go billing model.

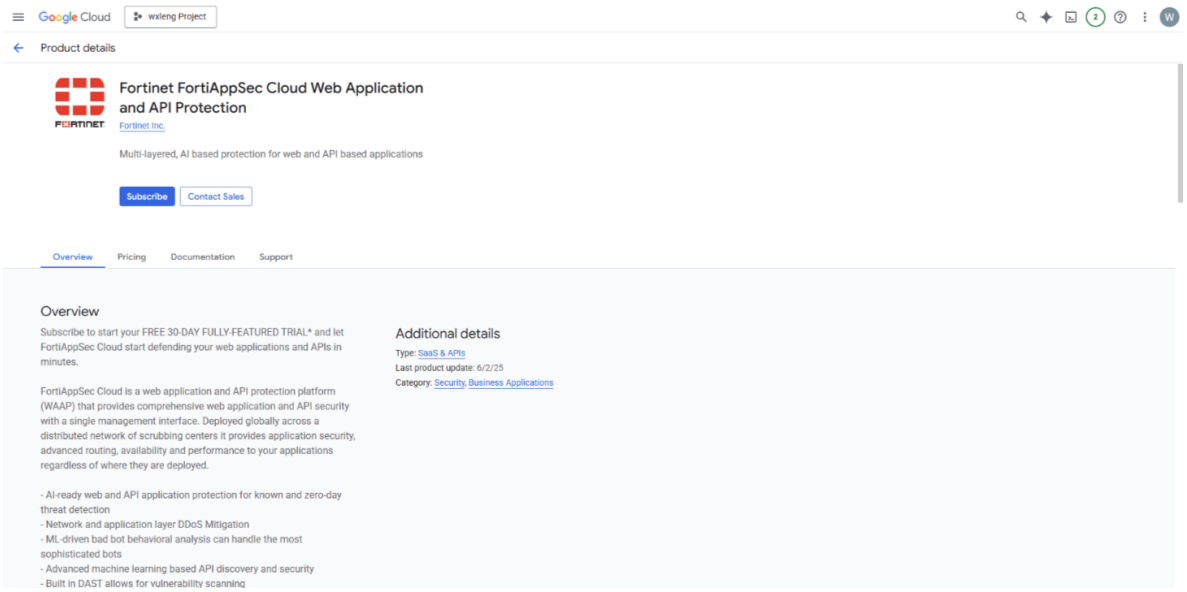
For usage details and consumption rates, please visit the **Fortinet FortiAppSec Cloud Web Application and API Protection** page on Google Cloud Marketplace.

If you are purchasing a contract for an existing account, please use the same email address associated with that account when completing the purchase. This ensures the new contract is correctly linked to your existing FortiCloud account.

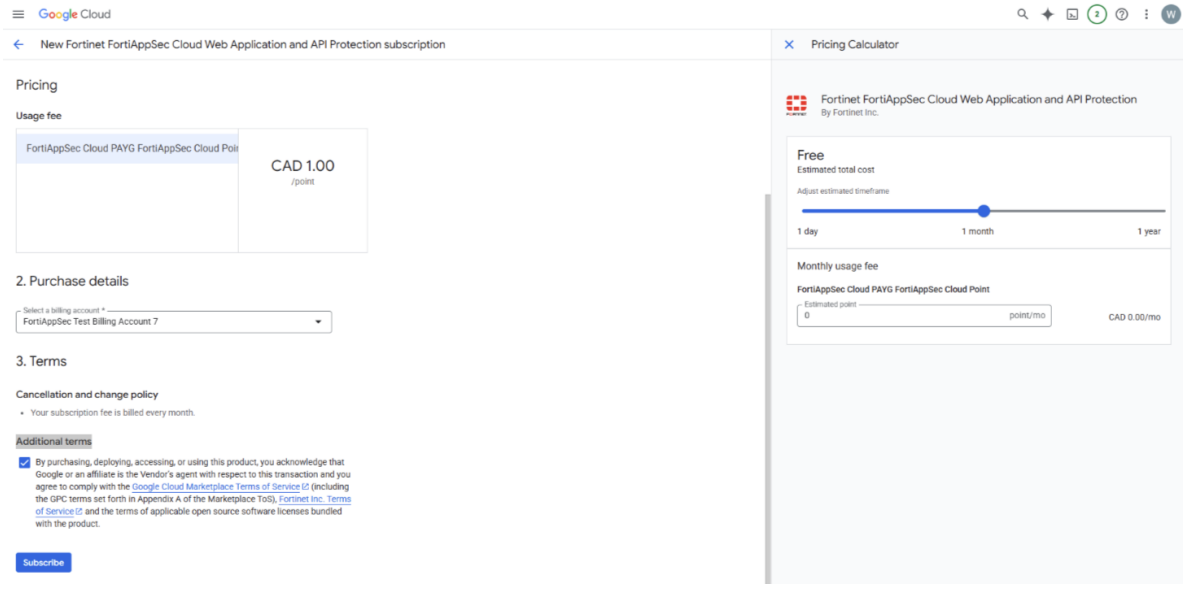
Subscription Steps

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

1. Log in to Google Cloud. Search **FortiAppSec Cloud** in Google Cloud Marketplace or click here: Google Cloud Marketplace.
2. Click **Subscribe**.



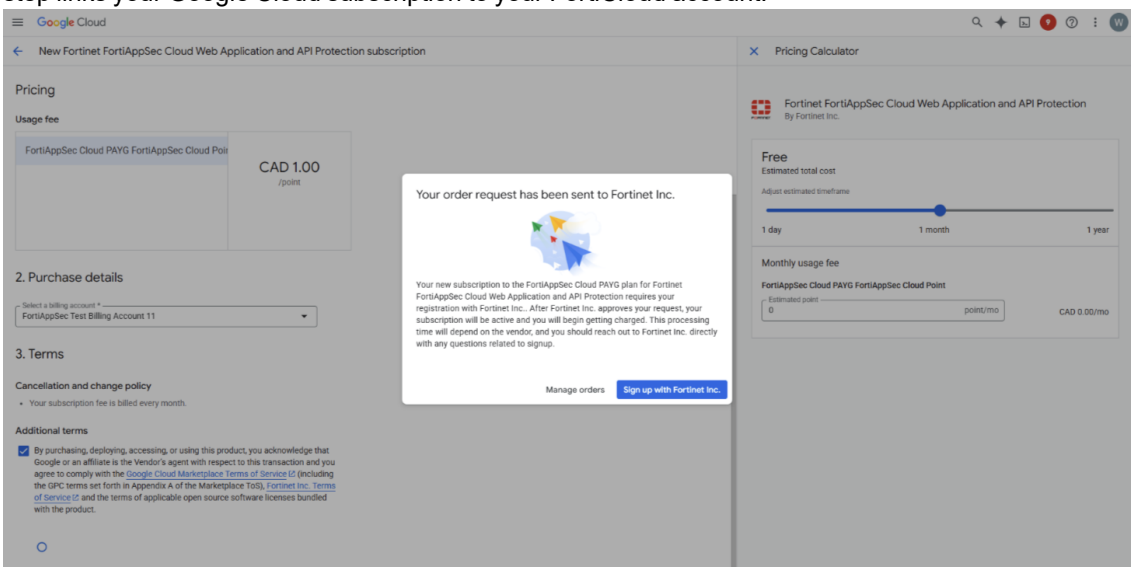
3. Click **Subscribe**.



4. This step depends on whether you have previously subscribed to a Fortinet service using this email address.

If this is your first time subscribing to a Fortinet service on Google Cloud:

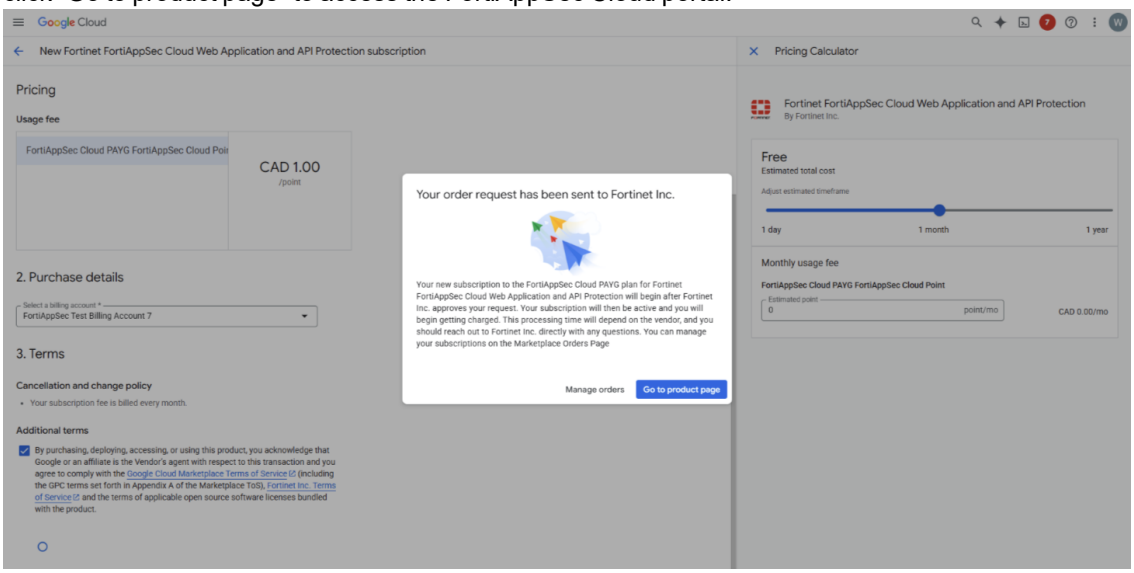
- Click **Sign up with Fortinet Inc.** and complete the registration in the FortiCloud pop-up window. This step links your Google Cloud subscription to your FortiCloud account.



  Make sure you are using the same browser when subscribing FortiAppSec Cloud and logging in to FortiCloud account.

If you have previously subscribed to any Fortinet service on Google Cloud:

- Your new subscription will automatically be associated with your existing FortiCloud account. Simply click “Go to product page” to access the FortiAppSec Cloud portal.



5. Log in to FortiAppSec Cloud, verify that your **GCP Subscription** appears under **General > Contracts**.
   - If it does not appear, return to the Google Cloud Marketplace and search for WAF-as-a-Service. You should see a notice prompting you to complete the subscription process again.

Billing

The billing rates are the same across all supported public cloud marketplaces (Azure, AWS, and GCP).

- Annual subscription customers prepay for a set number of usage points (e.g., 10,000 points) at the time of subscription. They are only charged extra if their monthly usage exceeds the pre-purchased amount.
- PAYG (Pay-As-You-Go) subscription customers subscribe at no upfront cost and are billed monthly based on the number of points they actually use.



- **FortiAppSec WAF Minimum Charge:** A daily charge for 5 Mbps of bandwidth applies whenever a WAF application exists.
- **FortiAppSec GSLB DNS Query Minimum Charge:** A daily charge for 20 QPS applies when GSLB DNS is enabled.

WAF

Standard

Includes core WAF and API security features to protect against common threats.

- 0.14 points per application per hour
- 4.38 points per 5 Mbps per day

Advanced

Adds machine learning-based WAF and API protection, Web Vulnerability Scanning (DAST), and Threat Analytics.

- 0.21 points per application per hour
- 6.56 points per 5 Mbps per day

Enterprise

Includes all Advanced features plus Advanced Bot Protection, Global Server Load Balancing (GSLB), and additional custom rules.

• 0.27 points per application per hour

• 8.77 points per 5 Mbps per day

GSLB

Global Server Load Balancing (GSLB) can also be purchased separately:

- Health Checks – 0.02 points per 10 checks per hour
- Query Capacity – 0.99 points per 20 QPS per day

Unsubscribing from FortiAppSec Cloud on Google Cloud

You can unsubscribe from FortiAppSec Cloud anytime. However, please note that all data in your account will be permanently deleted one week after unsubscription. This data cannot be recovered, even if you resubscribe. Be sure to export any necessary information before unsubscribing.
Before unsubscribing, to avoid service disruption to your web application, ensure that the CNAME record is replaced with the correct IP address in your DNS settings.

1. Log in to Google Cloud Marketplace, and go to **Your Orders**.
2. Find the subscription you would like to cancel, and click **Cancel Order**.

Onboarding

After purchasing your contract or license, add applications to FortiAppSec Cloud to access the security features of its services.

Add Application

To protect your domain, add your application separately to each service. You can do this by selecting **Add Application** next to each service widget on the **Home** dashboard or by navigating to the desired service through the side menu.

FortiAppSec Cloud currently does not support adding an application for multiple/all services in one process.

However, please note the following:

- the **WAF** and **Threat Analytics** services share an onboarding procedure.
- To use Advanced Bot Protection (ABP) with WAF, we recommend onboarding your application to WAF first. Once complete, add the ABP module for the application, as this will automatically register it with the Advanced Bot Protection service.

For detailed instructions, please see the onboarding details of each service:

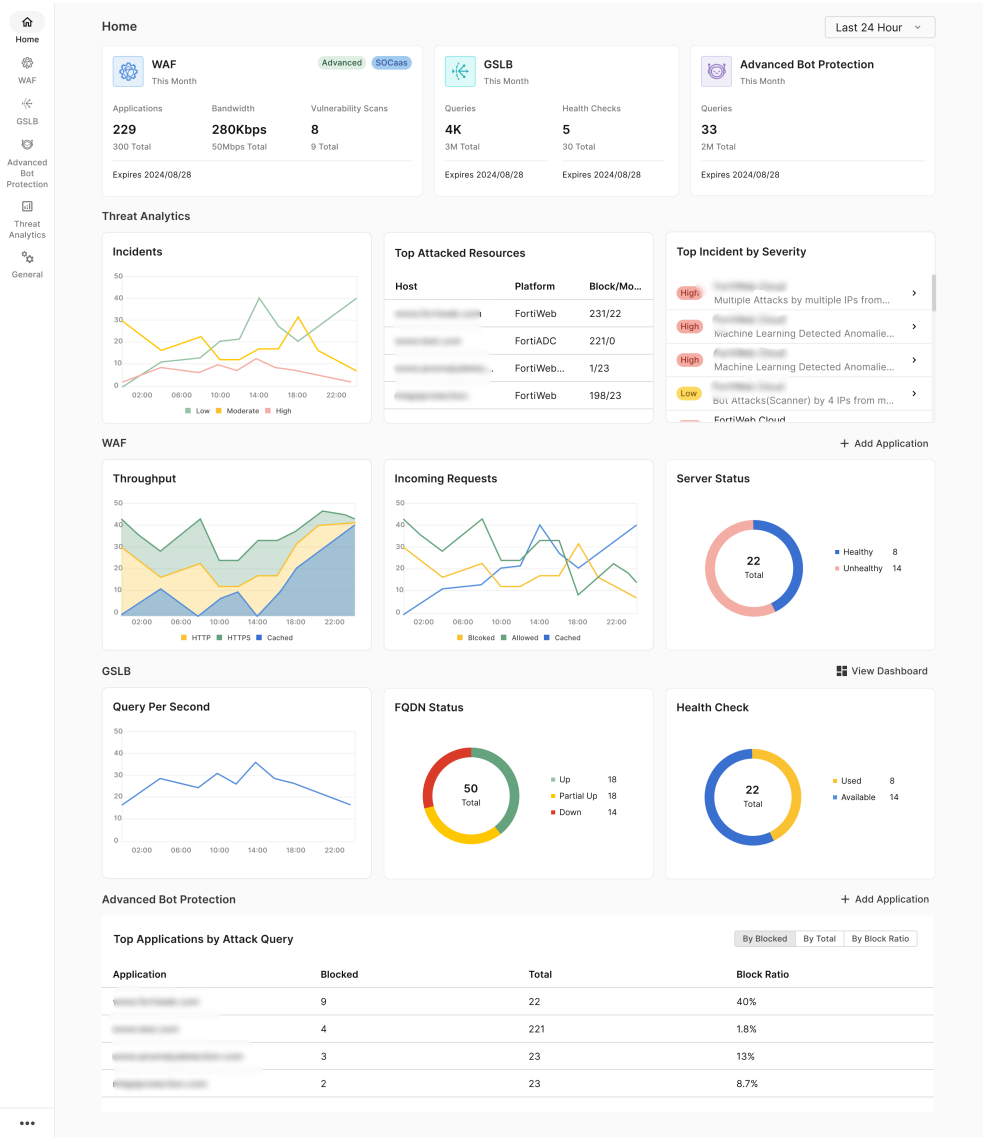
- Onboard WAF applications on page 65
- Onboarding GSLB Applications on page 316
- ABP Application on page 284

Many of the security features in the WAF and ABP services are specific to each application, and therefore must be accessed by selecting an application first. For details on the workflow for these services, please see the following pages:

- WAF Workflow and Dashboard Overview on page 82
- ABP Workflow and Dashboard Overview on page 256

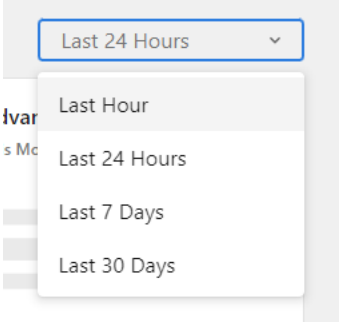
Home

The Home page displays a summary of insights on your application activity from your various services.



Understanding Insights

Select a date range or time frame to view insights on the traffic activity of your application.



Widget	Description
Threat Analytics	
Incidents	A line graph displaying the number of attack events by severity level. For more information on incident severity levels and how they are determined, please see Incidents on page 402.
Top Attacked Resources	A ranked table containing the applications with the highest number of detected attack events, the service that detected the attack events, and the numbers of blocked and monitored events. **Blocked** events indicates that the detected malicious traffic is immediately stopped by FortiAppSec Cloud. **Monitored** events indicates the event is logged without any interruption to traffic. This is helpful for monitoring and evaluating threats without affecting user traffic.
Top Incident by Severity	A list of significant attack events, ranked by severity. Click on an event to view details.
WAF	
Throughput	A stacked line graph of throughput on all of your applications over the selected time span in bits/second.
Incoming Requests	A line graph of the number of incoming requests over the selected time span.
Server Status	A pie chart displaying the server status of your various applications.
GSLB	
Query Per Second	A line graph of the queries per second on applications in your account over the selected time frame.
FQDN Status	A pie chart showings the status of your FQDNs.
Health Check	A pie chart displaying the ratio of used and available Health Checks.
Advanced Bot Protection	
Top Applications by Attack Query	This table displays counts for blocked and detected bot activities, as well as the block ratio, calculated from these two figures. To sort the table, click one of the following options:

Widget	Description
	• **By Blocked**: Orders from the highest to lowest number of blocked transactions. • **By Total**: Orders from the highest to lowest total number of bot queries. • **By Block Ratio**: Orders from the highest to lowest block ratio. Please note, an **Attack Query** doesn't always indicate a malicious bot attack. Instead, it refers queries exchanged between the FortiABP device and a FortiADC/FortiWeb device on the protected application.

FortiAI Assistant

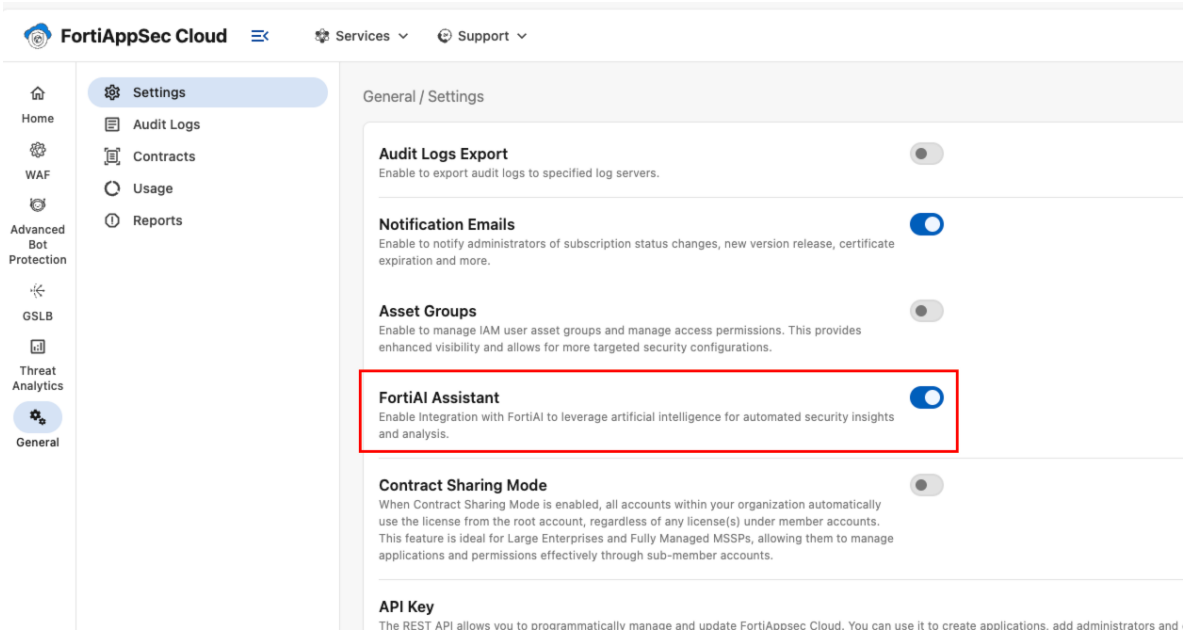
The FortiAI Assistant is a natural language processing interface integrated with FortiAppSec Cloud, designed to provide conversational assistance for security operations , management, network support, knowledge base. As a generative AI-powered tool, all its model updates pass rigorous security efficacy benchmarks before deployment.

This feature is currently in beta and available to all users at no cost. For information on usage limits, please see Token usage on page 60.

- Activate FortiAI Assistant on page 54
- How to use FortiAI Assistant on page 54
- Chatbot Limitations on page 59
- Token usage on page 60

Activate FortiAI Assistant

1. To use this feature, navigate to **General > Settings** and enable **FortiAI Assistant**.



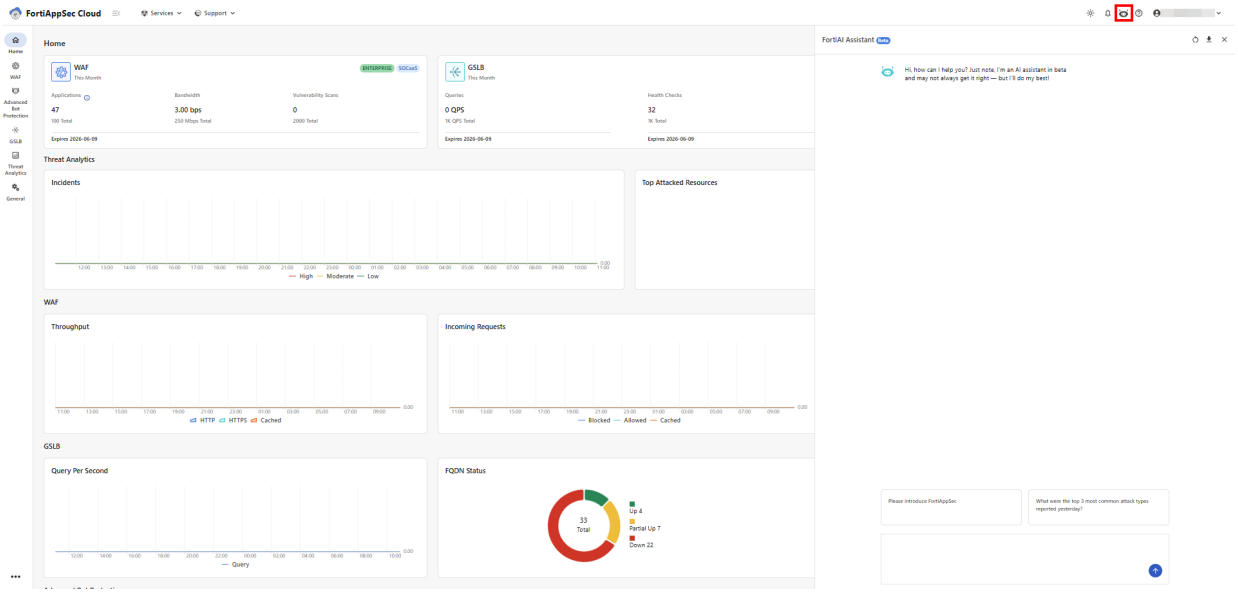
How to use FortiAI Assistant

The following capabilities are currently supported in release 25.3:

- **Knowledge Base:** Get instant answers on configurations, features, and best practices.
- **Log Analysis:** It summarizes Cloud WAF attack logs and analyzes traffic trends to help you spot anomalies and understand usage.
- **Dashboard Insights:** Provides performance summaries and detects anomalies.
- **Smart Communication:** It asks for clarification when a query is unclear and gracefully rejects non-security questions.

Launch the chat interface

Chat with the FortiAI Assistant by clicking the icon in the top-right corner of your screen.



The suggestions below offer some examples of how to get started with common security tasks.

- **Product Q&A:** Get quick answers about FortiAppSec Cloud features, deployment, and settings.
  Example prompts:
  - "How do I configure a custom WAF rule in FortiAppSec Cloud?"
  - "How do I set up geo-blocking for my API endpoints?"
  - "Explain the difference between brute force protection and rate limiting."

  Best practices:
  - Mention specific features or settings.
  - Try to use terms from our product UI or documentation. This helps FortiAI Assistant understand your request more accurately, leading to better results.

- **Log Analysis:** Identify false positives in attack logs with contextual analysis.
  Example prompts:
  - "Why was this request blocked? log ID: abc123"
  - "Explain this SQL injection attempt in log ID XYZ456."
  - "Which rule triggered for this XSS alert?"

  Best practices:

  - Include **Log IDs** or request snippets for precise analysis.
  - Ask for recommended actions (e.g., "Should I allowlist this request?").
- **Dashboard Log Insights:** Extract trends and analytics from your traffic logs.

  Example prompts:
  - "Show request volume trends for /checkout in the last 7 days."
  - "Compare attack patterns between last month and this month."
  - "Which endpoints had the most 5xx errors yesterday?"

  Best practices:
  - Specify time ranges (e.g., "last 24 hours").
  - Reference specific endpoints or APIs for targeted insights.
- **Audit Logs Insights:** Ask questions about log trends, filter by attributes, or request specific data.

  Example prompts:
  - "Show GSLB connector audit logs over the past 24 hours."
  - "Find auto-certificate audit logs for ROMANIA in the past week."
  - "Find login audit logs from 123.456.789.012 in the past 2 days."

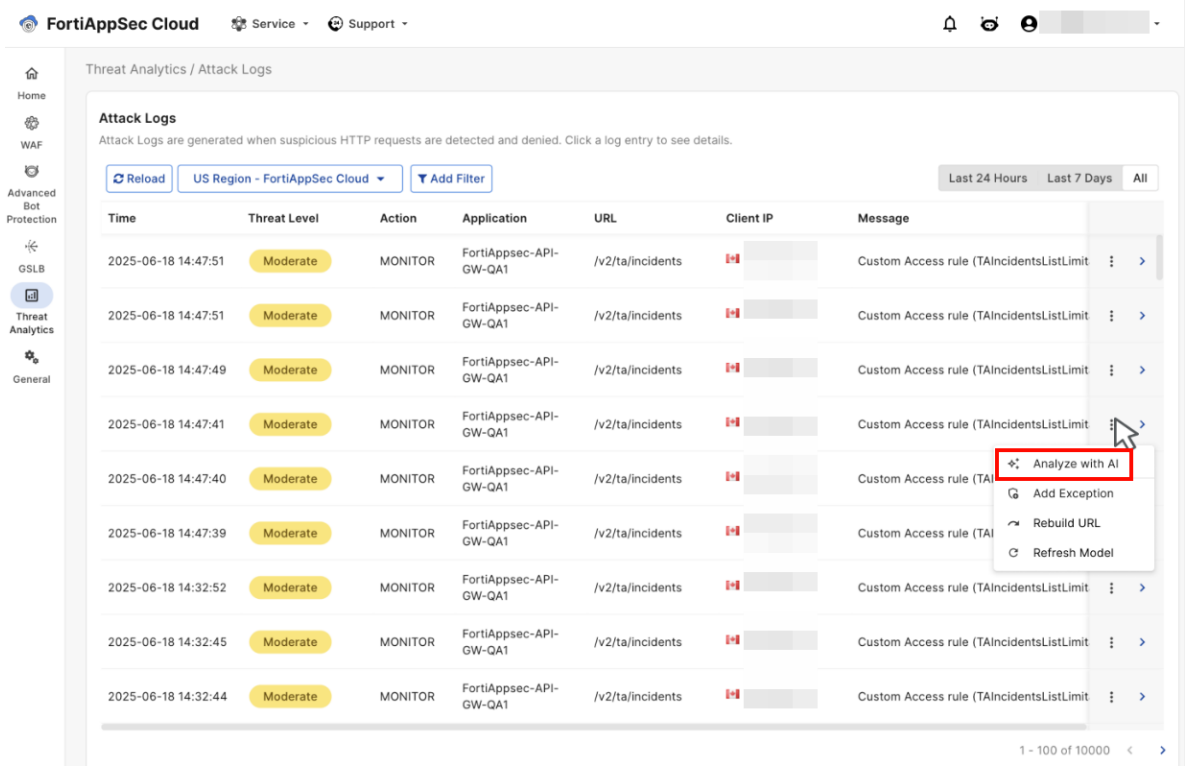
  Best practices:
  - Specify the exact type of audit logs you are querying, such as GSLB connector logs, auto-certificate logs, or authentication logs.
  - Specify time ranges (e.g., "last hour").

Analyze Attack Logs

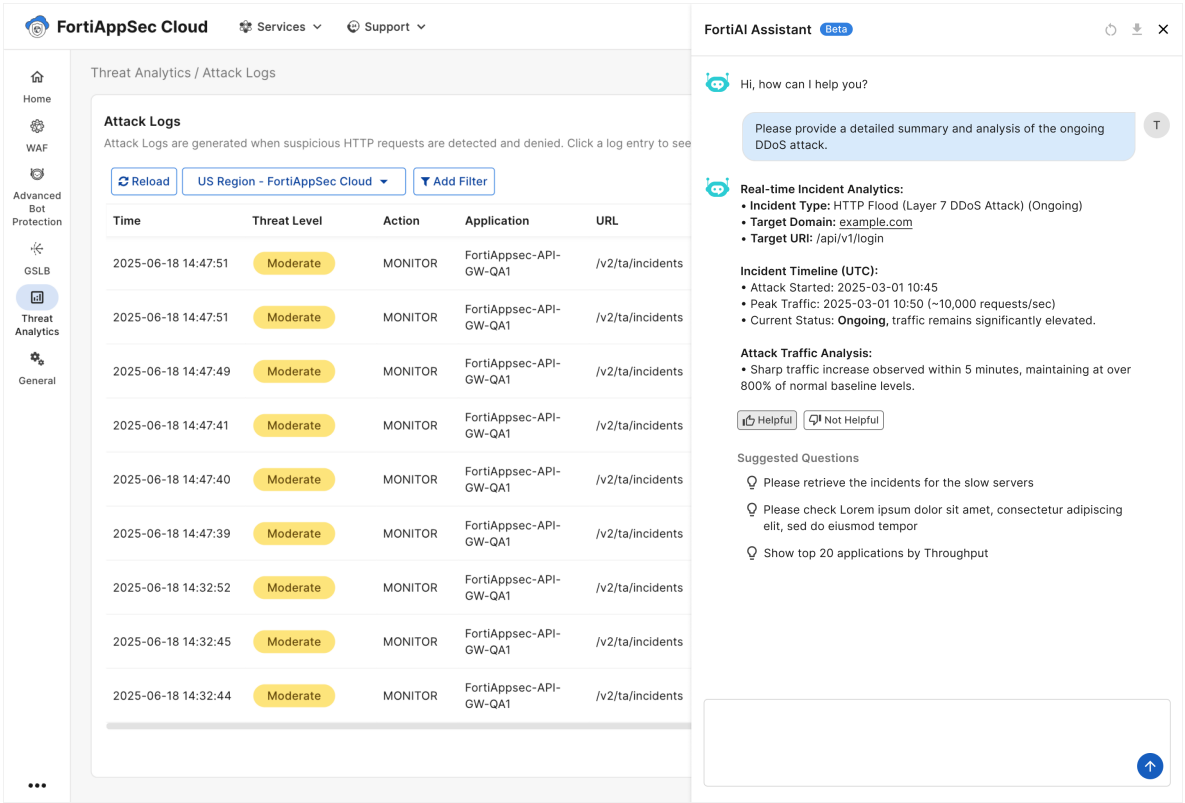
While reviewing activity on the **Threat Analytics > Attack Logs** page, you can use FortiAI to provide insights on specific events.

Please note, this feature only applies to Cloud WAF logs. FortiAI does not yet support ABP nor GSLB log analysis.

1. Navigate to **Threat Analytics > Attack Logs**.
2. In the row of the desired event, click the three dots icon to expand the actions menu, and select **Analyze with AI**.



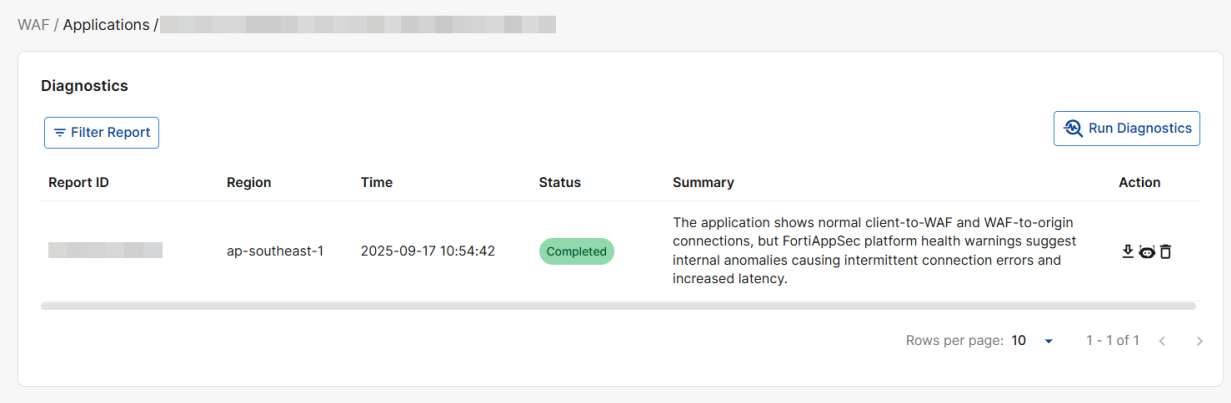
3. This launches the FortiAI Assistant, which generates a detailed analysis of the selected attack log event.



Analyze Diagnostics Report

The Diagnostics Agent helps identify abnormal connection statuses within their applications and provides insights for resolving connectivity issues.

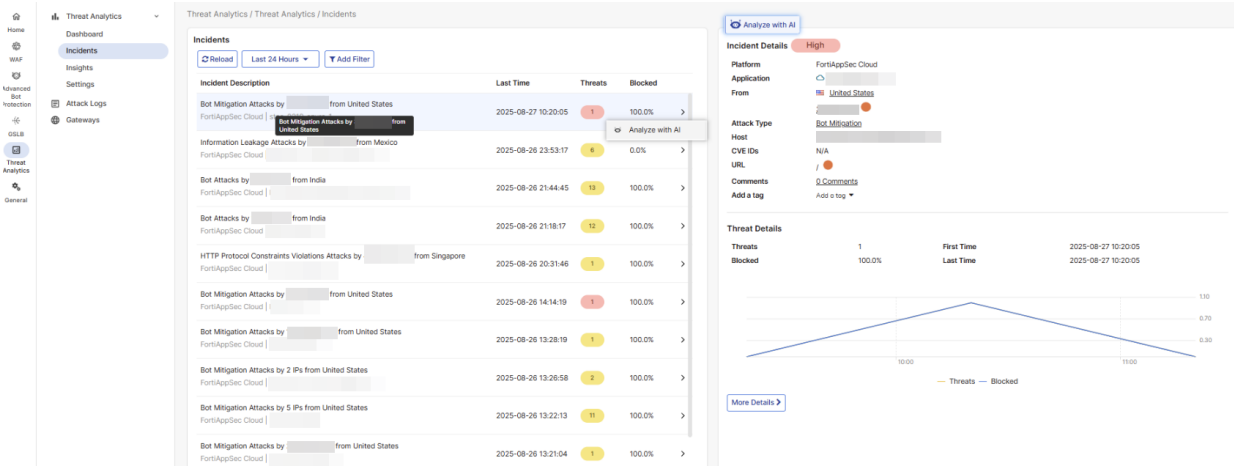
To activate the agent, click the icon under **Actions**.



For more information on the Diagnostics report, see Diagnostics on page 117.

Analyze Threat Analytics Incidents

Click **Analyze with AI** to see AI-generated summaries and insights for Threat Analytics (TA) incidents, streamlining incident review and decision-making. It combines automated contextual narratives with natural language query capabilities to help analysts quickly understand incident details and trends.

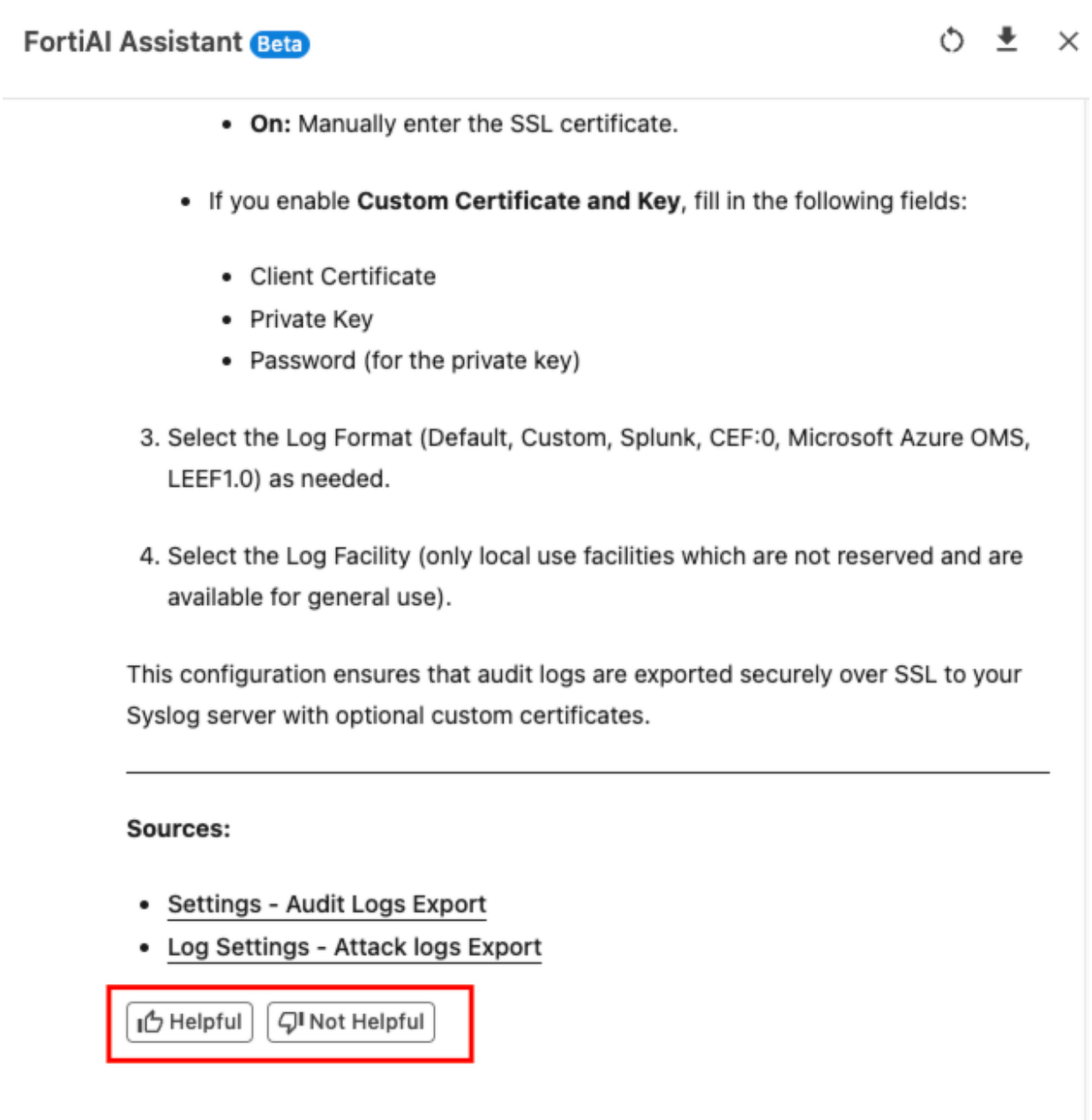


For more information on Threat Analytics Incidents, please refer to Incidents on page 402.

Help us improve

Your feedback is vital for training and refining the AI.

Please let us know how FortiAI Assistant is doing by clicking the thumbs up or thumbs down icons below each AI response.



Chatbot Limitations

FortiAI Assistant is a powerful tool, but it's important to understand its current limitations:

- **Product-Specific Knowledge**: FortiAI Assistant can only answer questions related to FortiAppSec Cloud. If you ask about other topics, it will let you know the question is out of scope.
- **Advisory Only**: This is an analytical and advisory tool. It cannot directly make configuration changes or create rules for you.
- **Log Analysis Scope**: FortiAI Assistant currently only supports analysis of Cloud WAF logs. It cannot yet analyze logs from ABP or GSLB.

- **Data Access**: FortiAI Assistant analyzes indexed log data only, and it does not have access to real-time logs. The data retention period is 2-3 months.
- **Usage**: There are no visible usage quotas or token tracking for your queries.

Token usage

FortiAI usage is measured in **tokens**, which are a unit of measurement for the size of both your questions and the AI's responses. Simply put, longer questions and longer answers consume more tokens.

Please note, these tokens are different from those used in FortiFlex license usage.

During the Beta Period

- Free for all users: FortiAI is currently free to use.
- Daily limit: Each user has a daily allowance of 500,000 tokens.
- Token tracking: While you can't view your usage in real time, the chatbot will notify you once you've reached your daily limit.

After the Beta Period

- Paid service: FortiAI Assistant will transition to a paid, token-based usage model. Detailed pricing will be announced before the official release.
- Legacy contracts: Legacy contract users will lose access to FortiAI Assistant and must upgrade to a FortiAppSec Cloud Contract to continue using the feature.

WAF

FortiAppSec Cloud's Web Application Firewall (WAF) is a SaaS, cloud-based Web Application Firewall (WAF) designed to protect public cloud-hosted web applications from the OWASP Top 10, zero-day threats, and other application layer attacks.

With no hardware or software requirements, FortiAppSec Cloud utilizes a network of WAF gateways hosted in AWS, Azure, and Google Cloud regions. This architecture ensures that application traffic is scrubbed within the same region where your applications reside, addressing performance and regulatory concerns while minimizing traffic costs.

To begin securing your applications, refer to Onboard WAF applications on page 65.

WAF Concepts

This section covers concepts to help navigate the different components of your web application firewall configurations.

- Application on page 61
- Endpoints on page 61
- Route on page 62
- Origin server on page 63
- Scrubbing Center on page 63

Application

The term **Application** can refer to one of two things:

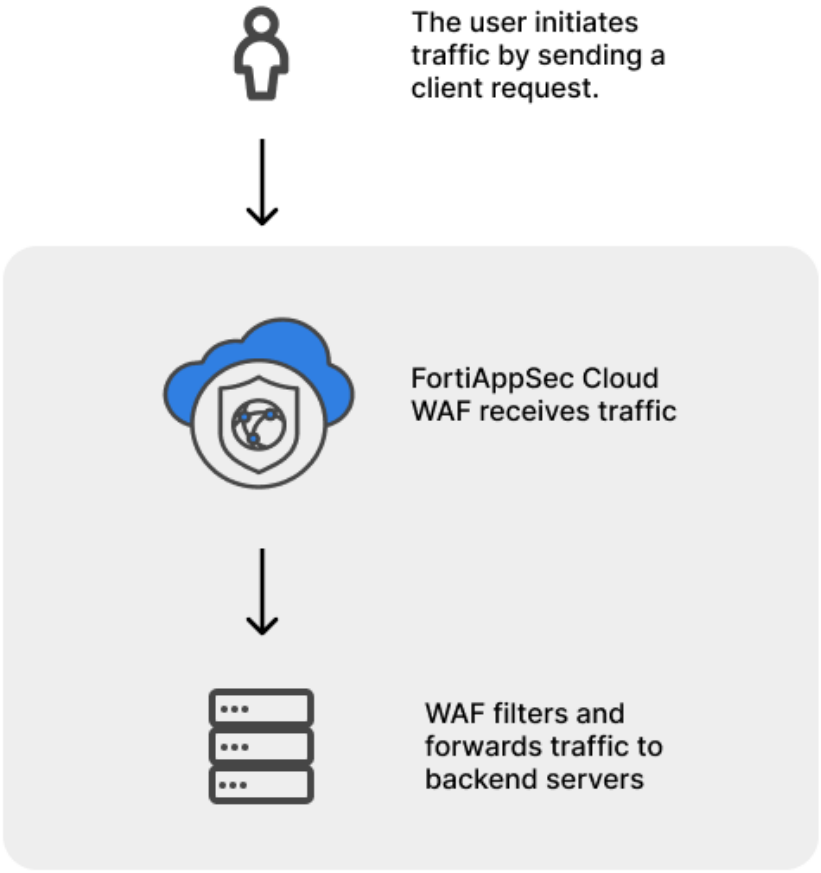
- A unique web application domain configured within your FortiAppSec Cloud deployment.
- A billing unit created when you complete the **Add Application** steps or add a **Content Routing** rule. Each billing application has a distinct **Web Application Name** but may share a domain name, such as in content routing or multi-port applications. This definition is used to calculate usage for billing purposes.

Different areas of the UI may refer to either of these definitions. The specific meaning will be indicated where applicable.

Endpoints

Your Endpoints on page 95 configuration determines the types of front-end traffic forwarded to your application's backend servers, helping to reduce potential security vulnerabilities.

An endpoint generally refers to any device or system that sends or receives network traffic. In this case, the WAF acts as the receiving endpoint for client requests, securing and distributing traffic to backend servers.

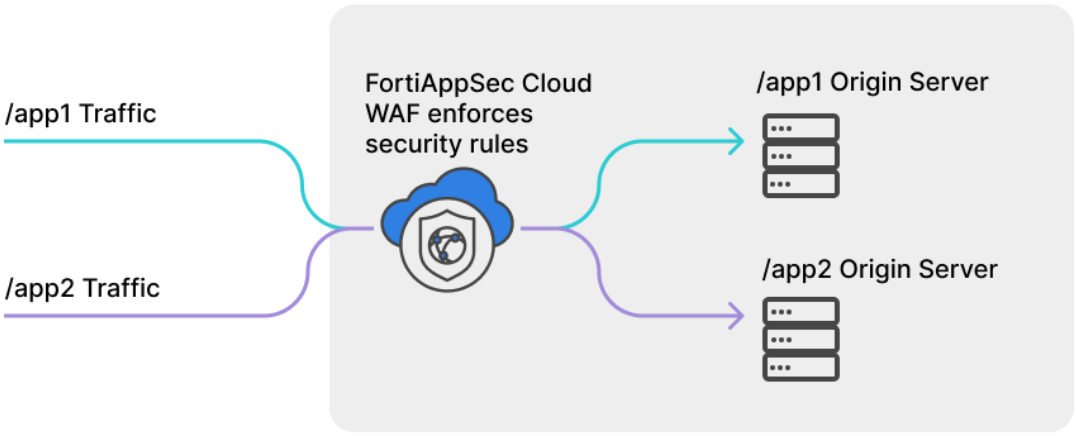


Route

A route refers to the configuration that determines how incoming web traffic is directed to the appropriate destination or origin server based on specified rules, such as URL paths, headers, or query parameters.

In FortiAppSec Cloud, the Content Routing on page 110 feature allows you to manage traffic distribution with greater granularity by defining specific routing rules within a shared WAF configuration.

For example, if multiple web applications are using the same fully qualified domain name (FQDN) but are hosted on different servers, you can create distinct routes for each application based on the requested URL. In the diagram below, traffic to **/app1** is routed to an origin server, and requests to **/app2** will be routed to a different origin server. To configure this for a web application domain or a specific unit within the **WAF > Applications** list in FortiAppSec Cloud, please see Content Routing on page 110.



Origin server

An origin server refers to the backend server or servers where your web applications are hosted. these servers handle the processing and delivering of content such as HTML pages, images, or API responses to users. The origin servers are the final destination for requests once they have been inspected and processed by FortiAppSec Cloud.

Configuring server pools under **Origin Servers on page 103** helps FortiAppSec Cloud effectively direct traffic to the desired origin servers, based on the configured load balancing algorithm and persistence method.

Scrubbing Center

A scrubbing center is a security point that filters malicious traffic, protecting against cyberattacks.

Fortinet scrubbing centers operate across AWS, GCP, and Azure platforms to inspect and scrub traffic before it reaches origin servers. They integrate with cloud security tools like load balancers, DDoS protection, and WAFs to enhance application security.

Scrubbing centers filter incoming traffic for threats, applying policies like rate limiting, IP reputation checks, threat intelligence, and bot protection. After filtering out malicious traffic, clean traffic is forwarded directly or distributed via load balancing or Global Server Load Balancer (GSLB) to origin servers.

WAF setup

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

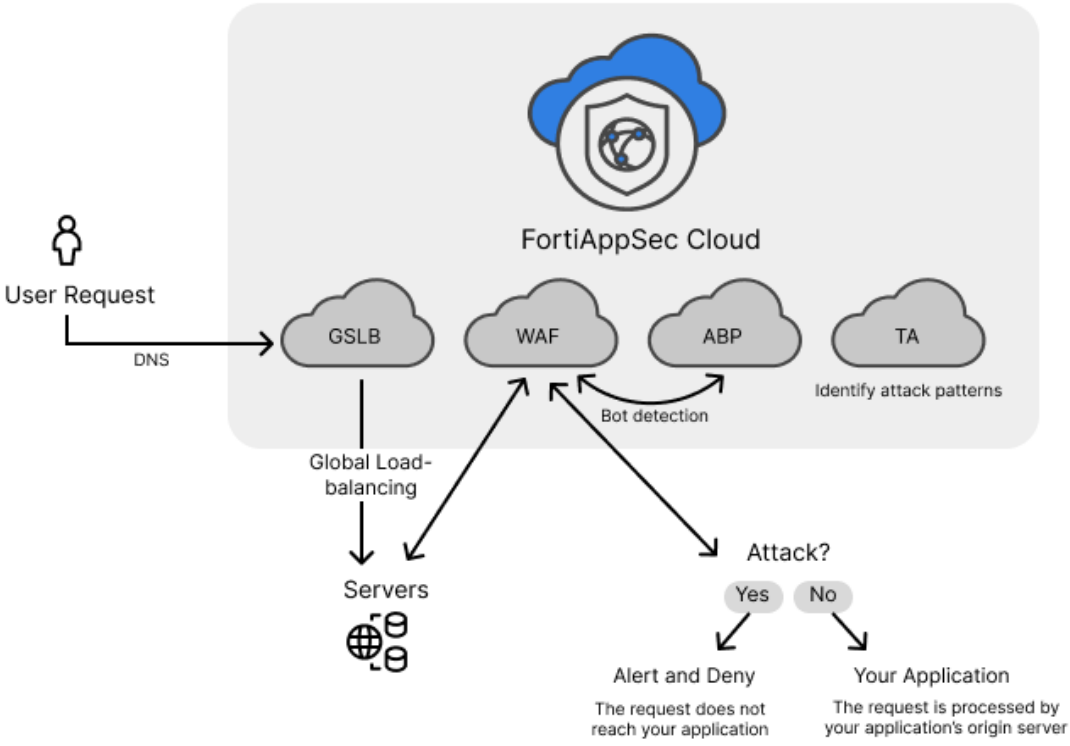
- Onboard WAF applications
- Change DNS record
- Changing IP addresses of origin servers

- Restricting direct traffic & allowing FortiAppSec Cloud IP addresses
- Restricting direct traffic & allowing FortiAppSec Cloud IP addresses
- How does WAF choose regions?
- CDN
- Understanding block mode and action

Onboard WAF applications

Onboarding an application to FortiAppSec Cloud's Web Application Firewall (WAF) activates protection features that defend against a variety of attacks. You can customize this protection by enabling or disabling specific WAF modules.

FortiAppSec Cloud intercepts and processes traffic to your application, where the WAF analyzes requests to detect and mitigate threats. Once onboarding is complete, the traffic flow should resemble the diagram below.

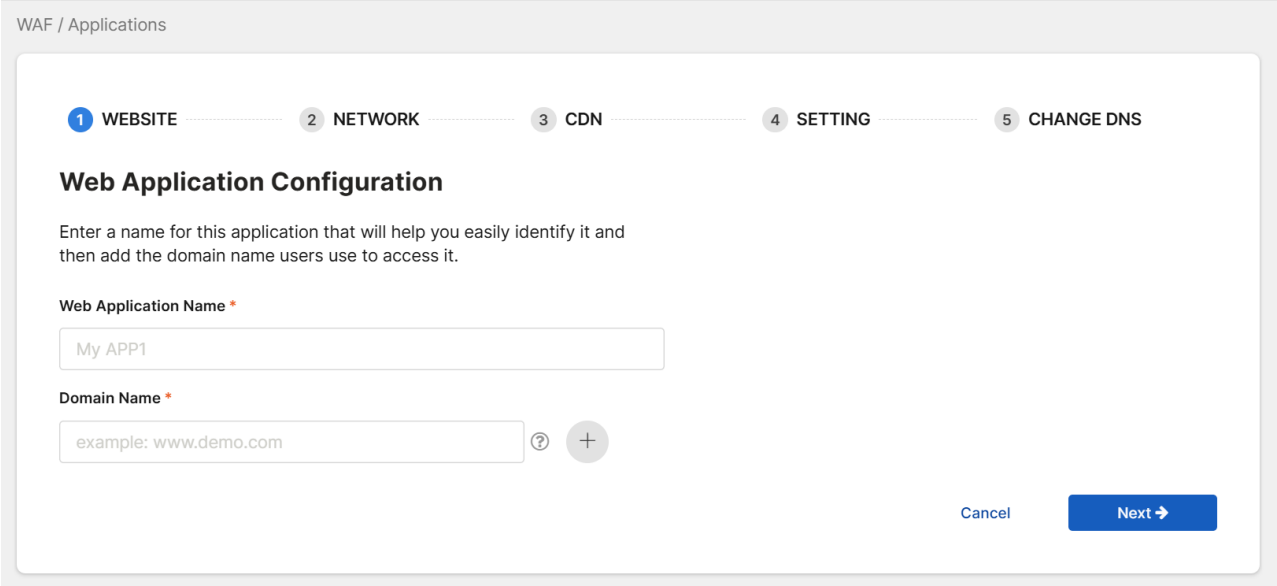


To onboard applications by DevOps tools, see DevOps tools on page 215.

Onboarding steps

1. Add the following IPs to the allowlist on your application server's firewall to enable FortiAppSec Cloud to access your application.
   - 3.123.68.65
   - 3.226.2.163
2. Go to appsec.fortinet.com and log in with your FortiCloud account credentials.
3. Navigate to **WAF > Applications**
4. Click **Add Application** near the top right corner of the page. The **Web Application Configuration** wizard will open.

5. **Web Application Configuration**

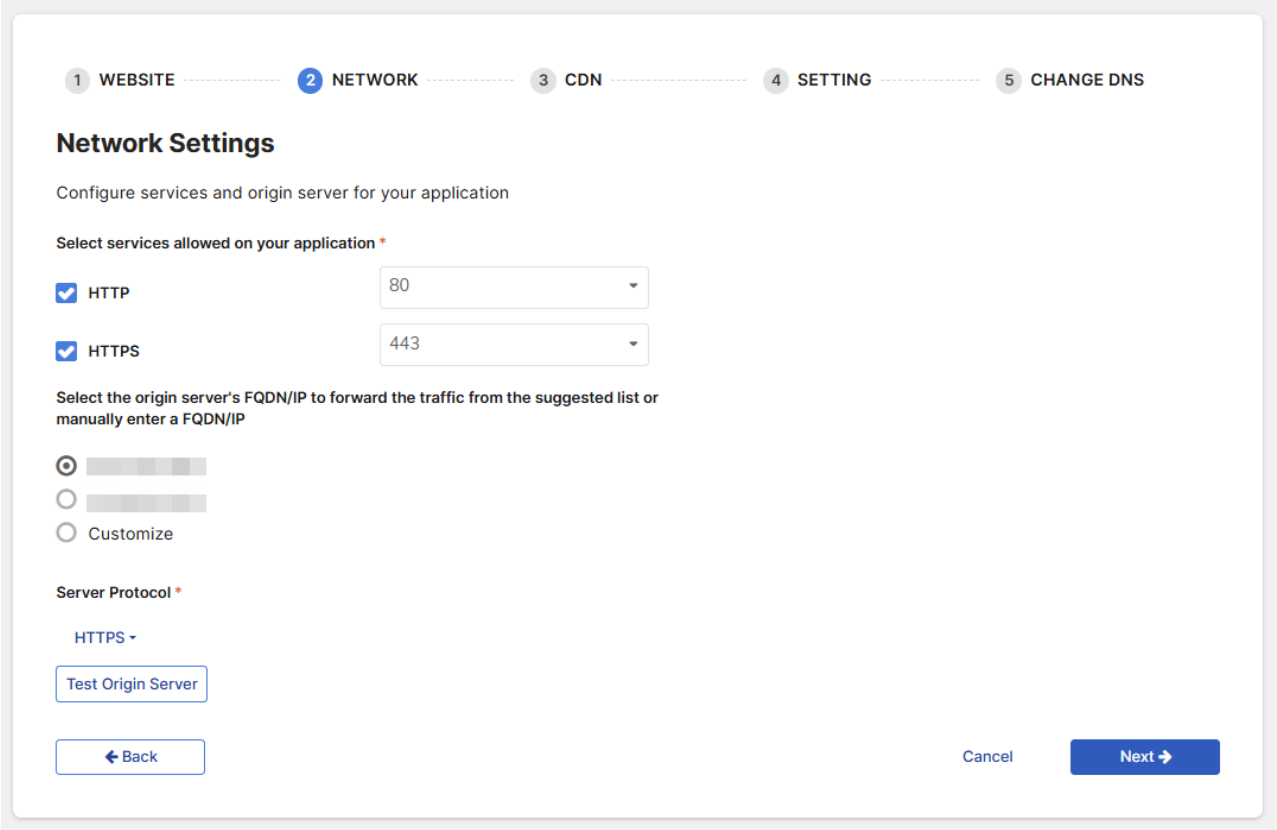


   a. **Web Application Name:** Enter a name for this application that will make it easy for you to identify within the FortiAppSec Cloud UI.
   b. Wildcard entries are allowed for all domains in the list except the first one. Ensure that domain name entries don't overlap; for instance, you can't add both "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.
      If you have multiple applications with different root domain names but sharing the same IP address, it requires special configurations. See Multiple domains sharing the same IP address on page 241.

6. **Network Settings**
   Configurations in this section ensure proper traffic routing and security protection.



a. Select the services allowed on your application and their corresponding ports. FortiAppSec Cloud listen for HTTP and/or HTTPS traffic on the selected ports to allow only legitimate traffic to pass through.
The default port number for HTTP is 80, and for HTTPS is 443. You can change it to a value between 1-65 535 (inclusive). Make sure the port numbers for HTTP and HTTPS are not duplicate.
If the port number you want to use is not in the drop-down list, please contact FortiAppSec Cloud Support or your sales representative to customize the port number. Please note that not all non-standard ports can be used. For details on port and traffic configurations, seeEndpoints on page 95.
If you would like to use additional ports on the same domain, please see Adding additional HTTP or HTTPS ports to your domain on page 72.

b. Select the IP address/FQDN for your web application. FortiAppSec Cloud will direct traffic to the specified IP address.
FortiAppSec Cloud automatically fetches and displays available IP addresses and/or FQDNs associated with your entered domain, using port 443 as the default. FortiAppSec 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**.

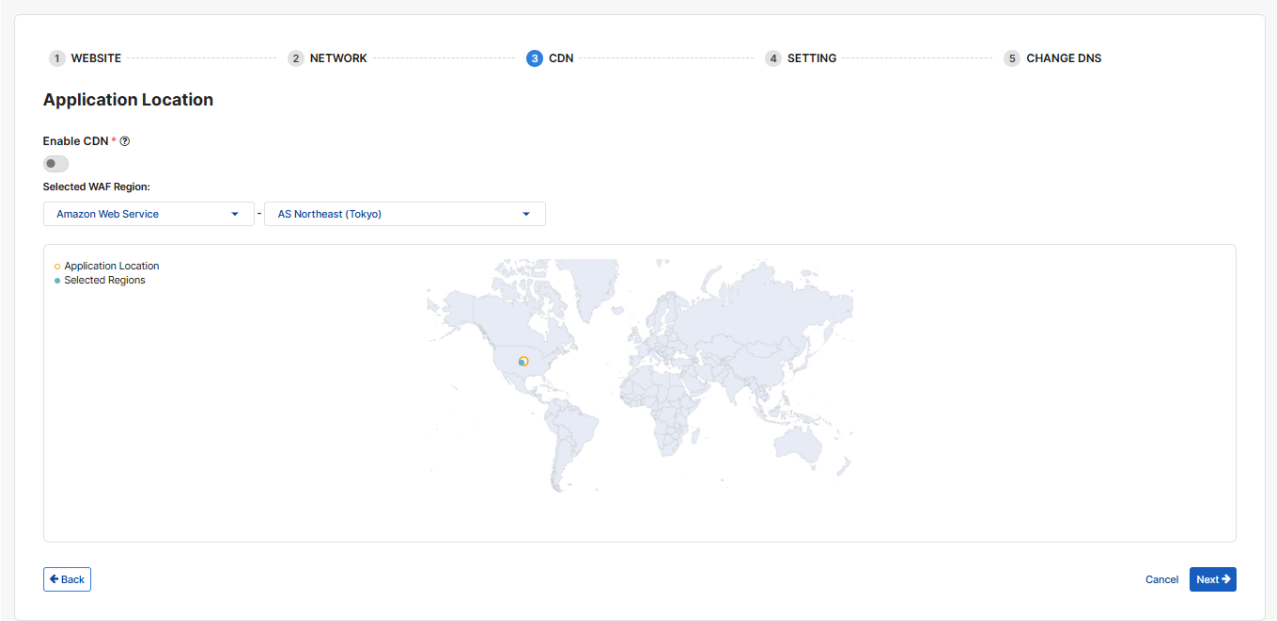
c. Under **Server Protocol**, you can configure the connection between FortiAppSec Cloud and the origin server. If you want to redirect HTTP traffic to HTTPS, ensure that you have selected HTTPS.

d. Ensure FortiAppSec Cloud service IPs from Step 1 are successfully added to your application's firewall before proceeding to the next step.

e. Click **Test Origin Server** to ensure that FortiAppSec Cloud can connect to the origin server. By default, FortiAppSec 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**.

7. **Application Location**

The settings in this section define how your application data is handled, including caching, cloud environment, and scrubbing center location for threat mitigation.



- **Content Delivery Network (CDN)**

  If you enable CDN, the data on your origin servers can be cached in FortiAppSec 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 79 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 **WAF > Applications** after this application is onboarded.

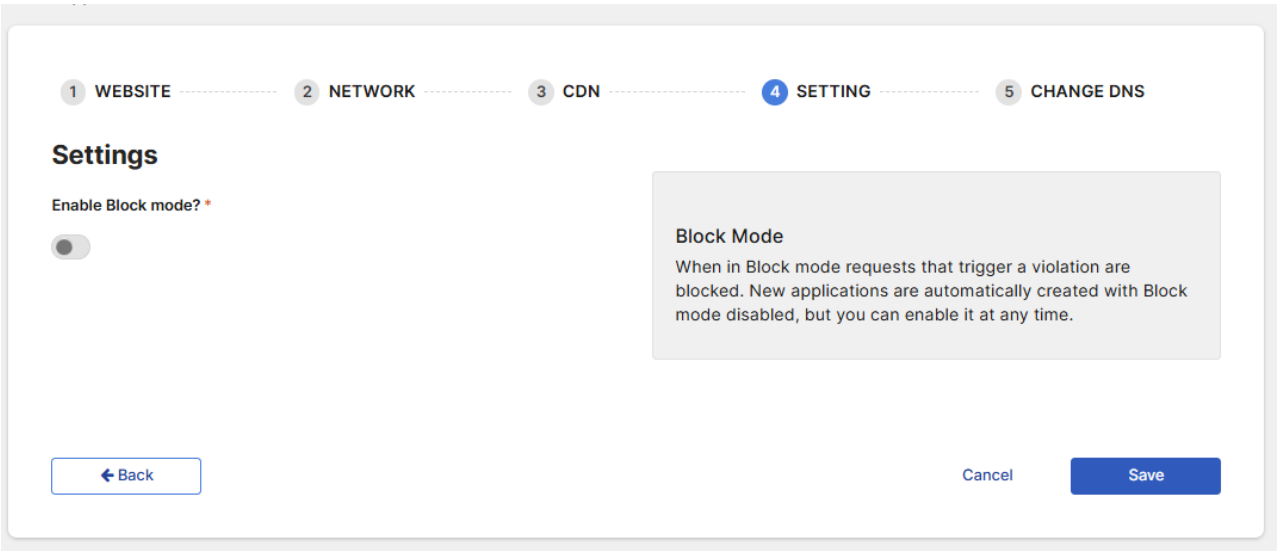
- **Cloud Platform and scrubbing center**

  To make this selection, you must enable **Preferred Platform** under **WAF > System Settings > Settings**.

  By default, **Preferred Platform** is disabled, and FortiAppSec Cloud automatically selects a scrubbing center based on your application server's cloud platform (AWS, Azure, or Google Cloud).

Cloud Platform	Specify the cloud platform for onboarding applications. Supported platforms include AWS, Azure, and GCP. After onboarding, you cannot change an application's cloud platform. To switch platforms, you must delete the existing application and create a new one with the desired platform.
Scrubbing Center	The scrubbing center region within the chosen cloud platform. To change the scrubbing center after onboarding, navigate to **WAF > Applications**.

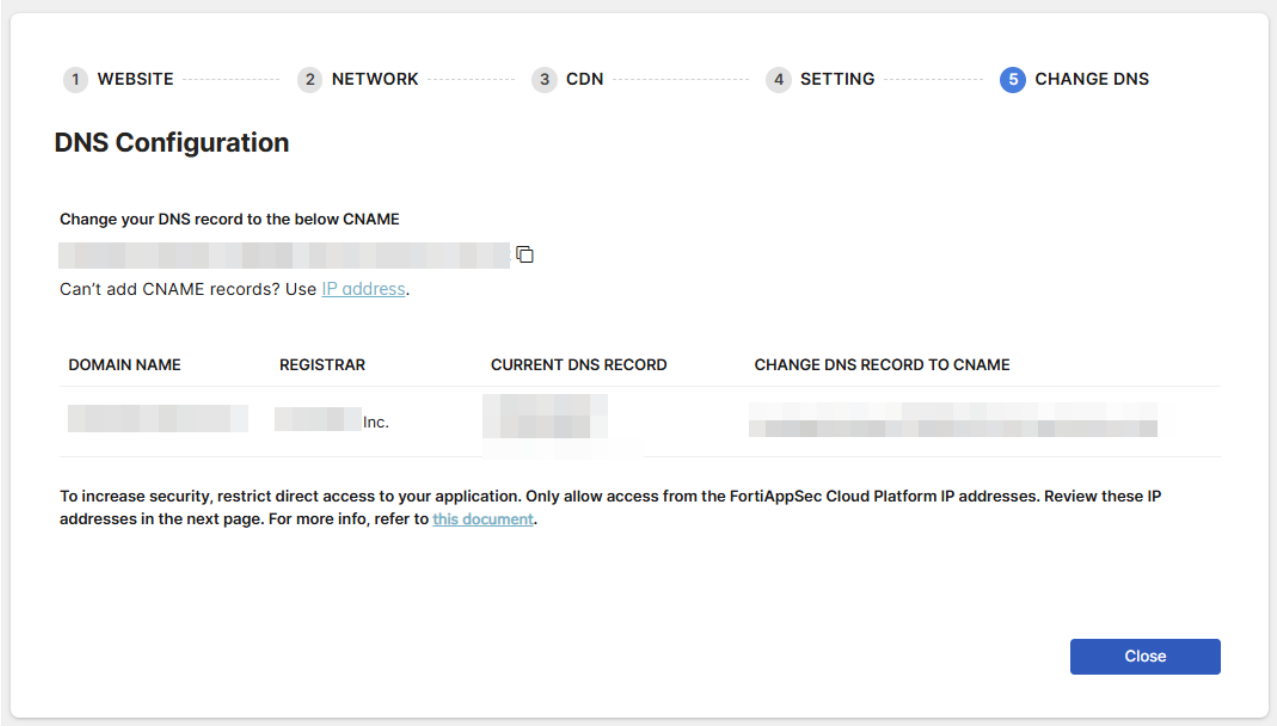
8. **Settings**



- When **Block mode** is enabled, FortiAppSec 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.
- Enable Templates if you would like to apply a predefined set of WAF configurations to your application. Assigning a template automatically configures the application with its settings, making it easy to standardize settings across multiple applications.
  You can use FortiAppSec Cloud's provided templates, or configure a custom template by going to **WAF > Templates**.

9. **DNS configuration**

   This section displays configuration instructions for settings managed outside FortiAppSec Cloud. Changing your DNS record according to the instructions below ensures that your application traffic is routed through FortiAppSec Cloud, where it is filtered for security before reaching your application servers.



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 FortiAppSec Cloud.

If there are multiple DNS records corresponding to the domain name, make sure to change all the records using the provided . 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 FortiAppSec Cloud for threat detection, refer to Using WAF behind a Content Distribution Service on page 233. Please note that FortiAppSec 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

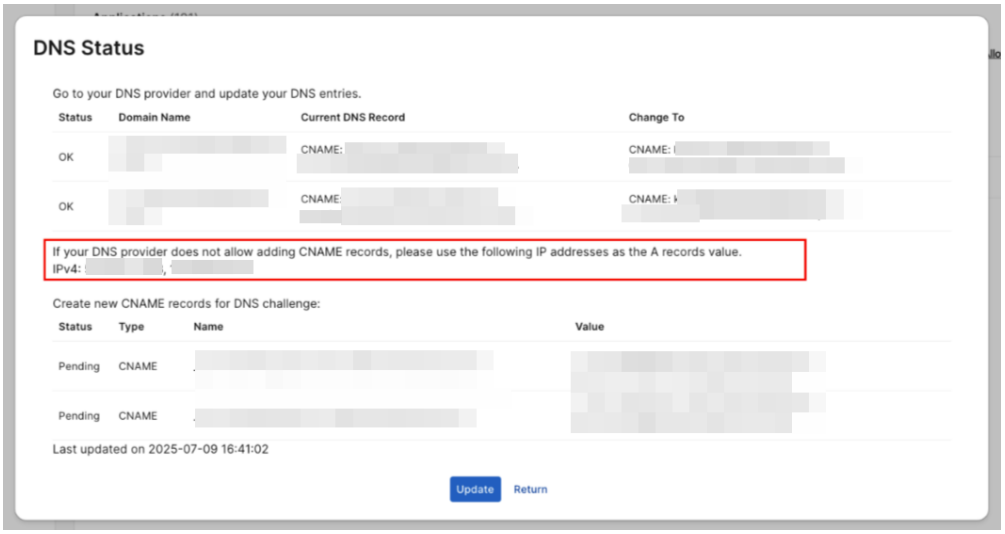
Note: You cannot directly access your website with the provided CNAME if you have not added the CNAME record in your DNS server. If you want to test it before changing the DNS record, follow steps below.

1. Run `ping` or `nslookup` command to get the IP address of CNAME.
2. Modify the hosts file on your Windows or Linux by adding your application's domain name (for example, `www.<domain_name>.com`) and mapping it to the IP address obtained from Step a.
3. Access the domain name with the browser to test it.

If your DNS provider does not support CNAME records, go to **WAF > Applications**, find your application, and click the **Pending** status under the DNS Status column.



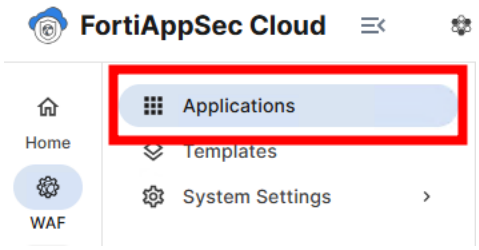
A popup will appear with the IP addresses you can use as A record values.



If other configuration options are available, using A records is not recommended due to the following risks:

- No automatic failover: Traffic will not be rerouted if a scrubbing cluster is under maintenance or fails.
- No auto-scaling support: When new nodes are added, A record configurations will not automatically update, which may result in service disruption.

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



11. The application security modules will appear in the navigation pane. FortiAppSec 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 Add and Remove Modules on page 128.

12. To ensure your application only receives traffic vetted by FortiAppSec Cloud, you must restrict traffic to only FortiAppSec Cloud IPs. Additionally, to prevent FortiAppSec Cloud from being flagged as a DDoS attack source, ensure you allow FortiAppSec Cloud IPs in your firewall. For instructions on doing this, please refer to Restricting direct traffic & allowing FortiAppSec Cloud IP addresses on page 76.

Adding additional HTTP or HTTPS ports to your domain

You can host multiple applications on the same domain and origin server, each distinguished by a different port. For example:

- app1 – www.example.com:443/app1
- app2 – www.example.com:8443/app2

To manage traffic across multiple HTTP or HTTPS ports, create multi-port applications by repeating the Onboarding steps on page 65, using the same domain but specifying different ports each time.

The following directions highlight the necessary configurations to consider when establishing multi-port applications.

1. Follow Onboarding steps on page 65 to create the first application for your domain, ensuring to enter your root domain as the first domain in the **Web Application Configuration** step. An example of a root domain is fortinet.com, whereas shop.fortinet.com would be considered a subdomain.

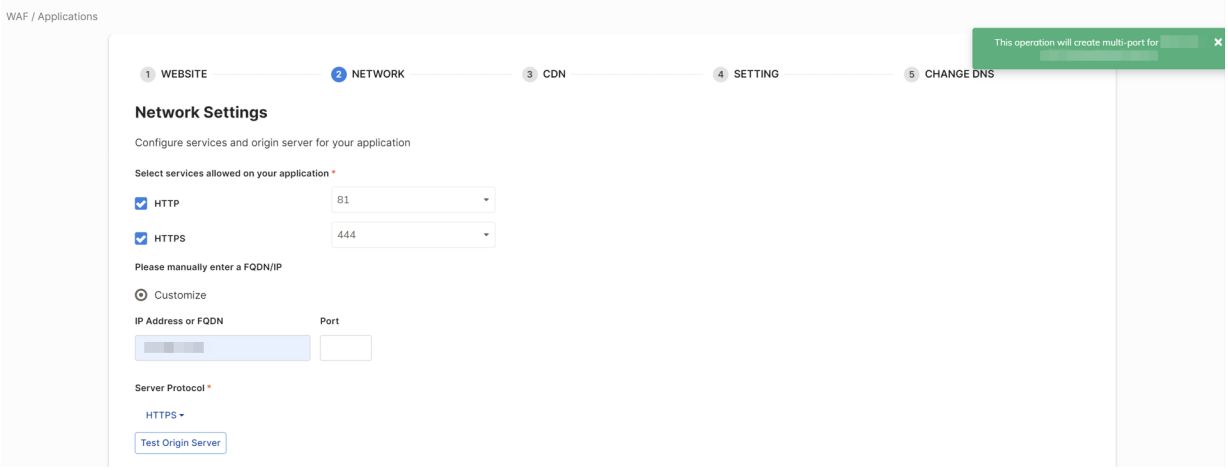


Before creating your first multi-port application, please note the following:

- If you need to onboard multiple ports using the same protocol (e.g., HTTPS port 443 and HTTPS port 8443) for the same domain, you must onboard each port as a separate application.
- You cannot change the region/CDN while multi-port is enabled. If you need to make edits to region/CDN on your application, we recommend doing this before adding any multi-port applications.
  - To switch regions or CDNs, delete all multi-port applications of a domain, leaving only the original application. After changing the region, you will need to manually recreate the multi-port applications to resume traffic from other ports.
- If you need to use a custom certificate on an application, please re-input the certificate for each multi-port.
- When managing sub-domains with different port requirements, it is best to create them as separate applications. This approach ensures each sub-domain can independently manage its specific port settings without overlapping configurations.

2. Return to **WAF > Applications** to add your first multi-port application.
3. Click **Add Application**.
4. In the **Web Application Configuration** step, ensure the root domain you used to create the first application for this domain is listed as the first entry under **Domain Name**. For more details on the configuration options on this page, see above.
5. Under **Network Settings**, select the HTTP and/or HTTPS ports you would like to add to your application.
   a. Since we are configuring a multi-port application, be sure to select **Customize** and manually enter the origin server.
   b. On the same page, click **Test Origin Server**. If FortiAppSec Cloud detects multiple applications with the same domain, you will encounter a message in the top-right corner of your window that indicates you are creating a

multi-port application.

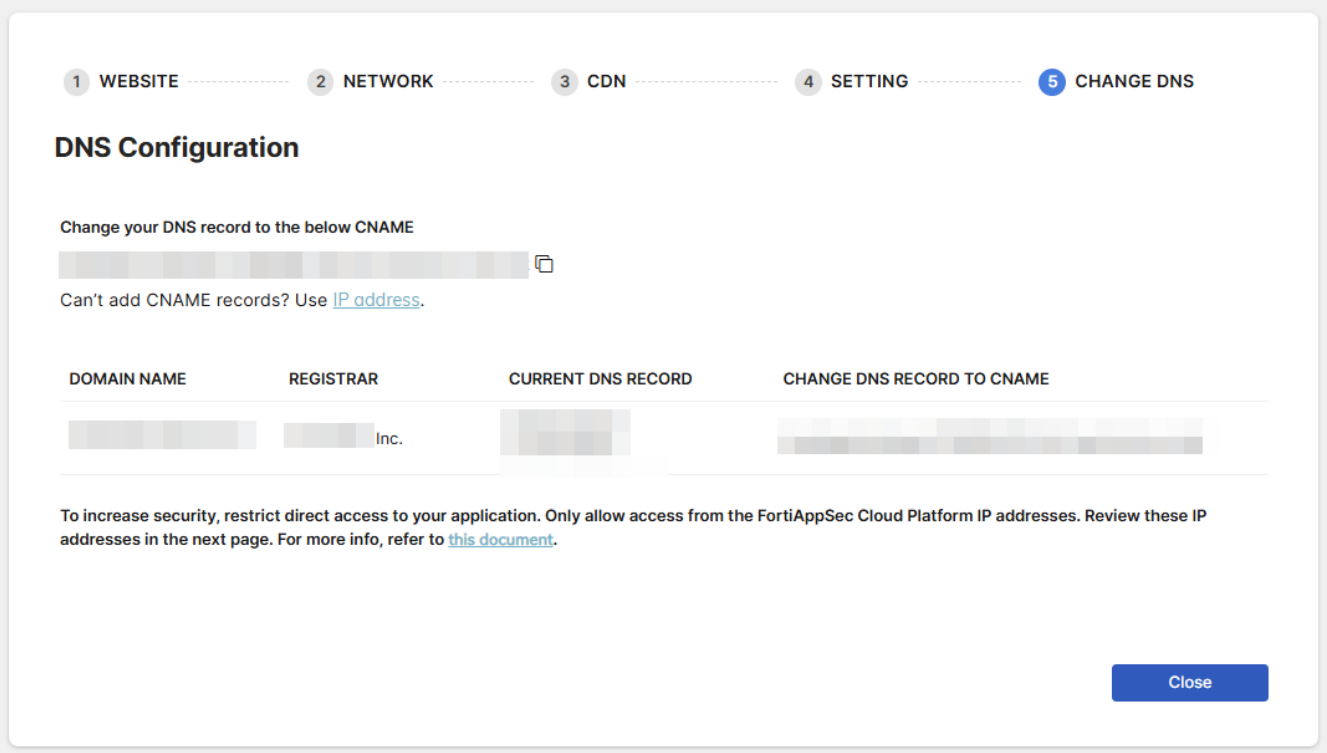


6. On the **CDN** step, you will be unable to change the settings on this page due to multiport being enabled. Click **Next** to move onto the next step.
   - To switch regions or CDNs, delete all multi-port applications of a domain, leaving only the original application. After changing the region, you will need to manually recreate the multi-port applications to resume traffic from other ports.
7. On the **Setting** step, configure **Block mode** and **Template** for your multiport application. For details on these configuration options, see above.
8. The **Change DNS** step provides the same instructions as when you first created your application's initial instance. If you have already completed these steps, you can simply click **Close** to exit the wizard, as there is no need to repeat them.

Change DNS record

FortiAppSec Cloud WAF protects your application by inspecting incoming traffic and blocking malicious requests before they reach the origin servers.

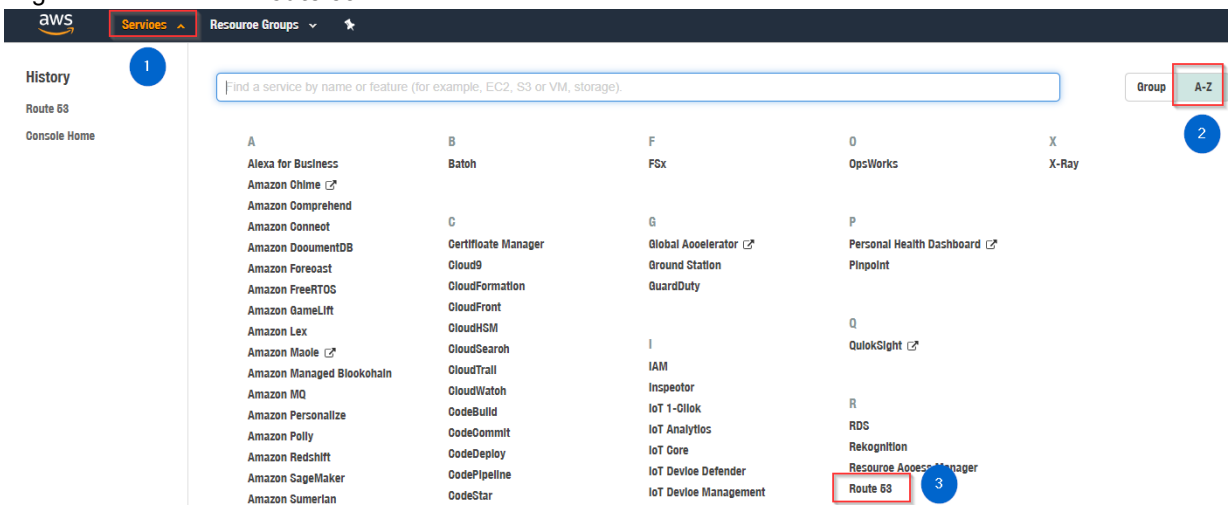
After onboarding a new WAF application, please change your DNS record to the CNAME displayed on the last page of the onboarding wizard.



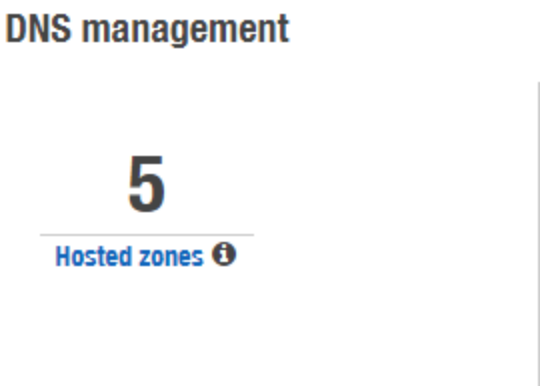
Configuration Example

The following example demonstrates how to perform this update using AWS Route 53. The exact process may vary depending on your DNS platform, but the fundamental principles remain the same. For more information or detailed configuration steps, consult your DNS provider's documentation.

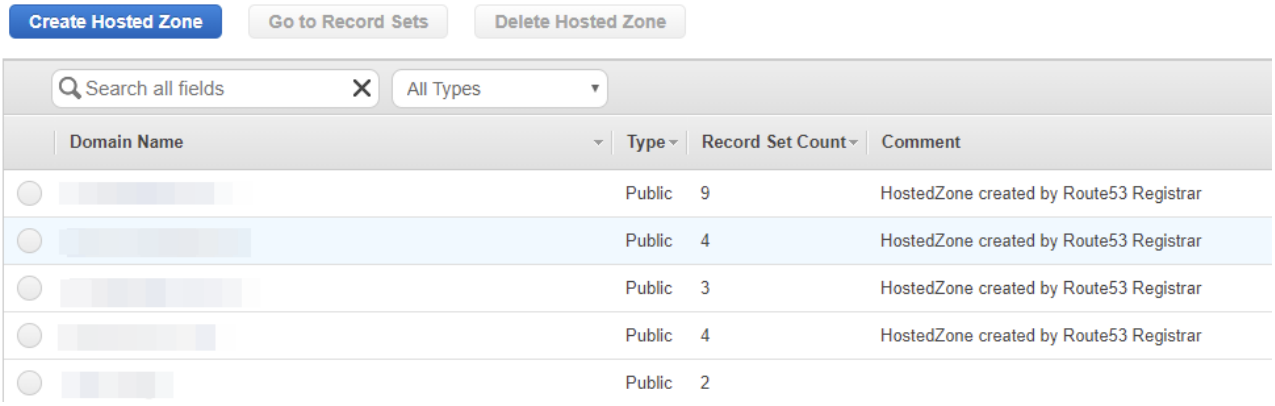
1. Navigate to the page for editing DNS settings.
   a. Log in to AWS. Select **Route 53**.



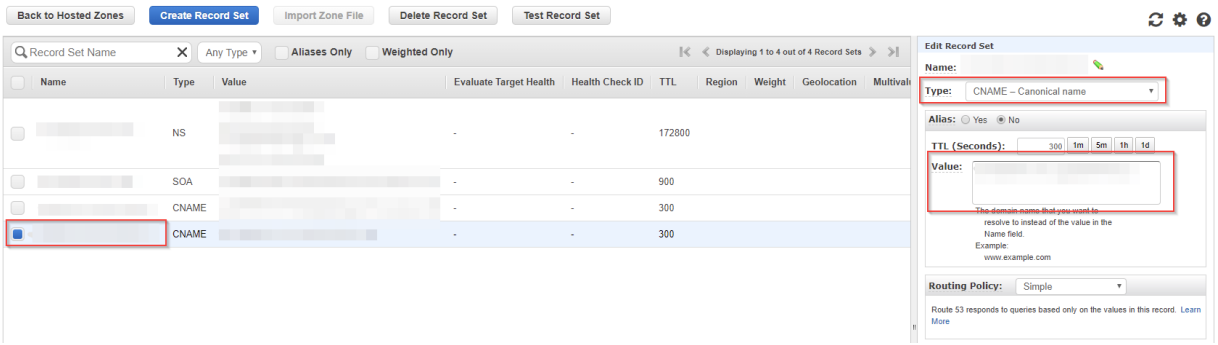
b. Click **Hosted zones** under **DNS management**.



2. Select the domain name of your application.



3. Update the DNS record for your domain to point to FortiAppSec Cloud's CNAME, replacing any existing IP addresses, so that traffic is routed through FortiAppSec Cloud.
   a. Check the box before the domain name starting with "www.". The **Edit Record Set** pane will appear at the right side.
   b. Select **CNAME - Canonical name** for the **Type**.
   c. Delete the IP address(es) in the **Value** field, then paste the CNAME provided by FortiAppSec Cloud.



Changing IP addresses of origin servers

After the DNS records are changed, when users visit your application, the traffic is directed to FortiAppSec 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 FortiAppSec Cloud service. This could allow an attacker to bypass FortiAppSec 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 > Origin Servers** so that FortiAppSec Cloud can correctly forward traffic to the new address.

Restricting direct traffic & allowing FortiAppSec Cloud IP addresses

Restricting direct traffic

Once you complete setting up FortiAppSec Cloud, configure your application servers to only accept traffic from FortiAppSec 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 WAF choose regions? on page 78

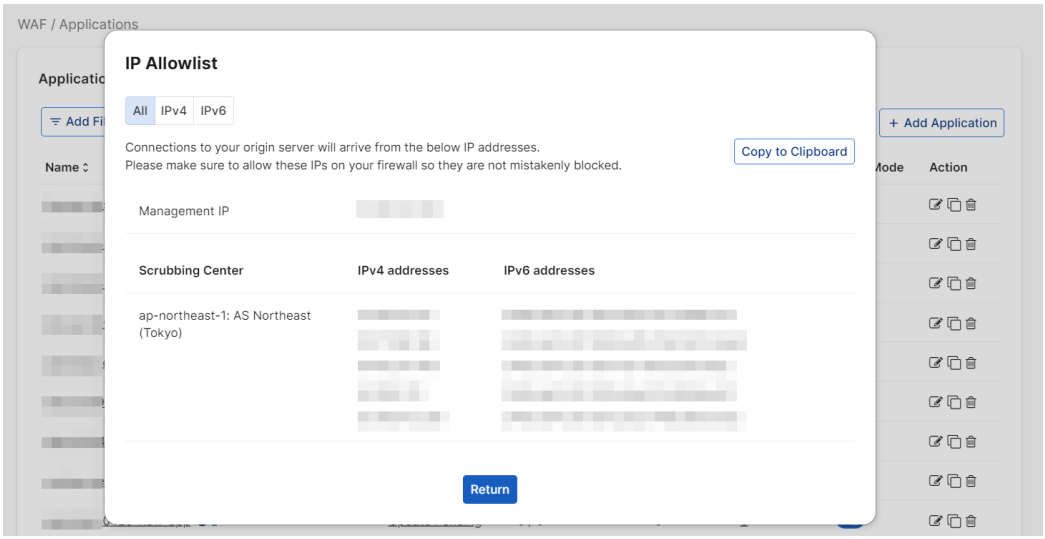
Allowing FortiAppSec Cloud IP addresses

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

To avoid this, we highly recommend you to **add FortiAppSec Cloud IP addresses to the allowlist of your DDoS device or system before onboarding applications.**

View the IP addresses of your region in **WAF > 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**.



We have provided two web pages listing all of the IPv4 and IPv6 addresses of the FortiAppSec Cloud scrubbing centers: https://appsec.fortinet.com/ips-v4 and https://appsec.fortinet.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.

FortiAppSec Cloud regions on AWS

- ap-east-1: Asia Pacific (Hong Kong)
- ap-southeast-1: Asia Pacific (Singapore)
- ap-southeast-2: Asia Pacific (Sydney)
- ap-southeast-3 Jakarta
- ap-south-1 : Asia Pacific (Mumbai)
- ca-central-1: Canada (Central)
- eu-central-1: Europe (Frankfurt)
- eu-west-1: Europe (Ireland)
- eu-west-2: Europe (London)
- eu-west-3: Europe (Paris)
- eu-south-1: Europe (Milan)
- Il-central-1: Israel (Tel Aviv)
- me-central-1: Middle East (UAE)
- sa-east-1 (São Paulo)

- us-east-1: US East (N. Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)

FortiAppSec Cloud regions on Azure

- West Europe
- West US2
- Central US
- East US
- East US2
- Australia East
- Brazil South (São Paulo State)
- Canada Central
- South Africa North (Johannesburg)
- Qatar Central

FortiAppSec Cloud regions on Google Cloud

- europe-west3 (Frankfurt)
- europe-west8 (Milan)
- me-central2 (Dammam)
- me-west1 (Tel Aviv)
- us-east1 (South Carolina)
- us-west1 (Oregon)

How does WAF choose regions?

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

- First, we determine if your application server is deployed on AWS, Azure, 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
For application servers located in Europe	EU (Frankfurt)	West Europe (Netherlands)	Europe-west3 (Frankfurt)

For application servers located in the rest of the world	US East (N. Virginia)	East US (Virginia)	Us-east1 (South Carolina)

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 FortiAppSec Cloud scrubbing centers are deployed.

CDN

If CDN is enabled, the data on your origin servers will be cached in FortiAppSec 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 FortiAppSec Cloud IP addresses on page 76.

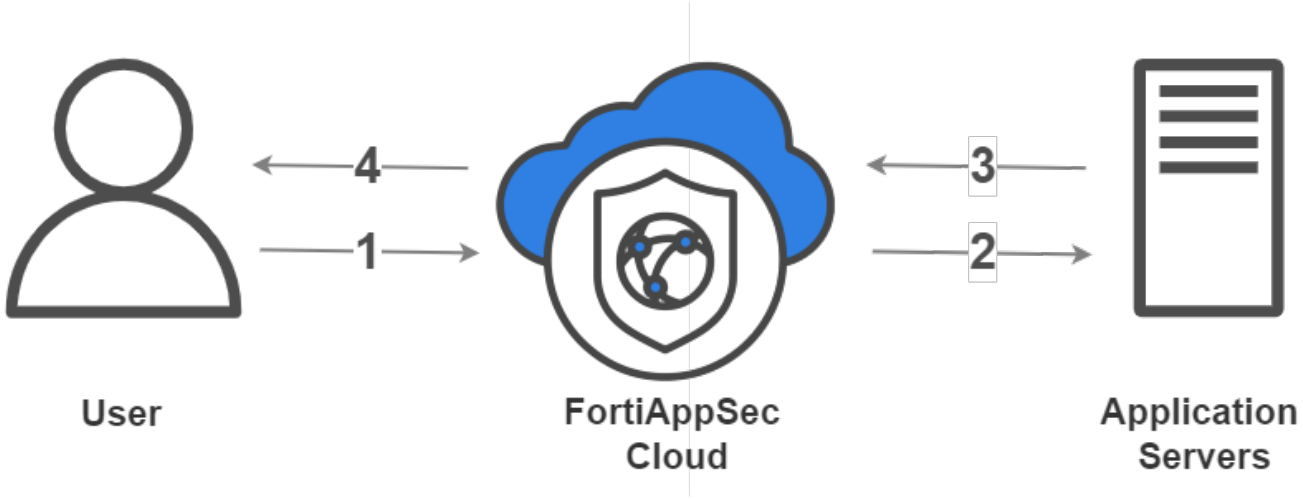
You can enable CDN when onboarding an application, or set this option in the **Application Settings** dialog (**WAF > Applications**).

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 FortiAppSec Cloud scrubbing center for threat detection.
2. FortiAppSec Cloud sends request to your application server to get the data requested by the user.
3. The application server sends response to FortiAppSec Cloud.
4. FortiAppSec 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 FortiAppSec Cloud to your application users. FortiAppSec 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 FortiAppSec 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 FortiAppSec 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 FortiAppSec 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, 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, FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud, FortiAppSec Cloud directly sends response to the user. As there isn't any traffic flow from your application server to FortiAppSec Cloud, no expense will incur. By caching data on FortiAppSec Cloud, it saves the cost to fetch data from your application sever every time when users request it.

Data Storage Management

FortiAppSec Cloud provides flexible, compliant data storage management for both cloud applications and on-premises devices, ensuring that your data is securely stored, easily accessible, and fully compliant with regulatory requirements.

It is important to research and understand the privacy regulations in the regions where you operate, as these laws can vary. For example, web applications in the EU must comply with the General Data Protection Regulation (GDPR), which ensures that personal data is stored in compliance with the law, enabling organizations to protect the privacy of EU citizens, ensure explicit consent, and respond quickly to data breaches.

The approach to managing data storage for FortiAppSec Cloud differs depending on whether the user is using a cloud application or an on-premises device.

Cloud application

WAF offers data storage in two regions:

- EU (AWS Frankfurt Region)
- US (AWS N. Virginia Region)

When you create your cloud application, the system automatically detects the IP of the Origin Server. If the IP is from Europe, the EU region is used, and all data is stored in the EU. For IPs from other regions, the data is stored in the US (AWS N. Virginia Region).

This setup ensures that data is stored in the appropriate region based on the geographic location of the origin server's IP address.

On-premises devices

For on-premises devices, attack and incident logs are typically stored locally. However, you have the flexibility to change the data storage location through the **Threat Analytics** interface and switch data storage region between the United States and the European Union. This feature allows on-premises users to select a storage location that meets their specific data governance and compliance needs.

To change the data storage location of your on-premise device,

1. Log into your FortiAppSec Cloud web service.
2. In the side navigation menu, go to **Threat Analytics > Gateways**.
3. Locate the desired device by serial number, and click on the edit icon  in the **Action** column.
4. In the drop down menu, select the desired data storage location.
5. Click **OK** to save your settings.

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, FortiAppSec Cloud will take actions as specified in Action of each WAF module. Requests that trigger security violations are blocked, preventing them from reaching your application server.
- When Block Mode is disabled, FortiAppSec Cloud only monitors violations and generates logs for them. FortiAppSec Cloud does not block the malicious requests.

Before you enable Block Mode, please check the following prerequisites:

- The endpoints and origin servers are configured properly. The traffic flow between the clients, FortiAppSec Cloud, and your application servers is stable.
- Observe the attack logs in **FortiView** or **Attack logs on page 412**. 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 Block Mode is disabled, FortiAppSec 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, FortiAppSec Cloud will block the request (or reset the connection) and generate a log message.

WAF Workflow and Dashboard Overview

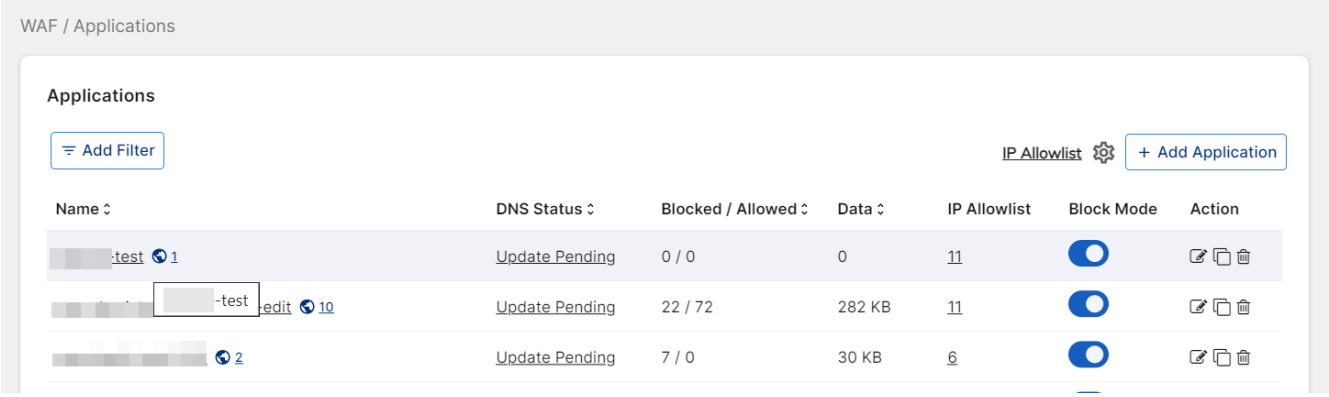
This section provides an introduction to the primary web portal pages for configuring settings and monitoring application activity in FortiAppSec Cloud's WAF service.

Application Page

Many WAF configurations specific to each application, making the **Application** page your central hub for configuring and monitoring individual applications.

On the **Application** page, you can perform actions like creating an application, adjusting the IP allowlist, and editing the name, CDN, and region for each application. For detailed instructions on these tasks, refer to WAF Applications on page 86.

To access WAF's security features, select one of your applications. This brings you to the selected application's WAF security dashboard, and updates the WAF side navigation menu to display the selected application's dashboard, FortiView, network settings, and enabled modules.

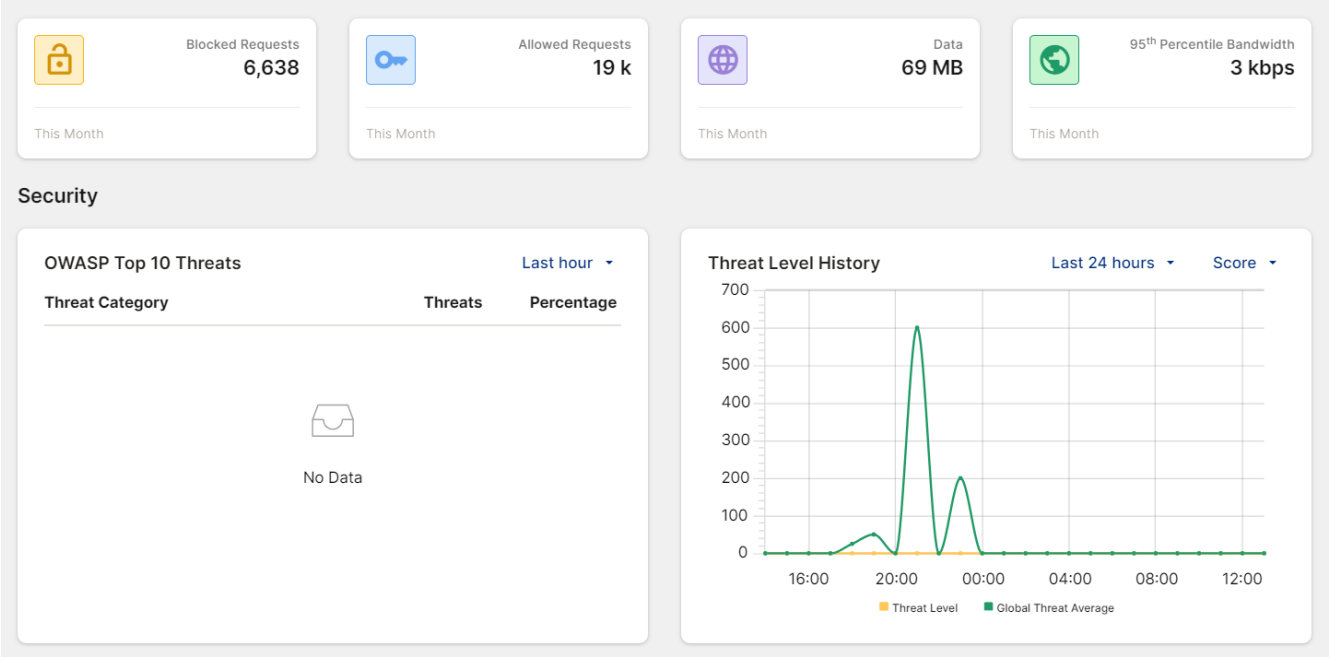


Individual Application pages

The pages in this section are accessed by clicking into an application as described above.

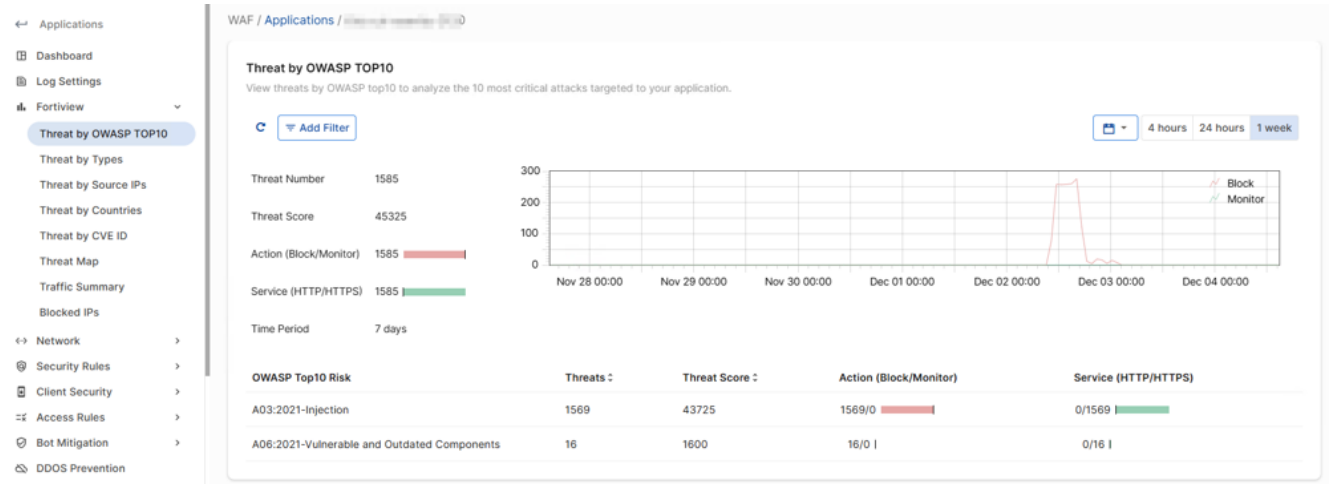
Dashboard

This dashboard displays general security insights from the WAF service. For details on the widgets on this page, please refer to WAF Application Dashboard on page 90.



FortiView

FortiAppSec Cloud WAF detects attacks to your application and displays the threats in **FortiView**. Navigate to any page within this section to explore detailed information on the available threat categories.

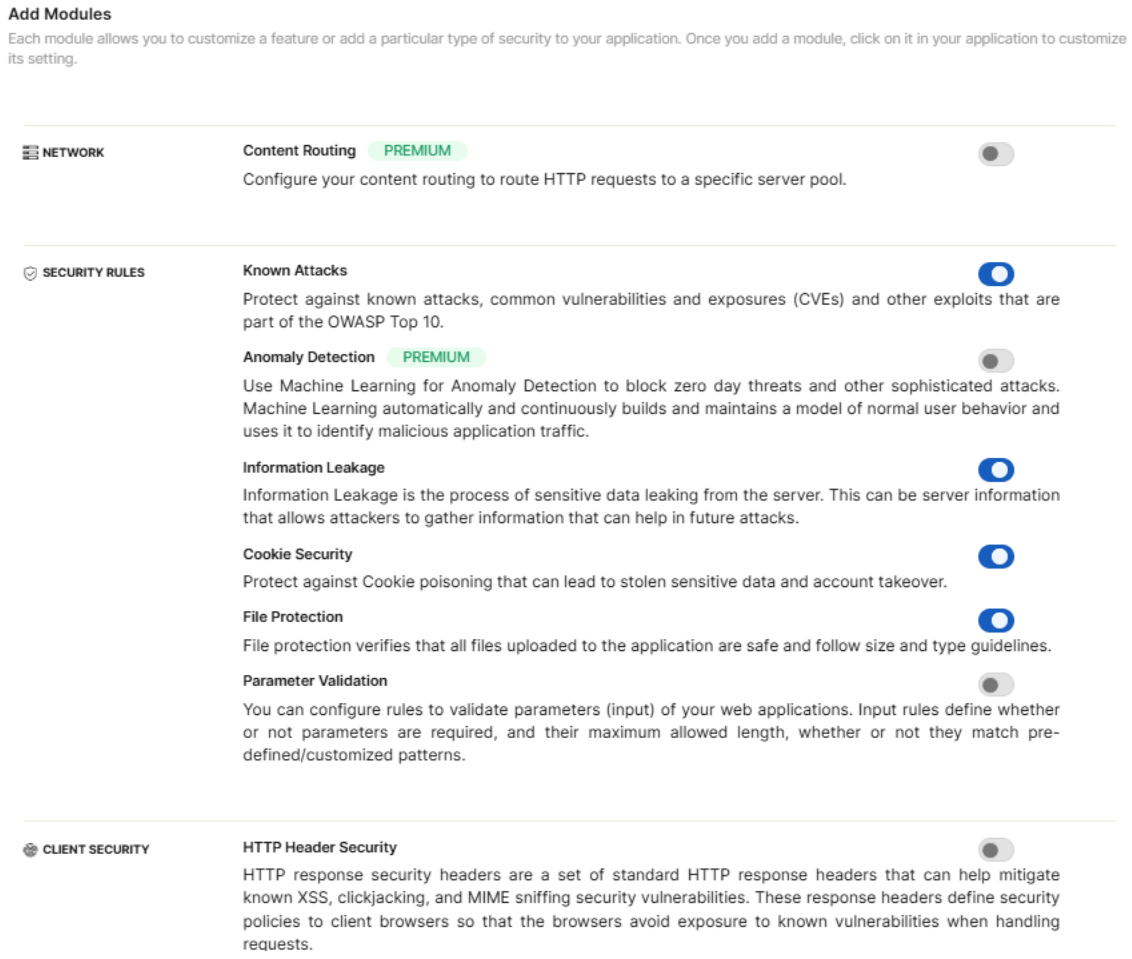


Network

After you complete onboarding applications, you can navigate to the pages under **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.

Modules

Navigate to **Add Module** to enable additional WAF features. Please note that feature availability may vary based on your FortiAppSec Cloud license.

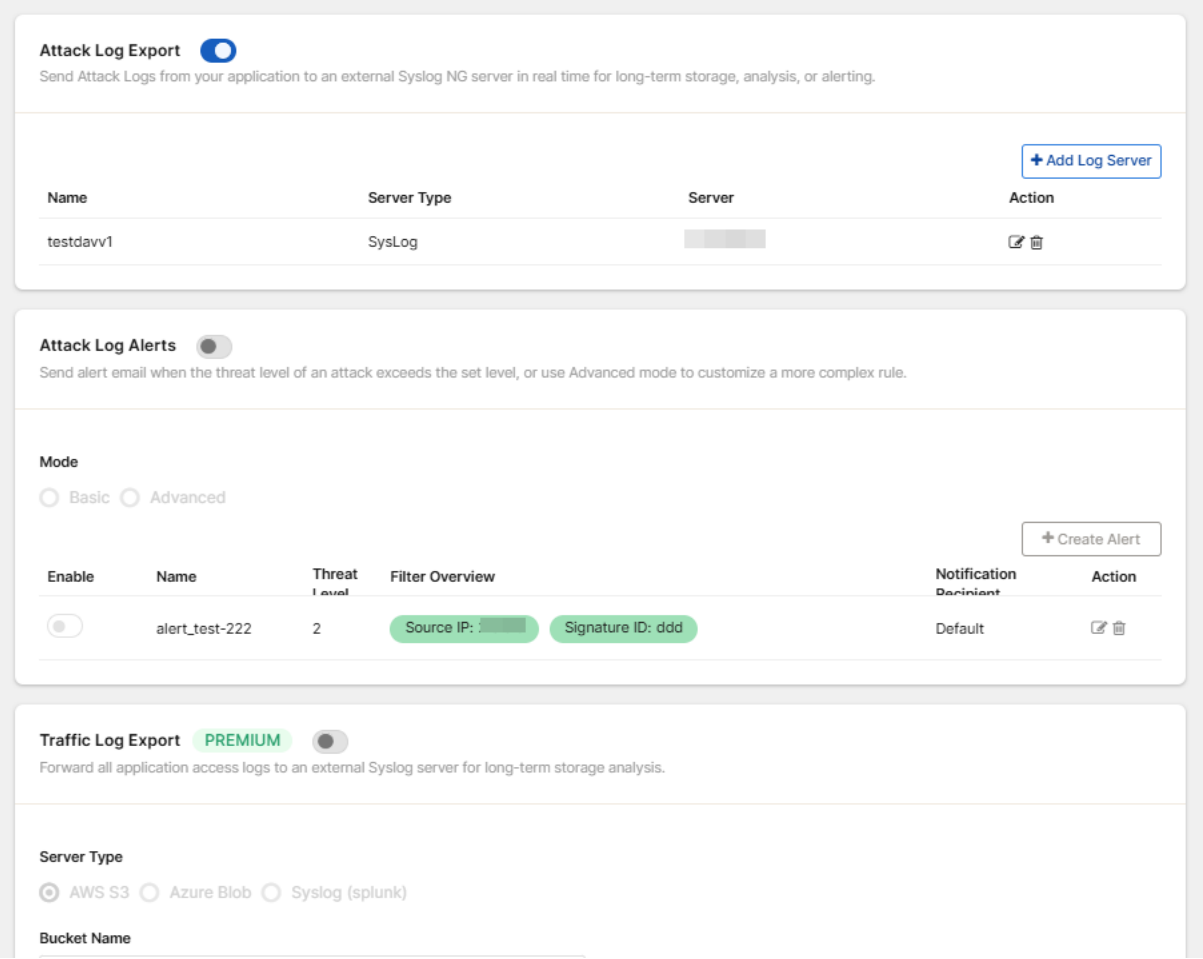


Vulnerability Scan

The Vulnerability Scan module identifies OWASP Top 10 vulnerabilities in web applications and provides a detailed report with remediation recommendations to enhance security.

Log Settings

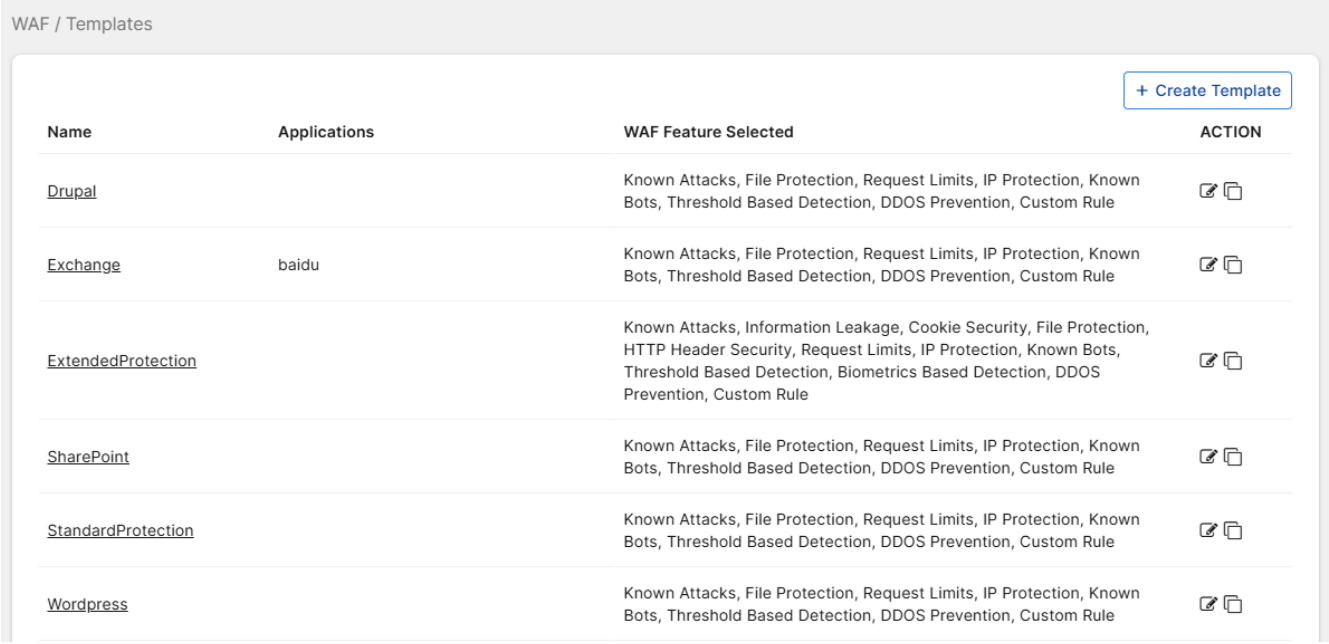
Adjust the export, alert, and sensitive data masking settings for your WAF logs.



Templates

A template is a collection of pre-defined WAF configurations. Assigning a template to an application automatically applies its WAF configurations to that application.

Templates are ideal if you're unsure which WAF configurations to use, providing a quick and effective way to set up protection. For details, please see Templates on page 202.



System Settings

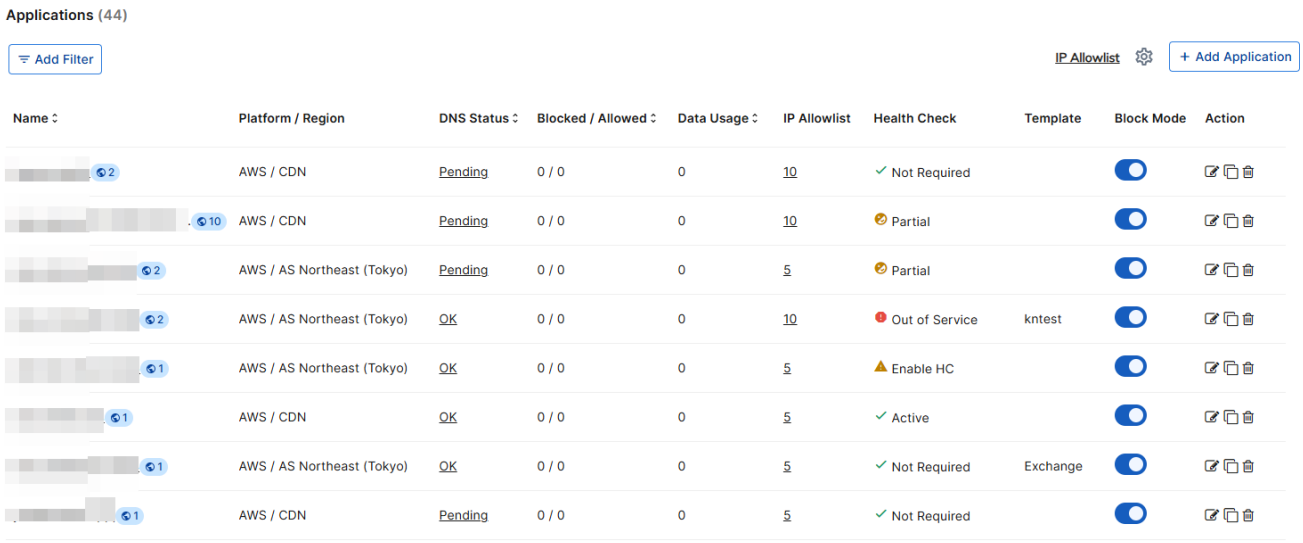
Configure settings that apply to all WAF applications.

WAF Applications

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

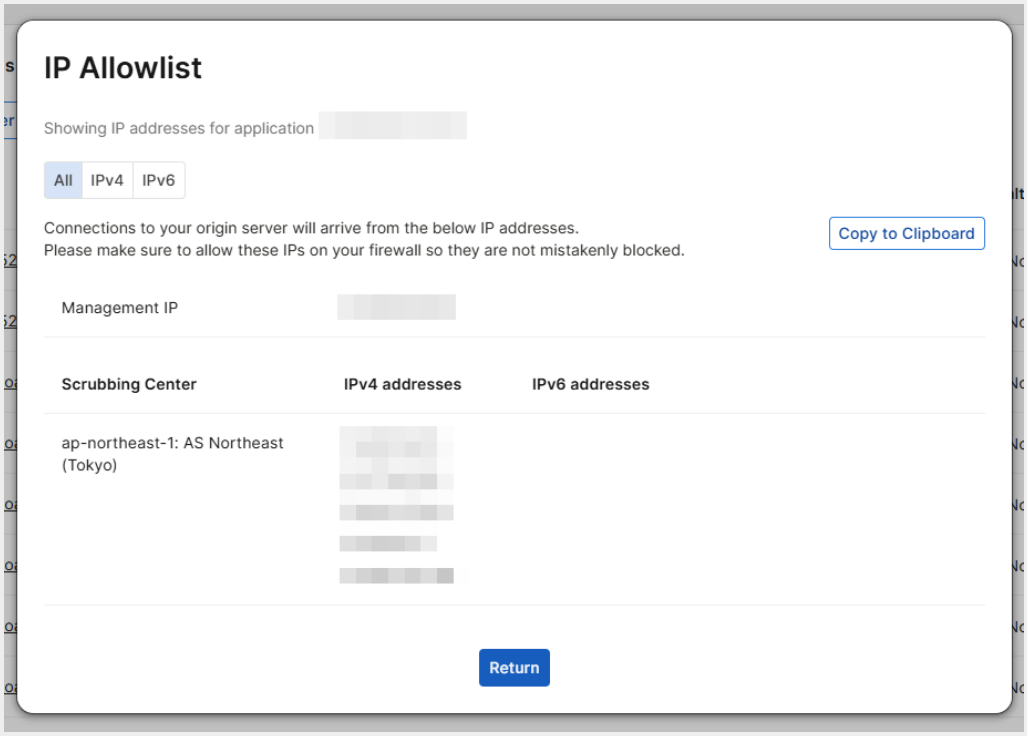
- Viewing application information
- Onboarding applications
- Cloning the application configurations
- Enabling/disabling CDN
- Changing FortiAppSec Cloud scrubbing center

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 FortiAppSec Cloud scrubbing center assigned to your application is located. You can click the edit icon to change the region.
Region	The FortiAppSec Cloud scrubbing center assigned to your application.
DNS Status	It shows **OK** if you have changed the DNS record to use the CNAME IP address provided by FortiAppSec Cloud. Refer to Change DNS record on page 73.
Blocked / Allowed	The ratio of blocked to allowed requests. **Blocked Requests:** number of requests blocked by FortiAppSec Cloud **Allowed Requests:** The number of requests that reached your application. To view the details, click the application name, then go to **Logs > Attack Logs**.
Data Usage	The volume of data processed by FortiAppSec Cloud, including the data accumulated by the blocked requests.
IP Allowlist	Displays the number of IPs used for connections to your origin server. Click to view the full list and add them to your firewall allowlist.



Health Check

Displays the status of the servers on your application.

- **Enable HC:** This application has origin servers with multiple pool members but no health check configured. We recommend enabling health checks for these origin servers.

  To enable Health Check:

  a. Click the name of the relevant application.

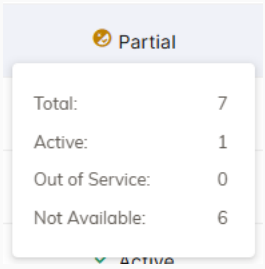
  b. Navigate to **Network > Origin Servers**.

  c. Find the server pool with the disabled **Health Check**, then click the **Edit** icon under **Actions**.

  d. In the row of the **Server Balance** settings, click the **Edit** icon under **Actions**.

  e. Scroll down to the Health Check option and select the radio button to enable it.

  For details on the other configuration options on this page, please refer to Origin Servers on page 103.
- **Active:** All servers on this application are healthy and operational.
- **Partial:** The servers on this application have different statuses. Hover over this status to view a detailed breakdown.



- **Out of service:** None of the servers in this application are operational.
- **Not Required:** This application does not require enabling health check.

Template	The configuration template applied to the application, if any. For more information, refer to Templates on page 202.
Block Mode	Enable or disable the block mode. Refer to Understanding block mode and action on page 81

Onboarding applications

See Onboard WAF applications on page 65 for instructions on 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.



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

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

Enabling/disabling CDN

Enable or disable CDN. For more information, refer to CDN on page 79

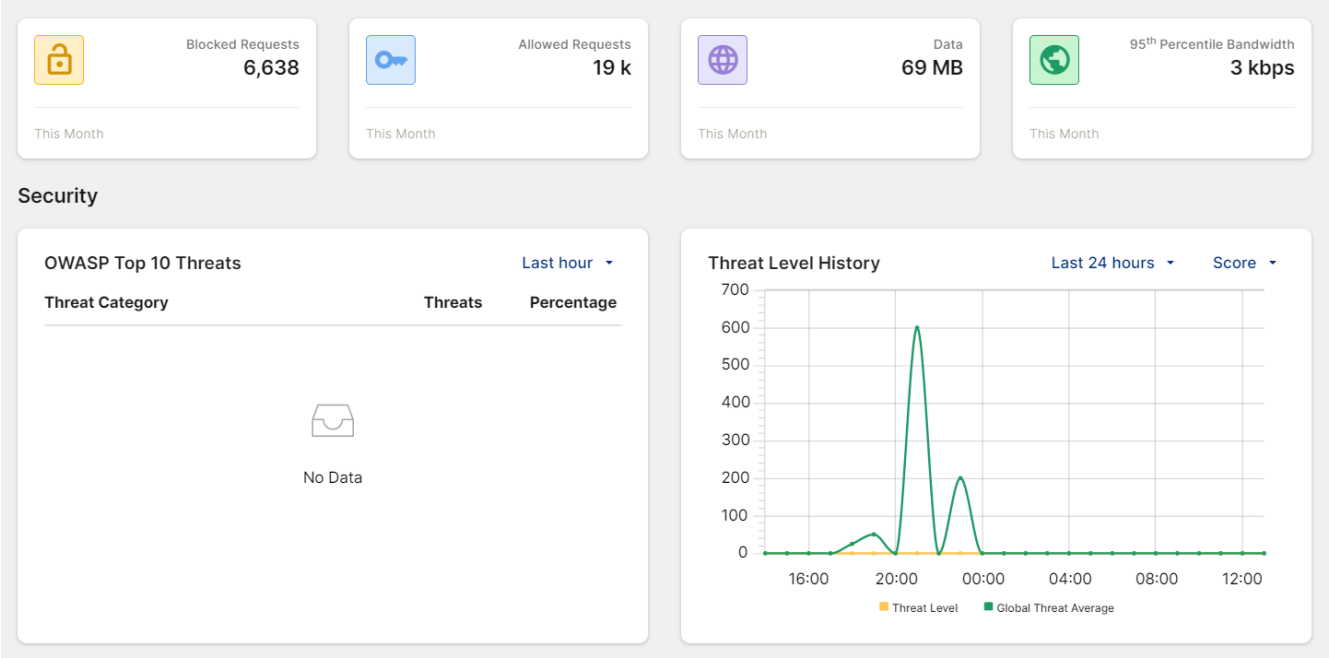
Changing FortiAppSec Cloud scrubbing center

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

1. Go to **WAF > Applications**.
2. Click the edit icon for the desired application.
3. Select the desired region.
4. Click **OK**.

WAF Application Dashboard

This dashboard displays general security insights from the WAF service.



Please see the table below for a description on each of the widgets displayed on this page.

Widget	Description
Monthly Counts	Shows the total number of the following transactions for the current calendar month: • Blocked Requests • Allowed Requests • Data • 95th Percentile Bandwidth
Security	
OWASP Top 10 Threats	The OWASP Top 10 risk(s) observed in your application traffic. The OWASP Top 10 is a list of the most critical security risks to web applications, published by the Open Web Application Security Project (OWASP).
Threat Level History	This graph shows the Threat Level of your application traffic over the adjustable time frame (default = last 24 hours). You can adjust the time frame, and choose to view the Threat Level (y-axis) as either a score (0-700) or a percentage. Attacks are assigned a score based on its severity: • Critical: 50 • High: 30 • Medium: 10

Widget	Description
	• Low: 5 The system calculates a **threat score** every 5 minutes by aggregating attack scores based on their severity. For instance, if there are two critical attacks (score of 50 each) and one high-level attack (score of 30) within this timeframe, the total threat score is calculated as 50*2+30=130. **Threat Scores** and their corresponding severity levels: • 1 (low) • 100 (medium) • 400 (high) • 700 (critical)
Threat Level	The threat level in the last hour on a scale from **low** to **critical**, followed by an ordered table with more information on the detected threats.
Incidents	A line graph displaying the number of incidents falling under **low**, **moderate**, and **high** threat levels over the adjustable time frame (default = last hour).
Top Incidents by Severity	A ranked list of incidents from the selected time frame (default: last hour), ordered by their threat level, starting with the highest. To view additional details, click on an incident in the list.
Top Known Threats	A ranked list of threats from the selected time frame (default: last hour), ordered by their threat level, starting with the highest. To view additional details, click on an incident in the list.
Vulnerability Scan	Insights from Vulnerability Scan.
Traffic	
Throughput	A line chart displaying the level of throughput of **HTTP**, **HTTPS**, and **Cached** traffic.
Incoming Requests	A line chart displaying **blocked**, **allowed**, and **cached** incoming requests.
Traffic Statistics by Country	A world map that highlights the countries with the highest traffic.
Other	
Server Status	Displays the numbers of servers that are **Healthy**, **Unhealthy**, and **Health Check Disabled** with a condensed list of all servers. Click **All Servers** to navigate to **Origin Servers on page 103**.
Subscription Services	Lists the WAF services available to you based on your license tier, along with their expiration date and status.

FortiView

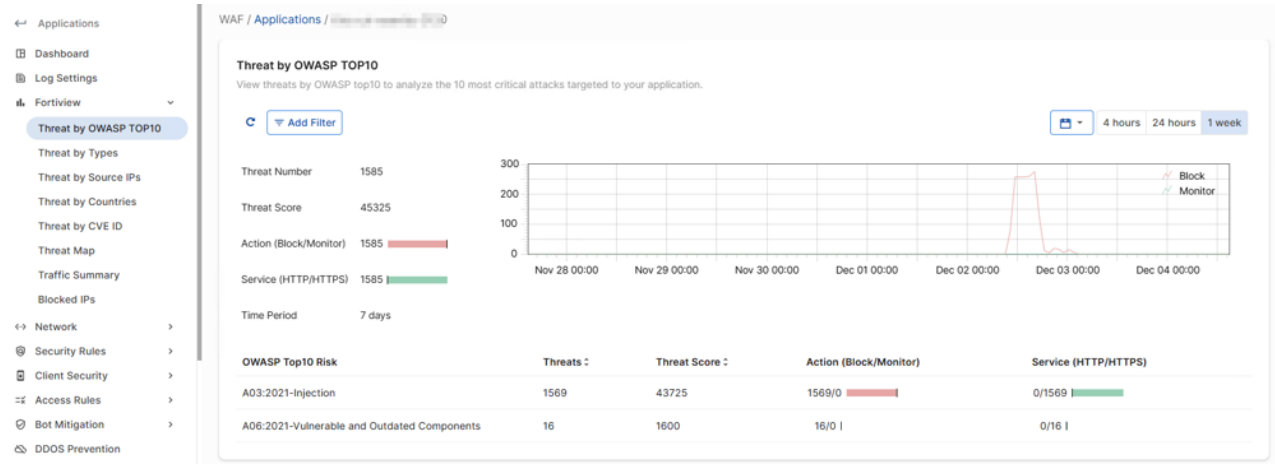
FortiAppSec Cloud detects attacks to your application and displays the threats in FortiView in the following categories:

- **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 94 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.

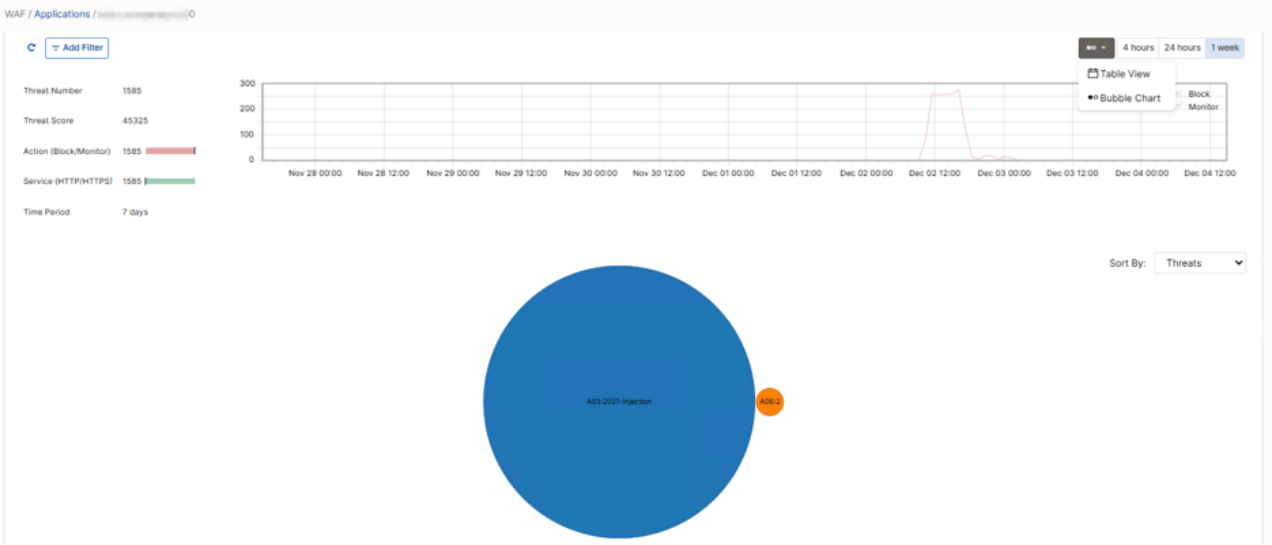
You can see the overview of the threats, such as the total number of threats, threat scores, the types of actions FortiAppSec CloudWAF carries out in response to specific types of attacks, and how severe attacks are.

Choose the way you would like to view application threat data:

- Table View



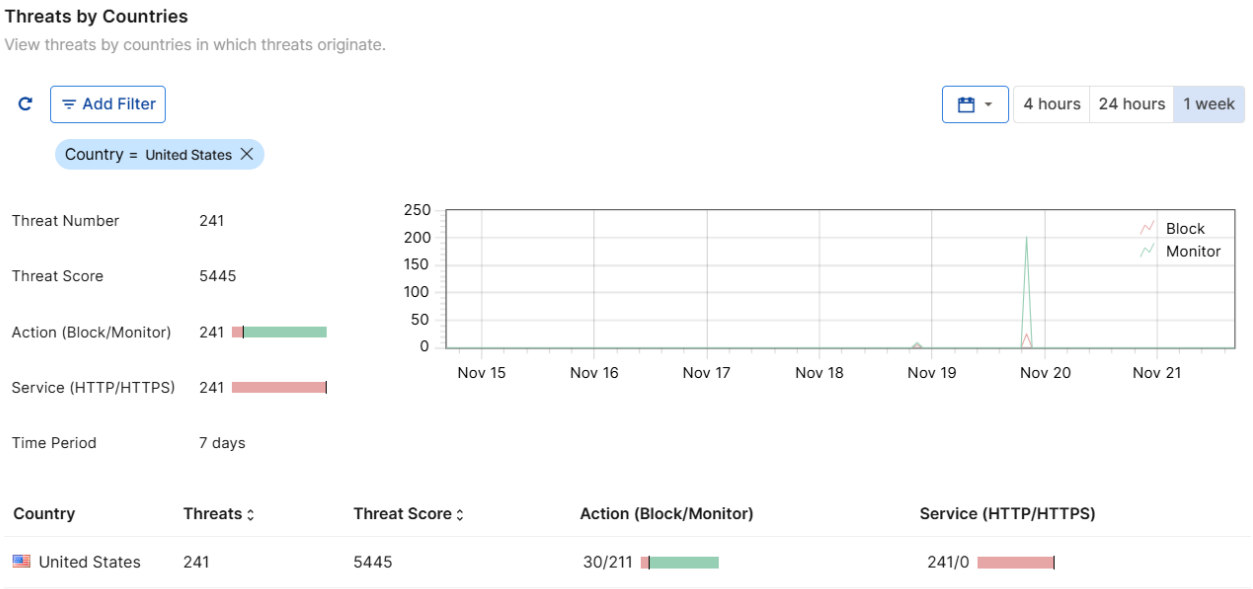
- Bubble Chart



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 Threat View > 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.



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**.
5. 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.

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, FortiAppSec 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, FortiAppSec 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 FortiAppSec 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

Navigate to **FortiView > Blocked IPs** to see a list of IP addresses that have been blocked by FortiAppSec Cloud, either by your application's security rules or by actions triggered by other applications that caused the load balancers to block them.

In your configuration, WAF modules on page 127 such as IP Protection, Bot Mitigation, or DoS Protection that are set to use the **Period Block** action can contribute to this list.

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.

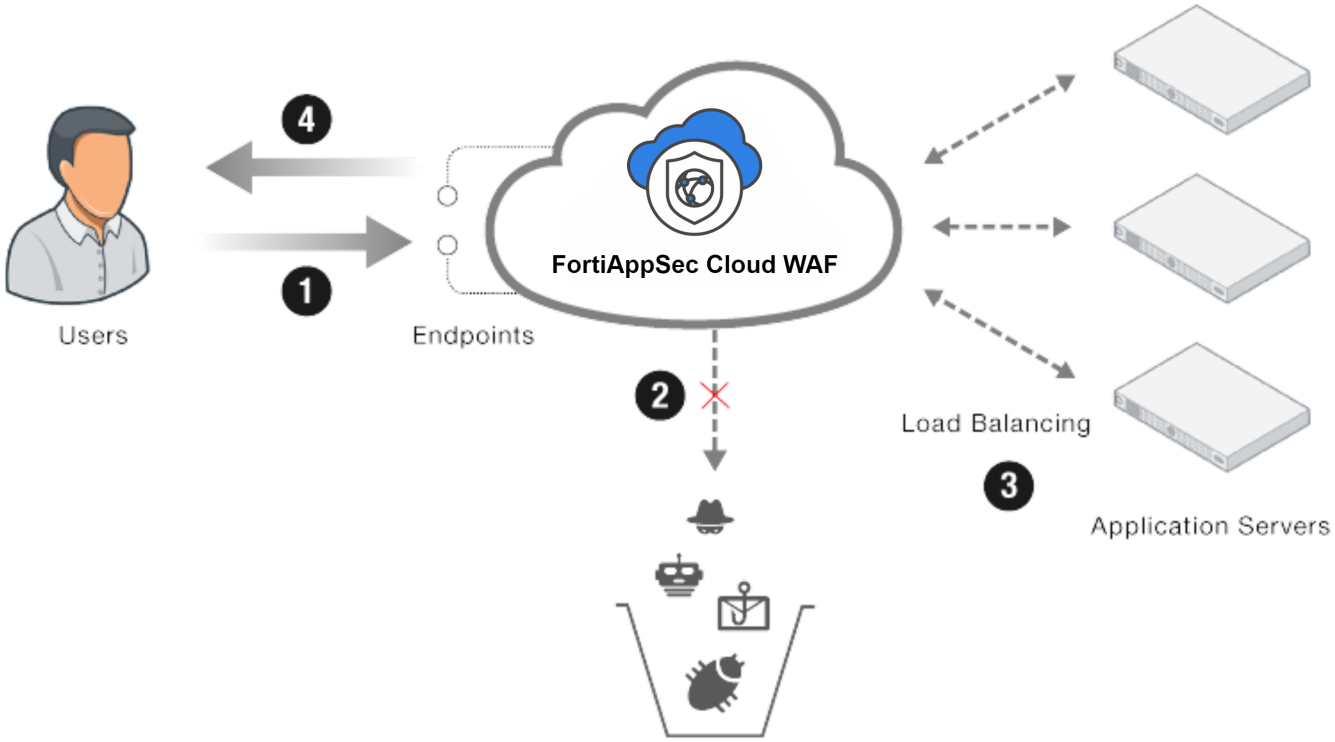
To remove an item from this list, click on the delete icon in the same row as the desired IP address to effectively unblock it.

Network

After you complete onboarding, you can navigate to the pages under **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, FortiAppSec Cloud WAF, and origin servers.



The figure above illustrates the following points:

1. When users visit your application, the traffic is directed to the endpoints on FortiAppSec Cloud.
2. FortiAppSec Cloud WAF 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 FortiAppSec 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.

Endpoints

Define the types of traffic allowed to access your application, such as HTTP or HTTPS, the specific TLS protocol versions supported, and the preferred cipher strengths.

Endpoint Configuration

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.

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

Field	Description
Endpoint CNAME	This field is autopopulated from your DNS configuration, and is not editable.
Domain	List the domains to protect. The protection policy configured for this application applies to all the domains. • Please enter the root domain as the first entry. • 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 for the first domain entry. 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.
HTTP	Enable to allow HTTP traffic, and select the port number for HTTP service.
HTTPS	Enable to allow HTTPS traffic. If HTTPS is allowed, you will be required to configure the **SSL/TLS Certificate Management** and **TLS and Cipher Configuration**. The default value for HTTPS is 443. See below for the list of all accepted HTTPS configuration options. Make sure the port numbers for HTTP and HTTPS are not duplicate.

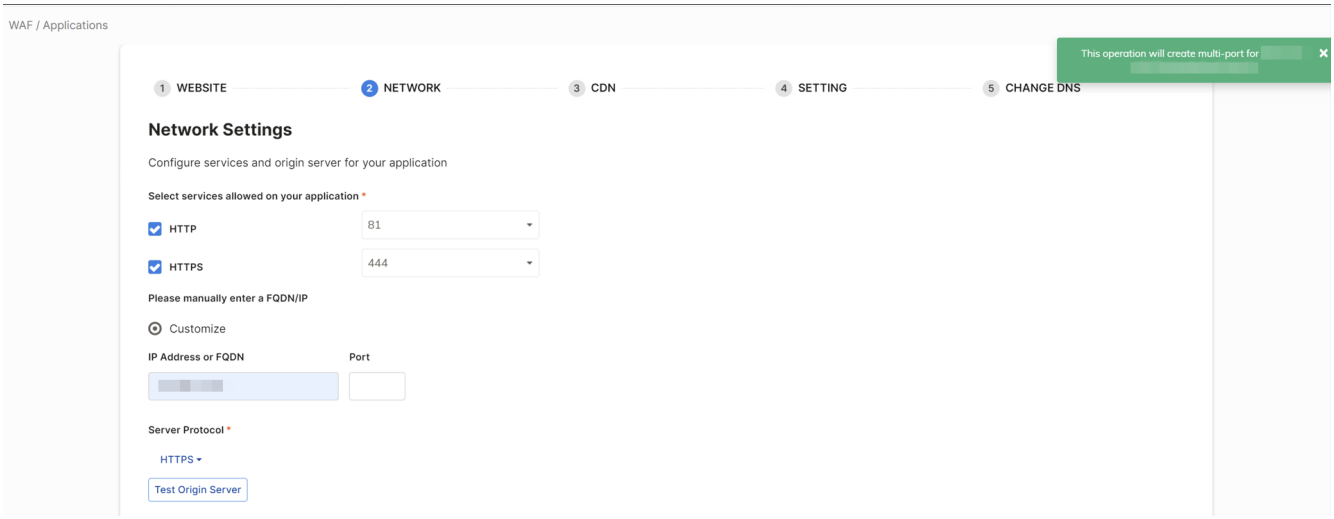
You can view the full, updated list of ports when adding an application under **Network Settings**, in the dropdown menus for **HTTP** and **HTTPS**.

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

Multi-port

Multi-port applications allow you to direct traffic on your application across multiple HTTP or HTTPS ports. To enable multi-port functionality, create multiple applications with the same domain. For instructions on creating applications, see Onboard WAF applications on page 65.

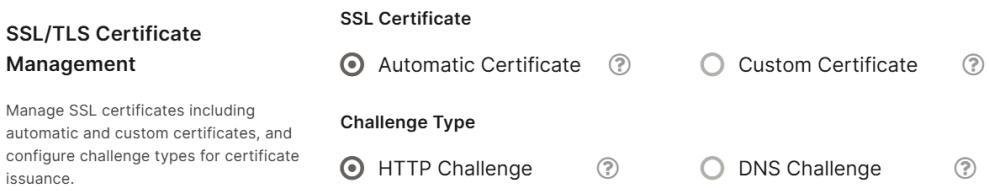
When FortiAppSec Cloud detects multiple applications with the same domain, you will encounter a pop message in the top-right corner of your window when you click **Test Origin Server** on the **Network** tab. This indicates you are creating a multi-port application.



When configuring a multi-port application, please note the following:

- You cannot change the region/CDN while multi-port is enabled.
  - To switch regions or CDNs, delete all multi-port applications of a domain, leaving only the original application. After changing the region, you will need to manually recreate the multi-port applications to resume traffic from other ports.
- If you need to use a custom certificate on an application, please re-input the certificate for each multi-port.
- Ensure that the first domain on the multi-port is the same as the first domain on the original application. This ensures that FortiAppSec Cloud will recognize the duplicate as a multi-port application.
- When managing sub-domains with different port requirements, it is best to create them as separate applications. This approach ensures each sub-domain can independently manage its specific port settings without overlapping configurations.

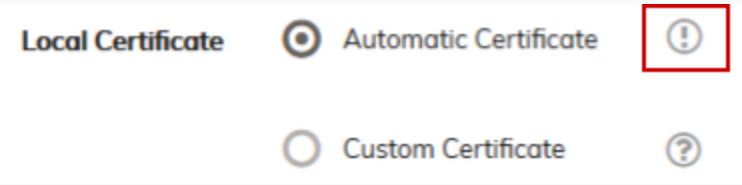
SSL/TLS Certificate Management

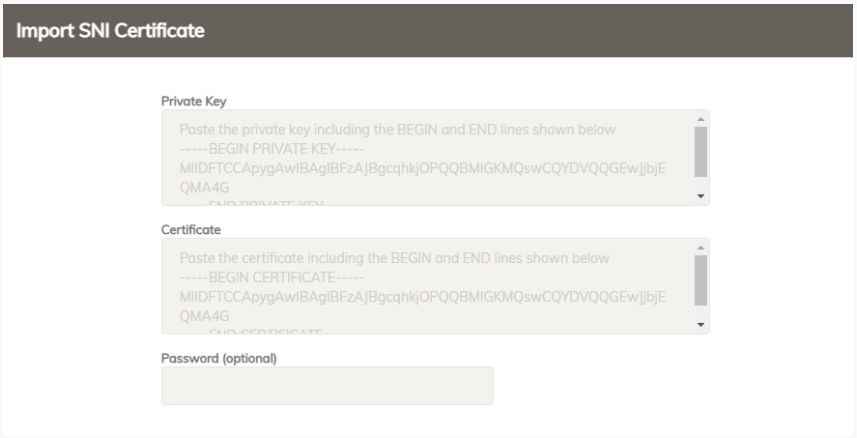


SSL Certificate

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

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

SSL Certificate Option	Description
Automatic Certificate	By default, FortiAppSec 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 FortiAppSec Cloud. **Before selecting Automatic Certificate, ensure the following is done:** • Ensure your DNS record is changed to the CNAME or A record shown in the last step of the Web Application Configuration wizard. • If using **HTTP Challenge**, ensure HTTP traffic is enabled and use port 80. The Certificate Authority sends HTTP requests to FortiAppSec 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 FAQ > Network on page 474. • Do not block requests from the United States in **Access Rules > IP Protection > Geo IP Block**, as this will prevent FortiAppSec Cloud from retrieving certificates from Let's Encrypt. • Ensure the server health check status is **OK** before retrieving a certificate. If not, disable the health check temporarily to avoid interruptions during certificate retrieval. Once the certificate is retrieved successfully, re-enable the health check and troubleshoot any server connection issues. When using **Automatic Certificate**, it is recommended to select **DNS Challenge** for **Challenge Type** to simplify the verification process and support automatic certificate issuance.
Custom Certificate	FortiAppSec 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.  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.

SSL Certificate Option	Description
	2. For **SNI Certificate**, click **Import** and copy the Private Key and Certificate values provided by your Certificate Authority. FortiAppSec Cloud automatically parses information of the SNI certificates including issuance, expiration, status, and certificate chain, and changes them to recognizable formats. For status, when FortiAppSec Cloud verifies the private key and certificate values are consistent, the status is OK; when FortiAppSec Cloud verifies the certificate has expired, the status is Expired; when FortiAppSec Cloud verifies the certificate is valid, while the certificate chain verification fails, the status is Invalid Chain. FortiAppSec 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  3. For **Intermediate Certificate (optional)**, click **Import** and copy the certificate value provided by your intermediate Certificate Authority. FortiAppSec Cloud automatically parses information of the intermediate certificates including issuance, and expiration, and changes them to recognizable formats. Also, FortiAppSec Cloud verifies the status and certificate chain. When an indeterminate certificate is successfully imported or deleted, FortiAppSec Cloud reverifies the expiration and certificate chain. You can import at most 32 SNI certificates and intermediate certificates respectively. Submit a support ticket if you want to extend the limits. If you have multiple applications with different root domain names but sharing the same IP address, you need to import the certificates for all the domains names. For more information, see Multiple domains sharing the same IP address on page 241.

Challenge Type

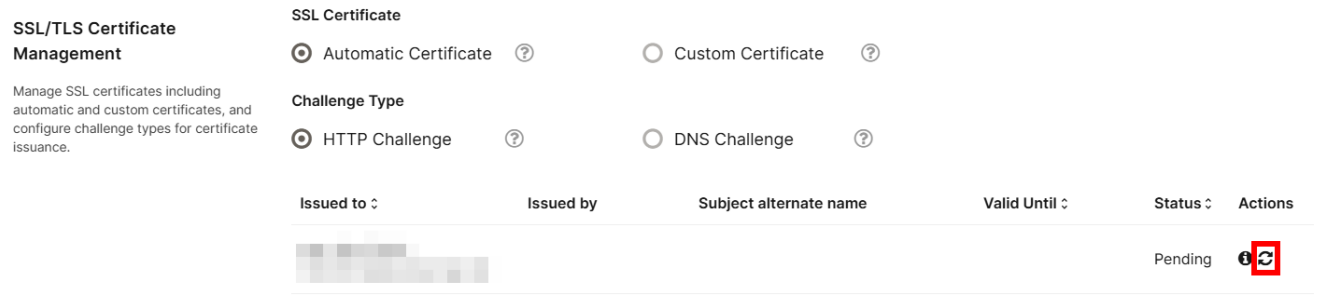
Let's Encrypt sends challenges to validate that you control the domain names you have listed while onboarding the application.

Challenge Type	Description
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 FortiAppSec Cloud. Please note that DNS challenge will be used for the wildcard domains regardless which challenge type you have chosen.

The challenge is automatically handled, but if you need to make more complex configuration decisions, it can be helpful to understand the process in more detail. For additional information, please see Challenge Types posted by Let's Encrypt.

Several minutes after the challenge is successfully completed, FortiAppSec Cloud automatically obtains an SSL certificate from Let's Encrypt installs it on your application. It will be used in HTTPS connections to encrypt or decrypt the traffic. If FortiAppSec 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, the retry frequency reduces to once per day until the certificate is successfully retrieved.

To retrieve the certificate immediately, click the **Refresh** button under the **Actions** column to restore the interval count to the 1st day. FortiAppSec Cloud will then retrieves certificate every 12 minutes, and so on.



Thirty days before your certificate expires, FortiAppSec Cloud will re-verify that your DNS CNAME record is still correct. If it is, FortiAppSec Cloud automatically renews your certificate for another 90 days, ensuring that it does not expire. This process helps maintain continuous encryption for HTTPS connections without manual intervention.

TLS and Cipher Configuration

Select which versions of SSL or TLS protocols are allowed for the HTTPS connections between FortiAppSec Cloud and the clients.

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

Field	Description
SSL/TLS Encryption Level: The HTTPS traffic is encrypted or decrypted with ciphers.	Controls how many ciphers are supported and the settings provide 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:** Select to select options from lists of all available TLS 1.3, 1.2, and 1.1 ciphers below.
TLS 1.3	Enable to allow TLS 1.3.
TLS 1.2	Enable to allow TLS 1.2
TLS 1.1	Enable to allow TLS 1.1
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. If enabled, also configure the following: **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. **Include Sub Domains**: When enabled, the HSTS header will include the `includeSubDomains` attribute, meaning this setting will be applied to all sub-domains of your applications. **Redirect all HTTP traffic to HTTPS**: Enable to redirect all HTTP traffic to HTTPS.
Redirect all HTTP traffic to HTTPS (recommended)	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 FortiAppSec 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 241

Advanced Security and Protocol Settings

Configure advanced security features such as HTTP/2, client certificate authentication, and other protocol settings.



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

HTTP/2	Enable to accept HTTP/2 traffic.
Client Certificate Authentication	Enable for FortiAppSec Cloud to require 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, the request will be rejected. **Strictly Require Client Certificate** When enabled, only clients presenting a valid certificate are allowed. **CA Certificate** Click **Import** to upload the trusted CA certificates so that FortiAppSec 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.、 **Certificate Revocation Lists (CRL)** Click **Import** to upload the Certificate Revocation Lists. To ensure that FortiAppSec 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).

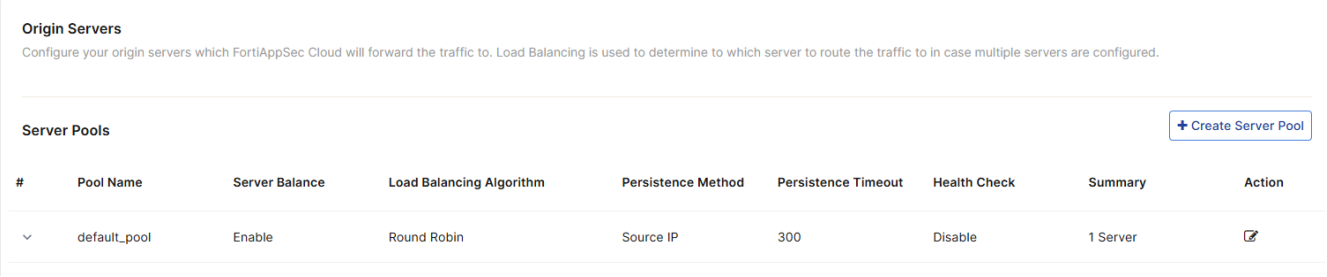
	Client Certificate Forwarding Enable to forward the certificate to your backend server for authentication, user-specific permissions, and access control. Please note, this feature is only available for Advanced and Enterprise tier WAF plans.
IPv6 Service	If IPv6 is enabled, both IPv4 and IPv6 are allowed to your application. If disabled, only IPv4 traffic is allowed.
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.
Custom Block Page	Select the block page that FortiAppSec Cloud displays to your users. It contains the following messages: • The error page FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud uses to differentiate between real users and automated users, such as bots. The custom block page is configured in **WAF > System Settings > Custom Block Pages**.

Origin Servers

Configure the origin servers which FortiAppSec 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.

- Create Server Pool on page 104
- Create Server on page 106
- Lock Origin Server on page 109

Create Server Pool



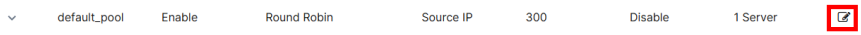
1. Navigate to **Network > Origin Servers**.
2. Click **Create Server Pool**.
3. Configure the following settings.

Field	Description
Pool Name	Supports letters (a-z, A-Z), numbers (0-9), dashes (-), and underscores (_). This cannot be changed after creation.
Server Balance	After the application is onboarded, **Server Balance** is enabled by default to apply load balancing algorithm to origin servers. If you disable this option, you can only configure one origin server, but both HTTP and HTTPS ports can be used for that server. We recommend keeping Server Balance on, even if you only have one server, because turning it off will delete all existing server settings. Additionally, server status monitoring won't be available when Server Balance is off. Only disable Server Balance if you need to use both HTTP and HTTPS with your origin server.
The following options are only available when **Server Balance** is enabled.	
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. • **Source IP Hash** — Distributes new TCP connections using a hash algorithm based on the source IP address of the request. When the status of a server is set to **Disabled**, or a health check indicates it is down. FortiAppSec Cloud will transfer any remaining HTTP transactions in the TCP stream to an active server according to the Load Balancing Algorithm.
Persistence	After FortiAppSec 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.

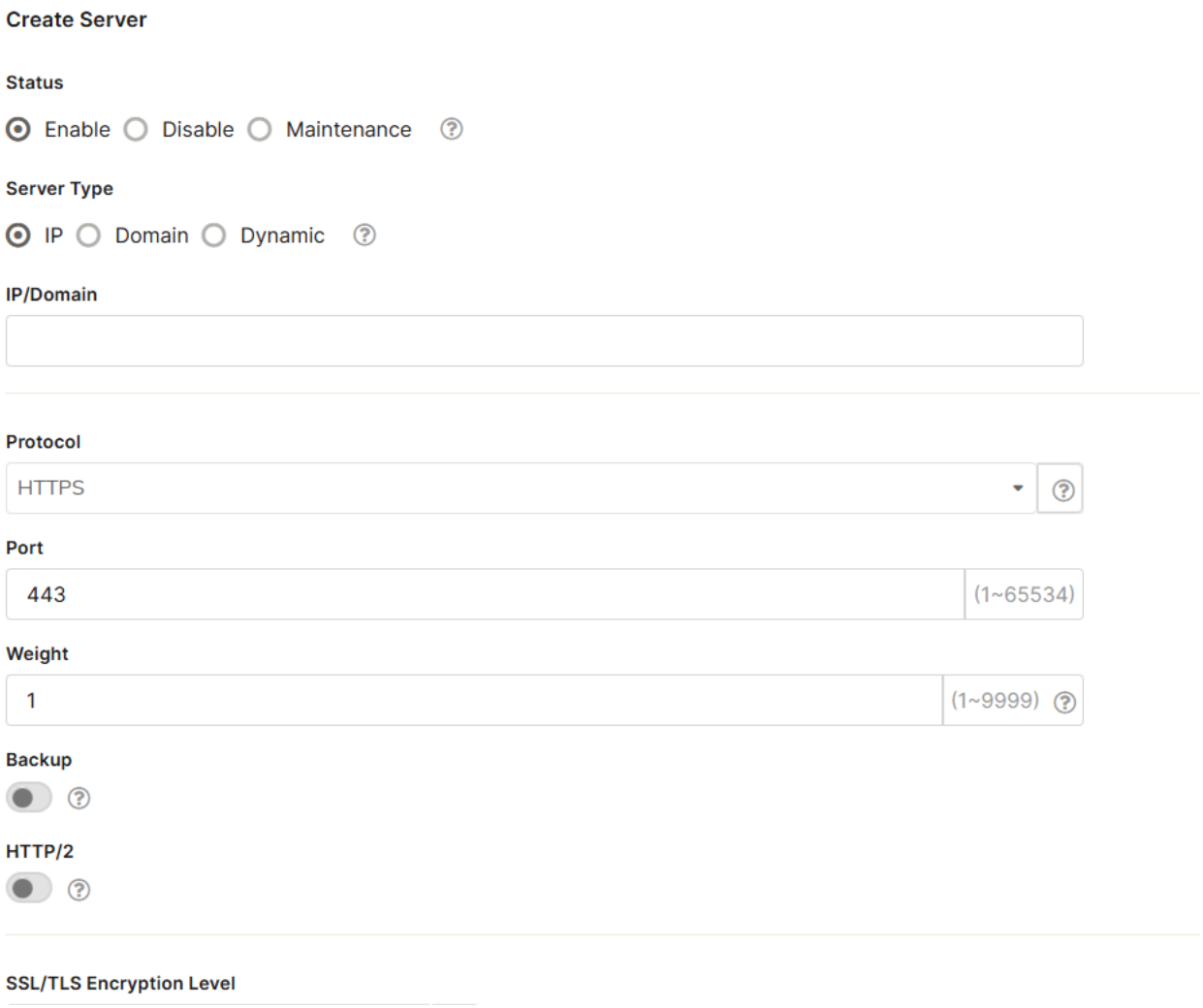
Field	Description
	Persistence specifies how FortiAppSec Cloud determines a request is the subsequent request from a client. • **Source IP**—The requests with the same client IP address and subnet as the initial request will be forwarded to the same server. • **Insert Cookie**—The requests with the same 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	Set the time, in seconds, after which an idle connection will cause FortiAppSec Cloud to select a new server from the pool.
Cookie Name	Specifies a value to match or the name of the cookie that FortiAppSec Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Cookie Path	Specifies a path attribute for the cookie that FortiAppSec Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Cookie Domain	Specifies a domain attribute for the cookie that FortiAppSec Cloud inserts. Available only when the **Persistence** is set to **Insert Cookie**.
Health Check	Enable to periodically test for server availability. If FortiAppSec 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.
The following options are only available when **Health Check** is enabled	
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, FortiAppSec 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 FortiAppSec 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.

Field	Description
	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.

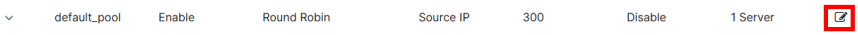
4. Click **OK** to save the newly created server pool and return to the **Origin Servers** page, where you should see the newly added server pool in the **Server Pools** table. The server pool will be empty initially; follow the instructions below to add servers to this pool.
5. Click the **Edit** icon on one of the server pools to add servers to the server pool.



Create Server



1. On the **Network > Origin Servers** page, click the **Edit** icon on one of the server pools to view/edit its nested servers.



2. Click **Create Server Pool**
2. Configure the following settings.

3.

Status	• **Enable**—Specifies that this server can receive new sessions from FortiAppSec Cloud. • **Disable**—Specifies that this server does not receive new sessions from FortiAppSec Cloud and it closes any current sessions as soon as possible. • **Maintenance**—Specifies that this server does not receive new sessions from FortiAppSec 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, FortiAppSec 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 FortiAppSec Cloud can be authorized to access the resources in your public cloud account. See Cloud Connectors on page 205. 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. FortiAppSec 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. FortiAppSec 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 FortiAppSec 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 Origin Servers on page 103 is on. If enabling HTTPS, see the next step for detailed configuration instructions.
HTTPS Port & HTTP Port	When the Origin Servers on page 103 is off, FortiAppSec 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 Origin Servers on page 103 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	If enabled, when other servers fail their server health check, FortiAppSec Cloud routes any connections for the failed server to this server. If you have enabled Backup for more than one server, FortiAppSec 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.
Server Certificate Authentication	Enable this option to secure the connection between FortiAppSec Cloud and the server. Please note this option is available to configure only when you have successfully added the server.
CA Certificate	If **Server 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 FortiAppSec 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).



FortiAppSec CloudWAF continuously verifies the IP address paired with the domain name, and if the IP address changes, WAF automatically updates the origin server IP in its configuration. The frequency that WAF 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 WAF 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.
3. Click **OK**. This saves the new server under the selected server pool
4. 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.

Lock Origin Server

Locking your origin server's IP ensures it can only be used by your account. This prevents other FortiAppSec Cloud accounts from targeting your server with malicious traffic.

Origin server lock is enabled by default.The first account to configure an IP/domain as the Origin Server will have it locked to their account, as long as it is not a shared IP from a CDN/WAF provider. Once locked, the IP/domain record remains tied to that account.



A server IP/domain cannot be locked if:

- It is already in use by another account.
- It belongs to a CDN or Application Load Balancer service, such as AWS, Azure, GCP, or Cloudflare.



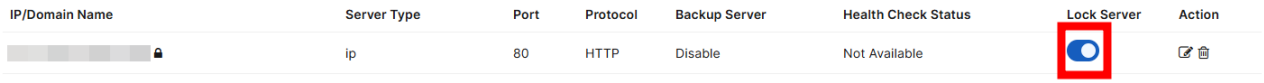
If the IP or domain has already been locked by another account, it cannot be added to the application's Origin Server. If you have any questions, please submit a support ticket.

To lock the origin server for an application:

1. On the **Network > Origin Servers** page, click the **Edit** icon on one of the server pools to view/edit its nested servers.



2. Under **IP/ Domain Name**, toggle the switch to enable **Lock Server**.

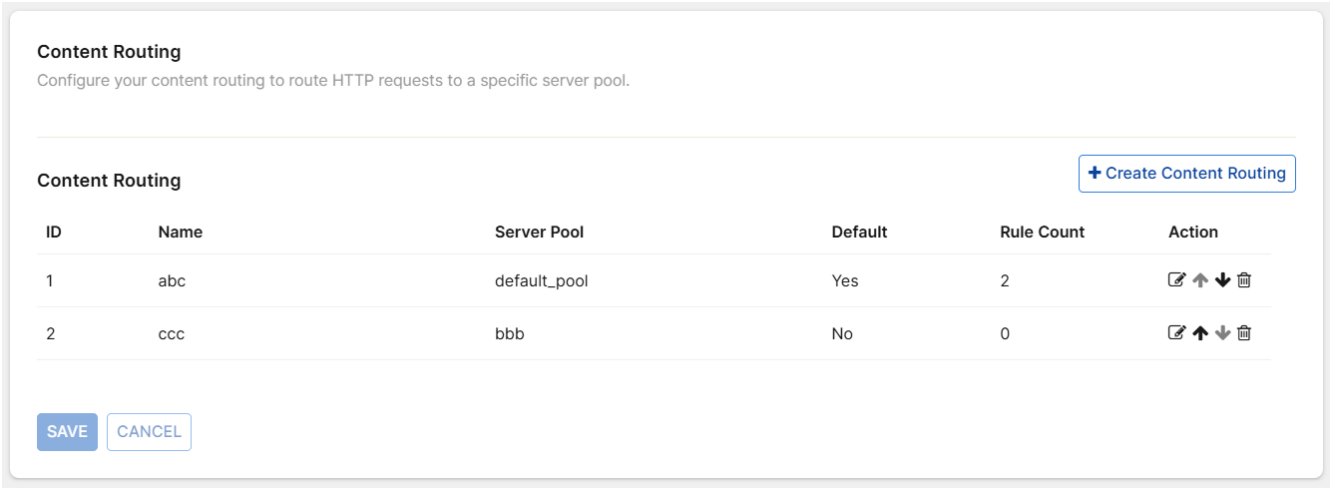


Content Routing

Configure content routing rules to direct traffic to origin servers based on URL, Header, Cookie, Parameter, or Source IP. Configuration for multiple server pools and content routings is supported.

- Each application can have up to 32 content routings, with each content routing supporting up to 32 rules.
- For those using licenses purchased from Fortinet, the number of content routings you enable directly corresponds to the application license requirement.

  For example, an application with one content routing enabled uses the license space for one application, while an application with two content routings enabled uses the space for two applications, and so forth.



Enable Content Routing

1. Click **Add Modules** in the side navigation menu.
2. Under **Network**, enable **Content Routing**.

Disabling **Content Routing** via the **Add Modules** wizard will do the following:

- Permanently remove all existing content routing configurations
- Delete all origin server pools except for the default server pool.

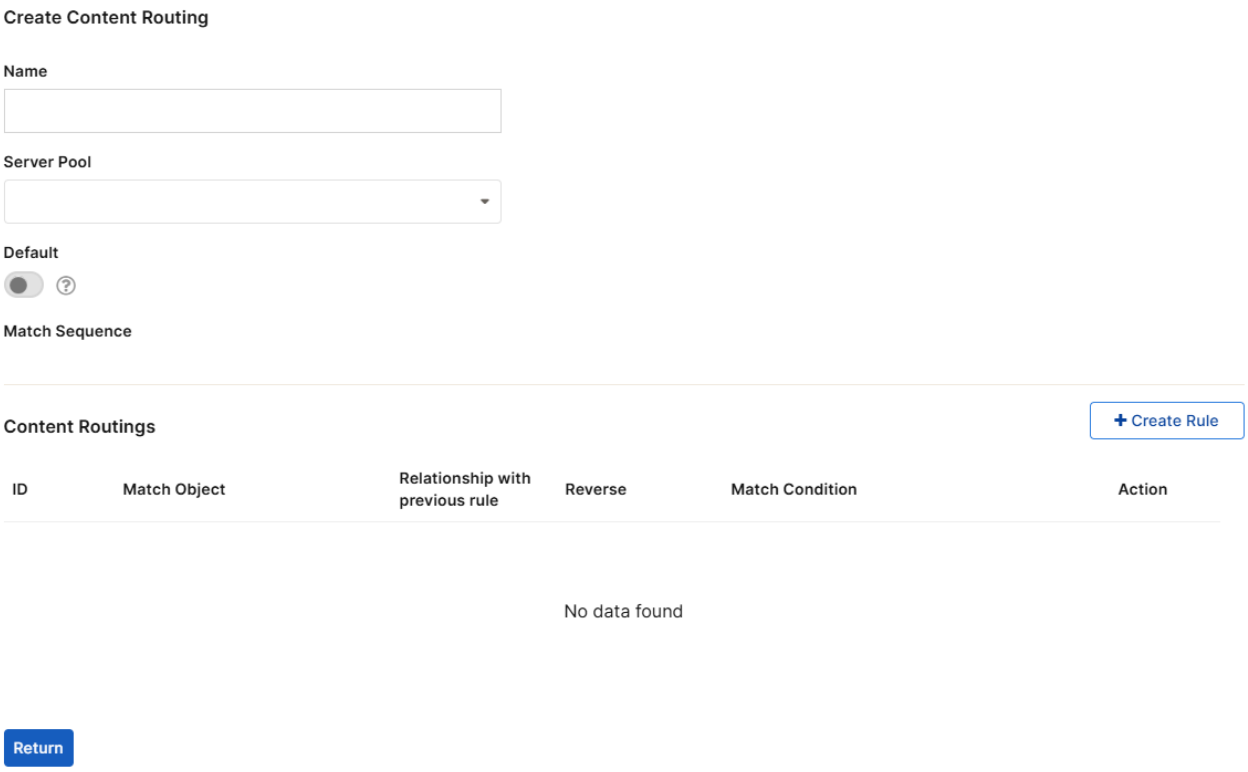
Once you enable **Content Routing**, you will be able to create server pools on **Network > Origin Servers**.

Please note, you cannot delete the default server pool. This ensures it remains available if you later disable the **Content Routing** module.

Create content routing rule

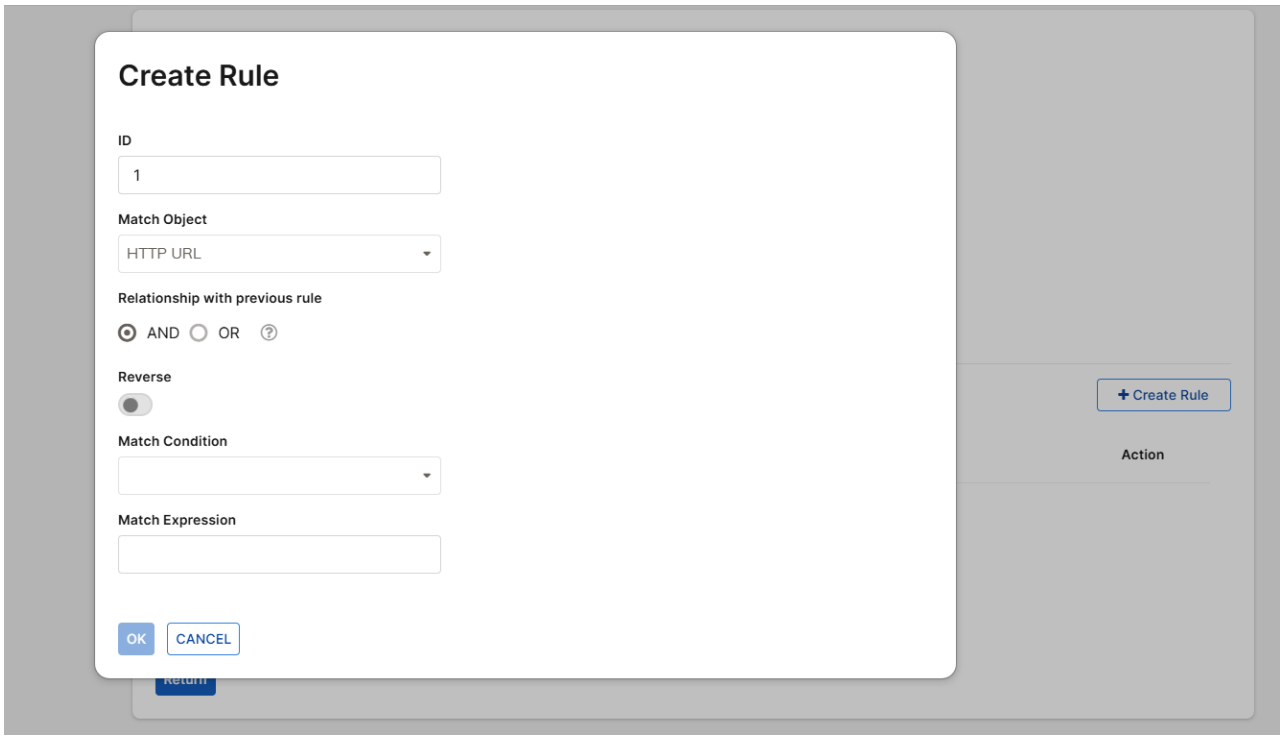
1. In the side navigation menu, click **Network > Content Routing**.
2. Click **Create Content Routing**.

   Please note, each application can have a maximum of 32 content routings, and each content routing can contain up to 32 rules.
3. Configure the following:



Field	Description
Name	Enter an identifiable name for your routing.
Server Pool	Select the Server Pool you would like to direct traffic to.
Default	When enabled, traffic that does not match the Rules in any content routing will be directed to the **Server Pool** in the current content routing. Configuring a default routing ensures that all traffic is processed by a server pool, avoiding dropped traffic. Each application can have one default routing.

4. Click **Create Rule** to configure the desired traffic behavior under this routing.



Field	Description
ID	A system-generated number that identifies the rule in its sequence within the content routing.
Match Object	The criteria used to base the rule for directing traffic. In this drop-down menu, you can select from the following options: • **HTTP Host** • **HTTP URL** • **URL Parameter** • **HTTP Referer** • **HTTP Cookie** • **HTTP Header** • **Source IP** • **X509 Certificate Subject** • **X509 Certificate Extension** • **HTTPS SNI** Note: To select **X509 Certiifcate Subject** or **X509 Certificate Extension**, you must first go to **Network > Endpoints** and enable **Client Certificate Authentication**.
Relationship with previous rule	Select whether the current rule should run concurrently with or as an alternative to the previous rule. For the first rule in a routing sequence, this field has no effect.

Field	Description
	Please note, rules bound by an AND relationship take precedence over those with OR relationships. This ensures all AND conditions must be met before considering OR conditions.
Reverse	If enabled, the rule will apply to all traffic that does not match the specified condition, rather than to all traffic that does match it.

The following configuration options will vary based on the selected **Match Object**.

If you set **Match Object** to **URL Parameter**, **HTTP Cookie**, or **HTTP Header**, configure the following:

Field	Description
Name Match Condition	Select an attribute in the traffic name that defines a match. • **Is equal to** — The rule applies to traffic names that fully match the specified value. • **Match prefix** — checks if the beginning of a string matches a specified prefix. For example, if the prefix is "api/", the condition will be true for strings like "api/v1/resource" but not for "web/v1/resource." • **Match suffix** — checks if the end of a string matches a specified suffix. For example, if the suffix is ".html", the "match suffix" condition will be true for URLs like "example.com/page.html" but not for "example.com/page.php". • **Match contains** — The rule applies to all traffic names that contains the specified value. • **Regular Expression** — The rule applies to all traffic names that match the specified regular expression.
Name	This field appears when **Match Object** is set to **URL Parameter**, **HTTP Cookie**, or **HTTP Header**. Enter what the **Name Match Condition** will use to match against.
Value Match Condition	Select an attribute in the traffic value that defines a match. • **Is equal to** — The rule applies to traffic values that fully match the specified value. • **Match prefix** — checks if the beginning of a string matches a specified prefix. For example, if the prefix is "api/", the condition will be true for strings like "api/v1/resource" but not for "web/v1/resource." • **Match suffix** — checks if the end of a string matches a specified suffix. For example, if the suffix is ".html", the "match suffix" condition will be true for URLs like "example.com/page.html" but not for "example.com/page.php". • **Match contains** — The rule applies to all traffic values that contains the specified value. • **Regular Expression** — The rule applies to all traffic values that match the specified regular expression.
Value	This field appears when **Match Object** is set to **URL Parameter**, **HTTP Cookie**, or **HTTP Header**. Enter what the **Value Match Condition** will use to match against.

If you set **Match Object** to **HTTP Host**, **HTTP URL**, **HTTP Referer**, **HTTPS SNI**, configure the following:

Field	Description
Match Condition	Select the attribute in the match object that defines a match. • **Is equal to** — The rule applies to traffic values that fully match the specified value. • **Match prefix** — checks if the beginning of a string matches a specified prefix. For example, if the prefix is "api/", the condition will be true for strings like "api/v1/resource" but not for "web/v1/resource." • **Match suffix** — checks if the end of a string matches a specified suffix. For example, if the suffix is ".html", the "match suffix" condition will be true for URLs like "example.com/page.html" but not for "example.com/page.php". • **Match contains** — The rule applies when the match object contains the specified value. • **Regular Expression** — The rule applies when the match object matches the specified regular expression. • **Match directory** — The rule applies when the match object contains the specified string between delimiting characters (slash) in a domain name. • **Match domain** — The rule applies when the match object contains the specified string between the periods in a domain name.
Match Expression	Enter what the **Match Condition** will use to match against.

If you set **Match Object** to **Source IP**, configure the following:

Field	Description
Match Condition	Select the attribute in the match object that defines a match. • **IPv4 Address/Range** — The rule applies when the match object is the specified IPv4 address or falls within the specified IPv4 address range. • **IPv6 Address/Range** — The rule applies when the match object is the specified IPv6 address or falls within the specified IPv6 address range • **Import From CSV File** — Instead of entering an IP range, upload a CSV file that contains a list of IP addresses. The rule will trigger when any of the listed IP addresses is detected in the match object.
IP range	Enter the IP range the **Match Condition** will use to match against.

If you set **Match Object** to **X509 Certificate Subject**, configure the following:

Field	Description
X509 Subject Name	Select the attribute in the match object that defines a match. • **Country Name (C)** • **Common Name (CN)** • **Email Address (E)** • **Locality Name (L)** • **Organization Name (O)**

Field	Description
	• **Organizational Unit Name (OU)** • **State or Province Name (ST)**
Value Match Condition	Select an attribute in the traffic value that defines a match. • **Is equal to** — The rule applies to traffic values that fully match the specified value. • **Match prefix** — checks if the beginning of a string matches a specified prefix. For example, if the prefix is "api/", the condition will be true for strings like "api/v1/resource" but not for "web/v1/resource." • **Match suffix** — checks if the end of a string matches a specified suffix. For example, if the suffix is ".html", the "match suffix" condition will be true for URLs like "example.com/page.html" but not for "example.com/page.php". • **Match contains** — The rule applies to all traffic values that contains the specified value. • **Regular Expression** — The rule applies to all traffic values that match the specified regular expression.
Match Expression	Enter what the **Match Condition** will use to match against.

If you set **Match Object** to **X509 Certificate Extension**, configure the following:

Value Match Condition	Select an attribute in the traffic value that defines a match. • **Is equal to** — The rule applies to traffic values that fully match the specified value. • **Match prefix** — checks if the beginning of a string matches a specified prefix. For example, if the prefix is "api/", the condition will be true for strings like "api/v1/resource" but not for "web/v1/resource." • **Match suffix** — checks if the end of a string matches a specified suffix. For example, if the suffix is ".html", the "match suffix" condition will be true for URLs like "example.com/page.html" but not for "example.com/page.php". • **Match contains** — The rule applies to all traffic values that contains the specified value. • **Regular Expression** — The rule applies to all traffic values that match the specified regular expression.
Value	Enter what the **Match Condition** will use to match against.

5. Click **OK** to save the new rule.
6. Click **Save** to apply changes.

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 Inter-mediate	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
ECDHE-ECDSA-AES128-SHA256			Yes

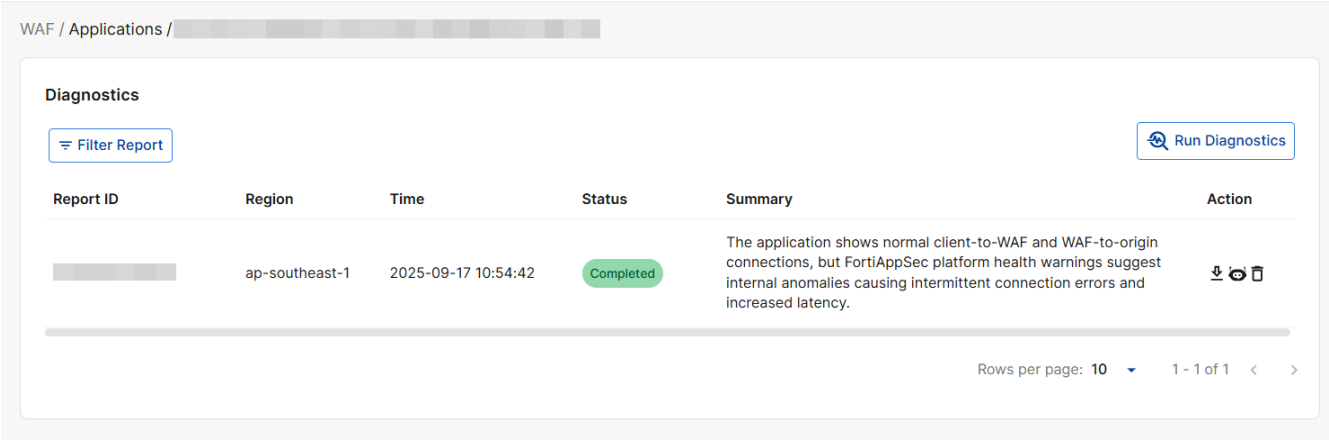
Cipher	Mozilla Modern	Mozilla Intermediate	Mozilla Old
ECDHE-RSA-AES128-SHA256			Yes
ECDHE-ECDSA-AES128-SHA			Yes
ECDHE-RSA-AES128-SHA			Yes
ECDHE-ECDSA-AES256-SHA384			Yes
ECDHE-RSA-AES256-SHA384			Yes
ECDHE-ECDSA-AES256-SHA			Yes
ECDHE-RSA-AES256-SHA			Yes
DHE-RSA-AES128-SHA256			Yes
DHE-RSA-AES256-SHA256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

Diagnostics

The Diagnostics page provides core traffic validation between clients, FortiAppSec Cloud WAF, and origin servers. It helps detect connectivity, certificate, and platform-related issues that could impact application availability.

- Create Diagnostics Report on page 118
- View Application Diagnostics Report on page 119
  - Troubleshooting on page 120
- FortiAI Diagnostics Agent on page 120

Use **Filter Report** to only display Diagnostics Reports with certain characteristics.



Report ID	Auto-generated value to identify this report.
Region	Region entered during report creation.
Time	Time of report creation.
Status	Indicates the current state of the diagnostic report: • **In Queue**: The request is waiting in the execution queue. • **In Progress**: The diagnostic is currently running. • **Completed**: The diagnostic has finished and the report is available for download. • **Failed**: The diagnostic could not be completed. Re-run the diagnostic or contact Fortinet Support.
Summary	This section displays summary section from the generated report.
Action	Click an icon in this column to perform the following actions: • : Download the generated **Applications Diagnostics Report** (PDF). See below for details. • : Launch FortiAI Diagnostics Agent. See below for details. • : Permanently delete the generated report.

Create Diagnostics Report

When you create a Diagnostics Report, the system runs connectivity checks between clients and the FortiAppSec Cloud WAF, as well as between the FortiAppSec Cloud WAF and the origin servers, and compiles the results into a PDF.

1. Click **Run Diagnostics**.
2. Configure the following:

Setting	Description
Affected IP	If the issue only occurs for a subset of client IP addresses, you can specify the Affected IP when creating the report. The system will verify whether the selected IP has been blocked by the FortiAppSec Cloud WAF.

Setting	Description
	Otherwise, leave this field blank.
Affected Region	For customers using CDN, select the affected Region where the issue is observed. This helps narrow the diagnostic scope. Otherwise, leave this field as default.
Certificate Diagnostics	Enable when you need to check SSL/TLS certificate presence, validity, and chain. The system will also provide recommendations for any issues detected. **Note:** This feature relies on shared global resources, so diagnostic capacity is limited. During peak demand, report requests with this setting enabled may be queued or rejected.

3. Click **OK** to save and apply changes.

View Application Diagnostics Report

The Application Diagnosis Report provides a comprehensive analysis of application connectivity and platform health, including findings, impact, and recommended solutions. To download an **Application Diagnostics Report**, locate the desired report in the table on the **Diagnostics** page, and click the icon under **Actions**.

Summary & Recommendations

This section summarizes key issues identified at each stage, their potential impact, and recommended resolutions.

Key Findings

Detailed diagnostics results are provided across three stages:

- Client → WAF Edge: Verifies client connectivity to the FortiAppSec Cloud WAF.
- WAF Edge → Origin Servers: Tests connectivity between the WAF and origin servers.
- FortiAppSec Platform Health: Validates the health status of FortiAppSec Cloud WAF services.

Failures & Warnings

This section lists common errors and warnings, along with their potential causes and recommended solutions.

- Client → WAF Edge
  - **DNS Resolution Failure**: The domain could not be resolved, or DNS is not pointing to FortiAppSec Cloud WAF.
  - **Certificate Issues**: SSL/TLS certificate is invalid or expired.
  - **IP Blocking**: The client IP is blocked by FortiAppSec Cloud WAF.
- WAF Edge → Origin Servers
  - **Connection Timeout**: The origin server's firewall may be blocking FortiAppSec Cloud WAF IPs, or the origin server is unresponsive.
  - **Certificate Issues**: SSL/TLS certificate is invalid or expired.
  - **Error Responses**: The origin server responds with HTTP error codes (4xx or 5xx) even when the connection is established.

- FortiAppSec Platform Health
  - Possible resource exhaustion or service-level anomalies within the FortiAppSec Cloud WAF platform.

Troubleshooting

1. Follow the recommendations in the report for initial troubleshooting.
2. If the issue persists, submit a support ticket, ensuring to attach the complete Application Diagnosis Report (PDF) to your ticket.

FortiAI Diagnostics Agent

The Diagnostics Agent helps identify abnormal connection statuses within their applications and provides insights for resolving connectivity issues. It evaluates multiple aspects of application health, including:

- DNS Status: Analyzing issues related to Domain Name System resolution.
- Pserver Status: Checking the status of the primary server connection.
- Auto Cert Apply: Examining the automatic certificates if alrady applied.

To activate the agent, click the  icon under **Actions**.

Log Settings

This page includes configuration information for attack logs and traffic logs. For information on audit logs, please see Audit Logs Export on page 426.

- Attack Log Alerts on page 120
- Exporting traffic logs on page 122
- Sensitive Data Masking on page 125
- Retention and Periodic clean on page 125

Attack Log Alerts

Enable to receive Attack Log alerts for this application. To export Attack logs, please navigate to **Threat Analytics > Settings**.

1. Navigate to **Log Settings**.
2. Enable **Attack Log Alerts**.
3. Select the **Mode**, which determines the set of configuration options available for defining your attack log alert settings.

a. If you selected **Basic**, configure the following:

Threat Level	Set the lowest threat level you want to receive notifications for. • **Low**: Receive notifications for all threat analytics events. • **Moderate**: Receive notifications for **Moderate** and **High** threat events. • **High**: Receive notifications for **High** threat events. • **Critical**: Receive notifications for **Critical** threat events.
Notification Recipient	• **Default**: Select to send attack log alerts to the email address already associated with this application. • **Custom**: Enter up to 10 email addresses to receive these notifications, separated by commas.

b. If you selected **Advanced**, click **Create Alert** and configure the following:

Name	The internal name by which this set of notification rules is displayed.
Threat Score	Set the lowest threat score you want to receive notifications for. The system calculates a threat score every 5 minutes by aggregating attack scores based on their severity. For instance, if there are two critical attacks (score of 50 each) and one high-level attack (score of 30) within this timeframe, the total threat score is calculated as 50*2+30=130. **Threat Scores** and their corresponding severity levels: • 1 (low) • 100 (medium) • 400 (high) • 700 (critical)
Notification Recipient	• **Default**: Select to send attack log alerts to the email address already associated with this application. • **Custom**: Enter up to 10 email addresses to receive these notifications, separated by commas.

Filter Overview	Click **Add Filter** to define more conditions for attack logs that should trigger alerts.
	1. In the left-most dropdown, select an attribute:
	  • Source IP
	  • User Agent
	  • URL
	  • Threat Main Type
	  • Threat Sub Type
	  • Signature ID
	2. Use the **Operator** and **Value** fields to specify the condition.
	3. Click **Save Filter** before adding another filter.

4. Click **Save** to apply changes.

Exporting traffic logs

Traffic logs record traffic events such as HTTP requests and responses, and the expiration of HTTP sessions. FortiAppSec 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.



Log timestamps may differ between the portal and exported files.

- Traffic Logs are recorded and exported in UTC. The portal automatically converts them to your local time, so portal times may differ from exported files.
- Attack logs include a time zone and are also converted to your local time in the portal. Most analysis tools (e.g., FortiAnalyzer, FortiSIEM) handle this conversion as well.

1. Go to **Log Settings**.
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.
Folder	Enter the 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.



To use an S3 bucket for traffic export, the IAM role must have the following permissions enabled:

- s3:PutObject
- s3:GetObject
- s3:GetBucketLocation

4. Click **Save**.

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

Region	Logstash IP
ap-east-1: Asia Pacific (Hong Kong)	16.162.29.183
ap-south-1: Asia Pacific (Mumbai)	15.207.118.191
ap-southeast-1.prod: Asia Pacific (Singapore)	18.142.59.230
ap-southeast-2: Asia Pacific (Sydney)	13.238.126.108
ap-southeast-3: Jakarta	108.137.118.125
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

Region	Logstash IP
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:

Region	Logstash IP	Logstash Private IP
Australia East	20.188.247.221	10.22.1.52
Brazil South (São Paulo State)	191.234.179.164	10.35.1.52
Canada Central	52.237.13.214	10.37.1.52
East US	52.191.198.64	10.3.1.57
East US 2	20.10.187.167 104.208.237.249 40.123.43.190	10.4.1.167 10.4.1.166 10.4.1.134
Qatar Central	20.173.78.67	10.39.1.40
South Africa North	4.221.143.107	10.40.1.10
West Europe	20.73.191.71	10.9.1.58
West US 2	40.125.64.146	10.15.1.58

Google Cloud:

Region	Logstash IP
europe-west3 (Frankfurt)	35.242.250.207
europe-west8 (Milan)	34.154.63.237
me-west1 (Tel Aviv)	34.165.47.110
us-east1 (South Carolina)	34.74.77.198
us-west1 (Oregon)	34.127.22.16

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 8 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 243. 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 243.

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	60 days
	Dashboard - Top Incidents by Severity	
	Threat Analytics - Incidents	

Category	Features	Retention
Attack log	Threat Analytics -Attack log	60 days
	FortiViewThreatView	
	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	90 days
On-Premise Device Attack log	Threat Analytics - Attack log (on-premise device only)	60 days, or until storage capacity (20 GB × number of devices) is reached, whichever threshold is met first.
Diagnostics Report	Diagnostics	90 days

WAF modules

When you onboard a new application on FortiAppSec 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 Add and Remove Modules.

The following modules are available for FortiAppSec Cloud:

- Security Rules on page 130
- Client Security on page 146
- Access Rules on page 150
- Bot Mitigation on page 161
- DDoS prevention on page 172
- Advanced Applications on page 174
- API Protection on page 180
- Account Takeover on page 191
- Application Delivery on page 192
- Global Trustlist on page 200
- Vulnerability Scan on page 201



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

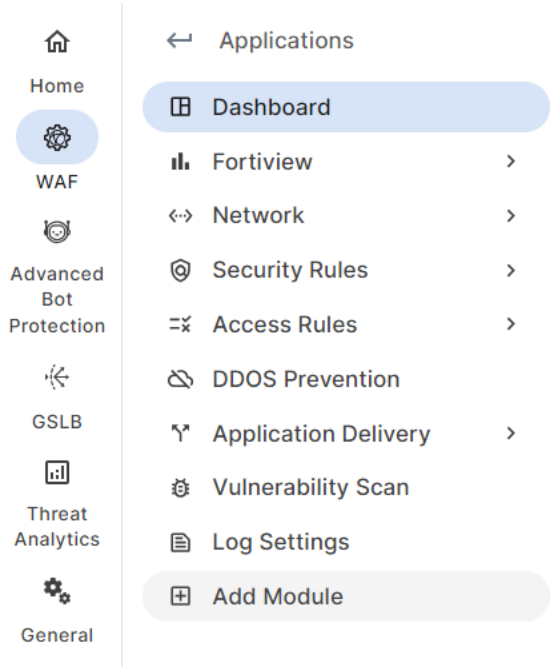
Add and Remove Modules

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 **WAF > Application** and click into the desired application.
2. Click **WAF** in the side navigation bar to expand the menu, and click **Add Module**.



3. In the module list, locate the modules you want to add.
4. Click to enable them.
5. Click **OK** to save changes.

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 Module**.
2. In the module list, locate the modules you want to remove.
3. Click to disable them.
4. Click **OK** to save changes.

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

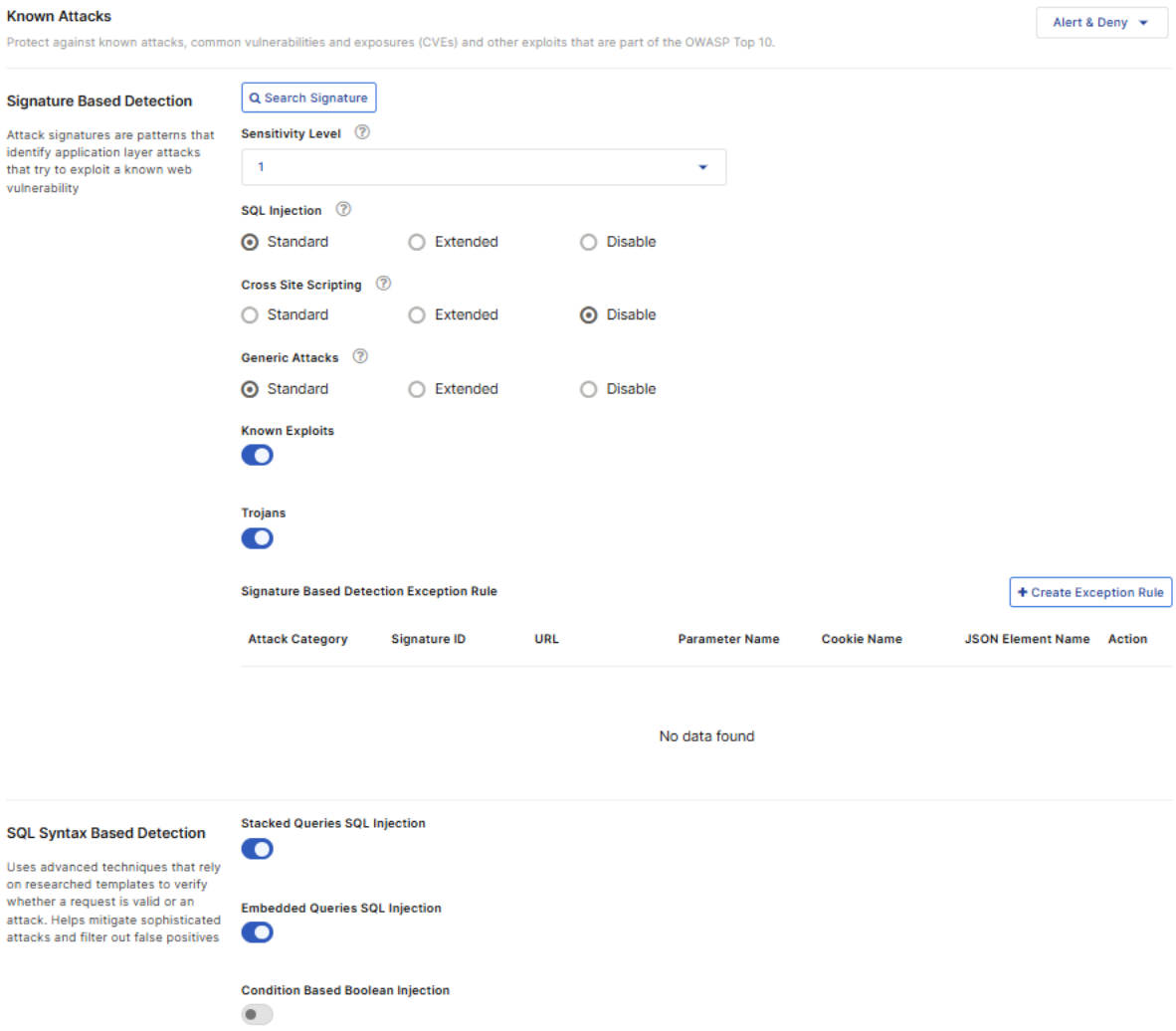
With security rules configured, FortiAppSec Cloud detects messages in HTTP requests that access web servers to prevent web servers from known attacks, protect the privacy-sensitive information in the messages such as Cookie, and restrict, scan uploaded files.

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

FortiAppSec Cloud leverages continuously updated signatures to defend against OWASP Top 10 threats, including Cross-Site Scripting (XSS), SQL Injection, Generic Attacks, Known Exploits, and Trojans. By parsing packet-level messages, comparing them against the signature database, and applying predefined actions,FortiAppSec Cloud ensures comprehensive protection for your applications.



The signature database is updated on the 15th and 31st of each month. You can view the latest updates on the FortiGuard Web Application Security page.

New signatures are set to **Alert** mode by default, and are not editable. Modifications related to known attacks are not applied to these new signatures until the following update cycle.

Example:

If signature **8888888** is released on **March 15th**, it will remain in Alert mode from March 15th to March 31st. Any modifications for known attack detection will be applied to this signature after April 1st, during the next update cycle.

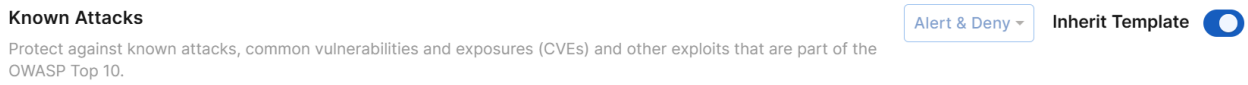
Configure Known Attacks

1. Go to **Security Rules > Known Attacks**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.

2. Select the action that FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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.

3. If your application is using a template, this page will display the **Inherit Template** switch next to the **action**. When enabled, this indicates the module's settings for the current application are inherited from the configured template.



Disabling **Inherit Template** switches the configuration source for all modules of this application from the template to the application's own settings. This allows for custom adjustments specific to the current application, without affecting other applications sharing the same template.

4. 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	The Sensitivity Level (SL) controls how aggressively FortiAppSec Cloud protects against application signatures across different attack categories. You can choose from four tiers, with SL1 being the least strict and SL4 being the most strict. While higher levels offer more protection by including more signatures, they can also increase the risk of false positives, which may block legitimate traffic. We recommend selecting an SL based on your application's security sensitivity, setting it to Monitor mode, and reviewing the Attack Log for signatures triggered during normal access. If too many false positives occur, adjust the SL accordingly. To see which signatures are included at each sensitivity level: 1. Navigate to **WAF > Application > Security Rules > Known Attacks > Signature Based Detection.** 2. Click **Search Signature**. 3. In the **Search By** dropdown menu, select **Sensitivity Level**. 4. Set the desired Sensitivity Level. 5. Click the magnifying glass icon to perform the search. The included signatures should appear under **Signature Information**. **Note 1:** This setting also affects the **Server Information Disclosure** and **Personally Identifiable Information** options under Information Leakage on page 140 because Sensitivity Level determines how many matching rules are applied to detect response headers and page content. After adjusting Sensitivity Level, review the safeguards described in the Information Leakage section to ensure full protection. **Note 2:** A signature's Sensitivity Level is independent of whether it is in standard or extended mode. Mode selection only determines which signatures are active.
SQL Injection	Enable to prevent SQL injection attacks, such as blind SQL injection.

	Standard: Detects attacks by comparing application traffic against a set of known malicious signatures. **Extended:** Detects attacks by comparing traffic against a larger set of signatures, enhancing detection rates with more granular rules but potentially increasing false positives.
Cross Site Scripting	Enable to prevent a variety of cross-site scripting (XSS) attacks, such as varieties of CSRF (cross-site request forgery). **Standard:** Detects attacks by comparing application traffic against a set of known malicious signatures. **Extended:** Detects attacks by comparing traffic against a larger set of signatures, enhancing detection rates with more granular rules but potentially increasing false positives.
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). **Standard:** Detects attacks by comparing application traffic against a set of known malicious signatures. **Extended:** Detects attacks by comparing traffic against a larger set of signatures, enhancing detection rates with more granular rules but potentially increasing false positives.
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, Signature ID, or Sensitivity Level.

5. Click **Create Exception Rule** to omit attack signature scans when you know that some parameters or URLs cause false positives by matching an attack signature during normal use. Traffic that matches the exception rule(s) bypasses the configured security measures and will not be blocked.



Enable at least one option between **Request URL** and **Parameter Name**. Requests matching the specified URL and/or parameter in the exception rule will be exempted from being flagged as attacks.

Request Host	Specify the host value (domain name) to match. For example, `www.test.com` or `api.test.com`. • If **String Match** is selected, is selected, enter the host name directly. Wildcards are supported (e.g., `*.test.com`). • If **Regular Expression Match** is selected, you can define a regex pattern to match one or more hostnames. For details, see Frequently used regular expressions on page 243.
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. • **String Match** may not correctly recognize URLs containing double slashes (//). To avoid matching issues, use **Regex Expression Match** and allow one or more slashes (e.g., `setup/+letter_templates_01`) to ensure compatibility with normalized URLs. • 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 243. 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.

6. **SQL Syntax Based Detection**, enable the options to detect the corresponding SQL injection types. FortiAppSec 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.

7.

Stacked Queries SQL Injection	Enable to block attacks that exploit vulnerabilities by appending multiple SQL queries to execute unauthorized commands.
Embedded Queries SQL Injection	Enable to block attacks that insert malicious queries within legitimate ones to manipulate database responses.
Condition-Based Boolean Injection	Enable to block attacks that evaluate true/false conditions in SQL statements to infer sensitive data.
Arithmetic Operation-Based Boolean Injection	Enable to block attacks that leverage arithmetic operations in SQL queries to deduce information based on responses.
Line Comments	Enable to block attacks that use SQL comments to bypass query syntax and inject malicious commands.
SQL Function-Based Boolean Injection	Enable to block attacks that exploit SQL functions to assess query behavior and extract data.

8. In **XSS Syntax Based Detection**, enable theEnable to block attacks that option to detect the corresponding XSS attack types. FortiAppSec 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.

9.

HTML Tag Based XSS Injection	Enable to block attacks that embed malicious scripts within HTML tags to manipulate webpage behavior.
HTML Attribute Based XSS Injection	Enable to block attacks that inject harmful code into HTML attributes to execute unauthorized actions.
HTML CSS Based XSS Injection	Enable to block attacks that exploit CSS properties in HTML to deliver malicious scripts or alter visual elements.
JavaScript Function Based XSS Injection	Enable to block attacks that insert harmful code into JavaScript functions to execute unauthorized operations.
JavaScript Variable Based XSS Injection	Enable to block attacks that manipulate JavaScript variables to inject and execute malicious scripts.
Syntax Based Detection Exception Rule	Enable to block attacks that excludes specific syntax patterns from triggering security rules, allowing controlled exceptions.

10. 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. Traffic that matches the exception rule(s) bypasses the configured security measures and will not be blocked.

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 243. 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 */ ".

11. Click **SAVE**.

Anomaly Detection

Use machine learning-enabled Anomaly Detection to block zero day threats and other sophisticated attacks by automatically building and maintaining a model of normal user behavior. To determine if a request is legitimate or a potential malicious attack, the system performs the following tasks:

- Captures and collects inputs, such as URL parameters, to build a mathematical model of allowed behavior.
- Matches anomalies against pre-trained threat models.
- Identifies and flags potential attack attempts based on deviations from the established model.

Once an anomaly is triggered by the mathematical model, FortiAppSec 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.

This module is a **FortiAppSec Cloud Advanced** feature.

Model settings

FortiAppSec 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 Add and Remove Modules.
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**, FortiAppSec Cloud will or will not collect samples from the specified IP ranges.

3. Select the action that FortiAppSec 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 **WAF > 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.

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 FortiAppSec 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, FortiAppSec 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.



FortiAppSec Cloud requires at least one parameter rule to be added for each request URL to successfully apply parameter validations. Otherwise, FortiAppSec 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 Add and Remove Modules.
2. Click **Create Rule**.
3. 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** – FortiAppSec Cloud will record the invalid request in the attack log. • **Deny** – FortiAppSec 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)** – FortiAppSec 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. If **Period Block** is selected, specify the time period between 1 to 3600 seconds.

4. Click **Add Rule**.

5. 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 243.
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 243. Available only if you enabled **Use Type Check** and selected **Regular Expression** as the **Argument Type**.

6. Click **Save Rule**.
7. Repeat steps 2-6 until you have added all desired rules, or click **OK** to save configurations and return to the **Parameter Validation** page.
8. Click **SAVE** to apply configurations.

Information Leakage

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

How Known Attacks settings affect Information Leakage

The **Sensitivity Level** configured under **Signature Based Detection** on the **Security Rules > Known Attacks** page directly influences how effectively FortiAppSec Cloud mitigates Information Leakage. This is because Sensitivity Level determines how many matching rules are applied to detect response headers and page content.

Higher sensitivity levels include more signatures that add additional protection but can also introduce false positives that may block legitimate traffic.

Configuring **Sensitivity Level** too low can leave critical Information Leakage vulnerabilities unblocked. For more information, see Known Attacks.

Configure Information Leakage protection

1. Go to **Security Rules > Information Leakage**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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. Server-specific sensitive information includes information that could reveal known or potential vulnerabilities, such as software name/ version, backend technology frameworks and library versions, error messages, internal IP addresses, and authentication details
Personally Identifiable Information	Enable to detect and prevent the exposure of sensitive personal data, such as names, email addresses, and credit card numbers, in HTTP responses. It helps reduce the risk of data leaks by identifying PII patterns and allowing administrators to log, alert, or block such disclosures based on security policies.
Cloak Error Pages	Enable to replace HTTP 403 (Forbidden), 404 (Not Found), and 5XX (Server Errors) responses with a generic 500 (Internal Server Error) response. This enhances security by preventing attackers from gathering information about your server through specific error responses that distinguish between missing pages, permission issues, or server failures, making it harder to map vulnerabilities. You can add multiple HTTP headers in which the sensitive information will be hidden.
Erase HTTP Headers	Enable to remove server response HTTP headers. You can specify multiple HTTP headers in which the sensitive information will be hidden.

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

Request Host	Specify the host value (domain name) to match. For example, `www.test.com` or `api.test.com`. • If **String Match** is selected, is selected, enter the host name directly. Wildcards are supported (e.g., `*.test.com`). • If **Regular Expression Match** is selected, you can define a regex pattern to match one or more hostnames. For details, see Frequently used regular expressions on page 243.
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 243. 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.



You must enable at least one of the following: **Request URL** or **Parameter Name**. 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 FortiAppSec 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 **WAF > 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

FortiAppSec Cloud can protect against cookie poisoning and other cookie-based attacks. When **Cookie Security** module is added FortiAppSec 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 Add and Remove Modules.
2. Configure these settings.

Cookie Replay Protection	Enable to select whether FortiAppSec 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**—FortiAppSec Cloud does not apply cookie tampering protection or encrypt cookie values. • **Signed**—Prevents tampering (cookie poisoning) by tracking the cookie value. When FortiAppSec 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 FortiAppSec Cloud uses to detect tampering with the cookie from the backend server response. If FortiAppSec 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. FortiAppSec 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.
Set Same Site Cookie	Enable to restrict cookies that fall outside of a first-party or same-site context. **Same Site Value** • **Strict** — Cookies will not be included in any requests from third parties. • **Lax** — Cookies will not be included in third-party requests, except for GET requests that navigate to the destination URL. • **None** —Use this option if a cookie needs to be sent across different origins.

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.

3. Select the action that FortiAppSec 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 **WAF > 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**.

File Protection

You can configure FortiAppSec 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 FortiAppSec Cloud has identified as threats.

1. Go to **Security Rules > File Protection**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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. Please note that due to caching limits, this feature can only process files smaller than 5 MB.
Advanced Threat Protection	Enable to send matching files to FortiSandbox Sandbox for evaluation. Sandbox file evaluation is performed in the same region where the FortiAppSec 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.
JSON File Support	Enable if you want to further parse the information contained in uploaded JSON files. **File Name JSON Key Field**- Locate the value of the filename parameter, and compare it against the value you entered in this field. This is optional. **File Upload JSON Key Field**- Locate the value of the content parameter, and compare it against the value you set in this field.

3. Select the action that FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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 FortiAppSec 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 FortiAppSec Cloud can insert into responses.

To configure HTTP Header Security, you must have already enabled this module in **Add Modules**. See Add and Remove Modules.

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').
Referrer-Policy	Referrer-Policy HTTP header controls how much referrer information (sent via the Referer header) should be included with requests. The **Referrer-Policy Value** can be the following: • **no-referrer**: Never send the Referer header with requests. • **no-referrer-when-downgrade**: Send the full URL as referrer, unless navigating from HTTPS to HTTP. • **same-origin**: Send the Referer header only for requests to the same origin. • **origin**: Send only the origin (scheme + host + port) as the referrer. • **strict-origin**: Send the origin only for same or higher security level (e.g., HTTPS → HTTPS). • **origin-when-cross-origin**: Send the full URL for same-

	origin requests, but only the origin for cross-origin. • **strict-origin-when-cross-origin**: Like origin-when-cross-origin, but restricts referrer to secure-to-secure contexts. • **unsafe-url**: Always send the full URL as the referrer, regardless of origin or protocol (least secure).

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. FortiAppSec 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 Add and Remove Modules.

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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

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, FortiAppSec 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 , FortiAppSec 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, FortiAppSec 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 FortiAppSec 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, FortiAppSec 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.

FortiAppSec 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, FortiAppSec Cloud will take action according to your configuration.

To configure MITB Protection, you must have already enabled this module in **Add Modules**. See Add and Remove Modules.

- 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, FortiAppSec Cloud will take actions (alert, or alert & deny) accordingly.
- Select the action that FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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

- Click **SAVE**.

Access Rules

Control client access to your web applications and regulate request rates using various methods, depending on whether actions are based on the URL, the client's source IP, or more complex criteria.

This module is enabled by default, as the Request Limits option is automatically activated when 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 FortiAppSec 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 Add and Remove Modules.
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.
	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.
	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
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.
	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.
	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.
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.

	Missing Host	Enable to check if the Host header is missing. For HTTP/2, Missing Host violation appears only when both the Authority and Host headers do not exist
HTTP/2RST		
	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.
Content Length		
	Content Length	Specifies the maximum acceptable length in bytes of the request body. Length is determined by comparing this limit with the value of the Content-Length: field in the HTTP header. Attack log messages contain `Content Length Exceeded` when this feature detects a content length buffer overflow attempt.
	Present with Transfer Encoding	Enable to check if `content-length` and `transfer-encoding` coexist.
	Inconsistent with Body Length	Enable to check whether the response has redundant body than the `content-length` specified.
Others		
	Range Overlapping	Enable to detect RangeAmp Overlapping Byte Ranges (OBR) attacks. For more information on this attack, refer to https://www.linuxadictos.com/en/rangeamp-a-series-of-cdn-attacks-that-manipulate-the-range-http-header.html
	Multipart/ form-data Bad Request	Enable to detect whether the multipart request chunk contains the strings "Content-Disposition" and "Name". If it does not, the system will consider it a violation.

3. Select the action that FortiAppSec 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 **WAF > 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).
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 FortiAppSec 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 Add and Remove Modules.
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 243.
Action	Select the action that FortiAppSec Cloud takes when it detects a violation of the rule. • **Alert & Deny**—Block the request (or reset the connection) and generate a 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, FortiAppSec 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 Add and Remove Modules.

IP reputation

To block the following attacks, you can configure FortiAppSec 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, FortiAppSec Cloud 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, FortiAppSec Cloud 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.

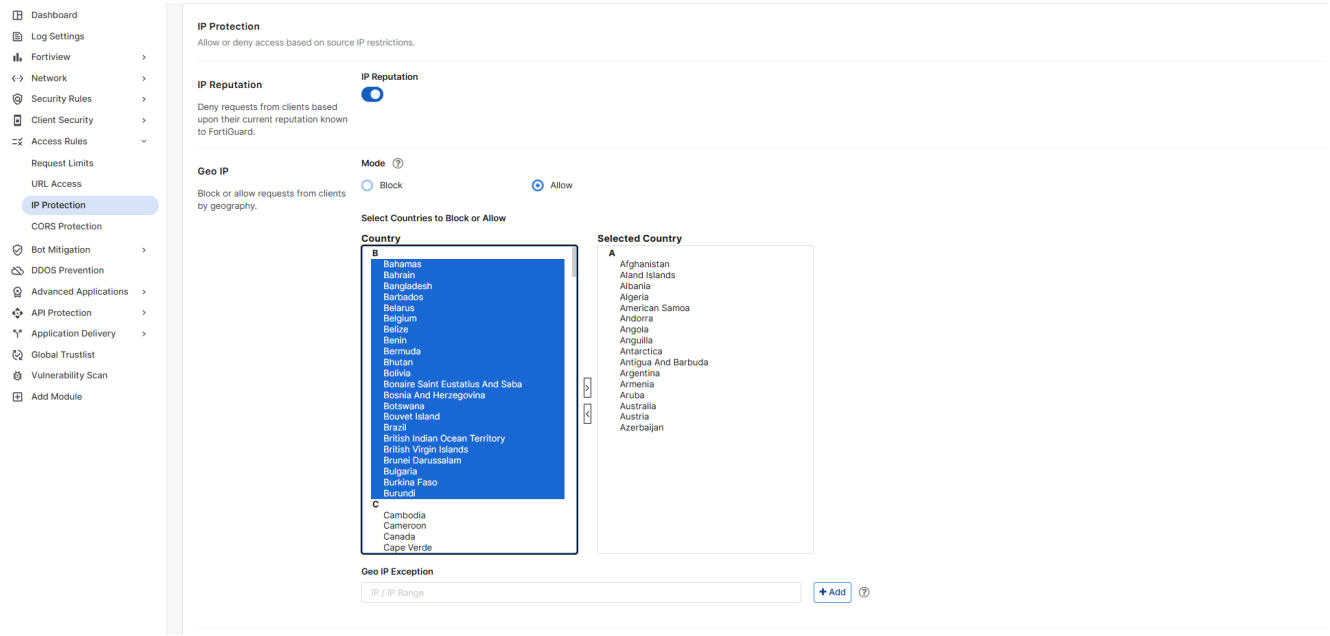
Check whether an IP address is malicious through FortiGuard IP Web Application Security Service: https://www.fortiguard.com/services/botnet.

If you believe an IP address is wrongly classified as a malicious IP, you can report it to our TAC team.

For help with Geolocation Service and issues, you can find more information at https://www.fortiguard.com/services/ipge, and submit a report at https://www.fortiguard.com/faq/ipge.

Go to **ACCESS RULES > IP Protection** to enable IP Reputation.

Geo IP



To configure blocking or allowing by geography, first choose whether to block or allow the countries in the **Selected Country** list.

Select one or more regions that you want to block traffic 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).

Geo IP Exception

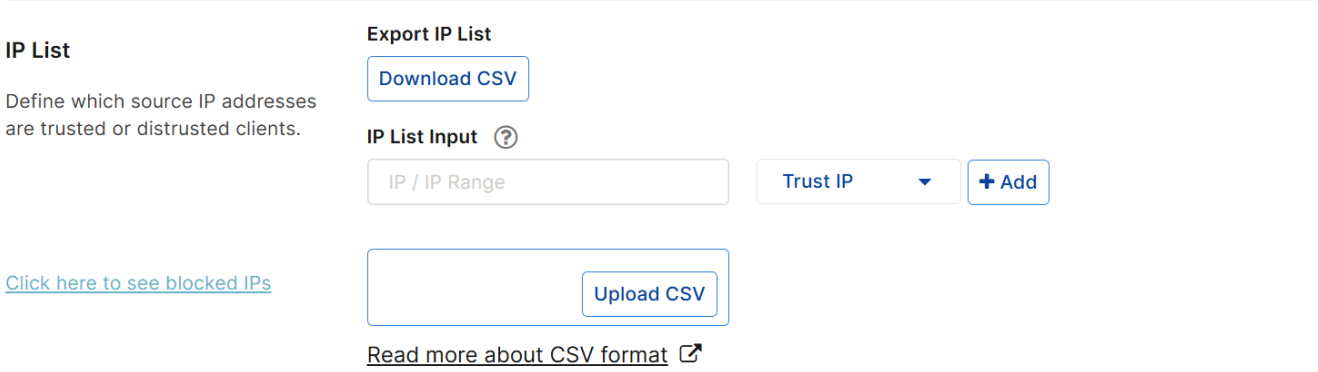
Add IP addresses from blocked geographic locations to the exception list so that traffic from those IP addresses is not blocked.

While there is no maximum number of supported IP addresses, the character limit for this list is 1 048 576. Therefore, the number of supported IP addresses will vary depending on their length.

IP list

Define trusted, distrusted, or allowed client IP addresses.

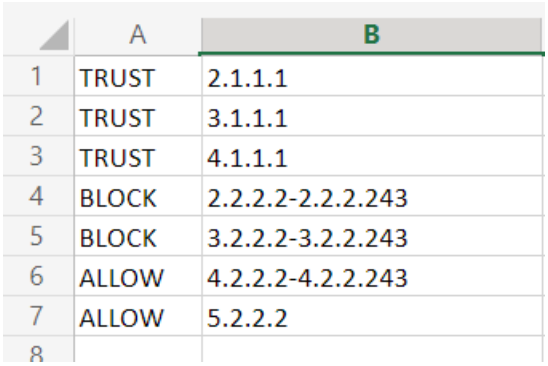
Click **Download CSV** to download a file of your trusted and untrusted IPs.



There are two ways to add IPs to your allowlist or blocklist:

- **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.
  Select a **Type** to indicate the action FortiAppSec Cloud takes on the input IP/IP Range. For more information on the selected **Type**, please refer to Type on page 157
- **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" . For more information on the selected **Type**, please refer to Type on page 157
  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>



	A	B
1	TRUST	2.1.1.1
2	TRUST	3.1.1.1
3	TRUST	4.1.1.1
4	BLOCK	2.2.2.2-2.2.2.243
5	BLOCK	3.2.2.2-3.2.2.243
6	ALLOW	4.2.2.2-4.2.2.243
7	ALLOW	5.2.2.2
8		

Type

Choose an action to take for each input IP/IP range:

- **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, FortiAppSec 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.

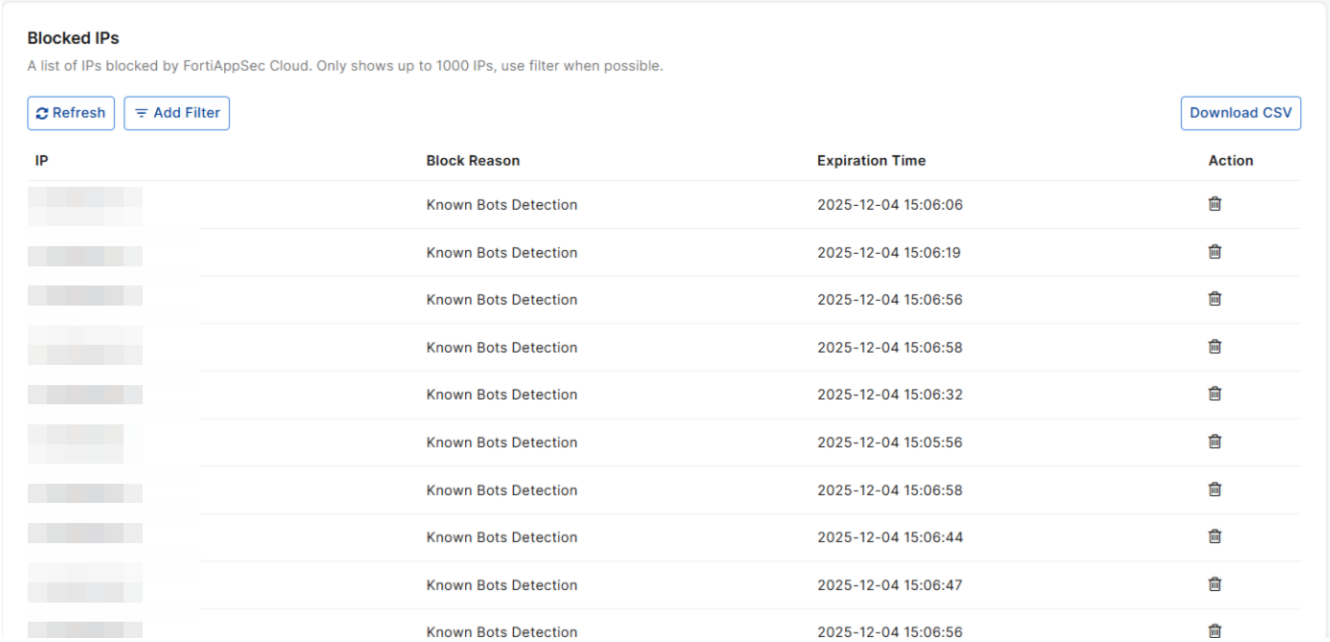
The scan sequence for processing IP addresses is as follows: **Block IP > Trust IP > Allow Only**. For example, if an IP address is present in the **Block IP** list, the system will block it immediately without proceeding to scan against the **Trust IP** and **Allow Only** IP lists.

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.

Blocked IPs List

Click the **Click here to see blocked IPs** link to view all IPs already blocked by FortiAppSec Cloud.



IP	The blocked IP address.
Block Reason	The reason an IP address was added to the blocklist
Expiration Time	The date and time when this blocked IP will be automatically removed from the blocklist and allowed to connect again.
Action	Click the **delete** icon to remove this IP from the blocklist and allow future connections.

To apply changes, 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 FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud can verify whether the headers used in the CORS requests are legitimate.
Exposed Headers	Click **Add** to add the exposed headers so that FortiAppSec Cloud can expose the specified headers in JavaScript and share with foreign applications.

7. Click **Save**.

Bot Mitigation

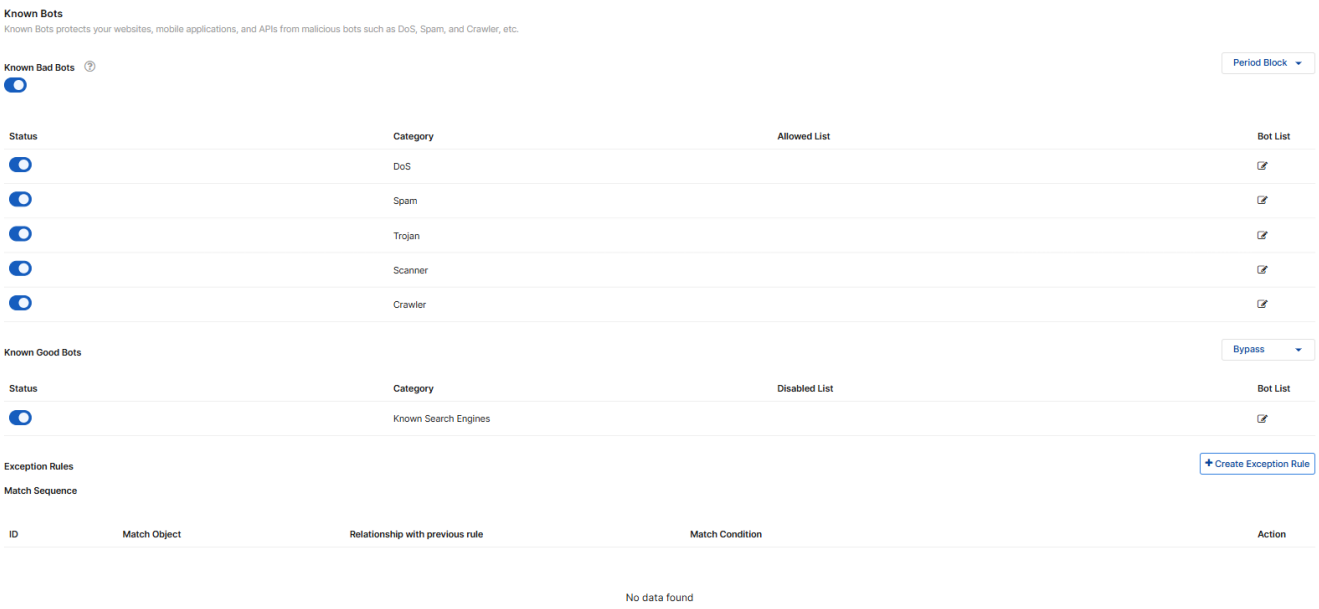
To quickly protect websites, mobile apps and APIs from automated threats, you can configure the bot mitigation feature to check more specific signatures such as client events, and occurrence of suspicious behaviors, etc. of regular clients.

- Known Bots
- Threshold Based Detection
- ML Based Bot Detection
- Biometrics Based Detection
- Bot Deception
- Advanced Bot Protection

Known Bots

Configuring Known Bots protects your websites, mobile applications, and APIs by blocking known malicious bots (e.g., DoS, Spam, Crawlers) while permitting activity from beneficial bots, such as search engines. This ensures robust security while maintaining the seamless 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.



Configure Known Bots settings

1. Go to **Bot Mitigation> Known Bots**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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 **Enabled List**. Click the **Edit** icon on each Bot List if you want specific bots to be exempted. The search engines moved to the **Disabled List** will not be screened against.

4. Select the action that FortiAppSec Cloud takes when it detects a Known Good or Bad Bot.

Bypass	Accept the request with no generated log or alert.
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).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.
Bypass	Accept the request and skip the subsequent scans after known bots in the Sequence of Scans.

5. Click **SAVE**.

Configure Exception Policy

Exclude specific parameters or URLs from bot mitigation scans. This is useful when certain elements are known to trigger false positives during normal operations.

For more details, please refer to Exception Policy on page 168.

Threshold Based Detection

With the occurrence, time period, and severity of the following suspicious behaviors predefined, FortiAppSec 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. Navigate to **WAF > Bot Mitigation> Threshold Based Detection**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.

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, FortiAppSec 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, FortiAppSec 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, FortiAppSec 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, FortiAppSec Cloud will take actions.
Credential Based Brute Force	Enable to block brute force attacks that try to obtain user credentials by detecting whether a user is accessing a specific URL too frequently after logging in. To enable Credential Based Brute Force, Account Takeover on page 191 must also be enabled. Please note, this feature only tracks users who have successfully logged in and can thus be monitored by Account Takeover.
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 243. 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, FortiAppSec 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 FortiAppSec 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, FortiAppSec Cloud applies specified actions. If the client appears to be a web browser, FortiAppSec 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, FortiAppSec 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 FortiAppSec 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 **WAF > System Settings > Settings**.



The default action for Threshold-Based Detection is Period Block, and it is not recommended to modify this configuration.

Period Block is the most effective action for Threshold-Based Detection. When the number of suspicious behaviors reaches the defined threshold, this action blocks all subsequent requests from the offending IP address for the next 10 minutes. In contrast, selecting Alert & Deny or Deny (no log) results in only the request that exceeds the threshold being denied, while subsequent requests are allowed until the threshold is reached again.

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).
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**.

Configure Exception Policy

Exclude specific parameters or URLs from bot mitigation scans. This is useful when certain elements are known to trigger false positives during normal operations.

For more details, please refer to Exception Policy on page 168.

ML Based Bot Detection

The AI-based bot detection model enhances existing signature- and threshold-based rules by identifying sophisticated bots and credential-stuffing (CC) attacks that may evade traditional detection methods.

Unlike conventional bot detection mechanisms, which require manual threshold configuration to distinguish normal from abnormal user behavior, the machine learning (ML)-based model automates this process. For example, determining an appropriate threshold for the number of HTTP requests a user can make before being flagged as suspicious often requires iterative adjustments and continuous log monitoring.

The ML-based bot detection model leverages a Support Vector Machine (SVM) algorithm to construct a self-learning model that profiles legitimate client traffic. Incoming traffic is analyzed against these learned profiles, and deviations result in anomaly classification. When application usage patterns change—such as due to feature updates—the model automatically recalibrates to maintain accuracy.

Additionally, testing indicates that the ML-based bot detection model significantly improves detection accuracy, particularly for crawlers and scrapers. By evaluating traffic across 13 dimensions, it enhances detection precision while reducing false positive rates.

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 Add and Remove Modules.
2. Select the **Model Settings** tab.
3. Configure the following settings.

Client Identification Method	FortiAppSec 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 the configured count of anomalies from a user, it takes action(s) such as sending alerting emails or blocking the traffic from this user. **Anomaly Count** controls the number of anomalies 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 enact the configured action(s). 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 user information. If the user revisits your application, they will be treated as new users and the system starts anomaly counting afresh. This feature may be useful for avoiding 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. FortiAppSec 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. (Optional) Add exception rules for traffic that meets the configured criteria so that it is not blocked.

Field	Description
Match Object	The criteria used to base the rule for directing traffic. In this drop-down menu, you can select from the following options: • **Client IP** • **Host** • **URI** • **Full URL** • **Parameter** • **Cookie**
Match Condition	Select a matching method. If **Match Object** is **Client IP**, select one of: • **Equal** • **Not Equal** For all other **Match Objects**, select one of: • **String Match** • **Regular Expression Match**
IP/ IP Range	Enter the IP address(es) and/or IP range(s) you wish to allow, separated by commas. For example: 1.2.3.4, 1.2.3.4-1.2.3.40
Relationship with previous rule	Select whether the current rule should run concurrently with or as an alternative to the previous rule. • **AND** • **OR** For the first rule in a match sequence, this field has no effect. Please note, rules bound by an AND relationship take precedence over those with OR relationships. This ensures all AND conditions must be met before considering OR conditions.

5. Select the action that FortiAppSec 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 **WAF > 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.
Deny (no log)	Block the request (or reset the connection) without generating a log message.

6. Click **SAVE**.

Biometrics Based Detection

By checking the client events such as mouse movement, keyboard, screen touch, and scroll, etc in specified period, FortiAppSec Cloud judges whether the request comes from a human or from a bot.

Configure Biometrics Based Detection Settings

1. Go to **Bot Mitigation> Biometrics Based Detection**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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 FortiAppSec 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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

7. Click **SAVE**.

Configure Exception Policy

Exclude specific parameters or URLs from bot mitigation scans. This is useful when certain elements are known to trigger false positives during normal operations.

For more details, please refer to Exception Policy on page 168.

Bot Deception

To prevent bot deception, you can configure the insertion of a link into HTML-type response pages. For regular clients, the link remains invisible, while for malicious bots, such as web crawlers, the bots may attempt to request the resource that the invisible link points to, revealing their behavior.

Configure bot deception

1. Navigate to **WAF> Application > Bot Mitigation > Bot Deception**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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.
   - This Deception URL should not point to a real, existing page on your server. It should be a nonexistent or fake path that no normal user would ever click or see.
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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.

6. Click **SAVE**.

Configure Exception Policy

Exclude specific parameters or URLs from bot mitigation scans. This is useful when certain elements are known to trigger false positives during normal operations.

For more details, please refer to Exception Policy on page 168.

Exception Policy

Create an exception policy to exclude specific parameters or URLs from bot mitigation attack scans when they are known to trigger false positives during normal use. The exception policy can be applied to Known Bots, Threshold Based Detection, Biometrics Based Detection, and Bot Deception to refine detection accuracy while minimizing unintended blocks.

Create an Exception Policy

1. Navigate to **Bot Mitigation >** **Known Bots**, **Threshold Based Detection**, **Biometrics Based Detection**, or **Bot Deception** and configure the applicable rules.
2. Click **Create Exception Rule**. This will define the criteria for applying the exception rule.
3. Select a **Match Object**, and configure its corresponding settings according to the table below.
4.

Client IP		
	Match Condition	• **Equal**—FortiAppSec Cloud does not perform a bot mitigation attack scan for requests with a client IP address or IP range that matches the value of **IP/ IP Range**. • **Not Equal**—FortiAppSec Cloud only performs a bot mitigation attack scan for requests with a client IP address or IP range that matches the value of **IP/ IP Range**.
	IP/ IP Range	Specify the client IP address or IP range that FortiAppSec Cloud uses to determine whether or not to perform a bot mitigation attack scan for the request.
Host		
	Match Condition	• **String Match**—**Value** is a literal host name. • **Regular Expression Match**—**Value** is a regular expression that matches all and only the hosts that the exception applies to.
	Value	Specifies the `Host:` field value to match.
URI		
	Match Condition	• **String Match**—**Value** is 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`. • **Regular Expression Match**—**Value** is a regular expression that matches all and only the URIs that the exception applies to.
	Value	Specifies a URL value to match. You can use up to 2048 characters in regex configuration for signature. The value does not include parameters. For example, `/testpage.php`, which match requests for `http://www.test.com/testpage.php?a=1&b=2`. If **Operation** is **String Match**, ensure the value starts with a forward slash (/) (for example, `/causes-false-positives.php`). If **Operation** is **Regular Expression Match**, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash.

	Do not include a domain name or parameters. To match a domain name, use the **Host** element type. To match a URL that includes parameters, use the **Full URL** type.
Full URL	
Match Condition	• **String Match**—**Value** is 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`. • **Regular Expression Match**—**Value** is a regular expression that matches all and only the URLs that the exception applies to.
Value	Specifies a URL value that includes parameters to match. For example, `/testpage.php?a=1&b=2`, which match requests for `http://www.test.com/testpage.php?a=1&b=2`. If **Operation** is **String Match**, ensure the value starts with a forward slash (/) (for example, `/testpage.php?a=1&b=2`). If **Operation** is **Regular Expression Match**, the value does not require a forward slash (/). However, ensure that it can match values that contain a forward slash. Do not include a domain name. To match a domain name, use the **Host** element type. To match a URL that does not include parameters, use the **URI** type.
Parameter	
Match Condition	• **String Match**—**Name** is the literal name of a parameter. • **Regular Expression Match**— **Name** is a regular expression that matches all and only the name of the parameter that the exception applies to.
Name	Specifies the name of the parameter to match.
Check Value of Specified Element	Enable to specify a parameter value to match in addition to the parameter name.
Value	Specifies the parameter value to match.
Cookie	
Match Condition	• **String Match**—**Name** is the literal name of a cookie. • **Regular Expression Match**— **Name** is a regular expression that matches all and only the name of the cookie that the exception applies to.
Name	Specifies the name of the cookie to match.
Check Value of Specified Element	Select to specify a cookie value to match in addition to the cookie name.

Value	Specifies the cookie value to match.

5. Select the **Relationship with previous rule**:
   - **AND:** The rule will apply concurrently with the previous rule, meaning both conditions must be met. This creates a stricter condition where all linked rules must be met.
   - **OR:** The rule will apply as an alternative to the previous rule, meaning either condition can be met.

   For the first rule in a routing sequence, this field has no effect.

   Please note, rules bound by an AND relationship take precedence over those with OR relationships. This ensures all AND conditions must be met before considering OR conditions.
6. Click **OK**.
7. Repeat the steps above as needed to configure additional rules and exception rules.
8. Click **SAVE** to save your Exception Policy settings.

DDoS prevention

Connection Limits

FortiAppSec Cloud DDoS prevention Connection Limits 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.

FortiAppSec Cloud allows you to configure Connection Limits at two layers:

- Application layer (HTTP or HTTPS)
- Network and transport layer (TCP/IP)

With the public cloud infrastructure affront providing the first layer of defense against volumetric attacks, FortiAppSec Cloud enhances DDoS protection by focusing on sophisticated attacks targeting the application layer, such as low and slow attacks. Together they provide protection for the full layer 3-7 DDoS attack types. Additionally, Fortinet operations team also adds network and application protection customizations in real-time to help protect against the most sophisticated DDoS threats.

To configure **DDoS prevention Connection Limits** , you must have already enabled this module in **Add Modules**. See Add and Remove Modules.

Configuring application-layer DDoS prevention Connection Limits

For some DDoS prevention Connection Limits features, FortiAppSec Cloud uses session management to track requests.

1. When FortiAppSec 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, FortiAppSec Cloud examines the session cookie in the request.
   - If the cookie does not exist or its value has changed, FortiAppSec Cloud drops the request.
   - If the same cookie exists, the request is treated as part of the same session. FortiAppSec Cloud increments its count of connections and/or requests from the client. If the rate exceeds the limit, FortiAppSec 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 FortiAppSec 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 FortiAppSec 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 **WAF > 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).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.

Advanced Applications

With this module, you can configure XML protection to ensure no potential attacks in requests containing XML; also, you can configure FortiAppSec 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 Add and Remove Modules.
2. Click **+Create Rule**.
3. Configure these settings.

Name	Type a unique name for the custom rule.
Operation	Select which action the FortiAppSec 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.
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 FortiAppSec 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, FortiAppSec Cloud applies specified actions. If the client appears to be a web browser, FortiAppSec 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, FortiAppSec

	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 FortiAppSec 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 FortiAppSec 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. **Missing Header Name**: Once enabled, the request matches the condition if it does not contain the specified header. This setting cannot be enabled at the same time as **Empty Header Value Check**. Please note that this setting does not take effect for HTTP2 packets without the following headers:

- :method
- :scheme
- :path
- :authority
- :status HTTP2 packets without the above headers will not go far to be scanned against the custom rule settings. It will be considered as illegitimate and be abandoned directly when it arrives at FortiWeb at the first place.

Empty Header Value Check: Once enabled, the request matches the condition if it contains the specified header but the value of the matched header is empty. This setting cannot be enabled at the same time as **Missing Header Name**.

- **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.
  Missing Header Name: Once enabled, the request matches the condition if it does not contain the specified header. This setting cannot be enabled at the same time as **Empty Header Value Check**. Please note that this setting does not take effect for HTTP2 packets without the following headers:
  - :method
  - :scheme
  - :path
  - :authority
  - :status HTTP2 packets without the above headers will not go far to be scanned against the custom rule settings. It will be considered as illegitimate and be abandoned directly when it arrives at FortiWeb at the first place.

  Empty Header Value Check: Once enabled, the request matches the condition if it contains the specified header but the value of the matched header is empty. This setting cannot be enabled at the same time as **Missing Header Name**.

- **HTTP Method**
  - **Method Pattern**: Configure a regular expression for the HTTP method that FortiAppSec 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 FortiAppSec 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.

GEO IP	The request matching the specified countries will not be handled.
	• **Selected Country**: Choose the country or countries to use for matching. Requests that match this rule will not be handled.
	• **Match Exclusively**:
	  • **Enabled**: The rule matches traffic from all countries except the selected ones.
	  • **Disabled**: The rule matches traffic only from the selected countries.

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.

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.

FortiAppSec 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 > WebSocket Security**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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 FortiAppSec 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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

2. Click **SAVE**.

API Protection

FortiAppSec 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. FortiAppSec Cloud parses the contents of each API call against the schema/validation file and take appropriate actions to protect you from malicious traffic.

For full API documentation, see https://portal.appsec.fortinet.com/apidoc/api.html.

FortiAppSec 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

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 FortiAppSec Cloud to scan against. For example, if request URLs are defined in the validation file, FortiAppSec 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, FortiAppSec 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.



FortiAppSec Cloud only supports OpenAPI 3.0.

To configure an OpenAPI Validation rule

1. Go to **API PROTECTION > OpenAPI Validation**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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.



We recommend using **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 the icons  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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

6. 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.



When an application's API Gateway module starts or stops inheriting settings from a template, the system automatically regenerates API keys for all users within that module.

This ensures that the new keys are unique and independent from those defined in the source template.

Inheritance can stop in the following cases:

- The application is still linked to the template, but inheritance for the API Gateway module has been turned off.
- The application has been completely unlinked from the template.

Important: To prevent service disruptions, replace all existing API keys with the newly generated ones wherever they are in use.

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 Add and Remove Modules.
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 the plus icon  .
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 the plus icon  .

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 FortiAppSec 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, FortiAppSec Cloud obtains the API key from the request. When this option is enabled, FortiAppSec Cloud verifies the key to check whether the key belongs to an valid API user.
API Key In	Indicate where FortiAppSec 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 FortiAppSec 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 FortiAppSec 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 FortiAppSec 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 **WAF > 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).
Period Block	Block the current request. Moreover, all the subsequent requests from the same client in the next 10 minutes will also be blocked.

2. 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, FortiAppSec 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 Add and Remove Modules.
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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

4. 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 Add and Remove Modules.
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**, FortiAppSec 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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

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 Add and Remove Modules.
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**, FortiAppSec 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 FortiAppSec Cloud takes when it detects a violation of the rule from the top right corner.

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).

6. Click **SAVE**.

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 Add and Remove Modules.
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**: FortiAppSec Cloud collects API request samples only from the **Trust** source IP addresses. • **Block**: FortiAppSec 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, FortiAppSec Cloud will not collect samples from any Source IP address. If the IP List Type is **Block** and the **Source IP List** is empty, FortiAppSec 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 Add and Remove Modules.
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 FortiAppSec 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/

FortiAppSec Cloud supports the following types in parameter:

- boolean
- number
- string
- object (one level)

FortiAppSec 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" }
]
}
```

Account Takeover

Account takeover feature allows you to detect and protect against account takeover threats. FortiAppSec 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.

FortiAppSec Cloud uses a user tracking rule to track users. When FortiAppSec Cloud detects users that match the criteria you specify in the user tracking rule, it stores the session ID and username.

FortiAppSec 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 191.
- If the response does not match a condition in Authentication Successful Condition on page 191, FortiAppSec Cloud uses the default results `failed`.

FortiAppSec 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 Add and Remove Modules.
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, FortiAppSec 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, FortiAppSec 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. The **Test** button allows you to verify the functionality of the Credential Stuffing database. When clicked, it opens a modal window where you can input a username and password that might be compromised. The system will then indicate whether these credentials have been leaked.
Session Fixation Protection	Enable to configure FortiAppSec Cloud to erase session IDs from the cookie and argument fields of a matching login request. FortiAppSec 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, FortiAppSec 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 FortiAppSec 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 **WAF > 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).

4. Click **SAVE**.

Application Delivery

You can configure FortiAppSec 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 FortiAppSec 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 Add and Remove Modules.

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, FortiAppSec 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. FortiAppSec 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. • **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 FortiAppSec 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 FortiAppSec 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.

Rewrite HTTP Response Header	This action enables FortiAppSec Cloud to insert and remove HTTP headers for server response types.
	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 Location**: Enter the value of `Location:` 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.
	• **Header Insertion**:
	  • **Header Name**:The name of the header that you want to insert to a request, such as "Myheader".
	  • **Header Value**:The value of the header that you want to insert, such as "123". Then, the customized header Myheader: 123 will be inserted to the matched HTTP requests.
	  You can also insert the following variables:
	  • **$CLIENT_IP**: The client's IP address.
	  • **$CLIENT_PORT**: The port number of the client's request.
	  • **$HOST**: The host header from the request. This is useful for virtual host routing.
	  • **$URL**: The URL requested by the client. It doesn't include arguments and path.
	  • **$FULL_URL**: The full URL requested by the client, including arguments and path.
	  • **$UTC_STR**: The UTC time string. This can be useful for logging, caching, or setting custom headers.
	  • **$UTC_INT**: The current UTC epoch time, an integer in seconds. It represents the number of seconds elapsed since the Unix

	epoch, which is January 1, 1970, 00:00:00 UTC. • **$ORIGIN_IP**: The Real IP in x-forwarded-for header. If the real IP is unavailable, then the system will use CLIENT_IP. • **$VSERVER_IP**: The Virtual IP of the virtual server. • **$VSERVER_PORT**: The TCP port of the virtual server. • **Header Removal**: • **Header Name**: Click the Add icon to add the name of the header field that you want to remove. Up to 10 header names can be added in the list.
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 FortiAppSec 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 FortiAppSec 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 Add and Remove Modules.



When enabling caching, ensure that the web server’s **no-cache** and **no-store** directives are properly configured to prevent caching of sensitive data.



To verify a response came from cache, open Developer Tools (Inspect), go to **Network > Headers**, and check for the X-FWB-WebCache header.

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 FortiAppSec Cloud to forward the request to the server in order to cache the response again. Any additional requests will receive FortiAppSec 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 FortiAppSec 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 **Purge Cache** button at the top right corner of the page to clear the responses cached on FortiAppSec 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 FortiAppSec Cloud will not cache.

FortiAppSec 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`

FortiAppSec 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`

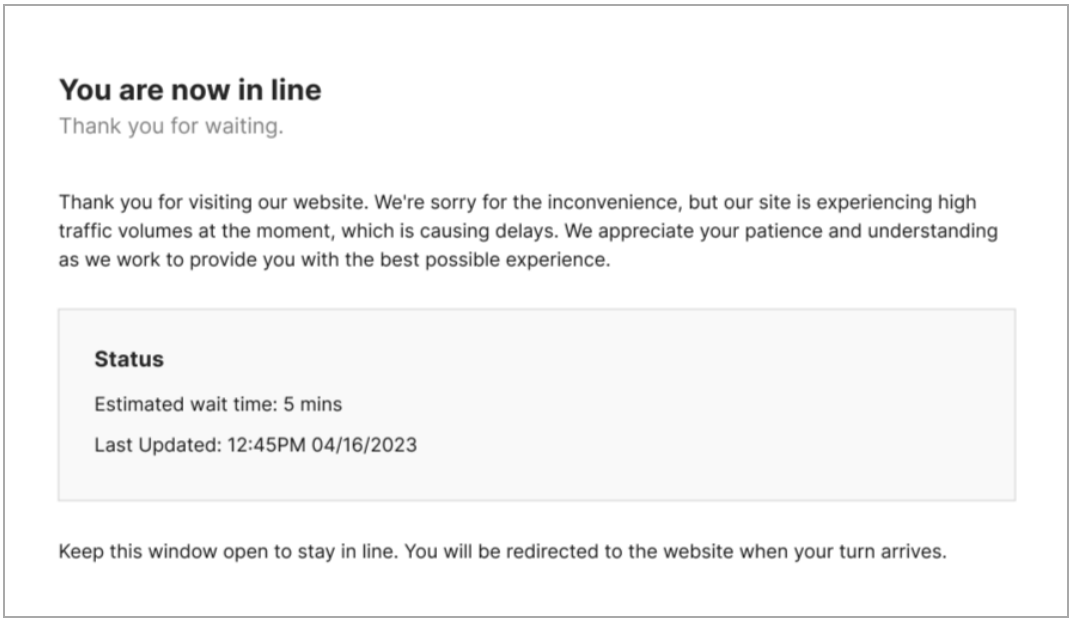
Waiting Room

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.

For information on configuring custom Waiting Room pages, please refer to Custom Pages on page 207.

Customizing the Waiting Room Page affects only the user-facing HTML. It does not change the queuing algorithm, capacity thresholds, or enforcement behavior.



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.

The Waiting Room module supports only clients using web browsers. Non-browser traffic, such as traffic from mobile applications, cannot be processed by the Waiting Room 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 FortiAppSec 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 **Global Trustlist**.
   You must have already enabled this module in **Add Modules**. See Add and Remove Modules.
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 243. 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  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 integrates FortiDAST's web vulnerability scanner (WVS) to help identify OWASP Top 10 vulnerabilities in web applications and provides a detailed report with remediation recommendations to enhance security.

By default, the Vulnerability Scan report reflects your current WAF configuration, highlighting vulnerabilities that remain exposed to attackers. This helps you fine-tune WAF settings to improve security.

Bypass WAF

To view vulnerabilities as if WAF protection were disabled, enable the **Bypass WAF** option at the top-right corner of the **Vulnerability Scan** page.

To scan the asset without enabling **Bypass WAF**, make sure the **action** for the following modules is not set to **Period Block**.

- Known Bot
- Threshold-Based Detection
- ML Bot Detection
- Bot Deception
- DDoS Prevention

Additionally, ensure that the following limits in **DDoS Prevention** are not set below 100:

- HTTP Request Limit
- TCP Connection Number Limit
- HTTP Request Rate Limit

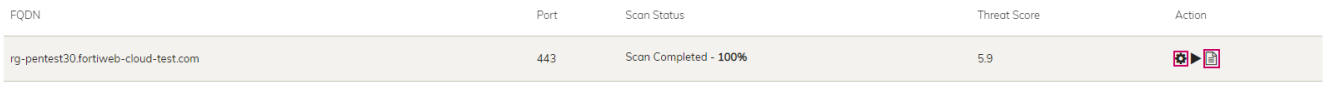
To add applications for vulnerability Scan:

1. Navigate 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. Check your contract information in **General > Contracts** .

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



To configure your Vulnerability Scan subscription from a public cloud marketplace:

Go to **WAF > 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.

Templates

A template is a predefined set of WAF configurations that can be applied to an application. Assigning a template automatically configures the application with its settings, making it easy to standardize settings across multiple applications.

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

- StandardProtection
- 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.

When an application's API Gateway module starts or stops inheriting settings from a template, the system automatically regenerates API keys for all users within that module.

This ensures that the new keys are unique and independent from those defined in the source template.

Inheritance can stop in the following cases:

- The application is still linked to the template, but inheritance for the API Gateway module has been turned off.
- The application has been completely unlinked from the template.

Important:To prevent service disruptions, replace all existing API keys with the newly generated ones wherever they are in use.

To create a template:

1. Go to **WAF > 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 **WAF > 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 127 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):

To manage an application's template settings, the following permission levels apply:

Read Only: Allows viewing the application list and dashboard.

Read & Write: Allows creating, deleting, or modifying applications and modules.

Ensure your account has the appropriate access level to perform the actions you need.

1. Go to **WAF > 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 **WAF > 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.

System Settings

Configure your preferred settings that apply to WAF as a whole.

- WAF Settings on page 204
- Cloud Connectors on page 205
- Custom Pages on page 207

WAF Settings

Fabric Connector

Connect to the Security Fabric with FortiGate version 7.0 or newer (except 7.2). For configuration instructions, see Connecting WAF to the Fortinet Security Fabric on page 242.

Preferred Platform

Enable **Preferred Platform** to allow choosing the preferred Cloud **Platform** and geographical **Region** during WAF Onboarding.

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.

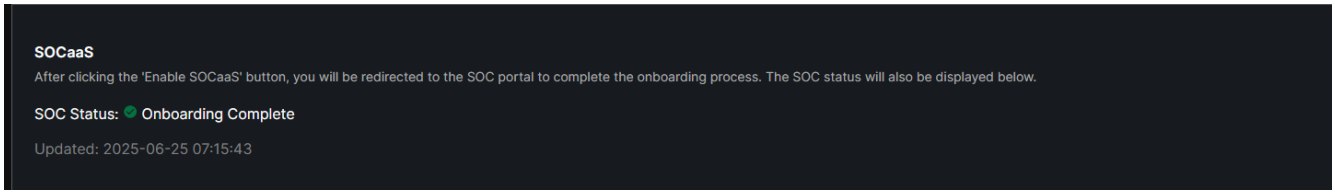
Please refer to the table below on levels of access for different user types:

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.

SOCaaS

Enable Security Operations Center-as-a-Service (SOCaaS) for your WAF applications and view your SOC service status. SOCaaS is available to customers with the **Enterprise bundle** or those who have purchased the **SOCaaS SKU** separately.

To avoid contract synchronization issues, we recommend enabling SOCaaS from the FortiAppSec Cloud portal before onboarding. If onboarding begins without first logging into the portal, SOC contract information may not be available to FortiAppSec, which can lead to SOC status update failures.



To enable SOCaaS for WAF applications, click the **Enable SOCaaS** button. This opens the SOCaaS portal to complete onboarding. For onboarding instructions within the SOCaaS portal, please refer to SOCaaS documentation.

If SOCaaS is enabled, switching the WAF license (e.g., activating a new license) must be coordinated by submitting a **Service request** from the SOC portal.

1. Log into FortiCloud.
2. Navigate to **Services > Cloud Services > SOCaaS**.
3. Navigate to **Service Requests**.
4. Click **Service Request** to add a service request.

   For the **Type**, select **License Renewal**. For additional information on the configuration options on this page, please refer to SOCaaS documentation.

SOCaaS for WAF applications currently does not support changing data regions through the FortiAppSec Cloud Portal. To request a region change, contact the SOC team at `socaas@fortinet-us.com`

For information on enabling SOCaaS for Gateways, please refer to Security Operations Center-as-a-Service (SOCaaS) on page 423.

Cloud Connectors

In certain cases, such as when your application server is deployed in auto-scaling mode on a public cloud platform, its IP address may change dynamically. Rather than manually updating the origin server's IP address, you can configure a Cloud Connector to authorize automatic retrieval of the latest IP addresses from your public cloud resources.

To create a Cloud Connector:

1. Go to **WAF > 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. If the selected type is **AWS**, configure the following.
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 FortiAppSec 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. If the selected type is **Azure**, configure the following.
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. If the selected type is **GCP**, configure the following.
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 FortiAppSec 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 FortiAppSec Cloud can access the resources with the provided information. If the test succeeds, click **OK** to save the settings.

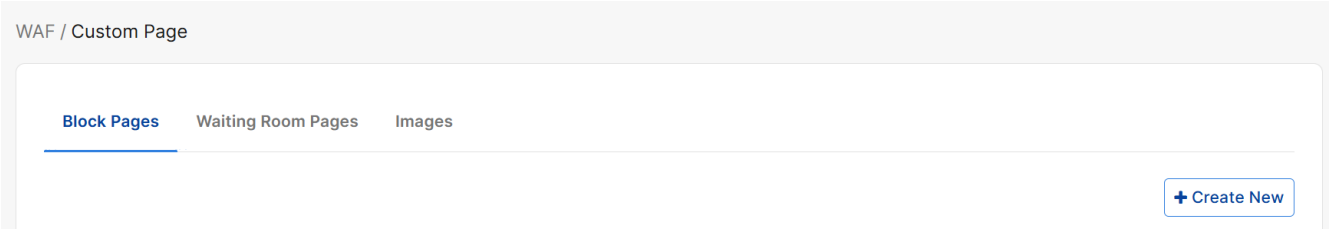
If you want to edit the settings or delete a Cloud Connector, click the Edit or Delete icon in the Cloud Connector row.

After the Cloud Connector is created, you can go to **Network > Origin Servers** to configure the dynamic server settings so that FortiAppSec Cloud can use the specified conditions to find the right VMs in our account and obtain their IP addresses. See Origin Servers on page 103.

Custom Pages

Customize pages shown to your users on the following tabs:

- **Block Pages**: Configure pages displayed when server unavailable or an HTTP request triggers the action **Deny** or Period Block.
- **Waiting Room Pages**: Configure pages displayed during periods of high visitor traffic to prevent server overload.
- **Images**: Upload images used in **Block Pages** and **Waiting Room Pages**.

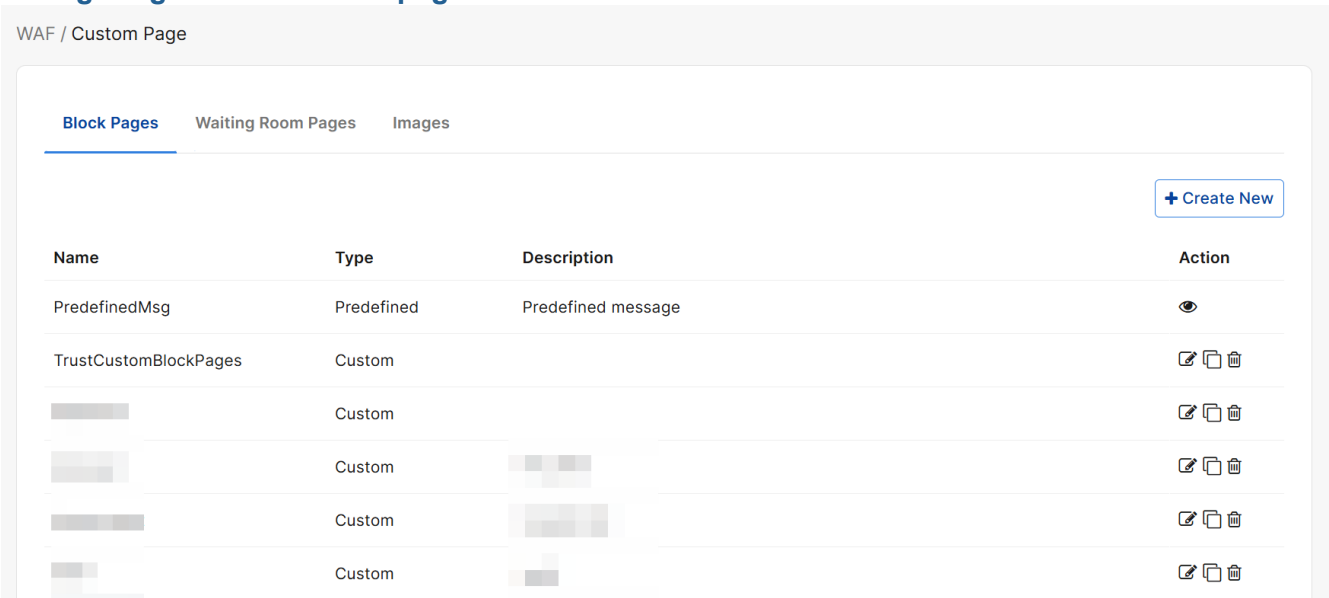


Block Pages

Examples of Block Pages include the following:

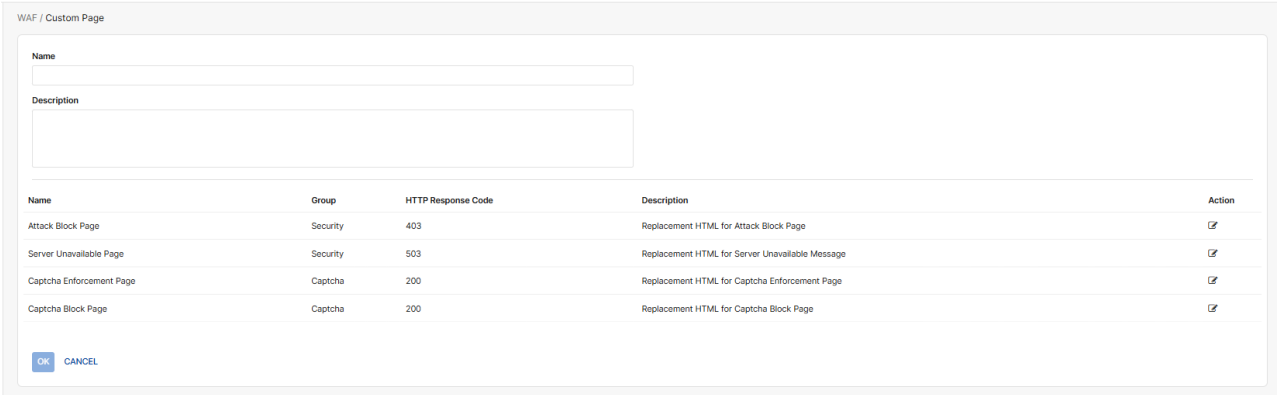
- Error pages shown when HTTP requests violate a policy, triggering the configured action **Deny** or **Period Block**.
- **Server Unavailable** pages returned to the client when none of the server pool members are available either because their status is **Disabled** or **Maintenance** or they have failed the configured health check.
- Captcha enforcement pages that FortiAppSec Cloud uses to differentiate between real users and automated users, such as bots.

Configuring a custom block page

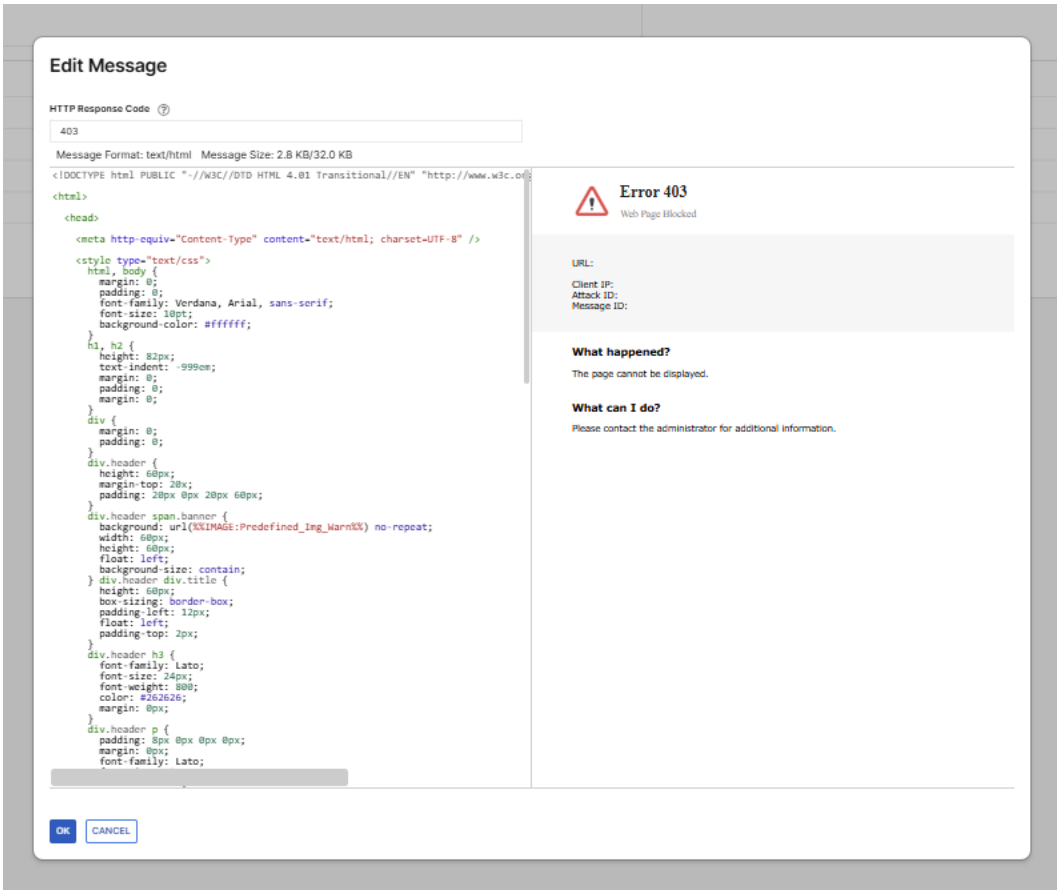


Follow steps below to configure a custom block page:

1. Go to **WAF > System Settings > Custom Block Pages**.
2. 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. The default configuration of a block page contains common messages for **HTTP Response Codes**. The **Descriptions** for each message indicate the circumstances that trigger them.



6. Click the **Edit** icon under **Action** for a message to customize what the users of your application see when the message is triggered.
7. 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.
   For instructions on adding images, see Images.



You cannot change macros such as `%%SOURCE_IP%%`. See Macros in custom block pages.

8. Click **Save** to save the changes of the message.
9. If you want to edit other messages, click the **Edit** icon in their rows.
10. Click **OK** to save the block page.
11. To apply a block page for an application, select it in the **Custom Block Pages** list in **Application > Network > Endpoints**.

FortiAppSec 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>
```

Waiting Room Pages

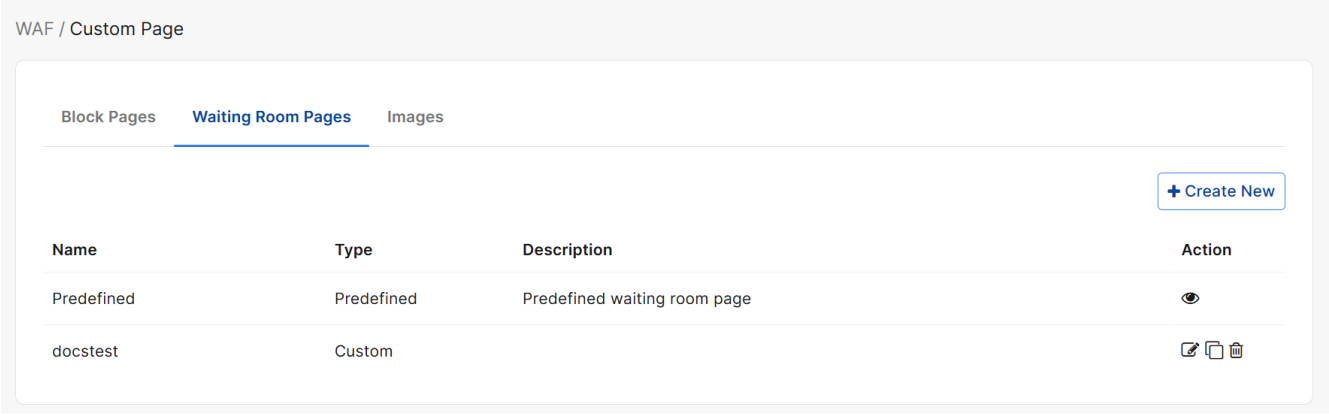
To manage high visitor traffic and prevent server overload, enable a virtual Waiting Room that queues users and shows them an estimated wait time before they can access your application.

With a custom page, you can tailor the in-queue experience while FortiAppSec Cloud handles traffic flow and protects your origin with a server-side queue.

A custom page is useful when you want to display your own branding, provide clearer messaging about delays, and maintain a consistent look and feel with your application.

Customizing the Waiting Room Page affects only the user-facing HTML. It does not change the queuing algorithm, capacity thresholds, or enforcement behavior.

This feature may be configured for your entire website, or specific URL paths.



Prerequisites and Limitations

- **Waiting Room feature enabled**: You must enable Waiting Room for the application before configuring a custom page.
- **Supported content type**: Only HTML content is supported. Stylesheets can be included via <style> blocks or inline CSS. External script tags are not allowed and may be sanitized for security.
- **Required placeholders and markers**: The custom page must keep the following placeholders and markers:
  - `%%WR_ETA%%`: This placeholder must appear at least once in the HTML. It is used to display the estimated waiting time to the end user. Pages that do not include this placeholder are considered invalid and cannot be saved.
  - `%%WR_TS%%`: This placeholder is also required and must be preserved in the template. It is used internally by FortiAppSec Cloud for waiting-room tracking and validation. Do not remove or modify this placeholder.
  - `<!-- Fortiweb Mask -->`: This HTML comment marks a block that contains system-required code (for example, scripts that FortiWeb / FortiAppSec Cloud needs for the Waiting Room to work correctly). We use this marker so you can easily recognize the part of the template that must be kept, without having to review a large amount of code on every update. You should not remove or modify this comment or the surrounding block; customize the rest of the HTML freely, but keep the masked section exactly as provided to ensure correct behavior and future compatibility.

The Waiting Room module supports only clients using web browsers. Non-browser traffic, such as traffic from mobile applications, cannot be processed by the Waiting Room module.

Security Considerations

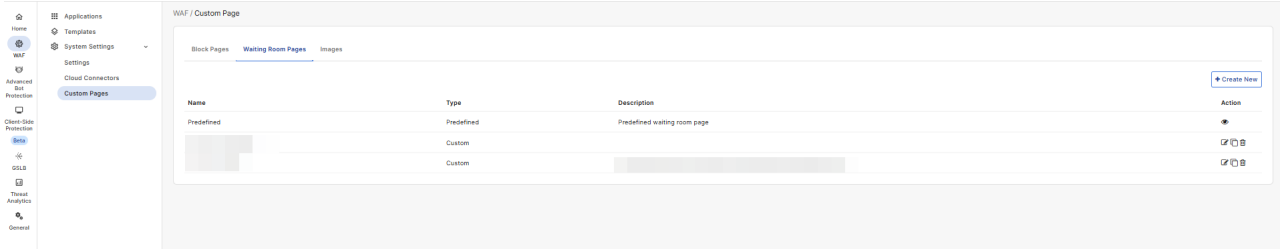
- Avoid embedding untrusted JavaScript or third-party trackers.
- Do not attempt to bypass or manipulate queue behavior from the page.
- FortiAppSec Cloud validates uploaded custom HTML to ensure it does not compromise the security or stability of the FortiAppSec Cloud platform itself. However, it does not guarantee that your customized content (such as redirects, external links, or inline scripts) is safe for your own application or business logic. Carefully review all custom HTML, links, and scripts to ensure they do not introduce additional security risks to your application.
- FortiAppSec Cloud may **sanitize** or **block** dangerous HTML constructs to maintain WAF security guarantees.

Size and Complexity

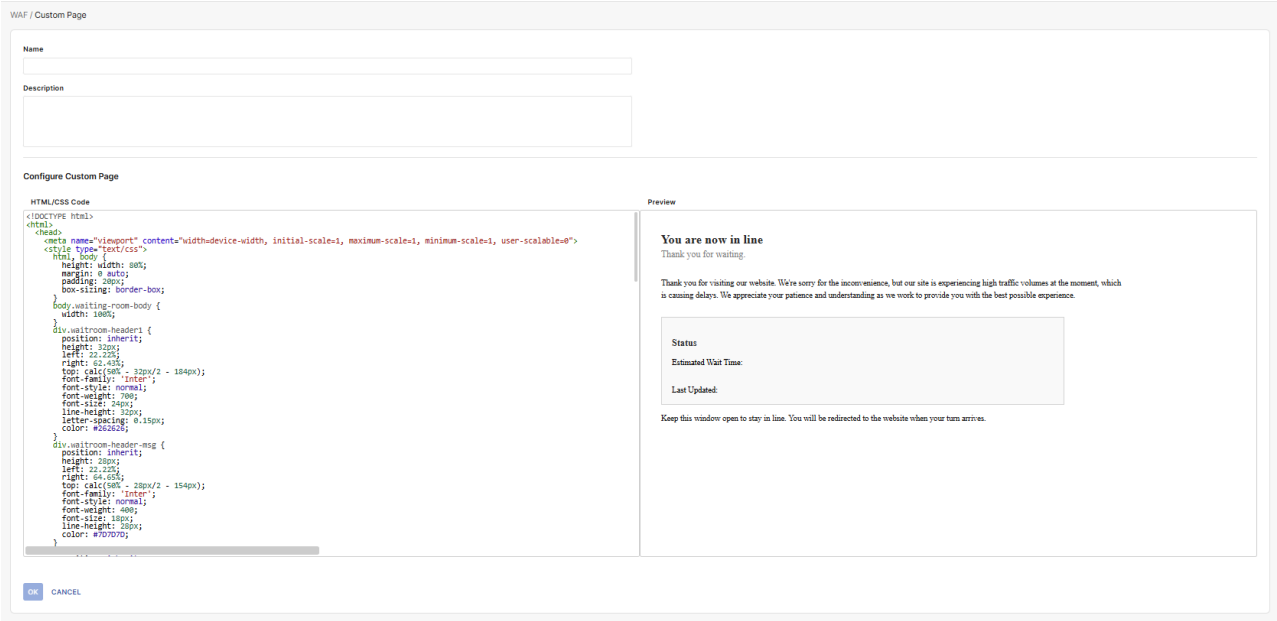
1. A single FortiAppSec Cloud account can create up to 8 custom pages in total. This quota is shared by all users under the same account.
2. Each custom page HTML file is limited to a maximum size of 32 KB.
3. Images can be referenced either by using external URLs or by uploading images to FortiAppSec Cloud and linking to them from the HTML. For usage patterns and examples, you can refer to the FortiWeb documentation for Custom Waiting Room pages.

Create and edit a custom Waiting Room Page

1. Navigate to **WAF > System Settings > Custom Pages> Waiting Room Pages**



2. Click **Create New**.



3. Enter a **Name** and **Description**.
4. Under **Configure Custom Page**, replace the default HTML with your custom content, ensuring you include all required placeholders and markers (`%%WR_ETA%%`, `%%WR_TS%%`, and `<!-- Fortiweb Mask -->`).

   For instructions on inserting images, see Images.
5. Click **OK** to save.

Once you have created a Waiting Room Page, you can **edit**, **clone**, or **delete** it under the **Action** column on the **Custom Pages > Waiting Room Pages** page.

Apply a Waiting Room Page to a WAF Application

1. Navigate to **WAF > Applications**.
2. Select the application you want to configure.
3. Navigate to **Application Delivery > Waiting Room > Settings**.
4. Select the desired page from the **Custom Waiting Room Page** dropdown.
5. Click **Save** to apply the changes.

Images

The default block and waiting room pages contain predefined images. To use your own images, upload the desired image file(s), then insert its image macro in the message body.

Uploading image files

1. Go to **WAF > 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 format `%%IMAGE:<image_name>%%` to add an image macro anywhere in a custom block message,

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;
}
```

Use cases

This chapter introduces the special configurations for different use cases.

DevOps tools

FortiAppSec Cloud's WAF service supports DevOps tools to provide more ways to efficiently deploy, manage, and automate application security.

You can use DevOps tools to automatically onboard or delete applications from FortiAppSec Cloud. You can also change the IP list in IP Protection using Ansible.

- Configuring WAF with Terraform on page 215
- Configure WAF with Jenkins on page 215

Configuring WAF with Terraform

Terraform is a DevOps tool that integrates with FortiAppSec Cloud using the FortiAppSec Cloud Terraform Provider, which automates the provisioning and management of FortiAppSec Cloud WAF resources.

Prerequisites for using Terraform with WAF

- FortiAppSec Cloud API access.
- FortiAppSec Cloud Provider version 1.0.0 or later.
- Terraform version 0.13 or later.
- Terraform template for setting up WAF
  - Download the template by following the instructions under **Installation** on the Github repository.
  - Obtain a template from the support team or your sales representative.

Configuration Instructions

For setup instructions on using FortiAppSec Cloud WAF with Terraform, please refer to the following external resources:

- **Creating new applications:** with Terraform, please see the README section of our GitHub repository, referring to Terraform documentation for Argument References covering OpenAPI validation and application creation use cases.
- **Migrating pre-existing Terraform integration settings from FortiWeb Cloud:** please refer to the instructions under Migrate FortiWebCloud private provider to FortiAppSecCloud.



State File Backup: Before modifying the state file, ensure it is backed up to prevent data loss.

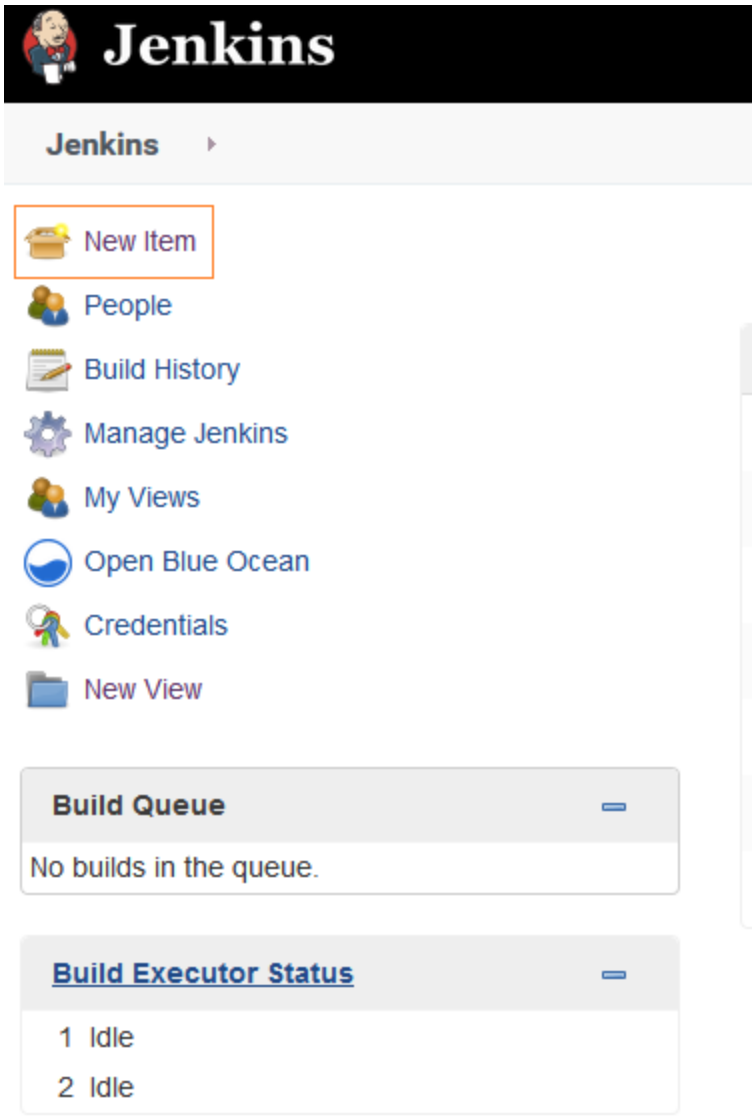
Configure WAF with Jenkins

The following example demonstrates how to use Jenkins to perform simple configuration changes on FortiAppSec Cloud. It requires the following:

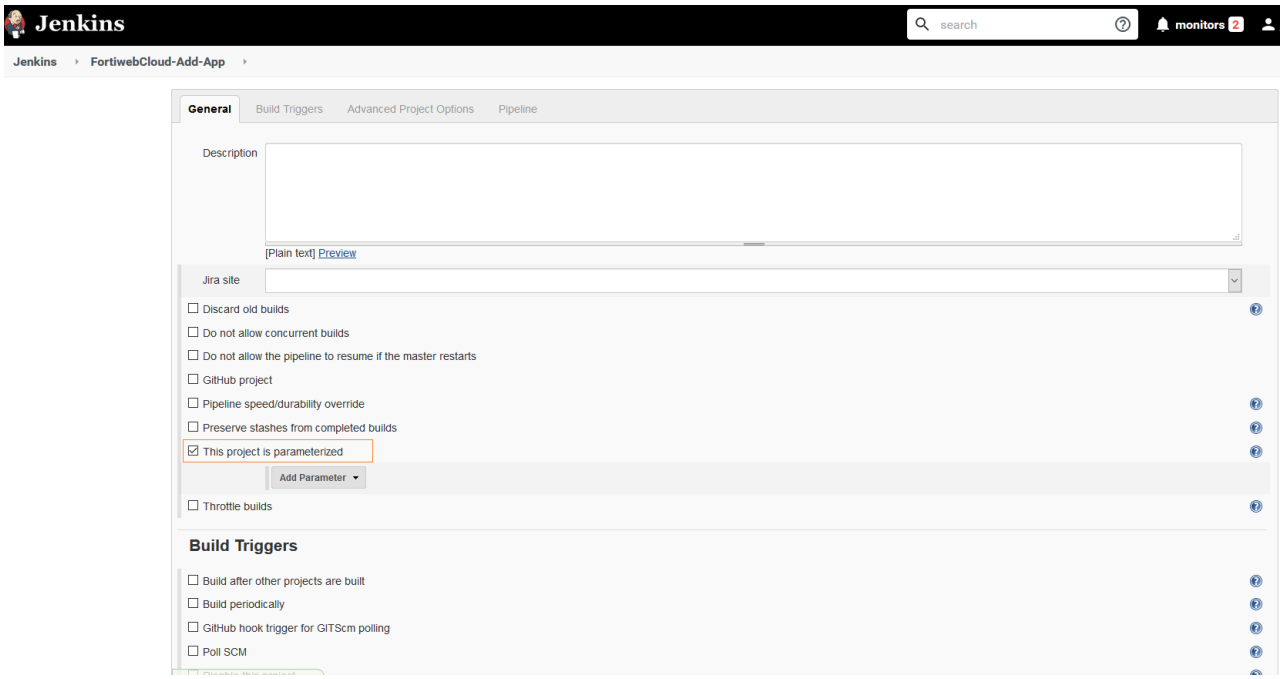
- Pipeline Template for integrating WAF with Jenkins, please su
- Jenkins: This example uses Jenkins 2.222.3+.

To onboard an application with Jenkins, follow the steps below:

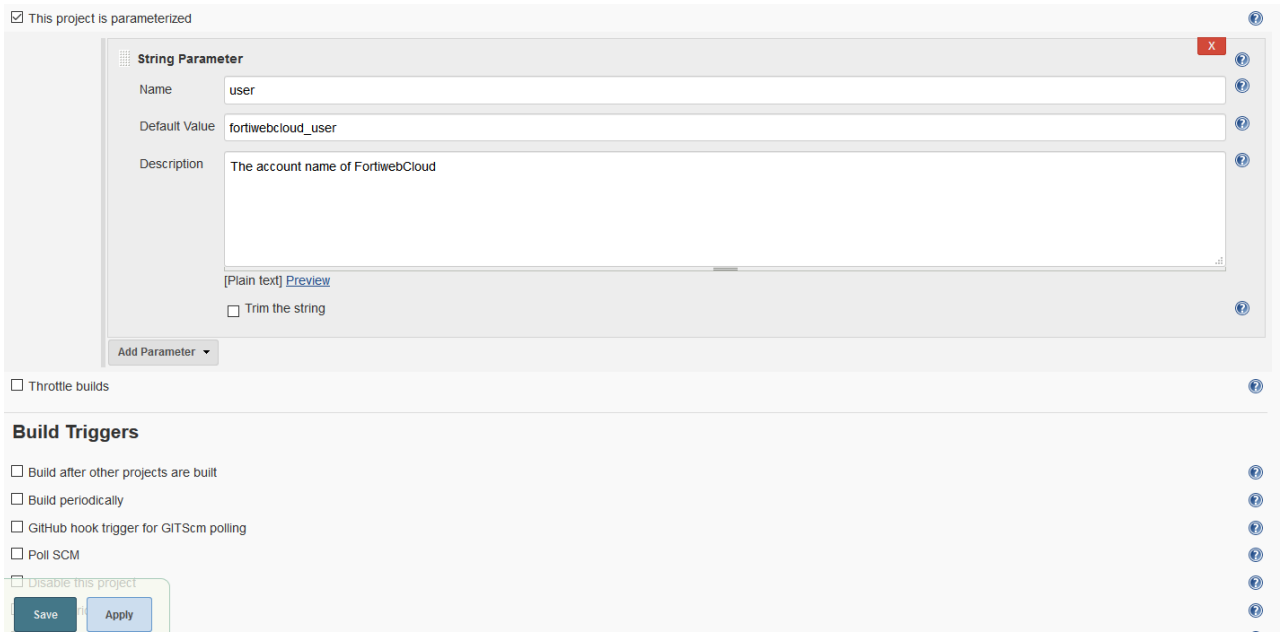
1. Log in to your Jenkins account.
2. Click **New Item**.



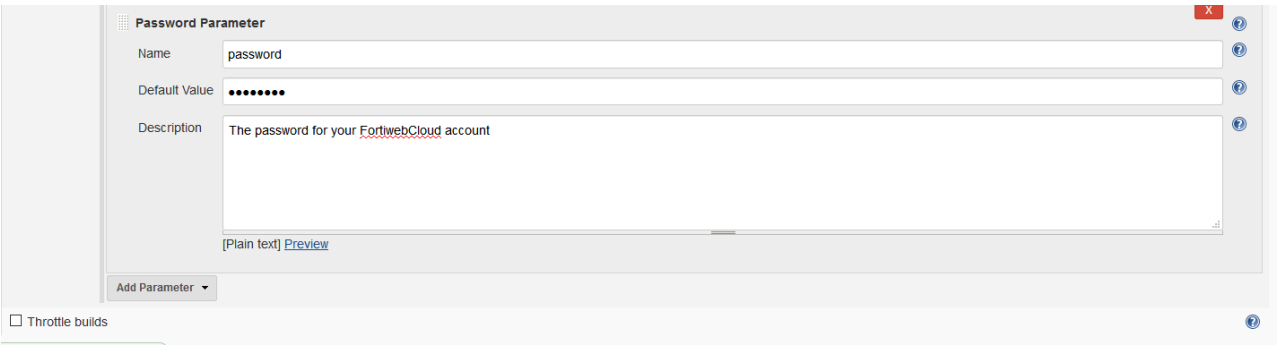
3. Name the item and select **Pipeline**, then click **OK**.
4. Select **This project is parameterized**.



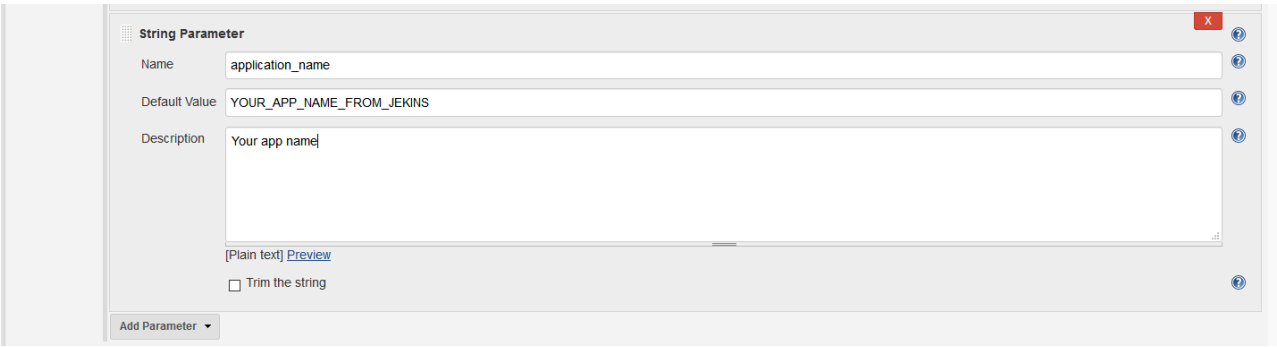
5. In **String Parameter**, enter **user** in **Name**, then enter your FortiAppSec Cloud's account name in **Default Value**. The account should have write privilege on FortiAppSec Cloud.



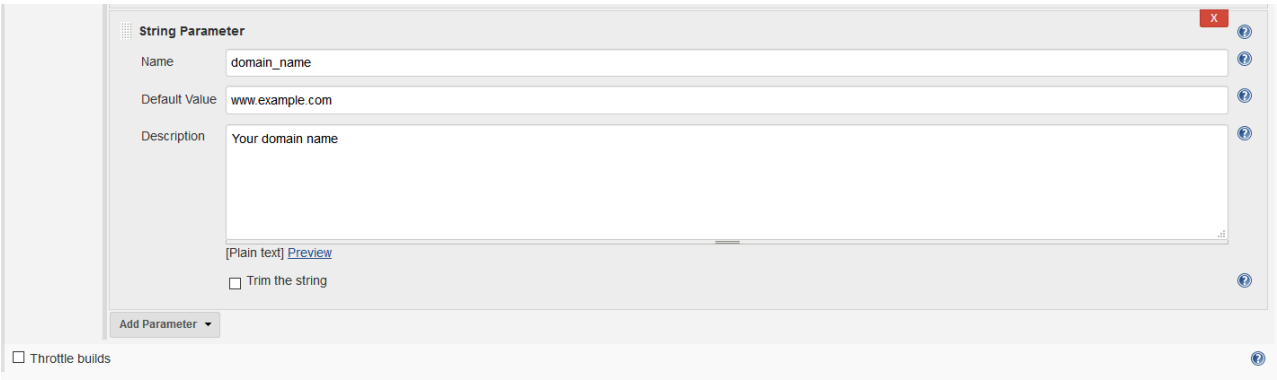
6. In **Password Parameter**, enter **password** in **Name**, then enter the password of the specified account in **Default Value**.



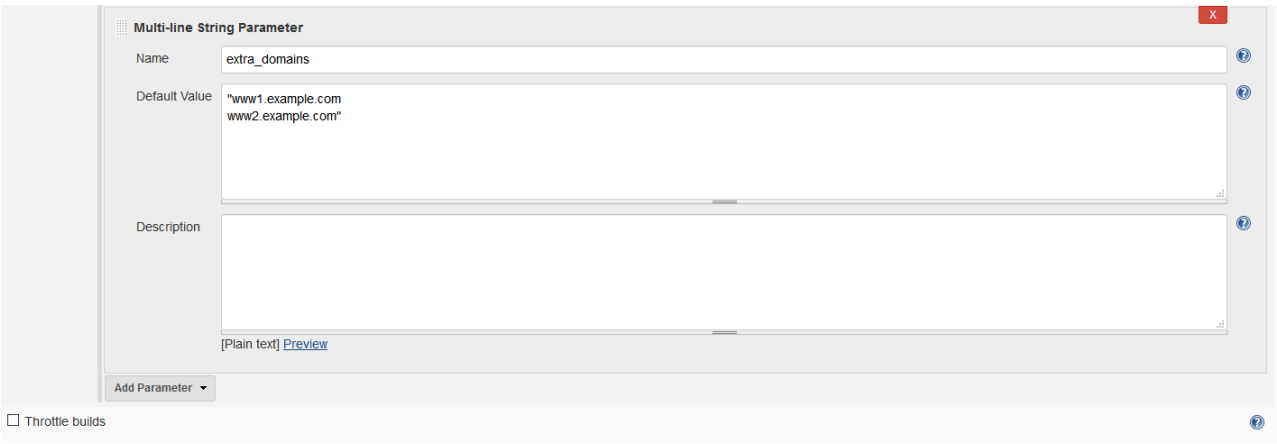
7. In **String Parameter**, enter **application_name** in **Name**, then enter a name for your application. It will be displayed on FortiAppSec Cloud's GUI to identify your application.



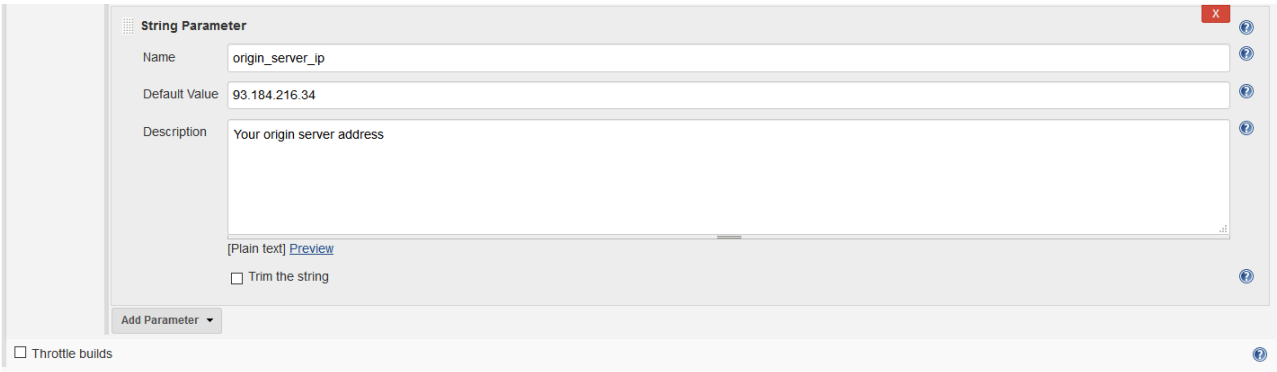
8. In **String Parameter**, enter **domain_name** in **Name**, then enter your application's domain name in **Default Value**.



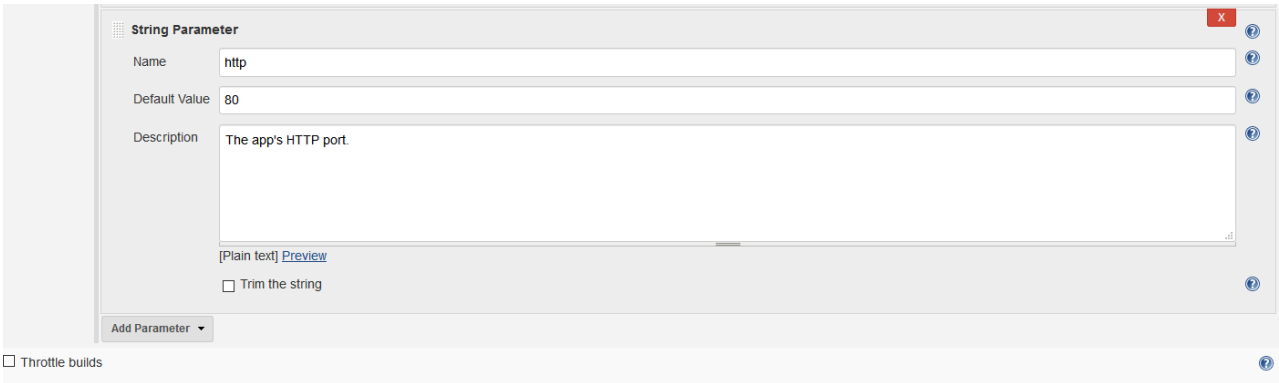
9. In **Multi-line String Parameter**, enter **extra_domains** in **Name**, then enter the domain names if your application has multiple domains.



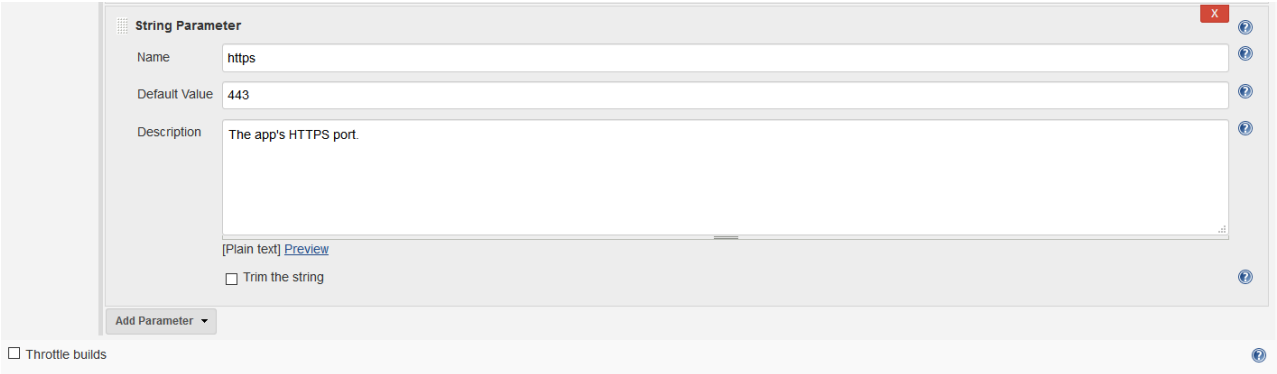
10. In **String Parameter**, enter **origin_server_ip** in **Name**, then enter your origin server's IP address in **Default Value**.



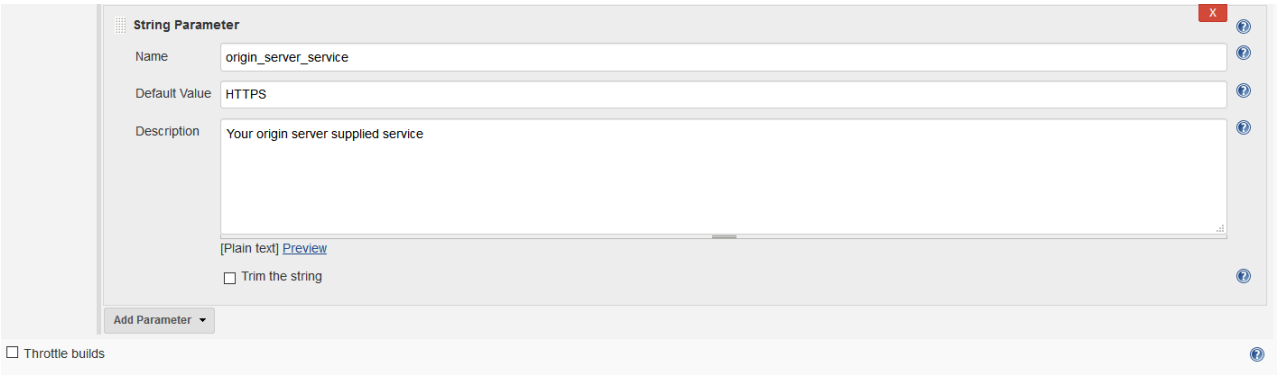
11. In **String Parameter**, enter **HTTP** in **Name**, then enter the port number used for HTTP service in **Default Value**.You must enter 80 as the default value.



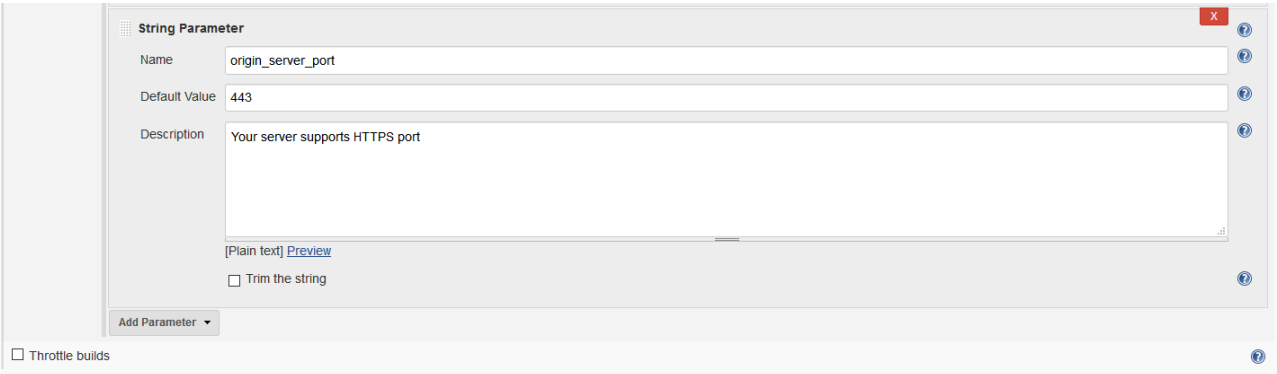
12. In **String Parameter**, enter **HTTPS** in **Name**, then enter the port number used for HTTPS service in **Default Value**. You must enter 443 as the default value.



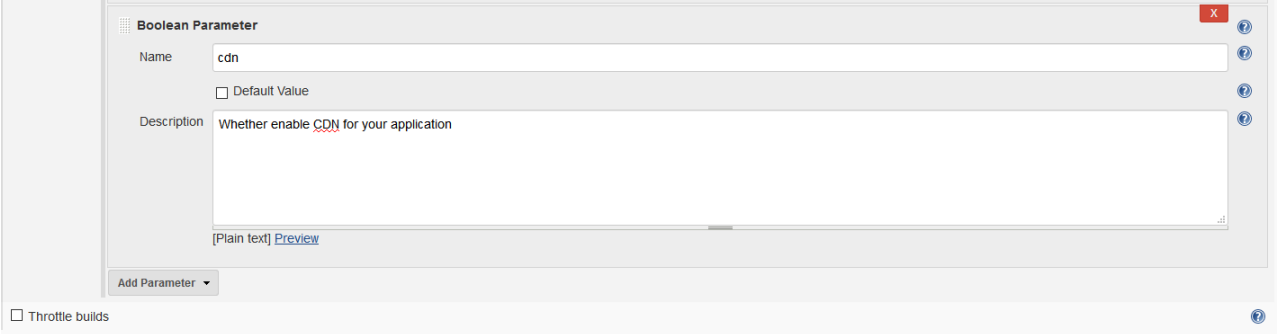
13. In **String Parameter**, enter **origin_server_service** in **Name**, then enter your origin server's service type in **Default Value**. You must input HTTP or HTTPS as the default value.



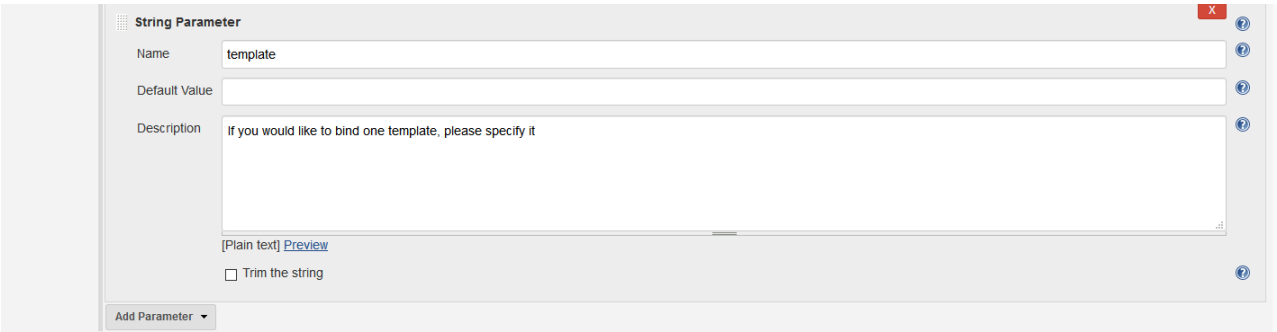
14. In **String Parameter**, enter **origin_server_port** in **Name**, then enter your origin server's listening port in **Default Value**. You can input 80 for HTTP or 443 for HTTPS as the default value.



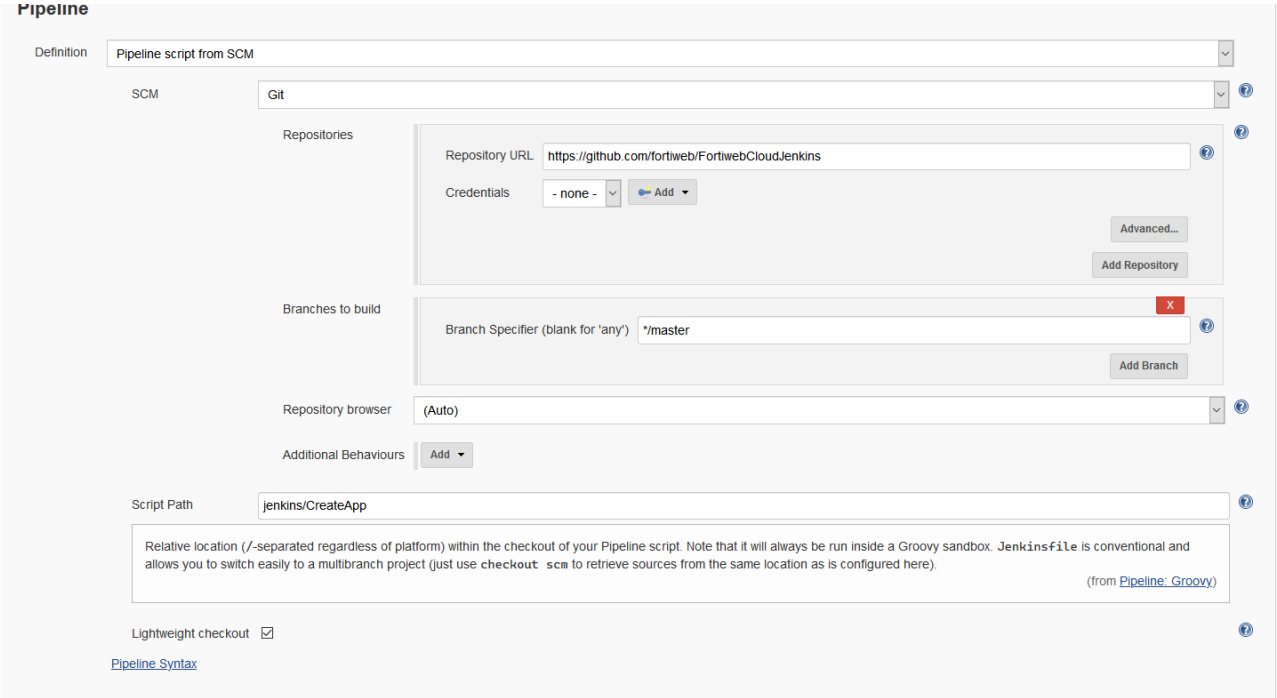
15. In **Boolean Parameter**, enter **cdn** in **Name**, then enable this option if you want your application to be accelerated in the global network.



16. In **Boolean Parameter**, enter **block** in **Name**, then enable this option if you want FortiAppSec 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.



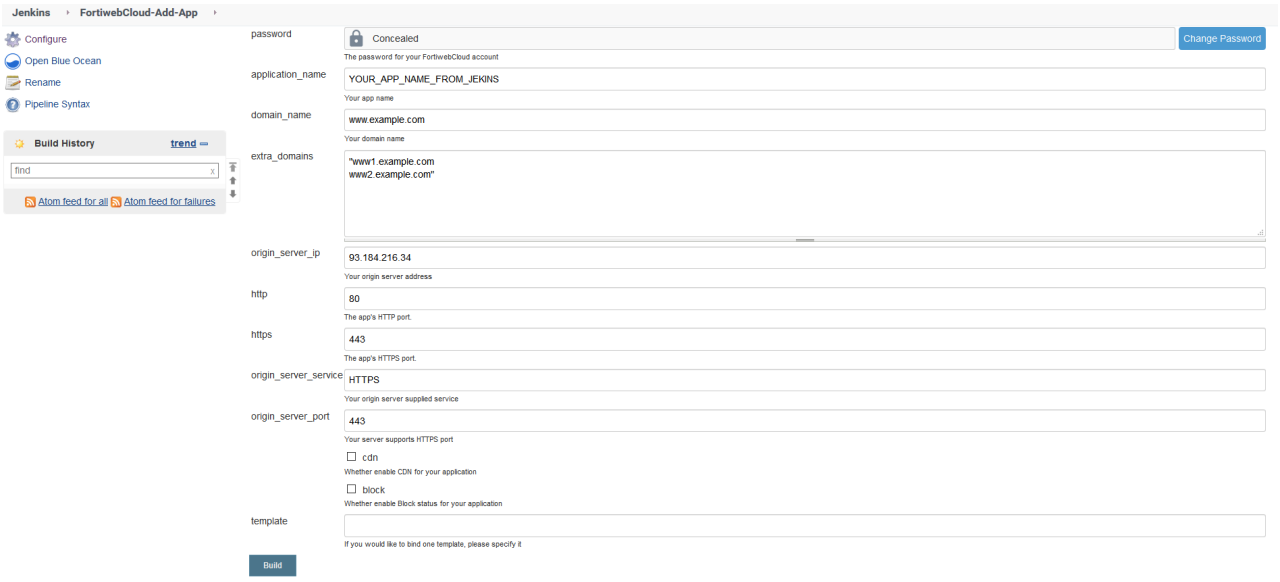
18. Specify the repositories in the pipeline. The repository URL is https://github.com/fortinet/fortiwebcloud-jenkins and the script path is "jenkins/CreateApp". Click **Save** to finish the setup.



19. Now you can schedule the build.



20. Review the configuration before running the build. Click **Build**.

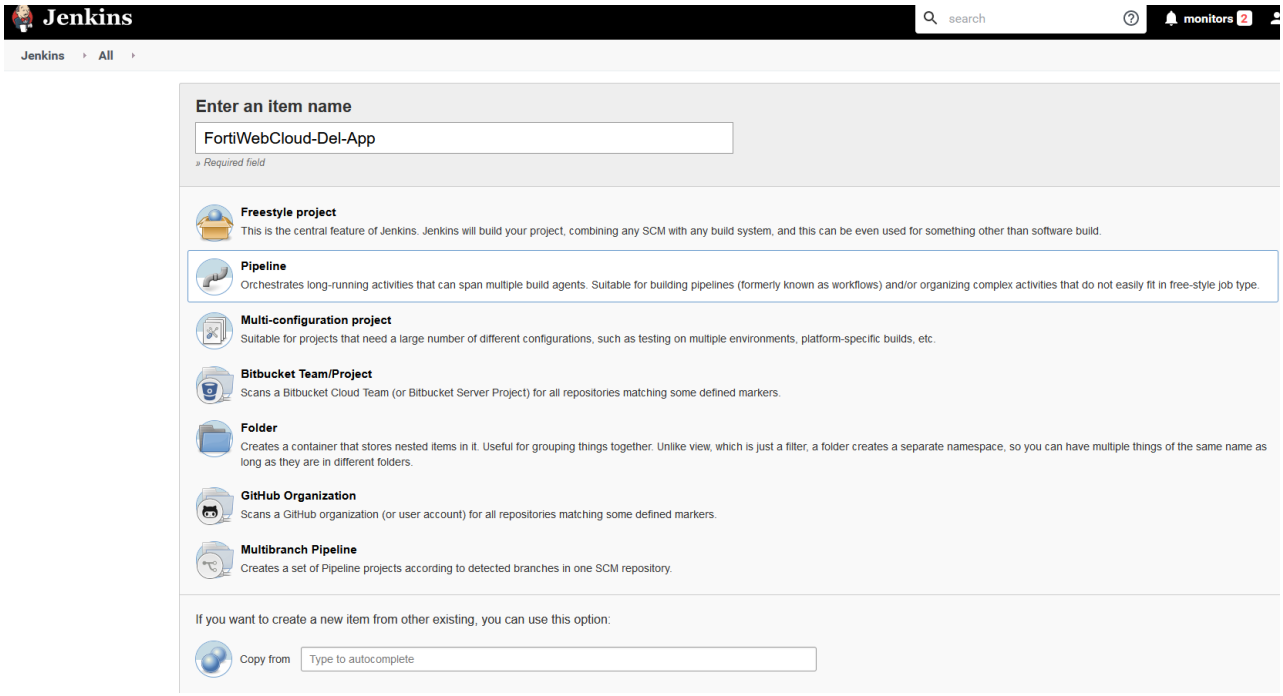


21. If the operation has succeeded, you will see this reflected in the Console Output.

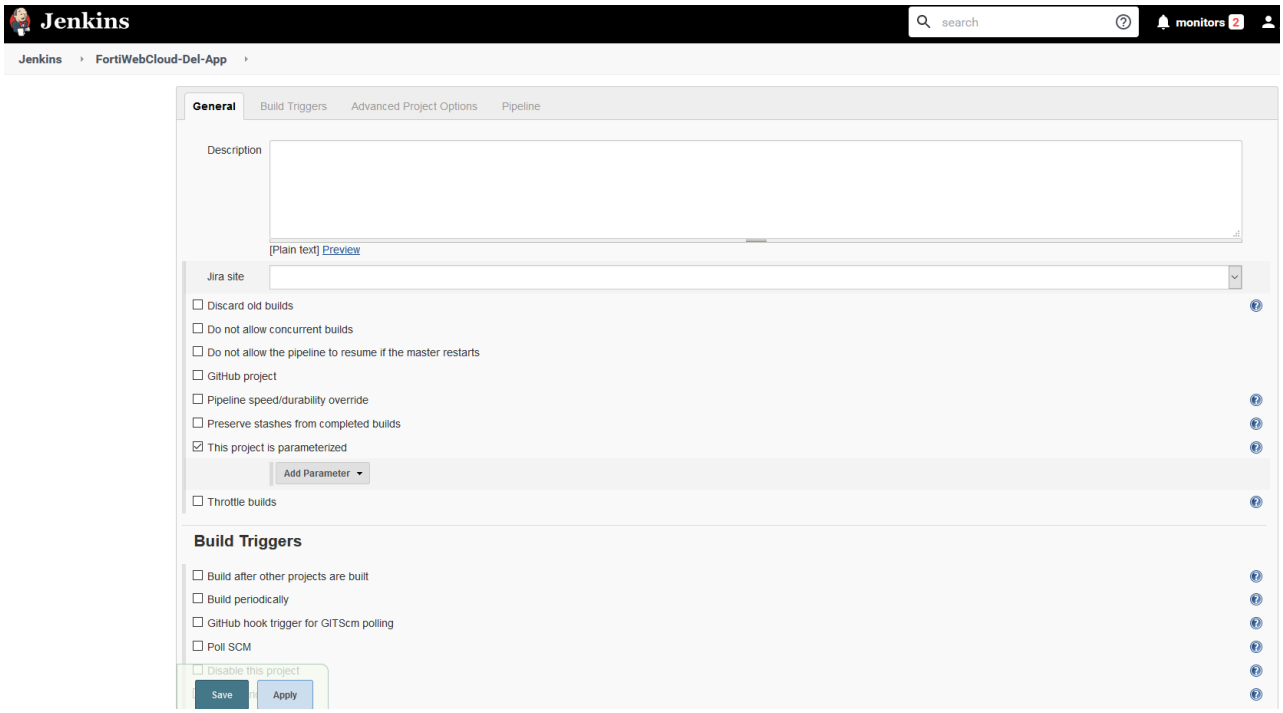


To delete app via Jenkins, follow the steps below:

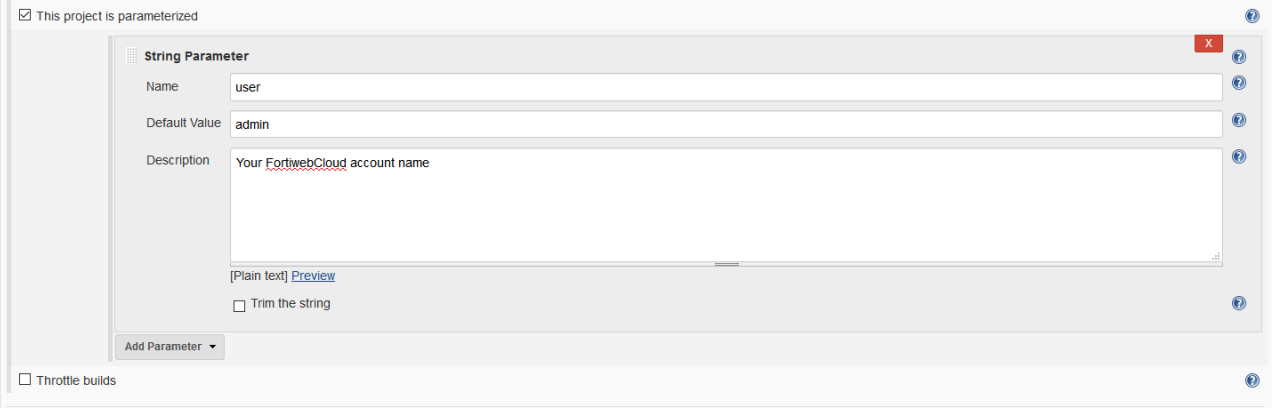
1. Click **New Item** to add a new item.
2. Name the item and select **Pipeline**, then click **OK**.



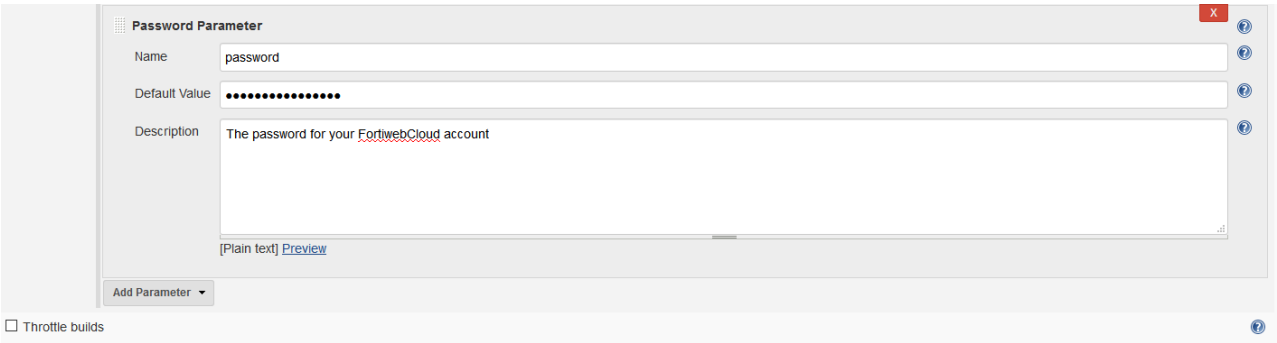
3. Select **This project is parameterized**.



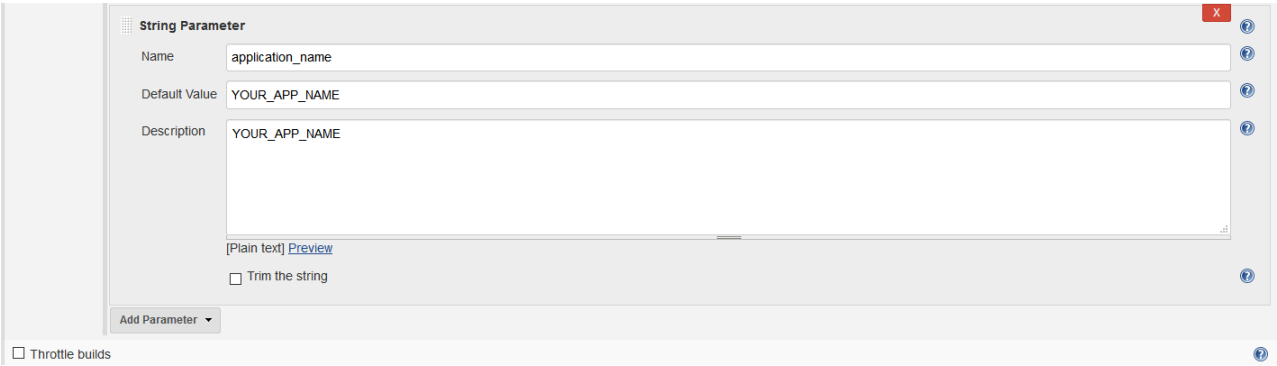
4. In **String Parameter**, enter **user** in **Name**, then enter your FortiAppSec Cloud's account name as its default value.



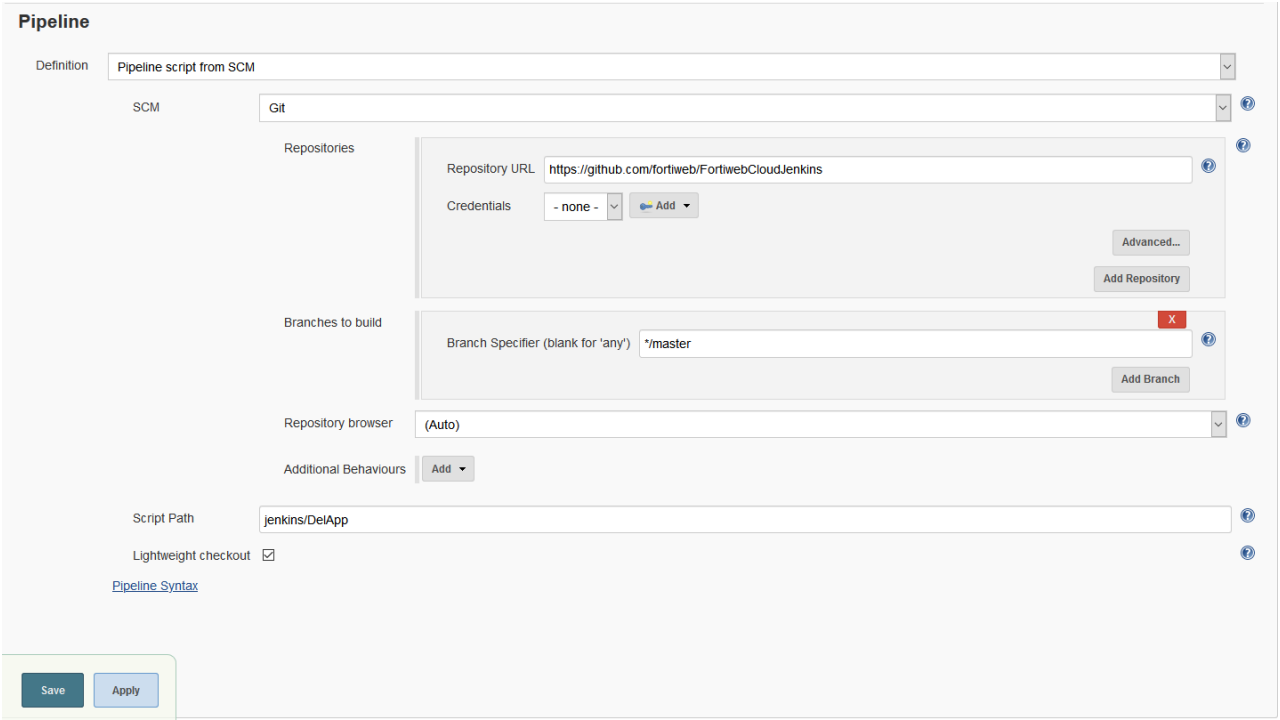
5. In **Password Parameter**, enter **password** in **Name**, then enter the password of the specified account in **Default Value**.



6. In **String Parameter**, enter **application_name** in **Name**, then enter the name of your application to be deleted.



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.



8. Run the build. If nothing is wrong, then the delete process will be output and your application will be deleted from FortiAppSec Cloud.

Using WAF with 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.

FortiAppSec Cloud App for Splunk

The FortiAppSec Cloud App provides real-time and historical dashboard on threats, performance metrics and audit information for FortiAppSec Cloud.

With the massive set of logs and big data aggregation through Splunk, the FortiAppSec 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.
FortiAppSec Cloud App for Splunk: https://classic.splunkbase.splunk.com/app/7748/



FortiAppSec Cloud WAF App depends on the Add-on to work properly. Make sure Fortinet FortiAppSec Cloud Add-on for Splunk has been installed before you proceed.

FortiAppSec Cloud Add-on for Splunk

FortiAppSec Cloud WAF 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 FortiAppSec Cloud, which includes attack and audit logs.

Fortinet FortiWebCloud Add-on for Splunk: https://classic.splunkbase.splunk.com/app/7749/

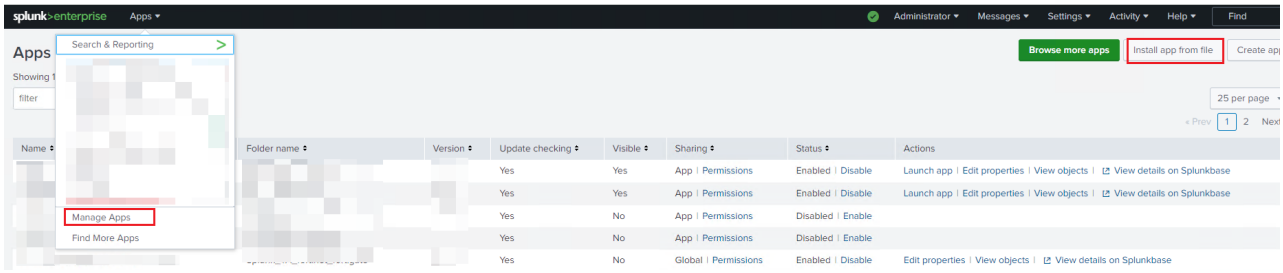
Deployment prerequisites

1. Splunk version 8.1.0 or later
2. FortiAppSec Cloud Add-On for Splunk (https://classic.splunkbase.splunk.com/app/7749/)
3. FortiAppSec Cloud App for Splunk (https://classic.splunkbase.splunk.com/app/7748/)
4. A Splunk.com username and password

Splunk configuration

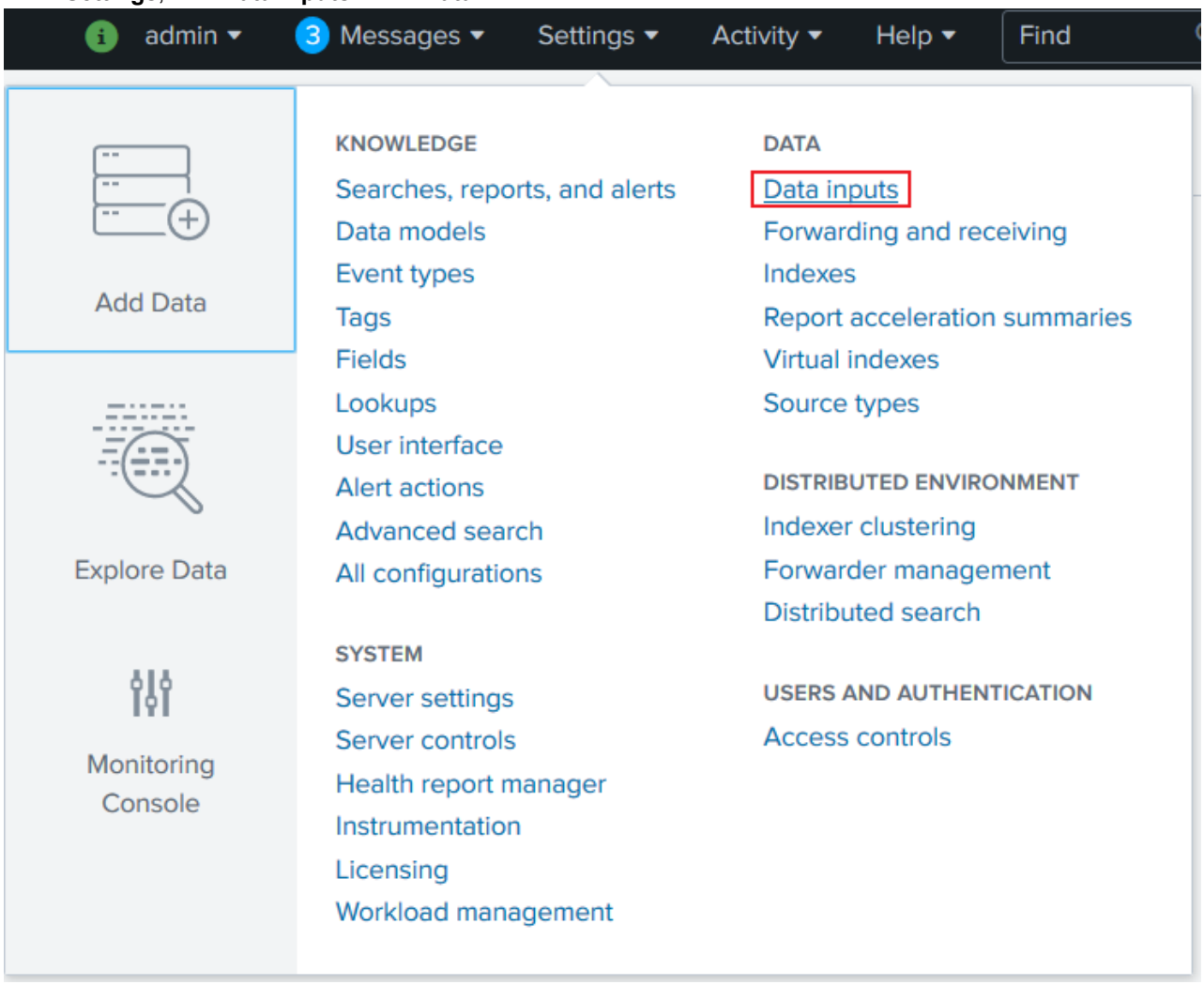
1. Click the gear (Manage Apps) from Splunk Enterprise.
2. Click **Browse more apps**, and search for FortiAppSec Cloud
3. Install **Fortinet FortiAppSec Cloud Add-on for Splunk**
4. Install **Fortinet FortiAppSec Cloud App for Splunk**.

   Note: If the **Fortinet FortiAppSec Cloud App for Splunk** and **Fortinet FortiAppSec Cloud 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**

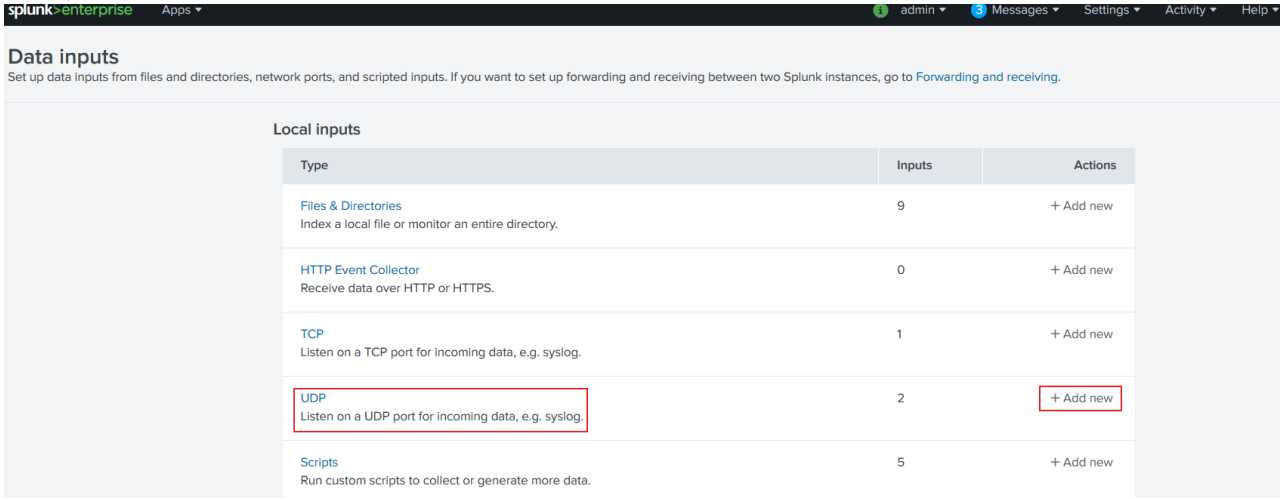


5. Restart Splunk Enterprise.

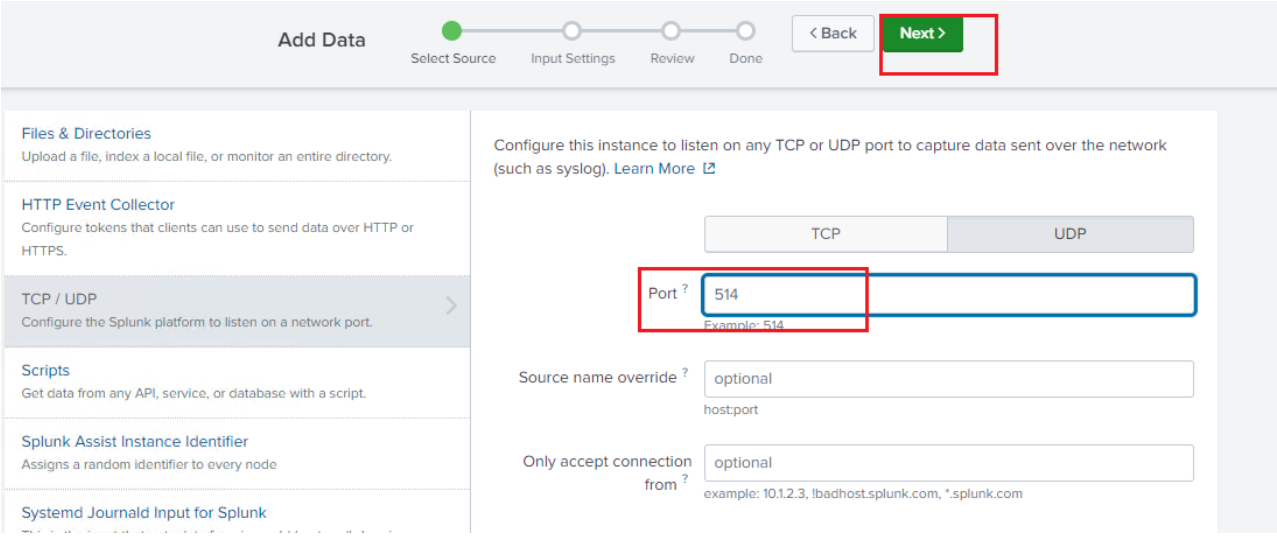
6. From **Settings**, click **Data Inputs** under **Data**.



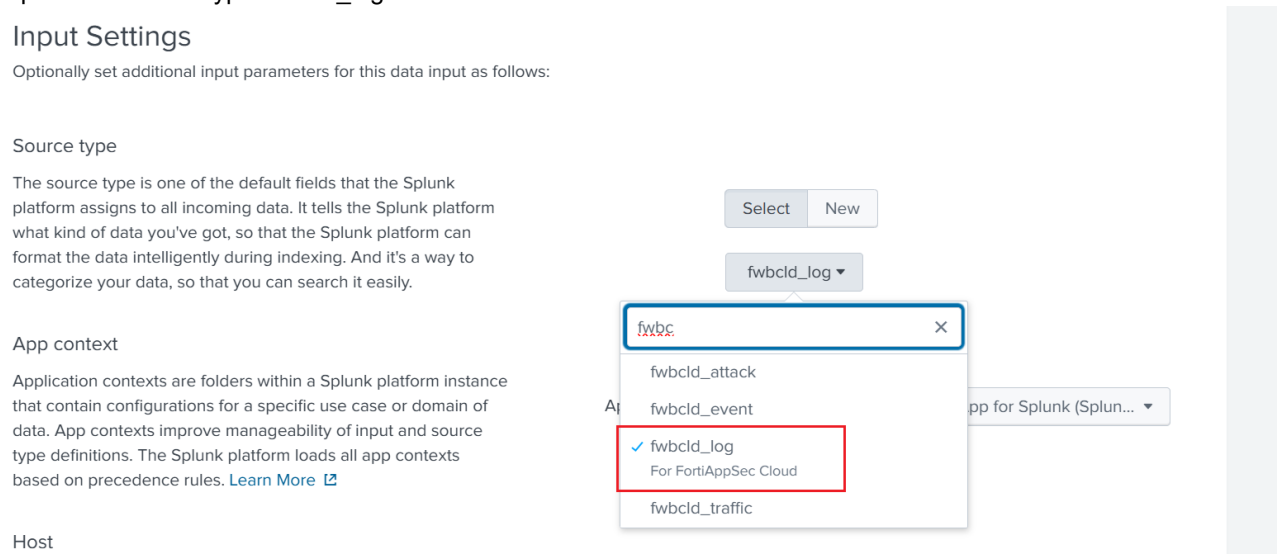
7. Click **Add new** in the UDP or TCP line to create a new input rule with corresponding protocol. See the UDP protocol example below.



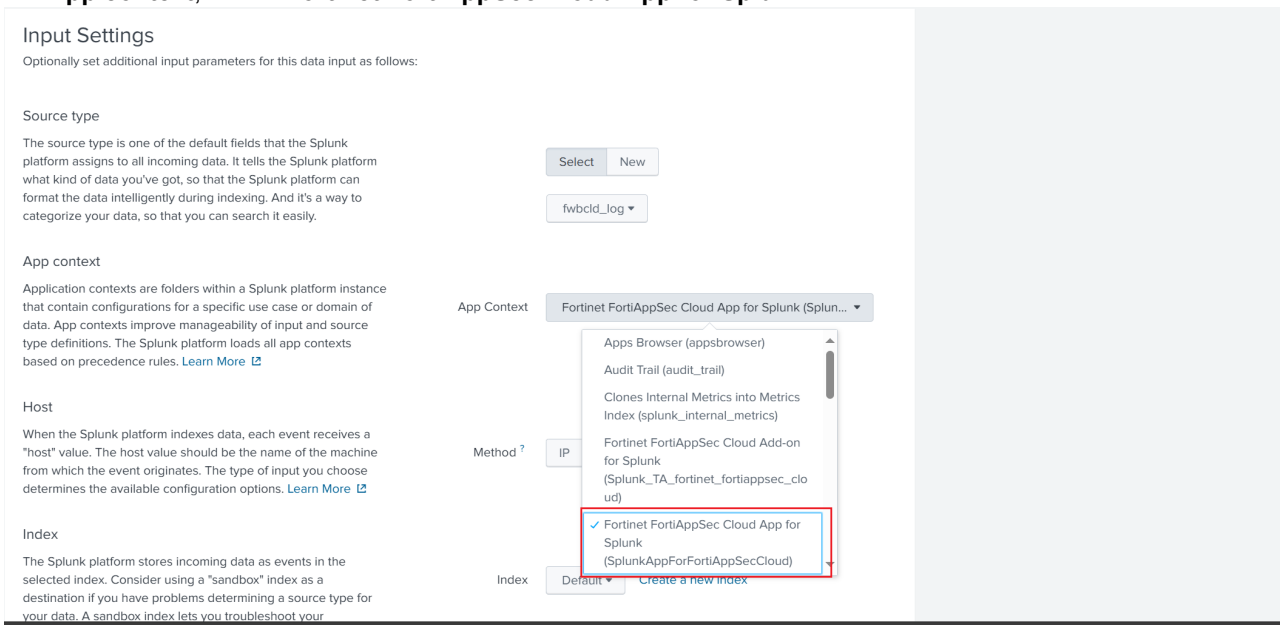
8. Create a UDP data source using your desired port. In the example below, Port 514 is used. Once configured, click **Next** to continue.



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 FortiAppSec Cloud App for Splunk** will automatically extract FortiWebCloud log data from inputs with source type 'fwbcld_log'.



10. For **App context**, select **Fortinet FortiAppSec Cloud App for Splunk**.



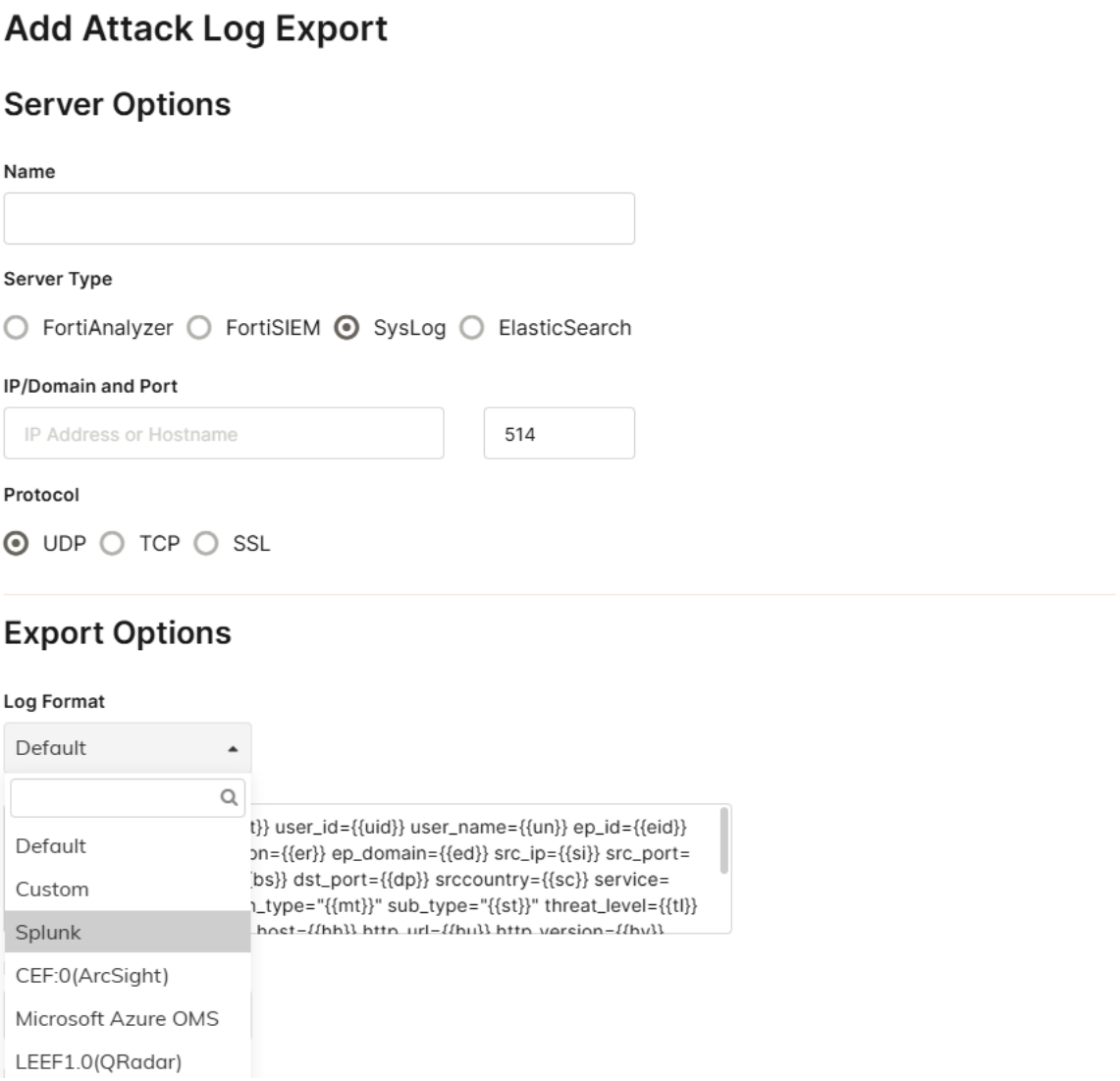
11. Click **Review** to check the items.
12. Click **Submit**.

FortiAppSec Cloud configuration

Configure FortiAppSec Cloud to send logs to Splunk server.

Attack logs

1. Go to **Log Settings**.
2. Enable **Attack Log Export**.
3. Click **Add Log Server**.
4. Configure the server and export options. See Log Settings on page 120 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 FortiAppSec Cloud App for Splunk, from the **Security Overview**, **Attack**, and **Event** tabs, you can see data parsed and presented.

Troubleshooting

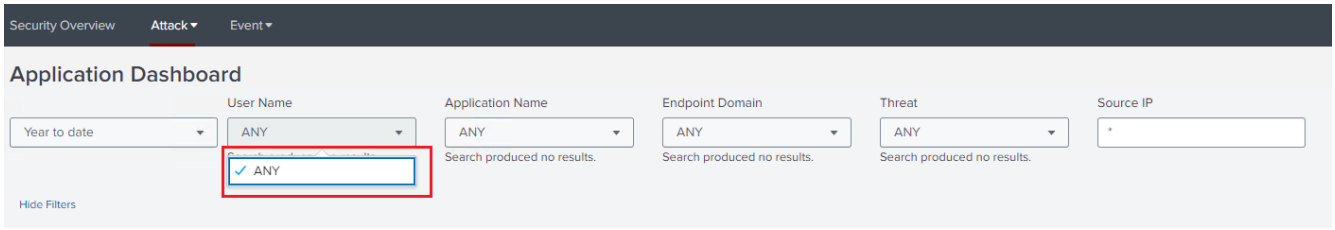
If data is not showing up in the Dashboards:

- 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 FortiAppSec 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 FortiAppSec Cloud service Management IP addresses are in the white list of your Splunk server.
- Verify the Splunk server is listening to the correct port.

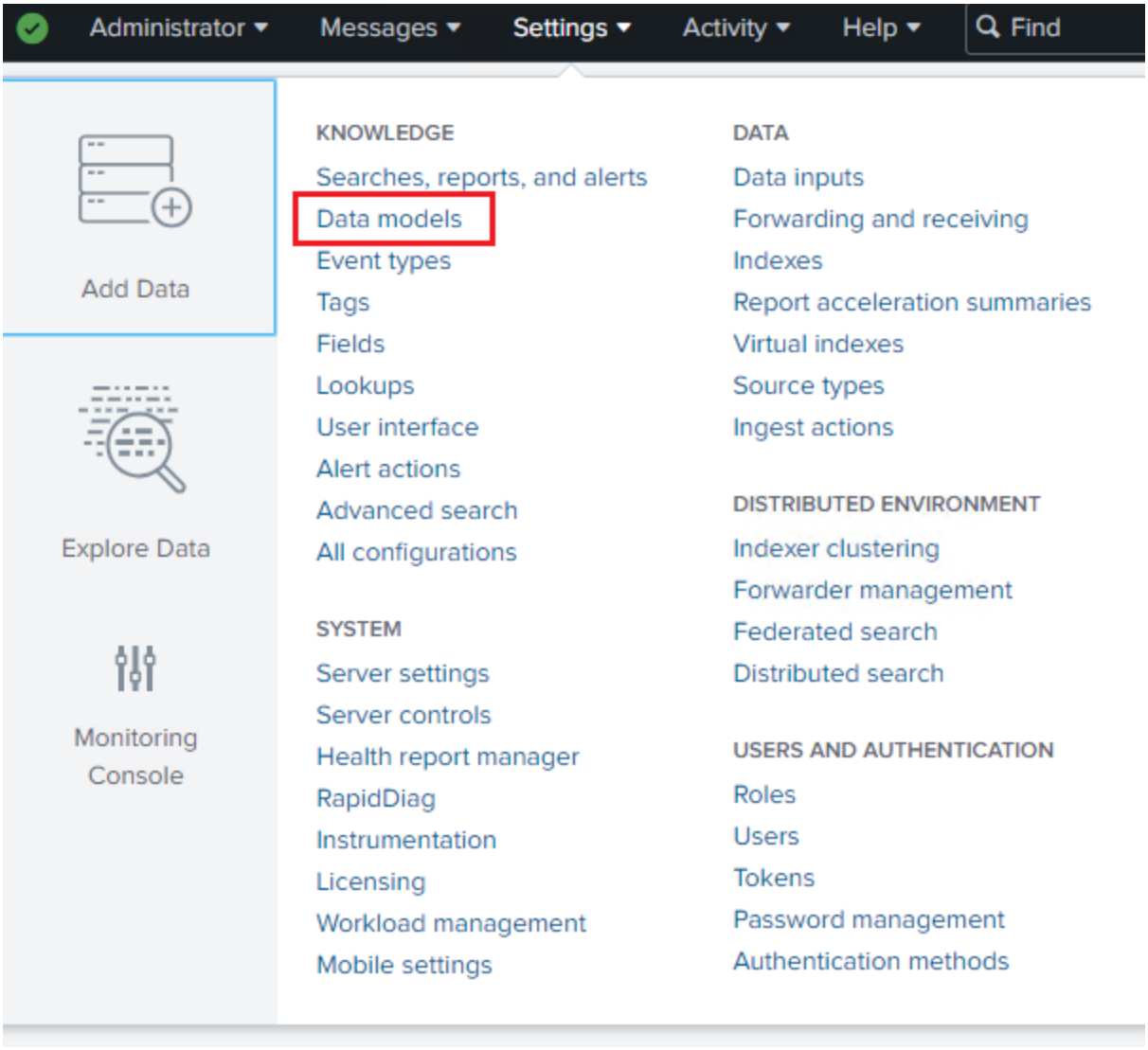
If the App and Add-on cannot be installed from **Browse more**:

- 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**.

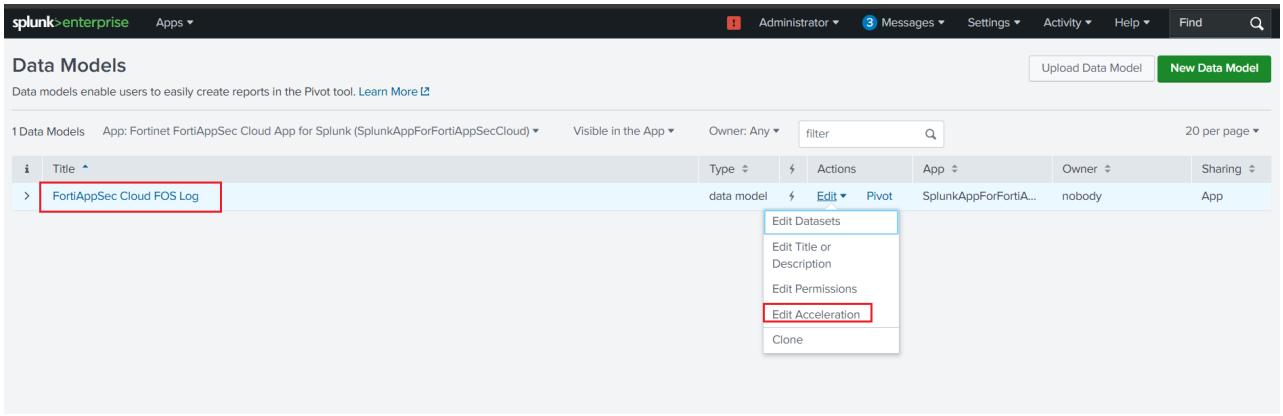
If the dropdown in Attack or Event dashboards does not have value:



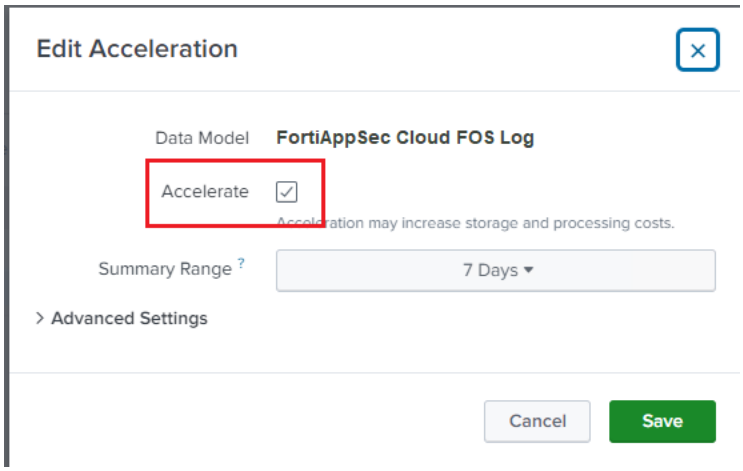
a. Go to **Settings > Data models**



b. Find **FortiAppSec Cloud FOS Log**. Under the **Actions** column, select **Edit > Edit Acceleration**



c. Enable **Accelerate**, then wait for 5 mins or restart Splunk. You will see the dropdown in App.



Using WAF behind a Content Distribution Service

If the traffic to your application server should be first forwarded to a Content Distribution Service, then flows to FortiAppSec 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.

Adding the WAF application on FortiAppSec Cloud

1. When using WAF behind a Content Distribution Service, please take note of the following configurations. For full WAF onboarding instructions, please see Onboard WAF applications on page 65.
   - Do not enable **CDN**, as a scrubbing center nearest to your application server will automatically be assigned. In this case, enabling the CDN is unnecessary because AWS CloudFront already handles content delivery.
   - Take note of the CNAME provided by FortiAppSec Cloud. You will need this when setting up your CloudFront service.
2. Go to **Network > Endpoints** to configure the **SSL Certificate** settings. For full configuration instructions, refer to Endpoints on page 95.
   - If you use **Automatic Certificate**, make sure to select **DNS Challenge** type, otherwise the SSL certificate cannot be successfully retrieved.
   - Make sure to include a CNAME record for the DNS challenge. You can locate this record in **WAF > Applications > DNS Status**.

   Please note that DNS status may show as "Unknown". This is an expected issue when using CloudFront in front of FortiAppSec Cloud. It does not affect the retrieval of the certificate, so there is no need to be concerned about it.

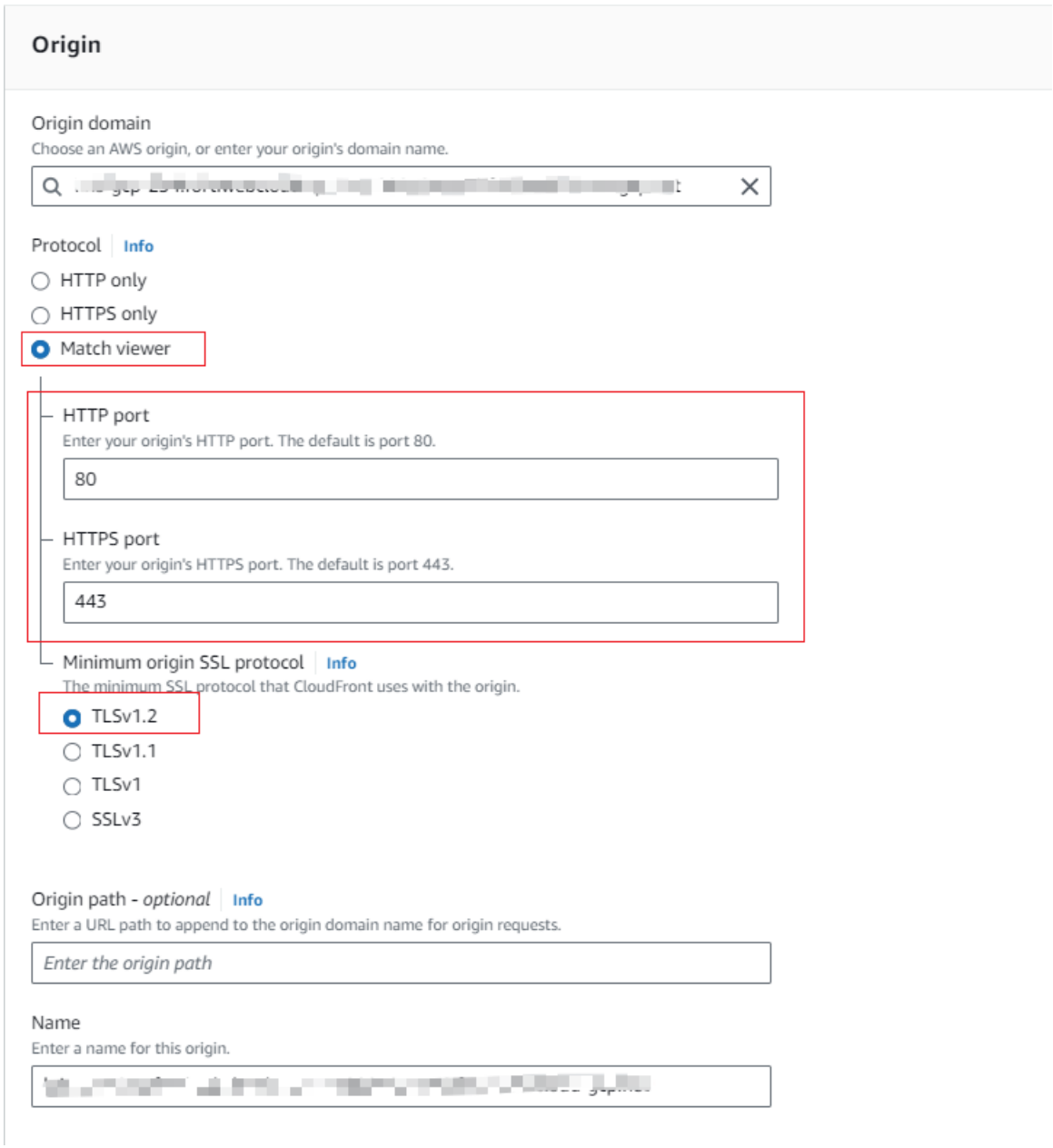
   If you would like to use your own SSL certificate instead of the certificate issued by Let's Encrypt, you can select **Custom Certificate** in **Network > Endpoint** to upload your own SSL certificate.

Creating a Distribution in CloudFront

1. Log in to AWS cloud portal. Navigate to **CloudFront**.
2. Click **Create Distribution**.

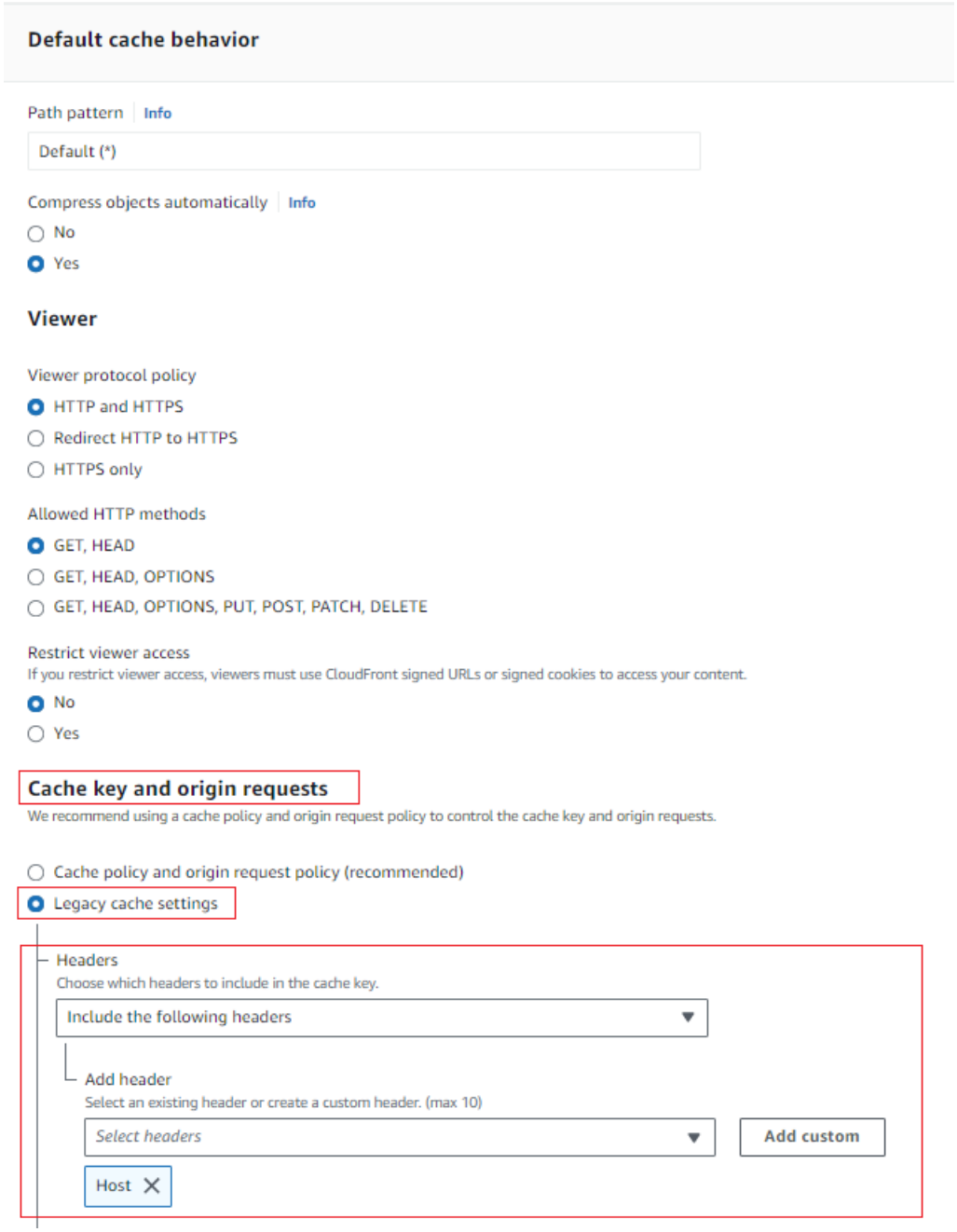
3. Configure the following options as described. You can set any option not specified here according to your preference. Refer to AWS online help for more information.

Origin	
Origin Domain	Enter the CNAME provided by FortiAppSec Cloud.
Origin Protocol Policy	Select **Match Viewer** so that the protocol used for the connections between CloudFront and FortiAppSec Cloud WAF 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 FortiAppSec Cloud WAF 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**.

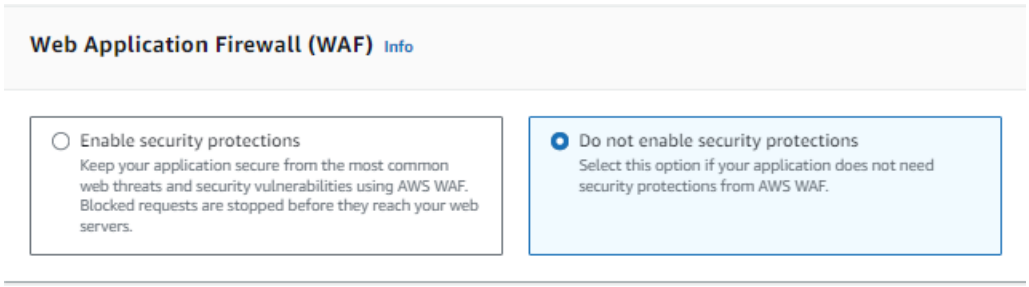


Default Cache Behavior	
Path Pattern	This field specifies to which requests you want this cache behavior to apply. For example, a path pattern of **images/*.jpg** would apply the cache behavior to .jpg images.
Compress objects automatically	Select "Yes" if you want CloudFront to automatically compress 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 FortiAppSec Cloud WAF. See Endpoints on page 95.
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 FortiAppSec Cloud WAF.

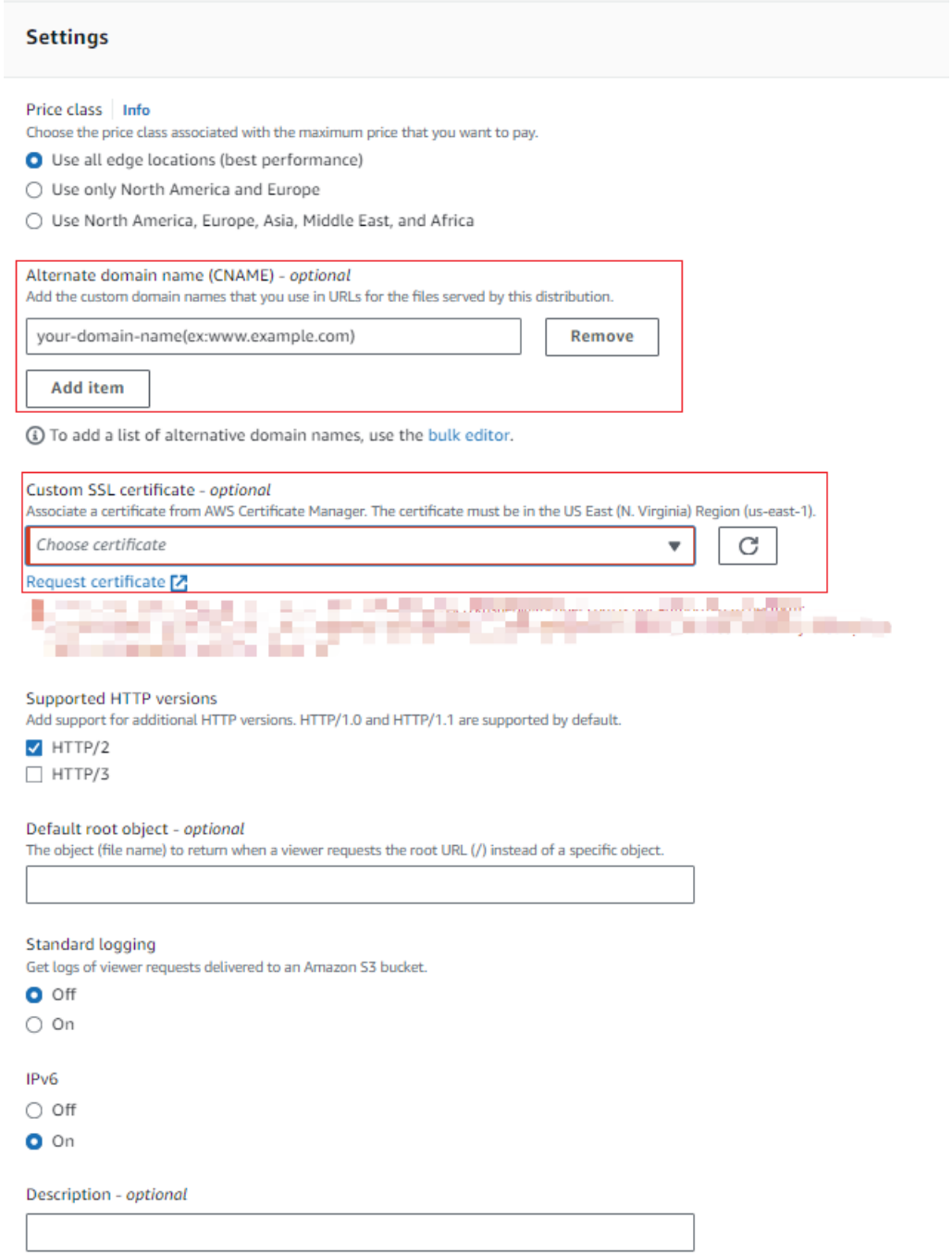


4. You can choose either WAF option.

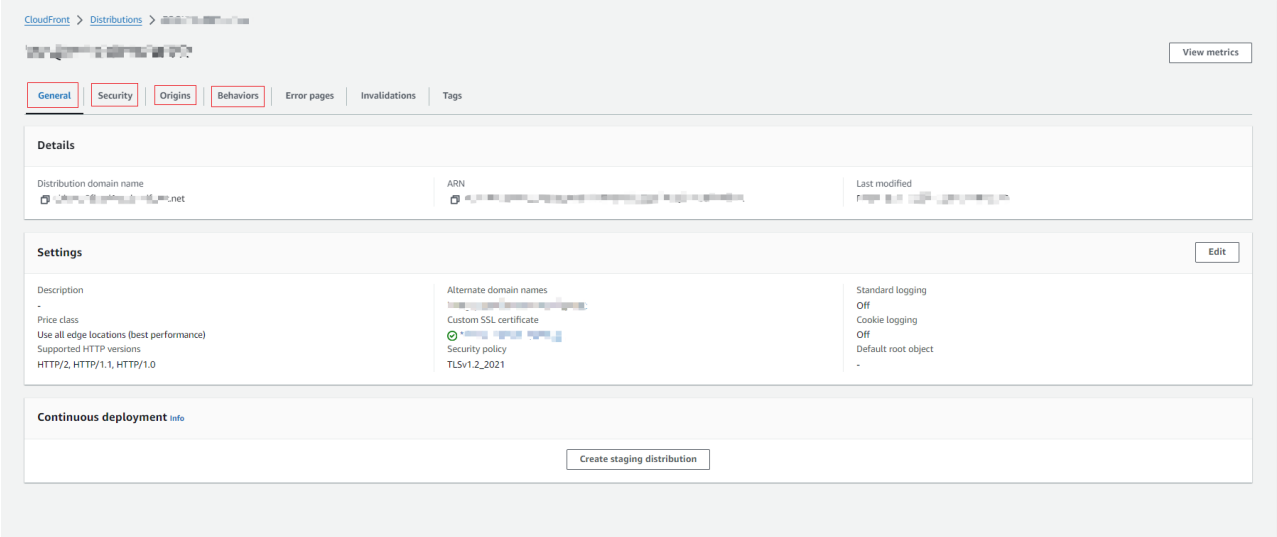


5. Configure the following options as described. You can set any option not specified here according to your preference. Refer to AWS online help for more information.

Settings	
Alternate Domain Names (CNAMEs)	Enter an additional domain name (e.g., www.example.com) that users use to access your application. FortiAppSec Cloud supports multiple domain names for a single application.
SSL Certificate	Select Custom SSL Certificate to upload the SSL certificate.



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 238).
   - **Security**: WAF configurations (details in WAF options).
   - **Origins**: Origin configurations (details in Origin on page 234).
   - **Behaviors**: Default Cache Behaviors Configurations (details in Default Cache Behavior on page 235).



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 FortiAppSec Cloud.

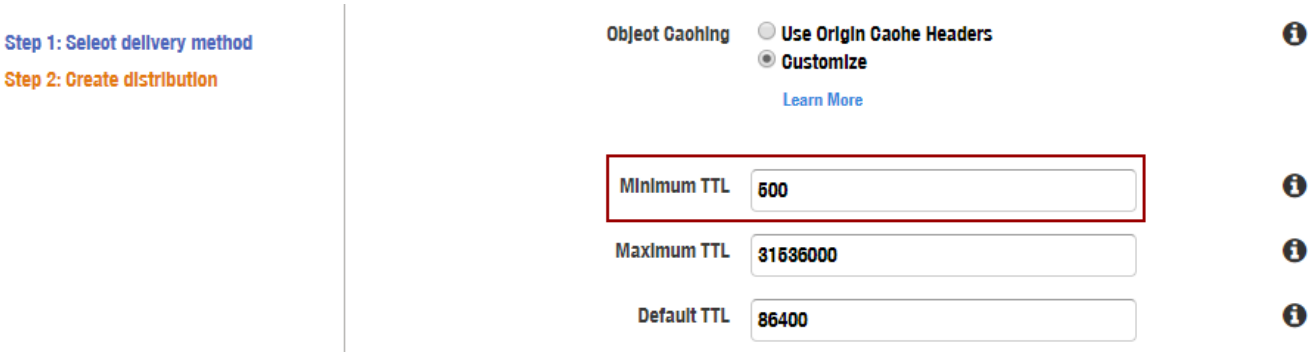
Configuring Error Pages

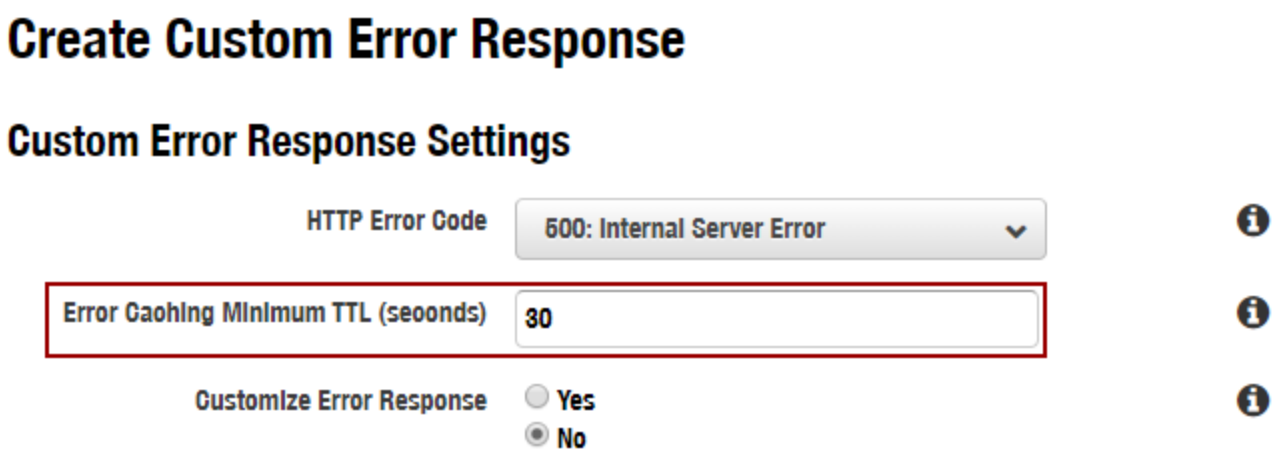
When FortiAppSec Cloud detects a violation to its security rules, it takes appropriate actions, such as blocking the request and returning an error code to the client who initiated this request. The error code is cached in CloudFront, so that when the same client initiates the same request next time, 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 FortiAppSec 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 FortiAppSec 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 500 seconds, while the Minimum TTL for the error code is set much shorter to 30 seconds. 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.





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 FortiAppSec Cloud to protect your application.

FortiAppSec 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 FortiAppSec 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 FortiAppSec 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.

Endpoints

In **Network > Endpoints**, or in the **Network Settings** step of the **Web Application Configuration wizard**, enable **HTTP** and **HTTPS**. Disable **Redirect all HTTP traffic to HTTPS**.

Servers

FortiAppSec Cloud communicates with your application server over both HTTP and HTTPS protocols when there is only one origin server.

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 FortiAppSec 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.
2. Turn off **Server Balance**. Please note the existing origin servers will all be deleted. You can add one server later.
3. Click **OK**.

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 103 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**.

Multiple domains sharing the same IP address

If you have multiple root domain names pairing with the same IP address, for example, both example1.com and example2.com map to 192.168.1.1, then follow the instructions below.

Onboarding applications

Even though there are multiple domains pairing with the same IP address, you only need to onboard one application, so that FortiAppSec Cloud knows the IP address to protect.

As long as the traffic is destined to this IP address, FortiAppSec Cloud will apply the web protection rules to the traffic regardless whether the applications are onboarded.

Importing local certificates

For the applications that are not onboarded, you need to import their certificates through **Custom Certificate** in **Network > Endpoints**. The certificates are used to encrypt the HTTPS connections between your application users and FortiAppSec Cloud. Without a valid certificate, users will see a certificate invalid warning when they visit your application. For how to import certificates, see Endpoints on page 95.

Connecting WAF to the Fortinet Security Fabric

FortiAppSec Cloud supports Fortinet Security Fabric. You can configure FortiGate to view statistics of sites secured by WAF from the FortiGate Dashboard page.

Add WAF 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 FortiAppSec Cloud's WAF service.
   a. Login to your FortiAppSec Cloud account, and go to **Global> System Settings > settings**.
   b. Scroll down to Fabric Connector and click **Create**. The **Add FortiGate Information** pane opens.
   c. 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 FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud's Cloud Services, including FortiAppSec Cloud, through a single account. When you access FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud based on their role.



This feature is only available for certain accounts upon request. Submit a support ticket to request setup.



When an IdP user clicks **Logout**, they are only logging out of the FortiAppSec 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 FortiAppSec 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
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

To match...	You can use...
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. ` ` 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))
All parameters that follow a question mark or hash mark in the URL	[#\?](.*)

To match...	You can use...
(e.g. `#pageView` or `?param1=valueA&param2=valueB...`; back-reference to this match does not include the question/hash mark itself)	

Operational Guidelines

The following topics describe the Operational Guidelines for using FortiAppSec Cloud WAF.

- Maximum configuration values on page 245
- Sequence of scans on page 247

Maximum configuration values

The following table provides the maximum number of configuration objects in each application.

Application item	Maximum value
Logs > attack log servers	2
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	24

Application item	Maximum value
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
WAF > Templates	16
WAF > Report	No Limit
WAF > Admin Management > Users	No Limit
WAF > System Settings > Cloud Connectors	No Limit
WAF > System Settings > Custom Block Pages	8
WAF > System Settings > Settings > API Key	1

Sequence of scans

FortiAppSec 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 FortiAppSec Cloud. **File Protection** is one of the scan items that involve scanning the whole packet. FortiAppSec 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 FortiAppSec 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, FortiAppSec 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 193. • 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 193.
Known Bots	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the SRC field in

Scan/action	Involves
	the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. • Source IP address of the client in the IP layer.
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 193. • 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 193. • `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 193. . • 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 193. • `Host:`

Scan/action	Involves
	• URL in HTTP header • Source IP of the client in the IP header
Mobile API Protection	• `Host:` • 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 193. • `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 193. • `Content-Type:` in `PUT` and `POST` requests • URL in HTTP header • The body of the file
Advanced Bot Protection	• `Host:` • URL in the HTTP header • `Cookie:`
Parameter Validation	• `Host:` • URL in the HTTP header • Name, data type, and length
Bot Deception	• `Host:` • URL in the HTTP header
ML Based Bot 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. • `Host:` • URL in the HTTP header • HTTP version • `Content-Type:` • Response status code

Scan/action	Involves
	• Request method in HTTP header • `Referer:` • `User-Agent:`
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 193. • URL • `Host:` • `X-Forwarded-For:`
XML Protection	• URL • HTTP header • Body
JSON Protection	• URL • HTTP header • 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 193. • 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 193. • URL in the HTTP header • HTTP header

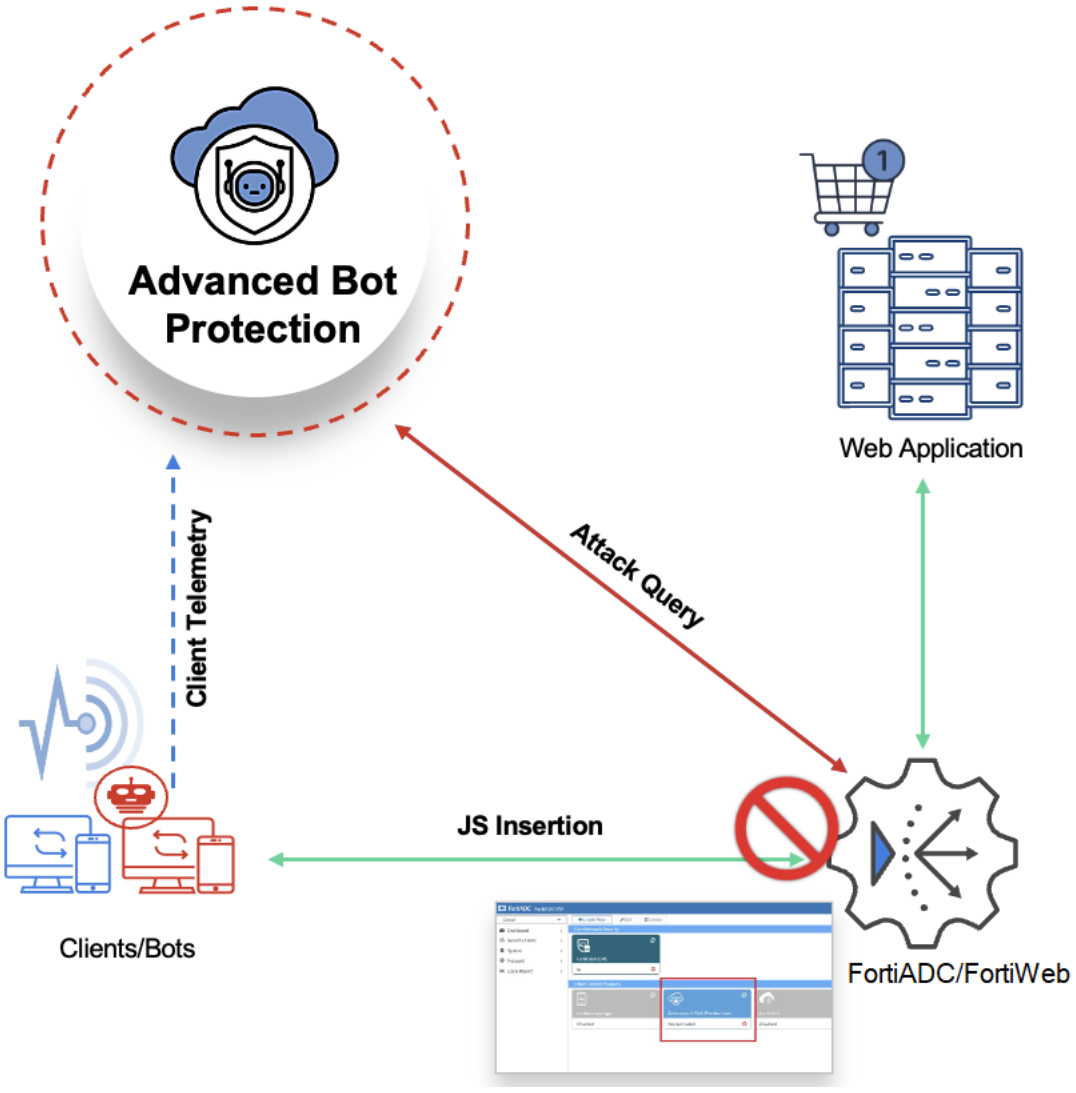
Scan/action	Involves
	• Parameter in the URL
Threshold Based Detection	• Source IP address of the client depending on your configuration of X-header rules. This could be derived from either the `SRC` field in the IP header, or the `X-Forwarded-For:` and `X-Real-IP:` HTTP headers. For details, see Rewriting Requests on page 193. • 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
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:`

Scan/action	Involves
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 150 • `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 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 150 • 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 150 • HTTP headers • HTML Body • URL in HTTP header • Parameters in URL and body • XML in the body of HTTP POST requests

Scan/action	Involves
	• 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
ML based API Protection	• HTTP response json body
HTTP Header Security	• HTTP headers

Advanced Bot Protection

FortiAppSec Cloud Advanced Bot Protection (ABP) is a Fortinet SaaS advanced bot mitigation solution designed to detect and protect against sophisticated bots that may be used to conduct malicious automated attacks on your online applications, such as data harvesting, credential stuffing, account take-over attempts, DDoS attacks, and other fraudulent activities. To safeguard your digital assets, websites, and applications, ABP employs advanced deep learning algorithms and behavior analysis to identify and block suspicious activities. It analyzes user behavior patterns, device fingerprints, and more to distinguish between genuine users and malicious bots.



FortiAppSec Cloud Advanced Bot Protection features a multidimensional deep learning engine that learns and tracks bot attacks over time using sophisticated AI model training. Here are some of the key ways that enable ABP to detect and stop malicious bots while allowing legitimate traffic through:

- **IP reputation database** — Maintains a real-time database of known or suspicious IP addresses associated with bots and blocks traffic from them.

- **Browser Fingerprinting** — Creates unique fingerprints for each visitor by cross-referencing various browser/device attributes to recognize repeat offenders. This includes detecting crawler-specific attributes, checking browser and OS inconsistencies.
- **Biometric detection** — Analyzes visitors' device interactions to determine if a user is a real human or a bot, as biometric signals are very difficult for bots to fake. This includes monitoring client events (over 250 characters), mouse movements (such as scrolling behavior and clicks), and keyboard clicks.
- **Machine learning models** — ABP uses AI to train models on vast datasets and continuously improve and refine bot detection capabilities.
- **Real-time threat intelligence (AI Score)** — Leverages global threat intelligence to stay on top of new and emerging bot threats and update protections. The AI Score is compiled through deep learning and data correlation, multi-dimensional comparison, and multivariate data over time.
- **Comprehensive analytics** — Provides detailed bot traffic analytics and attack forensics to enhance understanding of bot patterns and strategies.
- **Integration with FortiADC and FortiWeb** — Allows FortiADC and FortiWeb to send telemetry data to the bot protection system, providing deeper insights into sophisticated bots for more accurate detection and blocking.

The factors listed above collectively contribute to the calculation of the **Risk Score** — a numerical value ranging from 0 to 100 that reflects the likelihood of a user being a bot.

Overview

The following sections provide an overview of Advanced Bot Protection use cases and configurations.

- Security Fabric Integration on page 255
- ABP Workflow and Dashboard Overview on page 256

Security Fabric Integration

The FortiAppSec Cloud ABP system is designed to seamlessly integrate with your existing infrastructure, supporting various products in the Fortinet Security Fabric, including FortiADC and FortiWeb.

No.	Description
1	User request reaches FortiADC/FortiWeb (as Reverse Proxy).
2	FortiADC/FortiWeb inserts a JavaScript to the HTTP/S response for telemetric information.
3	The client and FortiADC/FortiWeb (via Fabric connector) share telemetry data (such as IP, headers, and device fingerprinting) with the Advanced Bot Protection engine.
4	Using Deep Learning, FortiAppSec Cloud ABP determines if the client is a human or a bot.
5	ABP sends instructions back to FortiADC/FortiWeb to initiate an action against the request (such as block, CAPTCHA, or allow).

Supported Fortinet Products for Integration:

- **FortiADC** — An advanced Application Delivery Controller (ADC) that provides Application availability using Server Load Balancing (in Layer 4 and Layer 7) and Global Server Load Balancing (GSLB), along with application Security features such as Web Application Firewall (WAF), IPS, DLP, Sandbox, AV and more. For integration instructions,

please refer to FortiADC Integration on page 277

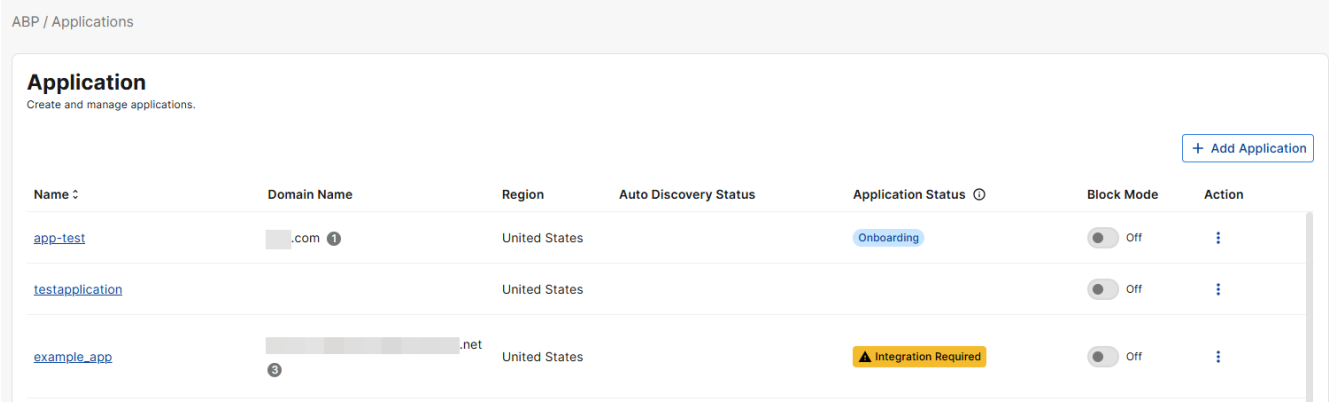
- **FortiWeb** — A web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day threats. The Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe. For integration instructions, please refer to FortiWeb Integration on page 281

ABP Workflow and Dashboard Overview

This section provides an introduction to the primary web portal pages for configuring settings and monitoring application activity in FortiAppSec Cloud's ABP Service.

Application

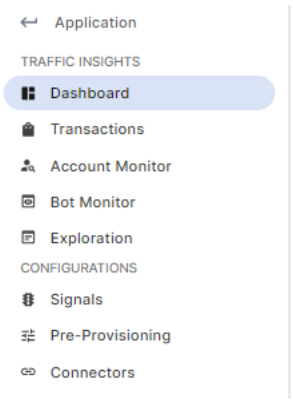
The **Application** page contains the management settings for the applications you want to protect through FortiAppSec Cloud. Here, you can add new applications and access the details on existing applications, most notably the **Application ID** and **Status** information. When you initially add an application, the status will be **pending** until it has been fully analyzed and Pre-Provisioning is complete. Once the application status is **ready**, you can connect ABP to your connector device using the Application ID.



Traffic Insights

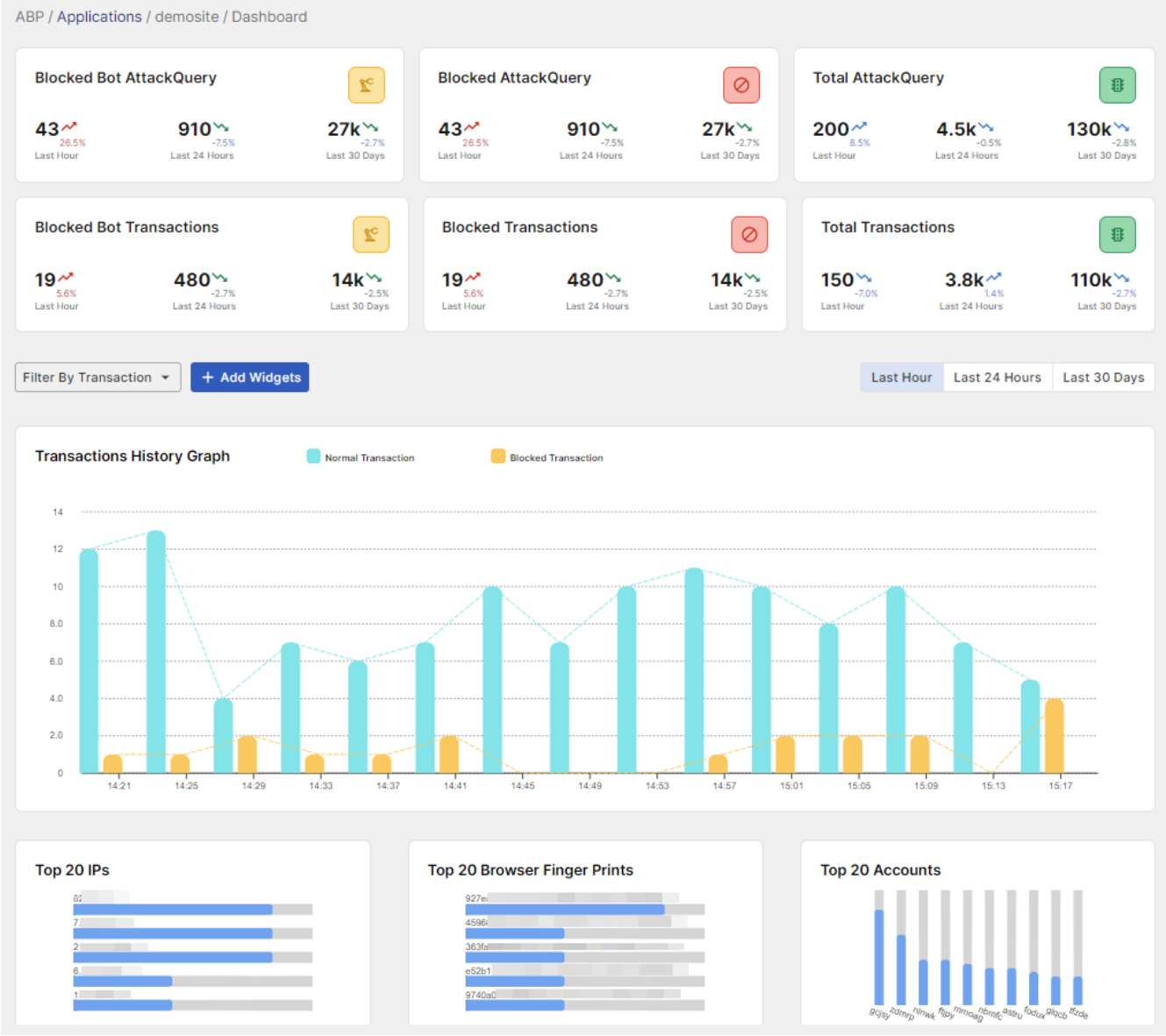
The **Traffic Insights** menu includes dashboards and monitors to view real-time reporting and analytics of your traffic, bot activity, and security incidents to provide insights to help you make informed decisions to enhance your bot protection strategy.

To access the **Traffic Insights** and **Configurations** pages, click the name of one of the applications on the **Application** page.



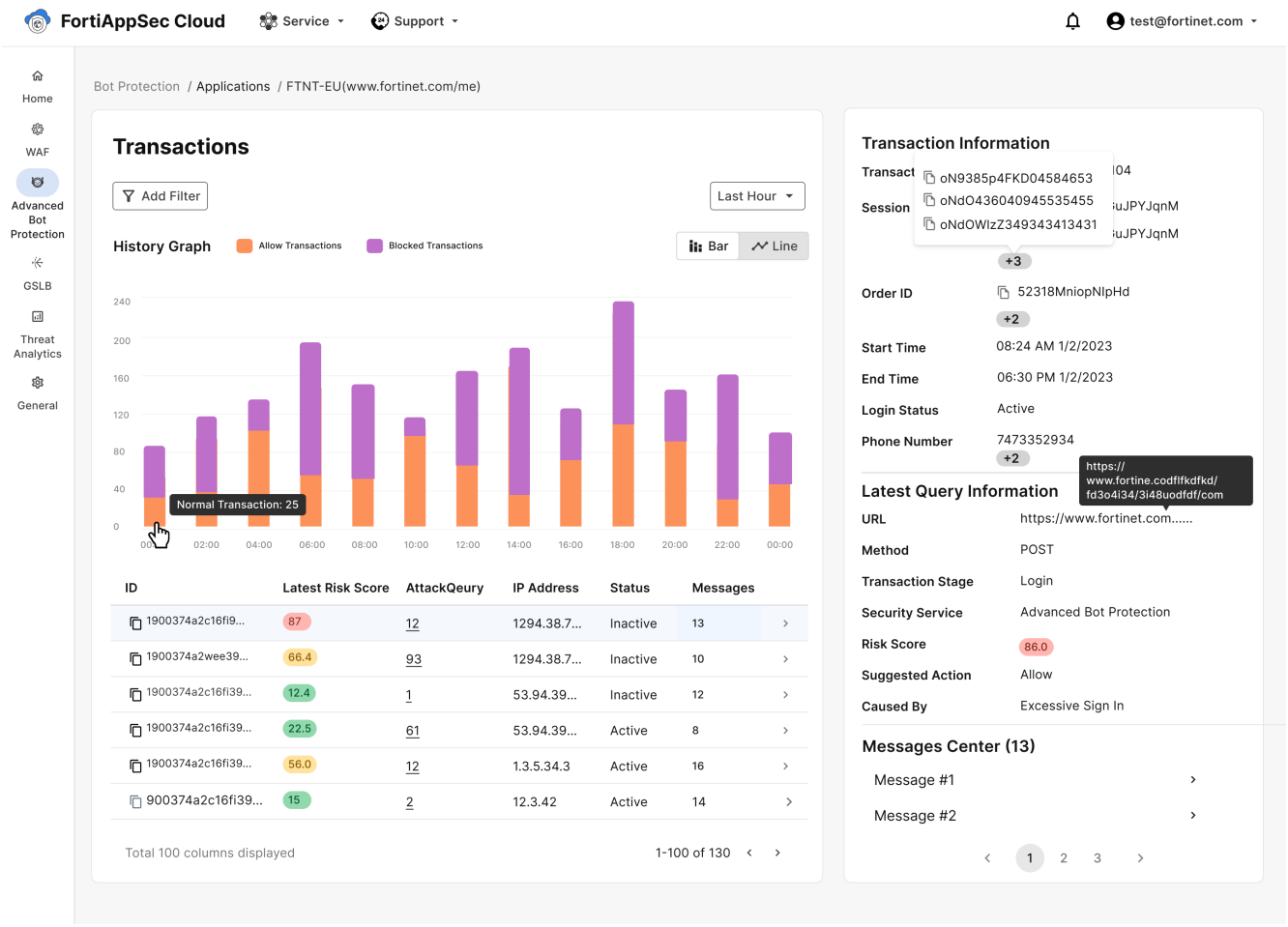
Dashboard

The **Dashboard** page contains widgets and graphs that provide data visualizations of the various data points collected and monitored in FortiAppSec Cloud.



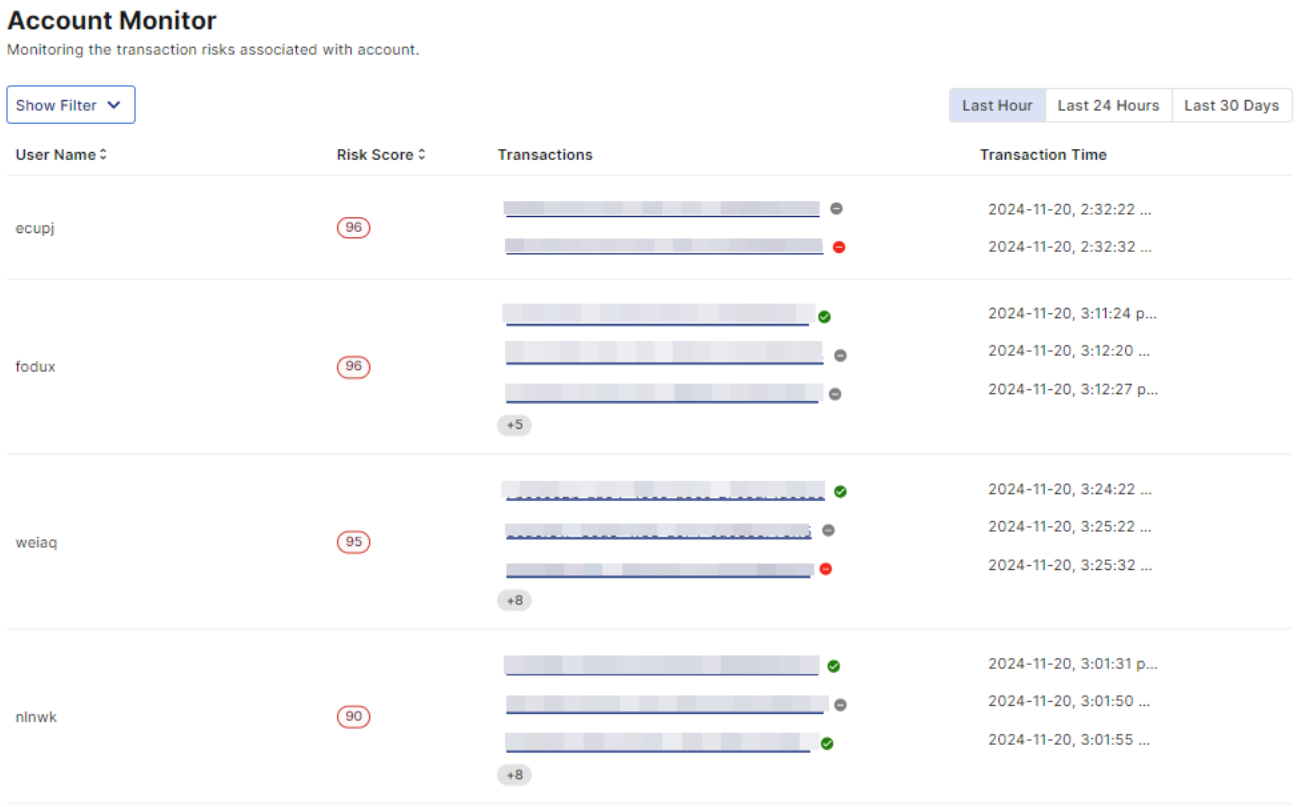
Transactions

The **Transactions** page contains the records of all user activities within your application, including login attempts, payment outcomes, idle periods exceeding a specified duration, and browser closure. You have the option to view records from the last hour, last 24 hours, or last 30 days.



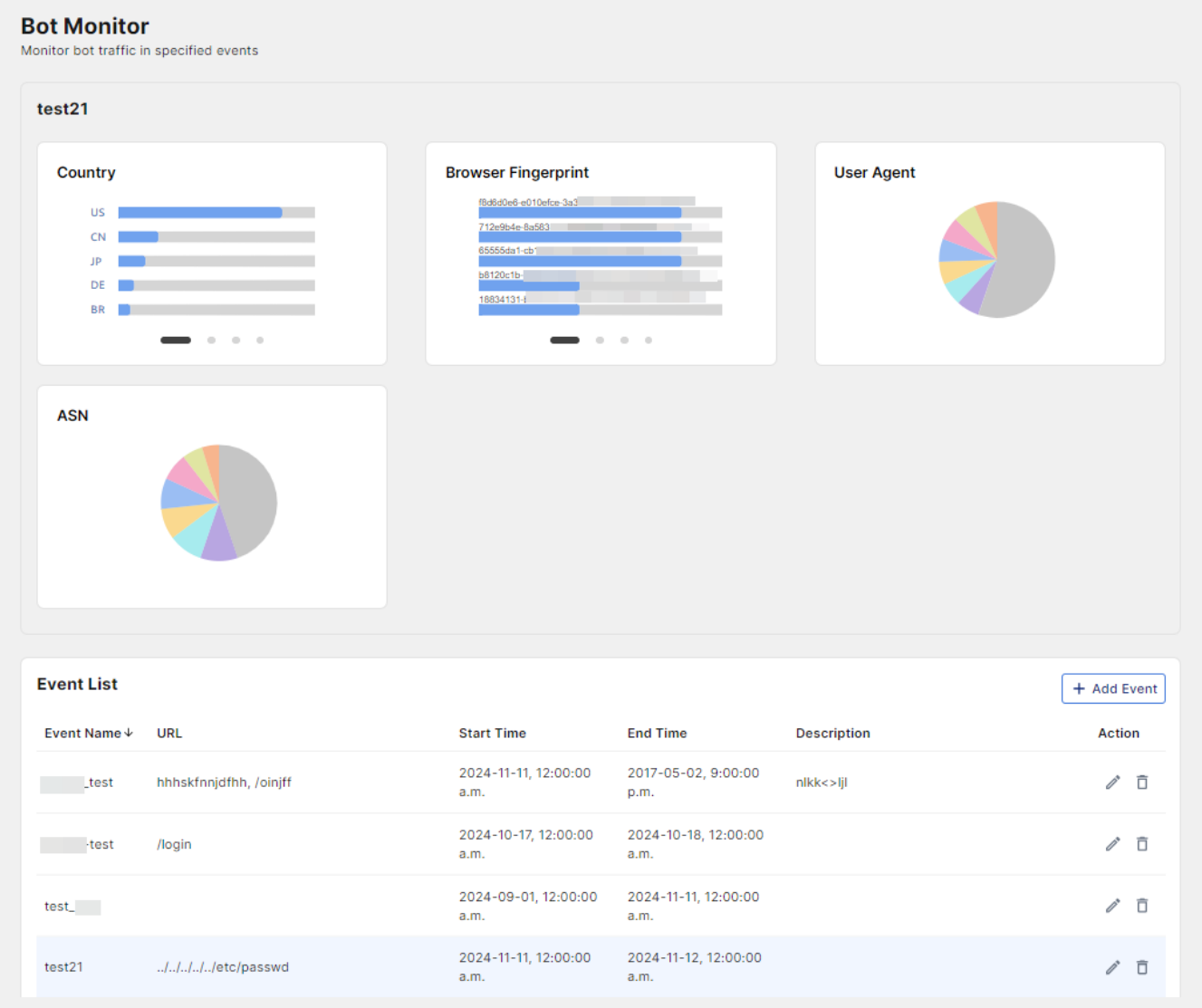
Account Monitor

From the **Account Monitor** page, you can monitor the transaction records based on the user to track the risk associated with each account over time.



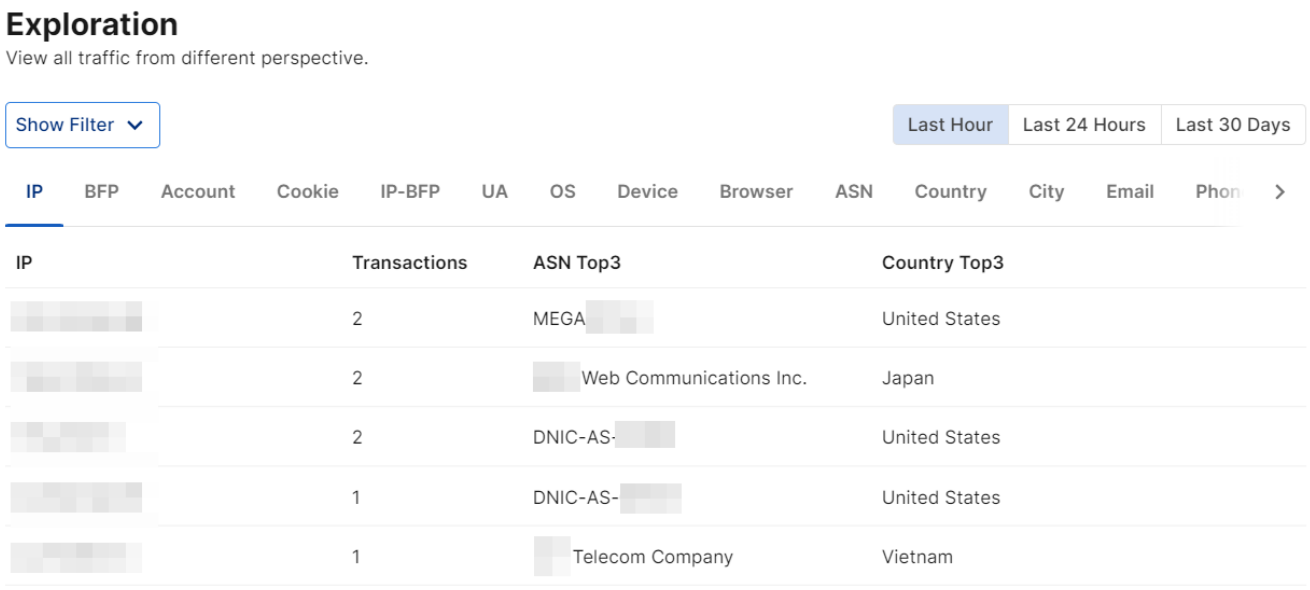
Bot Monitor

The **Bot Monitor** page allows you to define specified periods as bot monitoring events. This allows you to take snippets of bot traffic and analyze various data points such as the attack origin country, browser fingerprint, the cause of the bot attack, and more.



Exploration

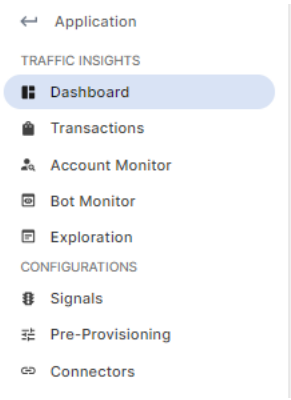
The Exploration page allows you to view all traffic information filtered through different data points to provide varied perspective and insight.



General

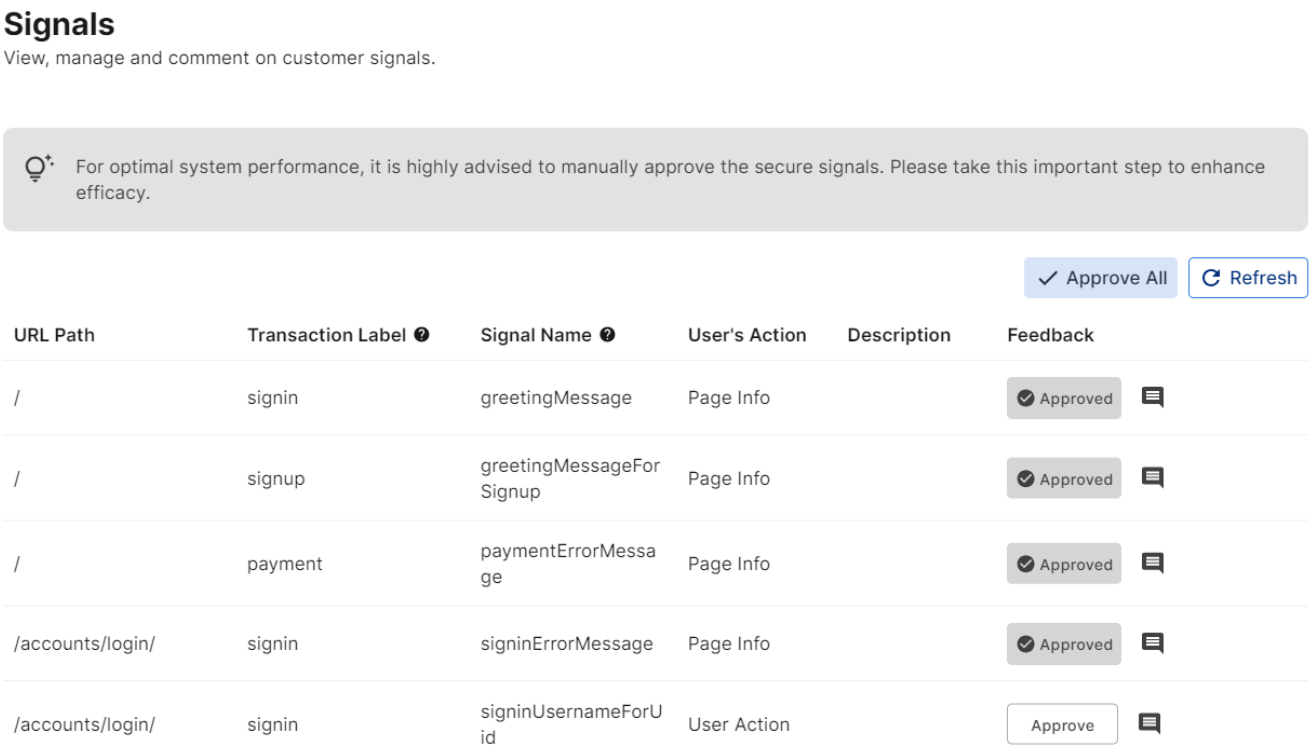
The **General** menu contains the elements for setting up and customizing the Advanced Bot protection system.

To access the **Traffic Insights** and **General** pages, click the name of one of the applications on the **Application** page.



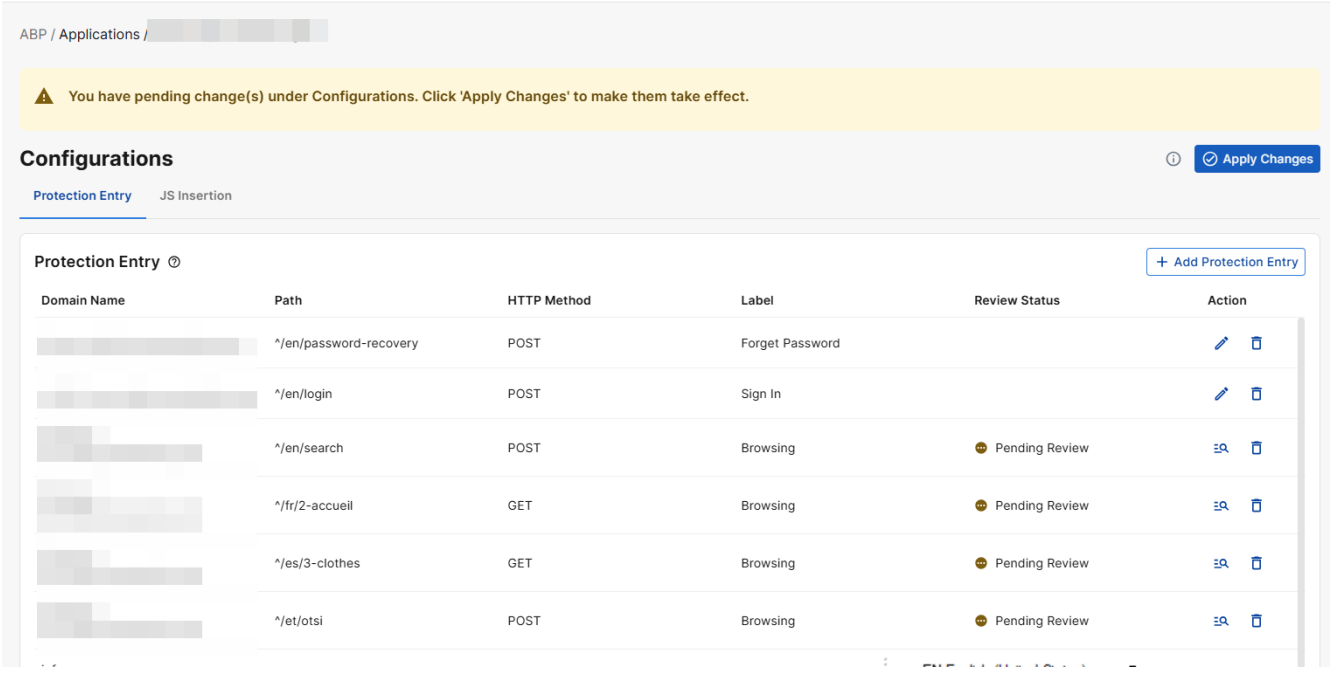
Signals

The **Signals** page contain "Signal" entries, transactions which involve sensitive data that are identified as potential bot signifiers to incorporate into the ABP machine learning model. User approval is required to track the sensitive data contained in these Signals, otherwise ABP will exclude these data points in its AI model training to identify similar suspicious activity.



Configurations

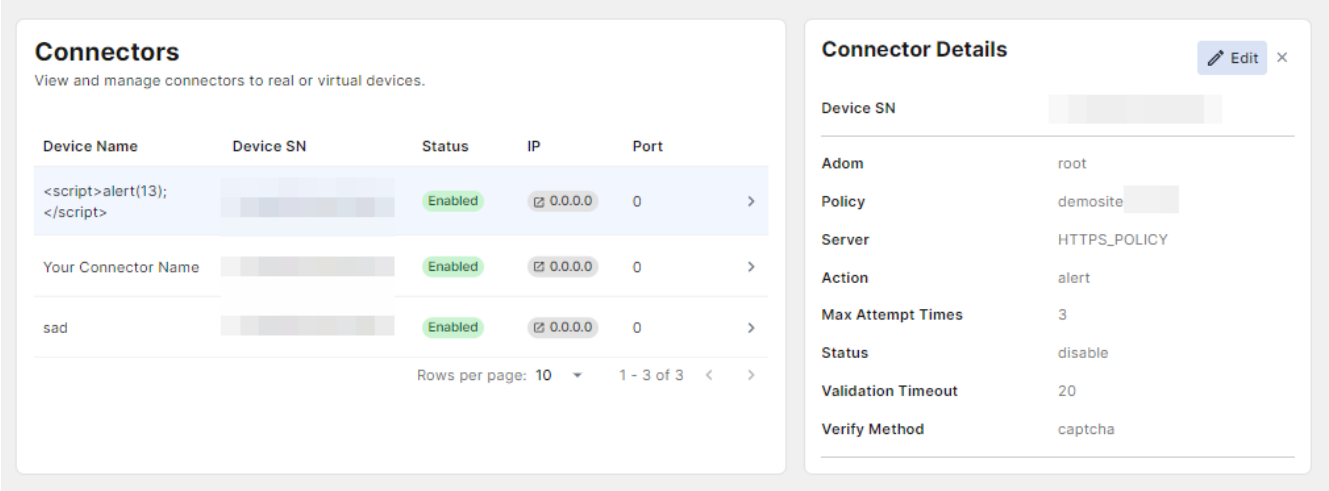
The **Configurations** page contains the analyzed resources required to protect your application, which includes the protected URL entries and the locations where JavaScript is inserted through your connector devices to collect client information for bot detection.



Connectors

From the **Connectors** page, you can view the Fabric devices connected to ABP. This page contains details of each connector device, including their device serial number, IP address, port number, and more.

In rare troubleshooting scenarios when ABP does not successfully fetch the device IP or Port, you may edit these fields.



ABP Setup

This section details the basic steps to onboard your FortiAppSec Cloud Advanced Bot Protection system.



Enabling **Advanced Bot Protection** on WAF will automatically generate a corresponding application on ABP if one has not been previously created for the application.

Therefore, if you intend to onboard your application to both ABP and WAF, we recommend first onboarding your application on WAF, then following the steps under Set up Advanced Bot Protection (ABP).

- Onboarding ABP Applications on page 264
- Integrate ABP on an on-premises device on page 276

Onboarding ABP Applications

This page provides a detailed explanation of each step in the ABP application onboarding process, followed by configuration steps. Please read through the **Overview and Concepts** before proceeding to configuration.

- Overview and Concepts on page 265
  - Auto Discovery on page 265
  - Entry points on page 266
- Configuration Steps on page 267
  - Create an ABP Application on page 267
  - Review Suggested Protection Entries on page 271

- Enable Block Mode on page 275
  - Block Mode Prerequisites on page 275

Overview and Concepts

The Advanced Bot Protection onboarding process is composed of the following stages:

1. **Create Application**
   a. Enter name and regions
   b. Add at least one on-premises Integration domain or FortiAppSec Cloud WAF Application.
   c. Enter Entry Points.
2. **Complete Onboarding on WAF or on-premises device**
   - Route traffic from your FortiAppSec Cloud WAF application to Advanced Bot Protection, or Integrate the newly created ABP application to your on-premises device.
3. **Auto Discovery**
   a. Auto Discovery analyzes your application. The duration of this process depends on the application's complexity, as well as the number of entry points and protection categories selected.
   b. You should be notified by email when Auto Discovery finishes.
   c. Once Auto Discovery is complete, ABP may suggest new protection entries to add to your configuration.
4. **Review Configuration**
   a. Review, edit, and apply Auto Discovery's suggested protection entries as needed.
   b. When you apply a suggested protection entry, the protection takes effect within a few minutes.
5. **Rule adjustment**
   - ABP tunes protection rules for two weeks based on real traffic to your application.
6. **Enable Block Mode**
   - Before you enable **BlockMode**, review the Block Mode Prerequisites on page 275. Enabling **Block Mode** too early may cause false positives, as rule adjustments are based on real-time traffic analysis.

Auto Discovery

Auto Discovery is an optional, AI-assisted feature that analyzes your provided information and application behavior to identify key application components and protection targets, such as login pages, APIs, and transaction flows. It requires manual review and adjustment of its results. If no entry points are provided, Auto Discovery will not run automatically. Users can also perform manual configuration under **Advanced Bot Protection > Application > Configurations**.

Auto Discovery differs from the previous Pre-Provisioning process by leveraging self-service and AI to reduce setup time from several weeks to a few hours.

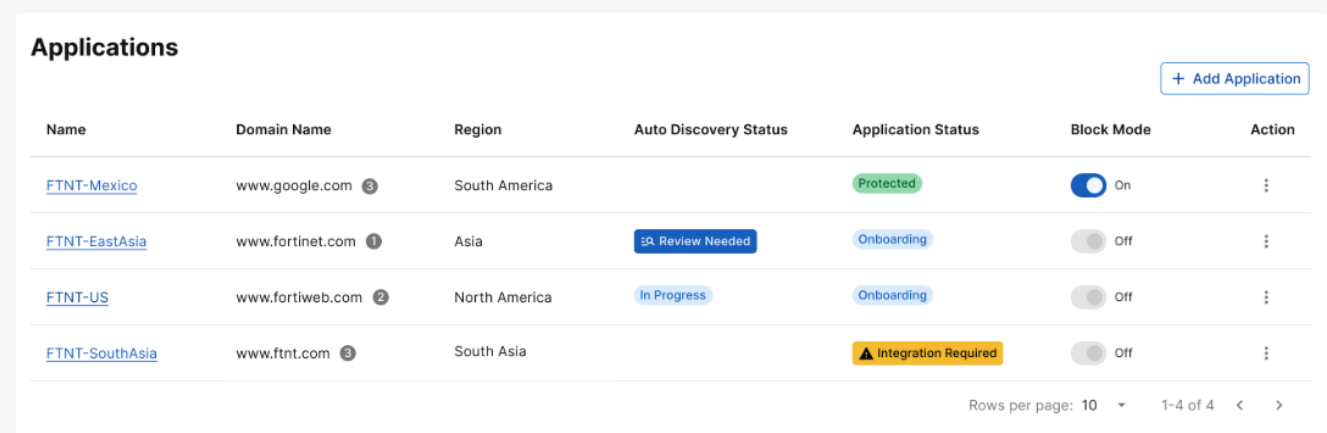
What it does:

- Detects potential entry points that need protection (pages, endpoints, APIs).
- Suggests protection entries automatically.
- Recognizes authentication patterns using return codes or HTTP responses.
- Reduces manual configuration effort during ABP onboarding.

The Auto Discovery Status indicates the current stage of the protection entry discovery process.

- **In Progress**: Auto Discovery is still analyzing your application. No urgent action required.
- **Review Needed**: Auto Discovery has suggested new protection entries. Please review and confirm the changes.
- **Connection Issue**: Advanced Bot Protection could not connect to the entry points you provided. Potential causes for this include:
  - The application's firewall is blocking ABP's management IPs.
    Add these IPs to your allowlist to prevent requests from being blocked.
    - FortiAppSec Cloud WAF: IP protection
    - FortiWeb: IP List - Blocklisting & whitelisting clients using a source IP or source IP range
    - FortiADC: Using the Geo IP allowlist

    If additional services are configured with firewall policies, ensure that ABP's management IPs are added to their allowlists.
  - There is an error in the entry point URL.
    To edit the entry point URL:
    i. From **Advanced Bot Protection > Applications**, click the three dots under **Action** .
    ii. Click **Edit Application**.
    iii. Go to the **Entry Points** tab, and edit the Entry Point text input field



Entry points

Entry points refer to URLs in your application that users or bots interact with. For Auto Discovery, add entry points that are common targets for bot activity. These typically include pages where users submit sensitive information, such as login, signup, or checkout pages.

Other recommended protection entries include:

- Search or product listing pages with dynamic content
- API endpoints handling authentication or transactions
- Contact or feedback forms
- Account management pages (e.g., password reset)

For any additional or customized protection goals, configure them manually under **Advanced Bot Protection > Application > Configurations**.

When adding entry points, select only the most relevant **protection categories** to speed up the auto-discovery process.

- **Denial of Service (DoS)**: Attempts to overwhelm your site with traffic, causing downtime or slow performance. AutoDiscovery primarily detects DoS activity targeting search pages.

- **Account Takeover**: Attempts to gain unauthorized access to user accounts. Typically targets login or password-reset pages.
- **Automated Account Creation**: Bots create fake accounts to exploit services or commit fraud. Typically targets registration or signup pages.
- **Content Scraping**: Bots extract content from your site, such as articles or images. Typically targets browsing pages.
- **Price Scraping**: Bots collect pricing information for competitive analysis. Typically targets browsing pages.

Configuration Steps

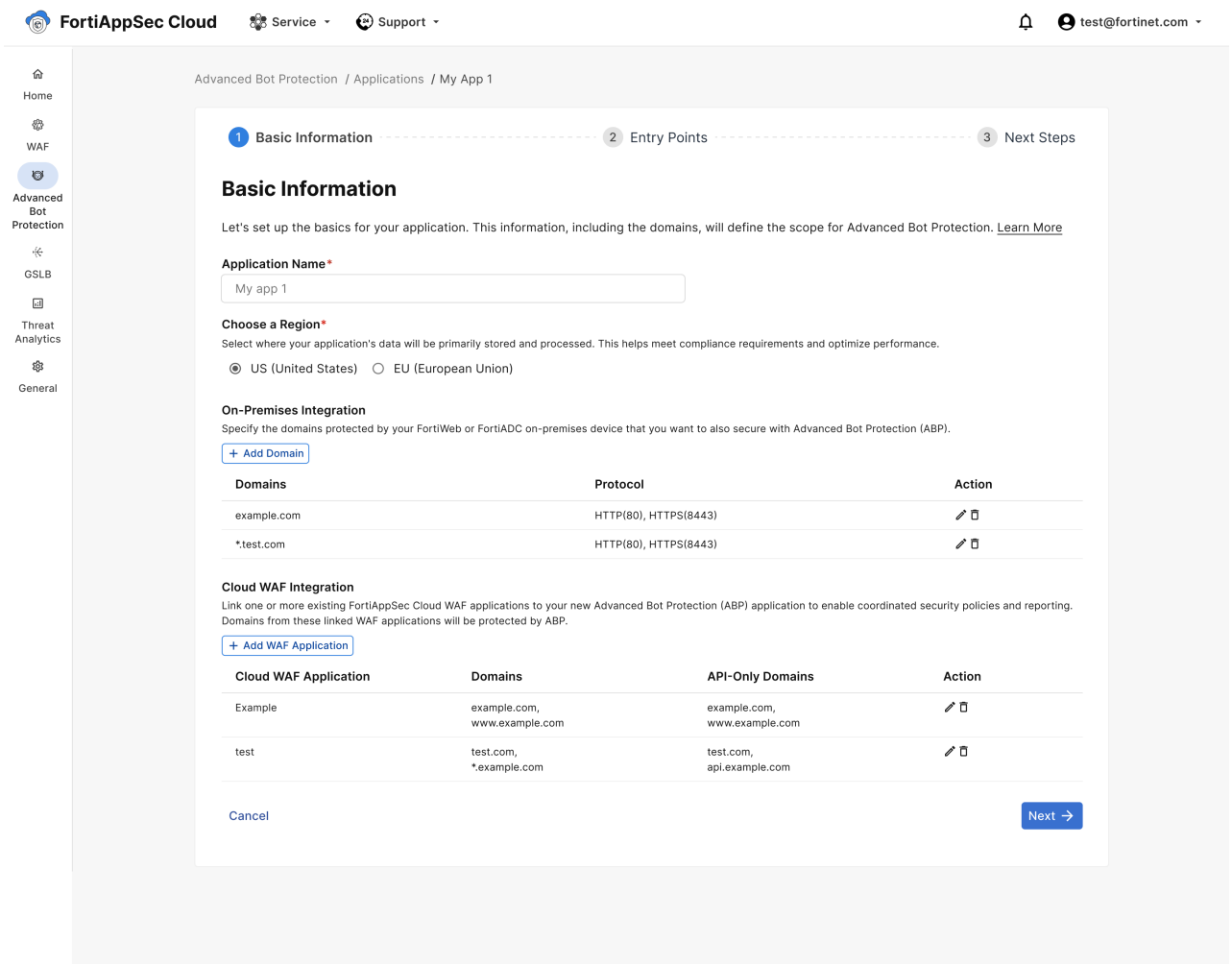


When you create an ABP application, make sure to add FortiAppSec Cloud's IP addresses to your security allowlist to ensure proper connectivity:

- 3.123.68.65
- 3.226.2.163

Create an ABP Application

1. Navigate to **Advanced Bot Protection > Application**.
2. Click **Add Application**.
3. **Basic Information**


FortiAppSec Cloud
Service
Support
test@fortinet.com
Home
WAF
Advanced Bot Protection
GSLB
Threat Analytics
General
Advanced Bot Protection / Applications / My App 1
1 Basic Information
2 Entry Points
3 Next Steps
Basic Information
Let's set up the basics for your application. This information, including the domains, will define the scope for Advanced Bot Protection. Learn More
Application Name*
My app 1
Choose a Region*
Select where your application's data will be primarily stored and processed. This helps meet compliance requirements and optimize performance.
US (United States)
EU (European Union)
On-Premises Integration
Specify the domains protected by your FortiWeb or FortiADC on-premises device that you want to also secure with Advanced Bot Protection (ABP).
+ Add Domain
Domains
Protocol
Action
example.com
HTTP(80), HTTPS(8443)
*.test.com
HTTP(80), HTTPS(8443)
Cloud WAF Integration
Link one or more existing FortiAppSec Cloud WAF applications to your new Advanced Bot Protection (ABP) application to enable coordinated security policies and reporting. Domains from these linked WAF applications will be protected by ABP.
+ Add WAF Application
Cloud WAF Application
Domains
API-Only Domains
Action
Example
example.com, www.example.com
example.com, www.example.com
test
test.com, *.example.com
test.com, api.example.com
Cancel
Next

a. Enter the following:

Setting	Description
Application Name	Enter a name for this application that will make it easy for you to identify within the FortiAppSec Cloud UI.
Region	The location of the service that processes the traffic of your application. • United States (US) • European Union (EU)

b. Add at least one **On-premises Integration** (FortiWeb or FortiADC) or **FortiAppSec Cloud WAF Application**.

- If adding an **On-Premises Integration**, click Add **Domain** and enter the following:

Setting	Description
Domains	Enter the domains associated with your on-premises integration.
Advanced Domain Options	Select whether your domain uses HTTP, HTTPS, or both. **Enable Special Port** to enter a custom port number if your domain uses a non-standard port (other than HTTP 80 or HTTPS 443).
API-Only Domains	Enter any domains belonging to your application that only handle API calls.

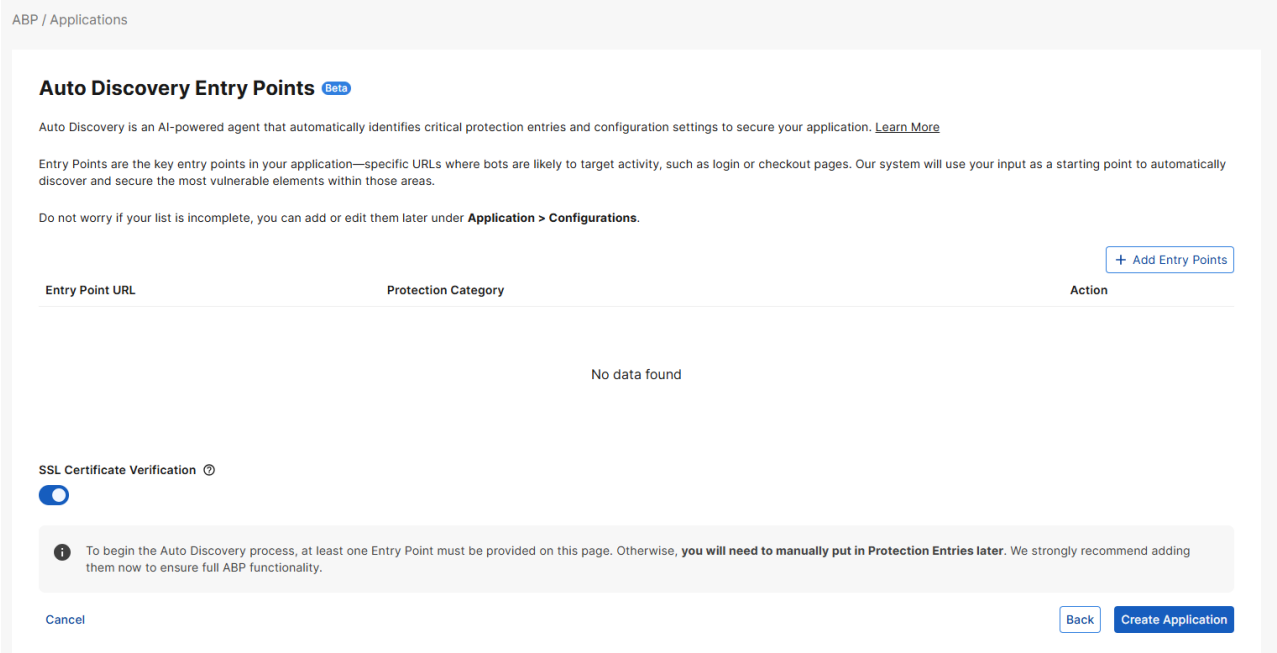
- If adding a **FortiAppSec Cloud WAF Application**, click **Add WAF Application** and enter the following:

Setting	Description
Cloud WAF Application Name	From the drop-down list, select the desired existing WAF Application under your account.
API-Only Domains	Enter any domains belonging to your application that only handle API calls.

c. Click **Next**.

4. **Entry Points**

Enter Auto Discovery Entry points. For more details on how Auto Discovery works, please refer to Auto Discovery on page 265.



a. Click **Add Entry Points**

b. Enter the following:

Setting	Description
Entry Point URL	Entry Points are URLs in your application that are likely targets for bots. This typically includes pages where users enter sensitive information, such as login or checkout pages. For more details on this concept, please refer to Entry points on page 266. If the port number is not 80 for HTTP or 443 for HTTPS, please include the custom port number in the Entry Point URL. Example input where the port number is 1111: `example.com:1111/login`
Protection Category	Select the attack categories relevant to the URL entered above. Note that selecting more protection categories may increase the time required for the AutoDiscovery process to complete. • **Denial of Service (DoS)**: Attempts to overwhelm your site with traffic, causing downtime or slow performance. AutoDiscovery primarily detects DoS activity targeting search pages. • **Account Takeover**: Attempts to gain unauthorized access to user accounts. Typically targets login or password-reset pages. • **Automated Account Creation**: Bots create fake accounts to exploit services or commit fraud. Typically targets registration or signup pages. • **Content Scraping**: Bots extract content from your site, such as articles or images. Typically targets browsing pages. • **Price Scraping**: Bots collect pricing information for competitive analysis. Typically targets browsing pages.

Setting	Description
Credentials	Optional; Provide the username and password for an existing, non-critical test account. This allows the system to determine the conditions for successful authentication, such as expected HTTP responses.

c. **SSL Certificate Verification** is enabled by default. When enabled, FortiAppSec Cloud verifies the server's SSL certificate when **Auto Discovery** connects to entry points.

Disable this only for self-signed or staging/test certificates not trusted by browsers.

d. Click **Save**.

e. Repeat steps **a** to **c** until you have finished adding **Entry Points**. You will be able to add additional entry points after creation.

f. Click **Create Application**, and confirm application creation.

5. **Next Steps**

At this stage, Auto discovery is initiated.

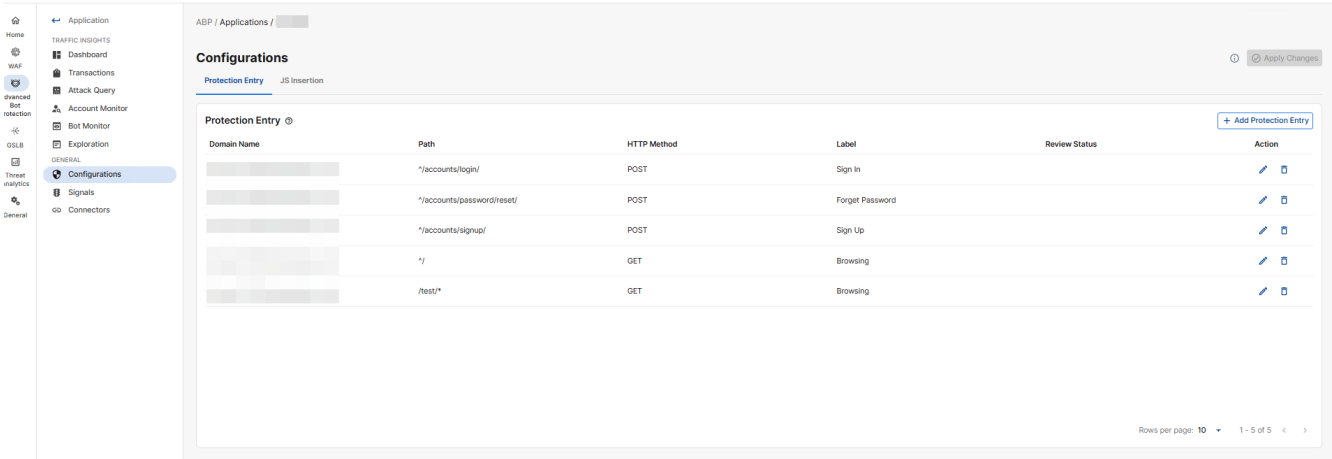
If your ABP application is connected to a FortiAppSec Cloud, please follow Instructions for Set up ABP on FortiAppSec Cloud WAF

If your ABP applicaiton is connected to an on-premises FortiWeb or FortiADC device, please follow the instructions for Integrate ABP on an on-premises device on page 276

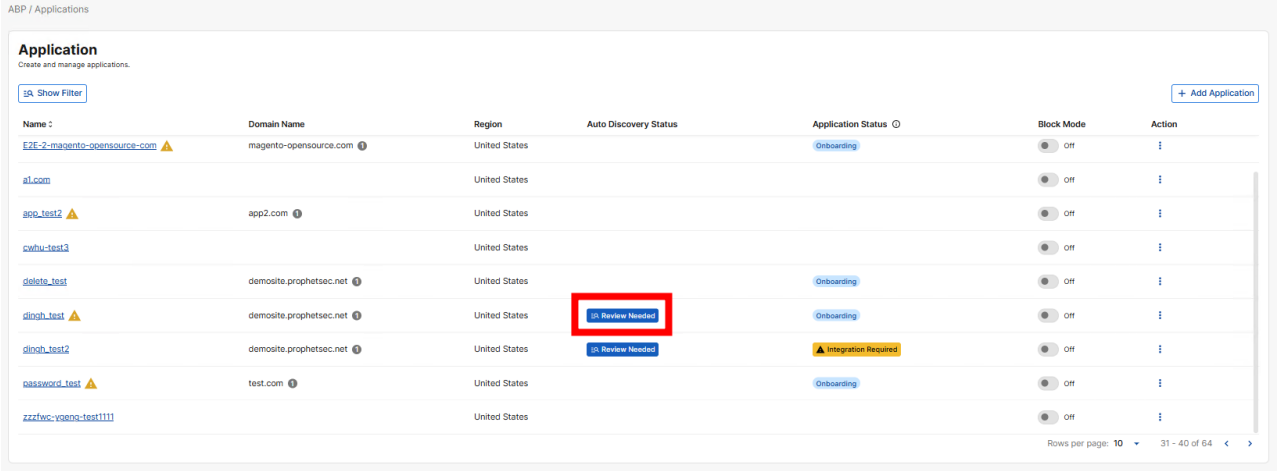
For more information on how to edit and delete applications, please see ABP Application on page 284.

Review Suggested Protection Entries

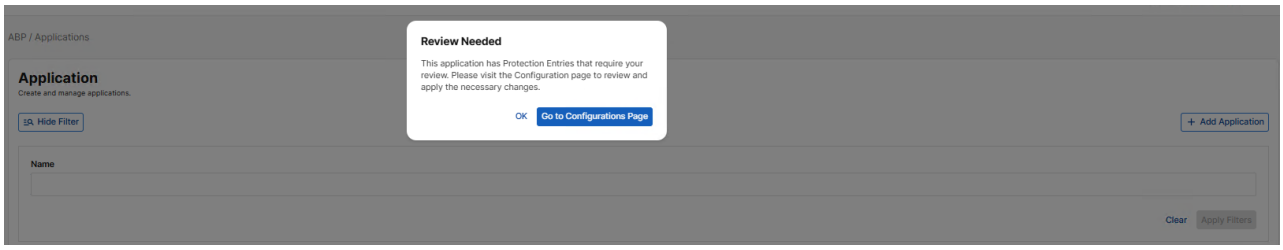
Once Auto Discovery is complete, ABP may suggest new protection entries for your configuration. Review, edit, and apply these suggested entries as needed. When a suggested protection entry is applied, the protection becomes effective within a few minutes.



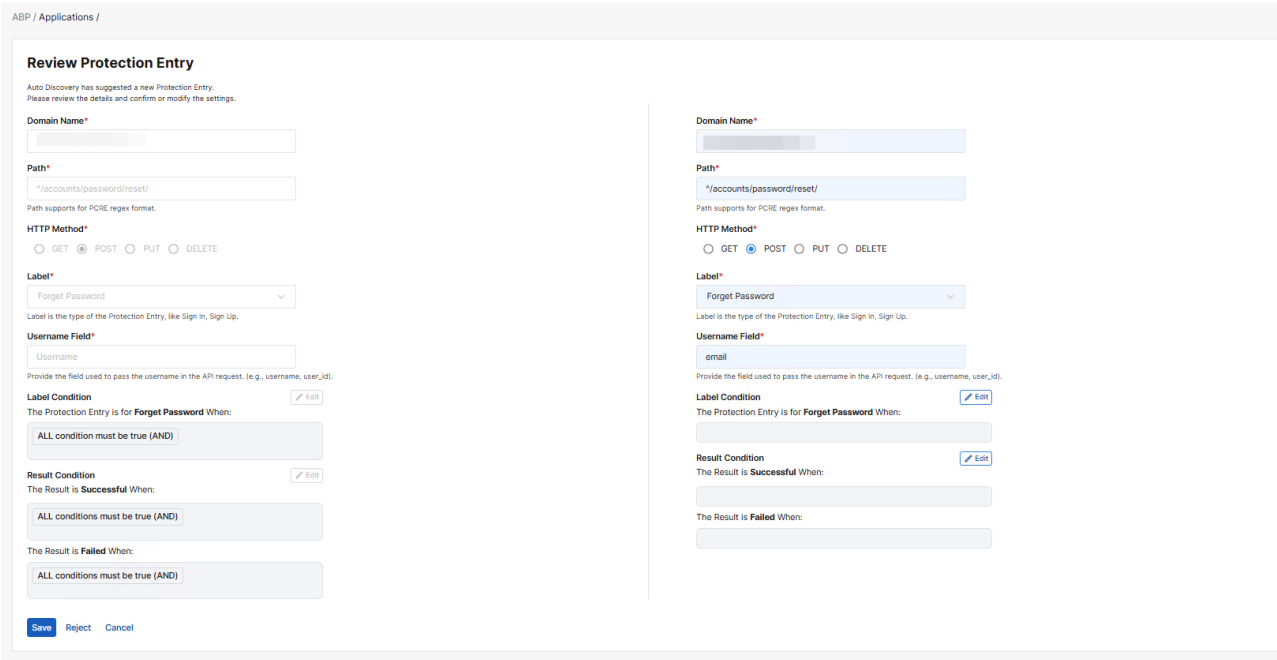
1. When an application's **Auto Discovery Status** displays as **Review Needed**, click the status to navigate directly to the suggested protection entry.



2. Click **Go to Configurations Page**. Alternatively, you can navigate to this page by going to **Advanced Bot Protection > Application > Configurations**, and clicking the **Review** icon under **Action**.



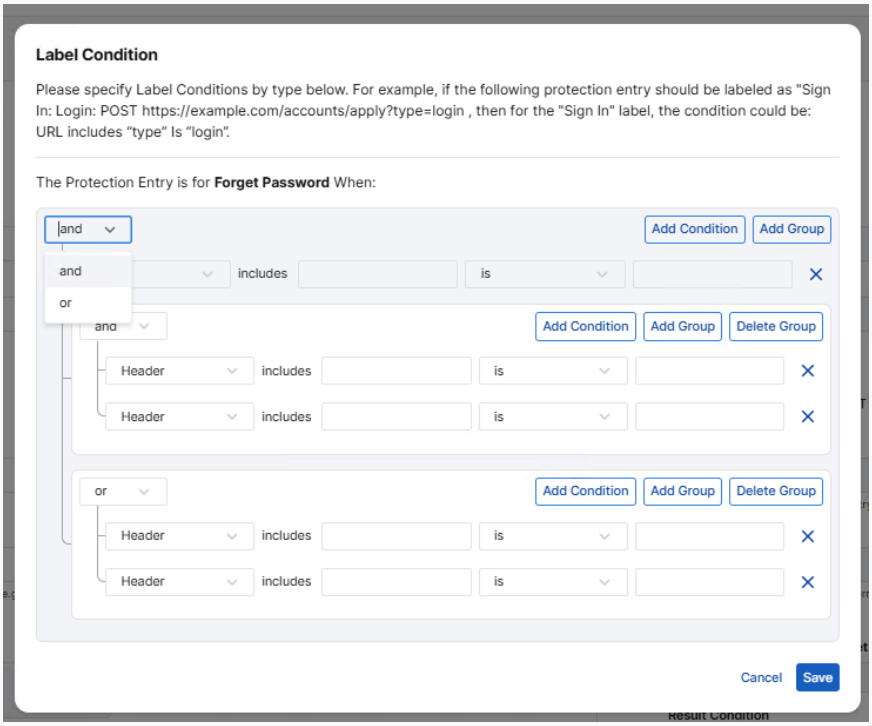
3. Review the detected inputs and choose whether to include them in your ABP configuration.

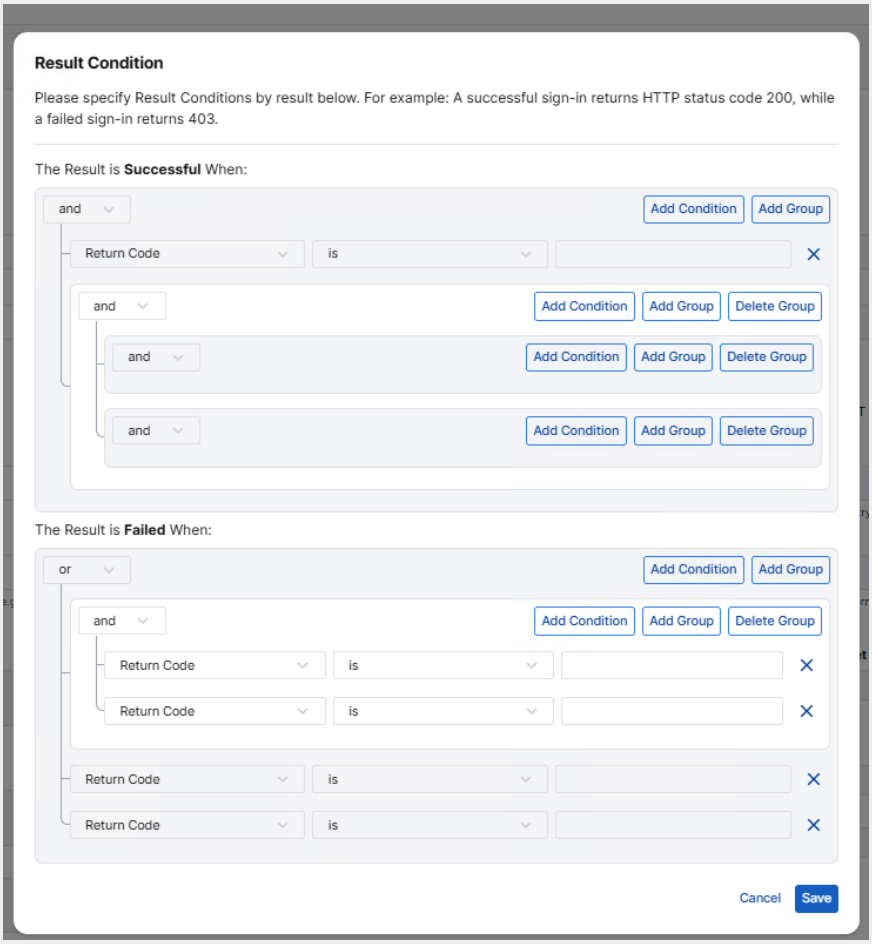


Setting	Description
Domain Name	The domain of the relevant application.

Setting	Description
Path	The path that indicates the page being protected on the relevant application.
HTTP Method	The HTTP Method to be protected in this protection entry. • GET – Retrieve data (e.g., loading a page) • POST – Submit data (e.g., login, form submission) • PUT / PATCH – Update resources • DELETE – Remove resources
Label	Select a label in the dropdown menu to indicate the primary function of the page. • Sign In • Sign Up • Search • Forget Password • Browsing
Username Field	Specify the field used for the username in the API request.

Label Condition	Click **Edit** to specify the **Label Conditions** for the selected **Label** type.
	For example, if the following protection entry should be labeled as **Sign In**:
	`Login: POST https://.com/accounts/apply?type=login`
	then the condition for the Sign In label could be:
	`URL includes "type" = "login".`
	To add a new condition, click Add Condition. To create a subgroup of related conditions, click **Add Group**.
	Define how the conditions within a group are evaluated by selecting a logical operator:
	• **and**: All conditions in the group must be met.
	• **or**: At least one condition in the group must be met.

Setting	Description
	
Result Condition	Define the conditions for both successful and failed actions. For example, if **Sign In** is selected as the **Label**, the **Result Condition** specifies what indicates a successful or failed sign-in.

Setting	Description
	 To add a new condition, click **Add Condition**. To create a subgroup of related conditions, click **Add Group**. Define how the conditions within a group are evaluated by selecting a logical operator: • **and**: All conditions in the group must be met. • **or**: At least one condition in the group must be met.

4. To apply the suggested protection entry, click **Save**.To discard it, click **Reject**. To keep it for review later, click **Cancel**.

Enable Block Mode

When **Block Mode** is enabled, Advanced Bot Protection blocks detected bot activity. Before you enable, review Block Mode Prerequisites on page 275. Enabling **Block Mode** too early may cause false positives, as rule adjustments are based on real-time traffic analysis.

Block Mode Prerequisites

Before enabling **Block Mode**, ensure you complete the following:

- If you are using a FortiWeb version earlier than 7.4.11, 7.6.6, or 8.0.2 and have CSP enabled, you may need to add the domain names shown in your browser's console error messages to the CSP configuration.

  Based on our experience, this typically applies to the following directives: default-src, script-src, script-src-elem, and connect-src.
  FortiWeb versions 7.4.11, 7.6.6, 8.0.2, and later do not experience this issue.

  If you are running an earlier version and cannot upgrade or find a suitable workaround, please submit a support ticket.
- Verify JavaScript Insertion

  Our JavaScript is designed to run safely without impacting your website. If you encounter any issues, please contact the support team.
- Review Traffic Insights

  If your server IPs or partner IPs are blocked, add them to your allowlist. For instructions on how to do this, please refer to the following:
  - FortiAppSec Cloud WAF: IP protection
  - FortiWeb: IP List - Blocklisting & whitelisting clients using a source IP or source IP range
  - FortiADC： Using the Geo IP allowlist
- If legitimate bots are blocked, enable **Known Bots**. For instructions on how to do this, please refer to the following:
  - FortiAppSec Cloud WAF: Known Bots
  - FortiWeb: Configuring known bots
  - FortiADC: Configuring a Bot Detection policy

Specify the web application to which you want to apply FortiAppSec Cloud Advanced Bot Protection (ABP) services. When you create an application, an **Application ID** will automatically be assigned to your application which can then be used to bind it to the Advanced Bot Protection policy in a connector device.

Integrate ABP on an on-premises device

After your Advanced Bot Protection Application has been created, you can integrate it with Fortinet Fabric devices to deploy Advanced Bot Protection for the Application traffic.

The FortiAppSec Cloud system is designed to seamlessly integrate with your existing infrastructure, supporting various products in the Fortinet Security Fabric.

Currently, the following Fortinet products are supported for integration:

- FortiADC — See FortiADC Integration on page 277 for detailed steps on how to set up the ABP integration with FortiADC.
- FortiWeb — See FortiWeb Integration on page 281 for detailed steps on how to set up the ABP integration with FortiWeb.

The ABP integration with FortiADC/FortiWeb works by using client information collected by JavaScript insertion, which allow the client and FortiADC/FortiWeb (via Fabric connector) to communicate with the Advanced Bot Protection Cloud for data telemetry information (such as headers and device fingerprinting). Once the FortiADC/FortiWeb is connected with ABP, an Advanced Bot Protection policy can be configured to apply to the server policy. The FortiADC/FortiWeb reports the telemetry data to ABP which then inspects the HTTP/S request to determine if the client is a human or a bot, and sends instructions back to FortiADC/FortiWeb to initiate an action against the request (such as block, CAPTCHA, or allow).

Before you begin:

- You must have access to the Fortinet connector device and have read-write permission for security settings.
- Ensure the account used to register for the ABP license matches the account information from your Fortinet Support Contract. Otherwise, the connector device will not be able to connect to ABP.
- You must have created a ABP Application and have obtained its Application ID.

FortiADC Integration

Login to FortiADC and follow the steps below to integrate ABP with FortiADC.
For more details about the ABP integration with FortiADC, see the FortiADC Handbook on Advanced Bot Protection.

1. **Enable the Advanced Bot Protection Fabric Connector**

   FortiADC is pre-configured to connect to the ABP server, so you only need to enable the connection via the Advanced Bot Protection Fabric connector.

   a. Go to **Security Fabric > Fabric Connectors**.
   b. Under **Other Fortinet Products** section, locate the **Advanced Bot Protection** connector.
   c. **Enable** the Advanced Bot Protection connector. Once the connector is enabled, the connection status will display.
   The Advanced Bot Protection connector is ready when the status is **Connected**.



   d. The and icons indicate whether the Advanced Bot Protection connector has successfully connected to the ABP server. Hover over the Advanced Bot Protection connector to see the status details. The table below lists the possible connection statuses for the Advanced Bot Protection connector.

Icon	ABP connector status	Guidelines
	Connected	The [[[Undefined variable Deployment Guide.ProductName]]] is successfully connected to to the ABP server.
	Account license invalid	The ABP license is not valid. Please verify your license details or contact Fortinet Support.
	Couldn't connect to server	Unable to connect to the ABP server. Please check your network settings.
	Couldn't resolve hostname	Unable to resolve the hostname of the ABP server. Please check your network settings.
	No available SN cert	The device does not have an available SN certificate. Please check your local certificate.

Icon	ABP connector status	Guidelines
	No available CA cert	The device does not have an available CA certificate. Please check your CA certificate.
	Problem with the local certificate	An error occurred with the remote server certificate. Please check your local certificate.
	SSL peer certificate or SSH remote key was not OK	An error occurred with the remote server certificate involving the SSL peer certificate or SSH remote key. Please check your local certificate.

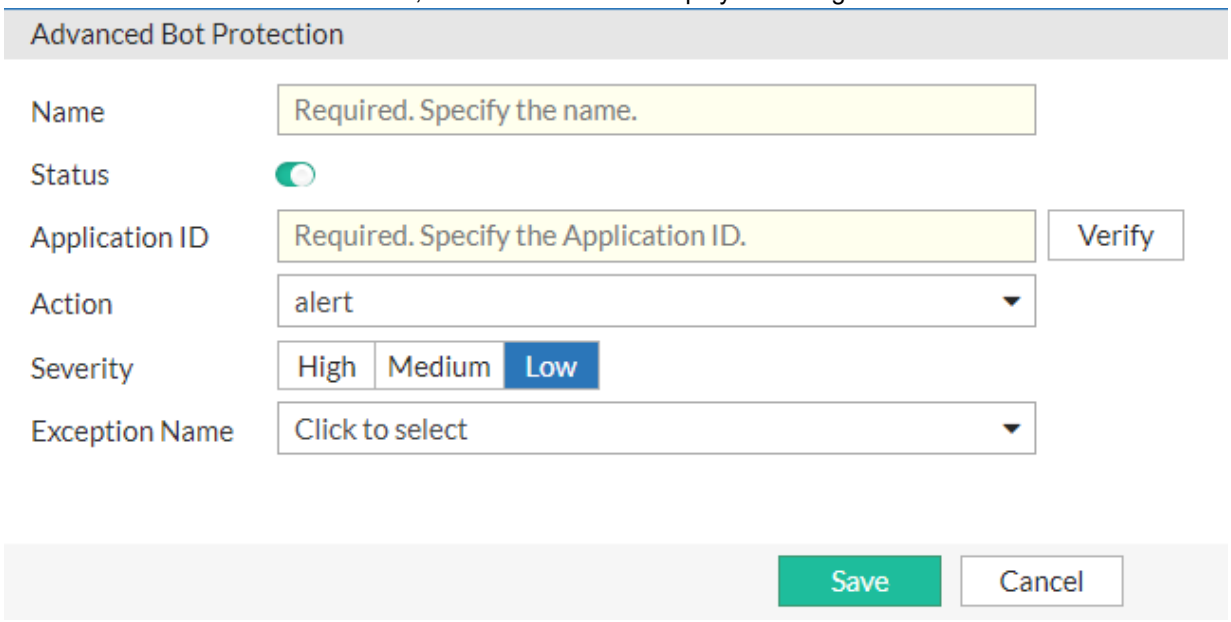
Once the Advanced Bot Protection fabric connector is successfully connected, the Advanced Bot Protection module becomes available under the Web Application Firewall menu in the GUI.

2. **Configure an Advanced Bot Protection policy**

Connect your ABP Application to the FortiADC Advanced Bot Protection policy by using the Application ID. Through the Application ID, the FortiADC will have access to the Pre-Provisioned resources to apply to the specified protected URLs and JavaScript insertion locations to collect client information for bot detection.

a. Go to **Web Application Firewall > Advanced Bot Protection**.

b. In the **Advanced Bot Protection** tab, click **Create New** to display the configuration editor.

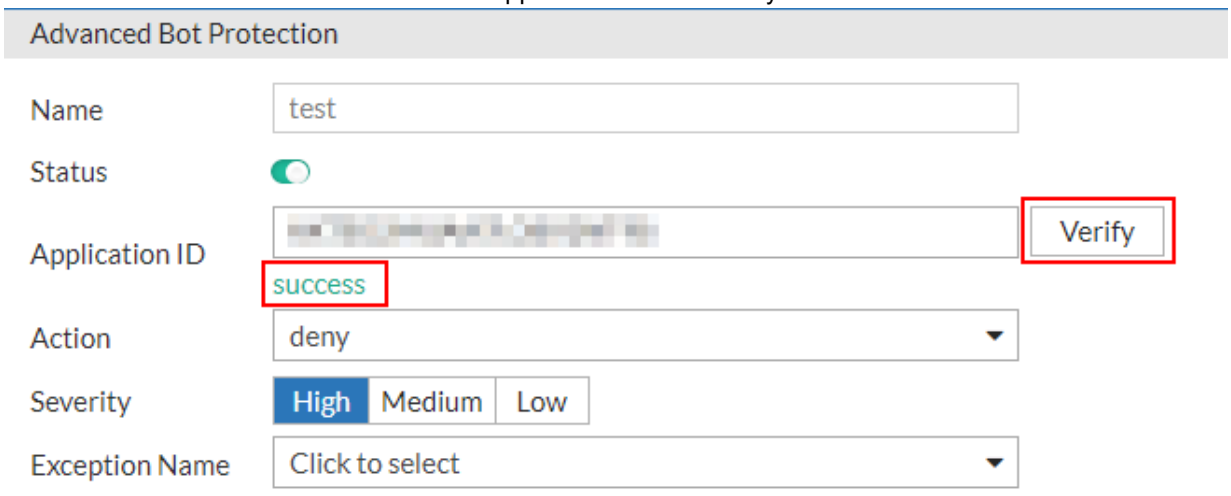


c. Configure the following Advanced Bot Protection settings:

Setting	Description
Name	Specify a name for the Advanced Bot Protection policy. Valid characters are `A-Z`, `a-z`, `0-9`, `_`, and `-`. No spaces. The configuration name cannot be edited once it has been saved.
Status	Enable/disable the status of this Advanced Bot Protection policy. **Status** must be **enabled** to display Advanced Bot Protection configuration options.

Setting	Description
Application ID	Specify the Application ID assigned to your ABP Application. The Application ID is used to bind this Advanced Bot Protection policy to the ABP Application. To obtain the ID, go to **Application** page of ABP, locate your ABP Application, click under **Action**, then click **Copy Application ID**.
Action	Specify a WAF action object to apply when a bot is detected. You can specify a predefined or user-defined WAF action profile. Predefined WAF actions: • alert — WAF policies will allow the traffic to pass and log the event. • block — WAF policies will drop the current attack session by HTTP 403 message and block the attacker (according the attacker's IP address) for 1 hour, and log the event. • captcha — WAF policies will allow the traffic to pass if the client successfully fulfills the CAPTCHA request, and log the event. • deny — WAF policies will the drop current attack session by HTTP 403 message, and log the event. • silent-deny — WAF policies will drop the current attack session by HTTP 403 message, without logging the event. The default action is alert.
Severity	Select the event severity to log when a bot is detected: • High — Log as high severity events. • Medium — Log as a medium severity events. • Low — Log as low severity events. The default is Low.
Exception Name	Select an exception configuration object. Exceptions identify specific hosts or URL patterns that are not subject to processing by this rule.

d. Optionally, click **Verify** to validate the inputted Application ID against multiple parameters to ensure the connection between FortiADC and the ABP Application is successfully established.



The Advanced Bot Protection policy can only function if the Application ID is valid and the connection to the

ABP server is successfully established. FortiADC validates multiple parameters, including if the Application ID is available, the ABP server connectivity, if the ABP license is valid. There are two types of messages as differentiated by text color: green text indicates a positive status where all required parameters are validated successfully; and red text that indicate one or more parameters did not pass validation.
The following table describes some common verification results.

Verification status message	Guidelines
Success (green)	All required parameters pass validation; application ID is available, ABP server certificate is valid, network connectivity is good, etc.
Application not found (red)	The Application ID does not exist. This could be an input error.
Account license invalid (red)	The ABP license is not valid. Please verify your license details or contact Fortinet Support.
Couldn't connect to server (red)	Unable to connect to the ABP server. Please check your network settings.
Couldn't resolve hostname (red)	Unable to resolve the hostname of the ABP server. Please check your network settings.
No available SN cert (red)	The device does not have an available SN certificate. Please check your local certificate.
No available CA cert (red)	The device does not have an available CA certificate. Please check your CA certificate.
Problem with the local certificate	An error occurred with the remote server certificate. Please check your local certificate.
SSL peer certificate or SSH remote key was not OK	An error occurred with the remote server certificate involving the SSL peer certificate or SSH remote key. Please check your local certificate.

e. Click **Save**.
Once the Advanced Bot Protection policy is saved, you can reference it in a WAF Profile configuration.



It is strongly recommended to verify the Application ID and ABP server connection prior to completing the Advanced Bot Protection policy configuration. Even though this is an optional step, it is helpful to diagnose any potential issues and apply fixes early.

When the Advanced Bot Protection policy is created, an internal verification is automatically conducted to verify the status of the Application ID and ABP server connection. If the Application ID is not valid, or any other validation parameters has failed, the Advanced Bot Protection policy will fail to function and the system will log the failure to send the ABP policy.

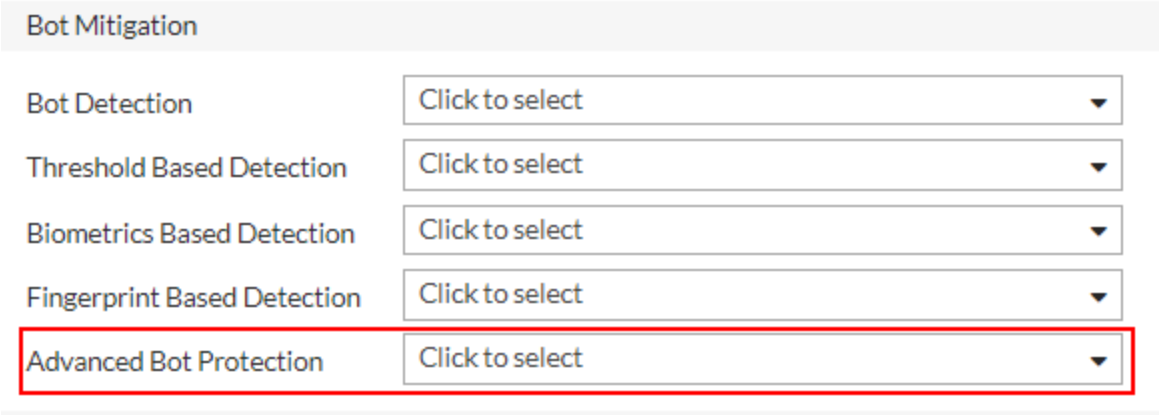
3. Apply the Advanced Bot Protection policy in a WAF profile and virtual server policy

After configuring the Advanced Bot Protection policy, apply it in a WAF profile. Then, apply the WAF profile that references the Advanced Bot Protection policy to a virtual server to activate Advanced Bot Protection for server load balancing.

a. Go to **Web Application Firewall > WAF Profile**.
The configuration page displays the **WAF Profile** tab.

b. Edit an existing WAF Profile configuration, or click **Create New** to create a new WAF Profile to apply the Advanced Bot Protection policy.

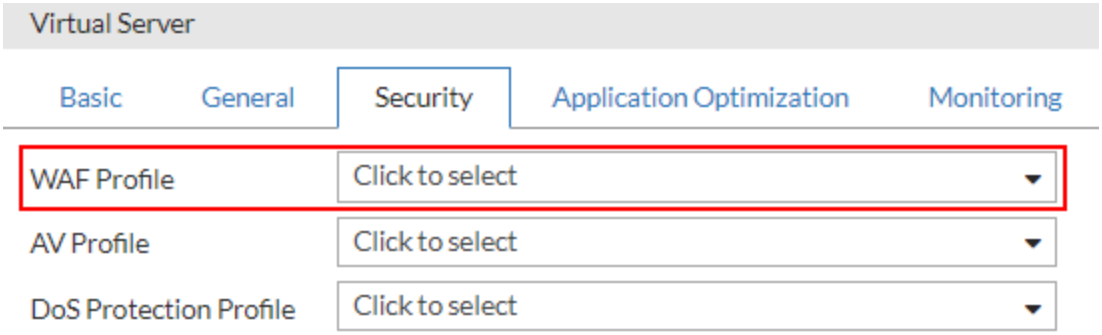
c. Under the Bot Mitigation section, select the Advanced Bot Protection policy you have previously configured and click **Save** to commit.



d. Go to **Server Load Balance > Virtual Server**.
The configuration page displays the **Virtual Server** tab.

e. Edit an existing Virtual Server configuration or click Create New > Advanced to create a new virtual server configuration to apply the WAF profile that references the Advanced Bot Protection policy.

f. Click the **Security** tab and select the WAF Profile configuration that references the Advanced Bot Protection policy. Click **Save** to commit.



Once the Advanced Bot Protection Policy is applied to the WAF Profile and referenced in a virtual server, whenever HTTP/S requests are made on the protected Application, FortiADC will report to ABP the telemetry data collected from the client via JavaScript insertion. Each HTTP/S request is inspected and ABP will determine if the client is a human or a bot and will send instructions back to FortiADC to initiate an action against the request (such as block, CAPTCHA, or allow). FortiADC will log eac h security action triggered by the Advanced Bot Protection.



The FortiADC Advanced Bot Protection policy activates once onboarding is complete.

FortiWeb Integration

Login to FortiWeb and follow the steps below to integrate ABP with FortiWeb.
For more details about the ABP integration with FortiWeb, see the FortiWeb Handbook on Advanced Bot Protection.

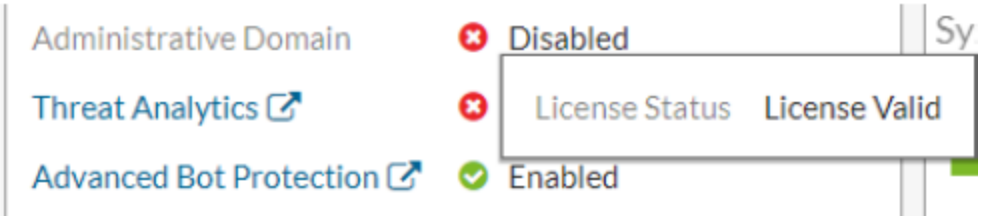
1. **Enable Advanced Bot Protection**

   FortiWeb is pre-configured to connect to the ABP server, so you only need to enable the connection via the Advanced Bot Protection Fabric connector.

   a. Go to **Dashboard > Status**.

   b. In the **System Information** widget, click **Enable Advanced Bot Protection**, then click **OK** in the pop-up window.

   c. Check the status of **Advanced Bot Protection** in the **Licenses** widget on the **Dashboard > Status** page. It should display as **Valid**.



2. **Configure an Advanced Bot Protection policy**

   Connect your ABP Application to the FortiWeb Advanced Bot Protection policy by using the Application ID. Through the Application ID, FortiWeb will receive bot detection suggestions from ABP regarding the traffic of this application, and then take corresponding actions.

   a. Go to **Bot Mitigation > Advanced Bot Protection**.

   b. Click **Create New** to display the configuration editor.

   c. Configure the following Advanced Bot Protection settings:

Setting	Description
Name	Enter a name for the Advanced Bot Protection policy. You can reference it in the Web Protection Profile.
Application ID	Enter the Application ID assigned to your ABP Application. The Application ID is used to bind this Advanced Bot Protection policy to the ABP Application. To obtain the ID, go to **Application** page of ABP, locate your ABP Application, click under **Action**, then click **Copy Application ID**.
Action	Select which action FortiWeb will take when ABP suggests the request is from a bot: • Alert — Accept the connection 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). • Block Period — Block subsequent requests from the same IP address for a number of seconds. • Client ID Block Period — Block a malicious or suspicious client based on the FortiWeb generated client ID. This is useful when the source IP of a certain client keeps changing. This option takes effect only when you enable Client Management in the Server Policy. The default value is Alert.

Setting	Description
Period Block	Enter the number of seconds that you want to block subsequent requests from a client. The valid range is 1–3,600 seconds (1 hour). This setting is available only if **Action** is set to **Period Block** and **Client ID Block Period**.
Severity	When request from a bot is recorded in the attack log, each log message contains a **Severity Level** (`severity_level`) field. Select which severity level FortiWeb will use: • Informative • Low • Medium • High The default value is **Medium**.
Trigger Policy	Select the trigger, if any, that FortiWeb will use when it logs and/or sends an alert email about ABP violation.
Exception	Select the exception policy which specifies the elements to be exempted from the ABP scan.
Bot confirmation	Enable it to send clients bot verification requests.
Verification Method	• CAPTCHA Enforcement — Requires the client to successfully fulfill a CAPTCHA request. CAPTCHA verification will not pop out for the bot confirmation again for the same user within 10 mins timeout. • reCAPTCHA Enforcement — Requires the client to successfully fulfill a reCAPTCHA request.
reCAPTCHA	Select the reCAPTCHA server you have created in the reCAPTCHA Server tab in **User > Remote Server**.
Validation Timeout	Enter the maximum amount of time (in seconds) that FortiWeb waits for results from the client.
Max Attempt Times	If **CAPTCHA Enforcement** is selected for **Verification Method**, enter the maximum number of attempts that a client may attempt to fulfill a CAPTCHA request. Available only when the **Verification Method** is **CAPTCHA Enforcement**.

d. Click **OK**.

3. **Apply the Advanced Bot Protection policy in a Web Protection Profile**

   After configuring the Advanced Bot Protection policy, apply it in a Web Protection Profile to activate Advanced Bot Protection.

   a. Go to **Policy > Web Protection Profile**.

   b. Select the **Inline Protection Profile** tab.

   c. Select an existing web protection profile to which you want to include the Advanced Bot Protection policy.

   d. Click **Edit**.

   e. For **Bot Mitigation > Advanced Bot Protection**, select the Advanced Bot Protection policy from the drop-down list.

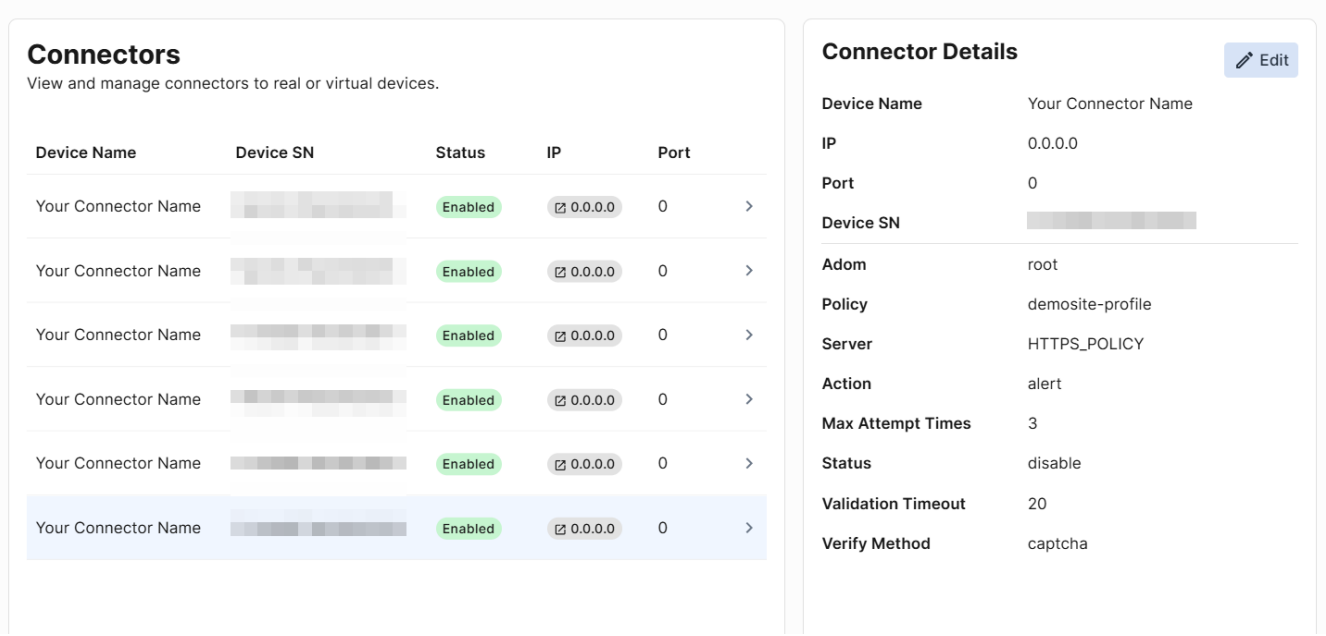
Note: To view details about a selected Advanced Bot Protection policy, click the view icon next to the drop-down list.

f. Click **OK**.

The FortiWeb Advanced Bot Protection policy activates once onboarding is complete.

After Integration

After connecting your ABP Application to FortiWeb or FortiADC, you can manage its connectors under **General> Connectors**.



For more information about the details displayed on this page, refer to Connectors on page 311.

To access this page, navigate to **ABP > Application** and click the **Application Name**。

ABP Application

On the Application page, you can set up and manage settings for your Advanced Bot Protection (ABP) applications. This involves tasks like adding new applications, checking application details, changing the application's name, and setting up login protection.

Click into each application to view its traffic insights and configurations.

For onboarding information, please refer to ABP Setup on page 264.

Application Information

The table on the **Application** page displays all the applications currently under your FortiAppSec Cloud account.

Column	Description
Name	The internal name by which this application is displayed within the web portal GUI. Click on the **Name** to access Traffic Insights on page 290 and General on page 307 modules.
Domain Name	The domain name of your application. For example, www.fortinet.com. This field cannot be edited.
Region	The region of the ABP service that processes the traffic of your application

Auto Discovery Status	The Auto Discovery Status indicates the current stage of the protection entry discovery process.
	• **In Progress**: Auto Discovery is still analyzing your application. No urgent action required.
	• **Review Needed**: Auto Discovery has suggested new protection entries. Please review and confirm the changes.
	• **Connection Issue**: Advanced Bot Protection could not connect to the entry points you provided. Potential causes for this include:
	  • The application's firewall is blocking ABP's management IPs. Add these IPs to your allowlist to prevent requests from being blocked.
	  • FortiAppSec Cloud WAF: IP protection
	  • FortiWeb: IP List - Blocklisting & whitelisting clients using a source IP or source IP range
	  • FortiADC: Using the Geo IP allowlist
	  • There is an error in the entry point URL.
	To edit the entry point URL:
	i. From **Advanced Bot Protection > Applications**, click the three dots under **Action** .
	ii. Click **Edit Application**.
	iii. Go to the **Entry Points** tab, and edit the Entry Point text input field

Application Status	This field displays the protection status of the application. • **Onboarding**: The application has been created, and is now being analyzed. The duration of this process depends on the application's complexity, as well as the number of entry points and protection categories selected. • **Integration Required**: Advanced Bot Protection has not detected any attack queries targeting your protected entries from any connected WAF, FortiWeb, or FortiADC device. Possible reasons include:

Column	Description
	• On-Premises integration has not been configured. Refer to the FortiWeb integration and FortiADC integration guides for detailed setup instructions. • DNS records are not routed to your FortiAppSec Cloud WAF application or On-Premises device. Refer to changing DNS records on AWS Route 53 for an example configuration. • **Rule Adjustment**: ABP tunes protection rules for two weeks based on real traffic to your application. During this time, please do not enable **Block Mode**. • **Protected**: The application's traffic is monitored and protected by ABP.
Action	Click to expand the available actions to be taken on the protection entry. • **Copy Application ID**: Securely copy the Application ID to your clipboard. The Application ID is not displayed for security reasons, and is used to enable integration with FortiADC and FortiWeb. • **Run AutoDiscovery**: Initiates the Auto Discovery process to analyze the entry points defined in this application. This process typically takes several hours to complete. • **Edit Application** • **Delete Application**

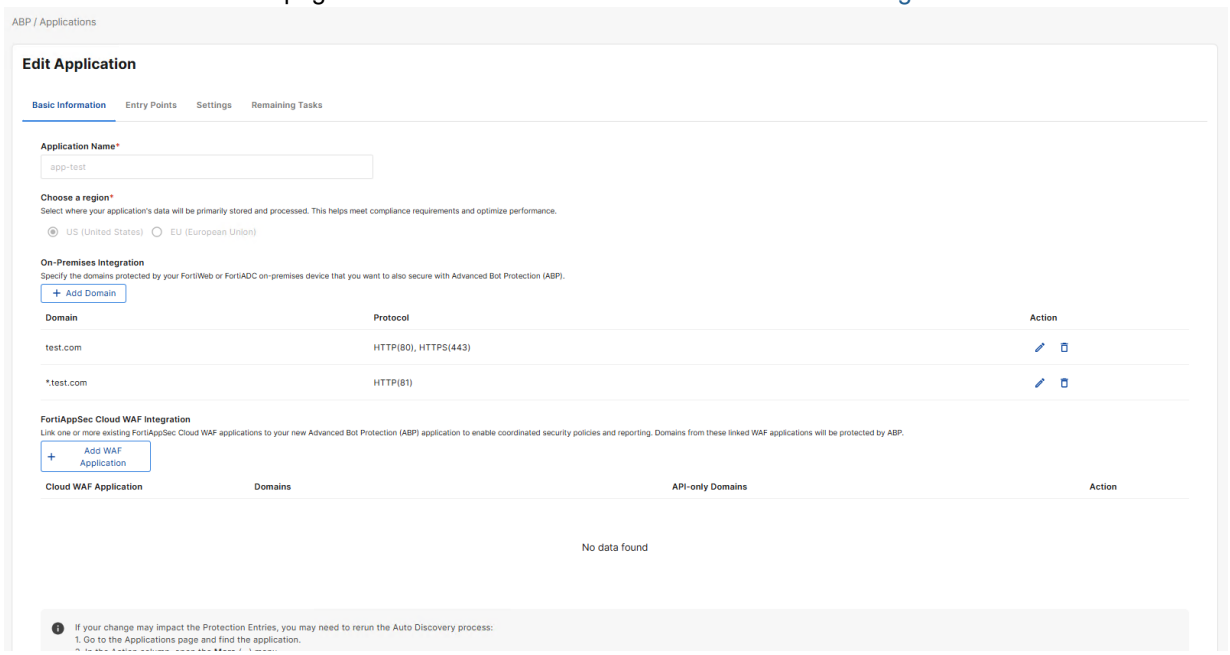
Edit Application

1. Find the row containing the preferred application name.
2. Click the **Edit** icon to open the **Edit Application** wizard.

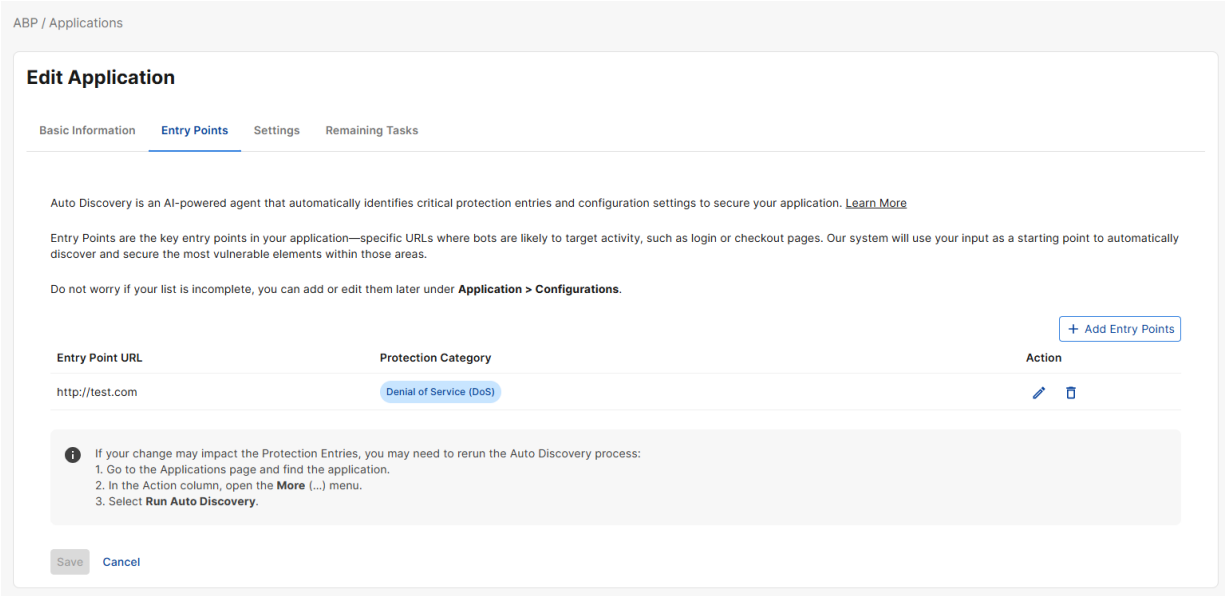


Changes to domain names or entry points require manually re-running **Auto Discovery** or adding a protection entry. Editing the application alone does not fully update the configuration.

a. **Basic Information**: This page contains the same fields as those in the onboarding wizard.

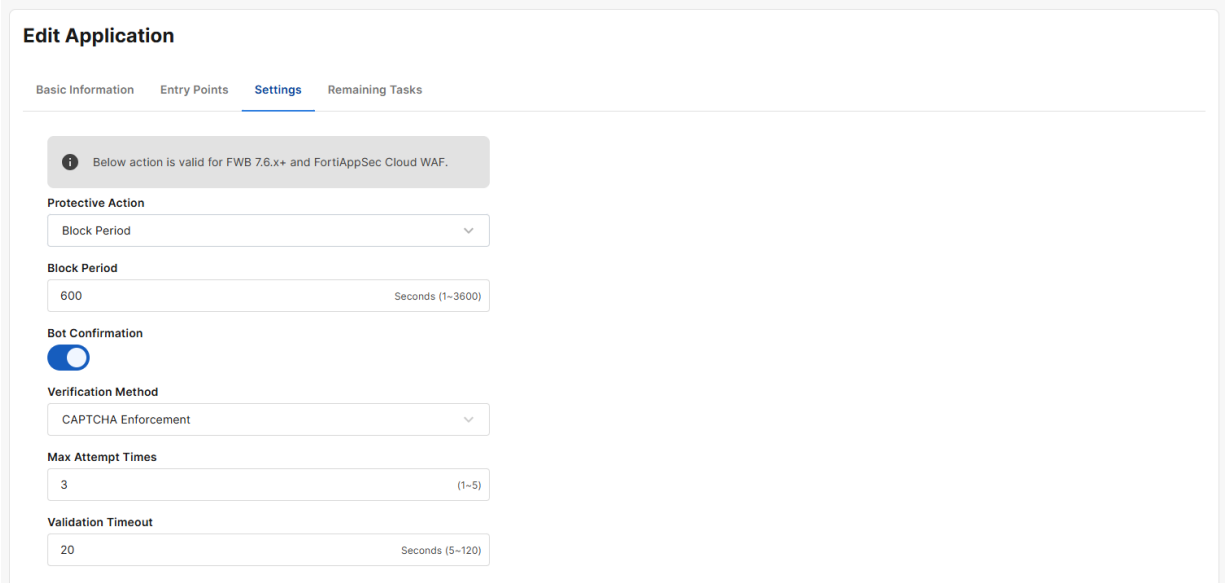


b. **Entry Points**: This page contains the same fields as those in the onboarding wizard.



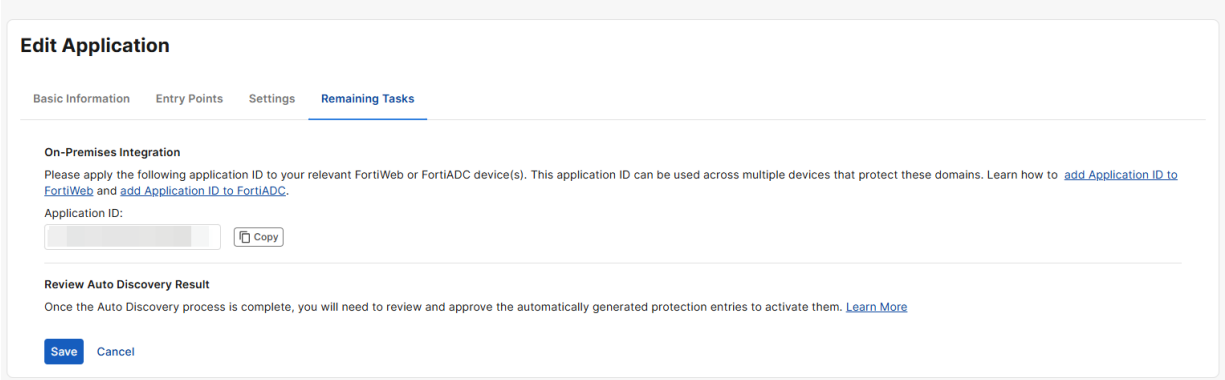
c. **Settings**: this page includes configuration options for protective action and bot confirmation.

Please note, the settings on this page apply to applications integrated with FortiWeb 7.4.12+, 7.6.6+, 8.0.3+, and FortiAppSec Cloud WAF.



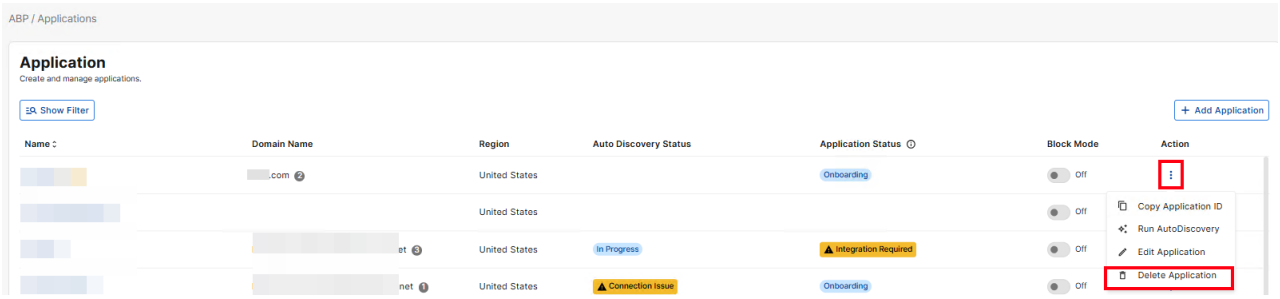
Setting	Description
Protective Action	Select the action ABP takes when bot activity is detected. • **Alert**: Record the invalid request in the attack log. • **Alert and Deny**: Block the invalid request and send a "block page" back to the browser, as well as record the request in the attack log. • **Deny (no log)**: Block the invalid request and send a "block page" back to the browser, without recording the request in the attack log. • **Block Period**: Block the current request and all subsequent requests from the same client for the configured duration. When this option is selected, you must also enter the **Block Period** in seconds.
Bot Confirmation	When enabled, the system displays a verification challenge to distinguish between human users and automated bots. • **Verification Method**: Currently, only **CAPTCHA Enforcement** is supported. • **Max Attempt Times**: Number of verification attempts allowed before the **Protective Action** is triggered. • **Validation Timeout**: The amount of time allowed for a user or client to complete the verification before the **Protective Action** is triggered.

d. **Remaining Tasks**: This page lists the outstanding actions that must be completed before your application can be fully connected and protected.



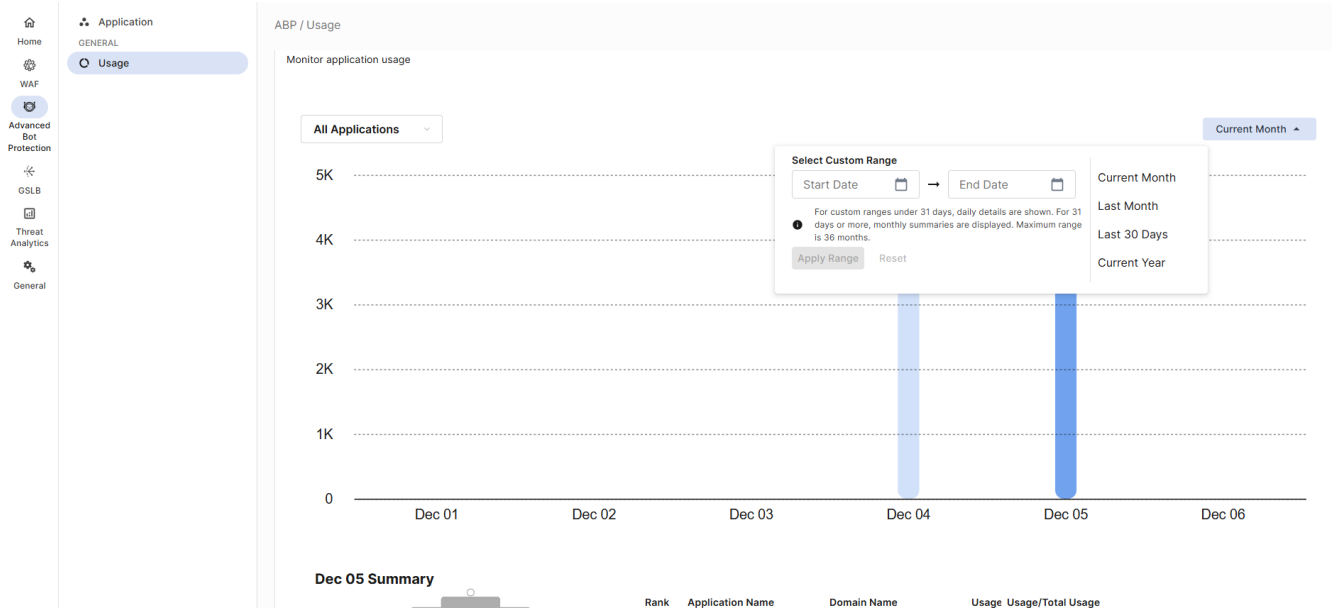
Delete Application

1. Find the row containing the preferred application name.
2. Click **Delete Application**.



Usage

Select one or all applications and date range to view its usage details on the **Usage** tab.



This page includes the following components:

- A bar graph showing the month-over-month number of requests protected by Advanced Bot Protection for the selected application(s) over the chosen time period.
  - Hover over a bar to see the number of protected requests for the selected month.
  - Click on a bar to change the other components on this page to reflect the data in the selected month.
- **Total Usage**: the total number of protected requests for the selected application(s) within a pie chart showing the total usage for the month compared to the total capacity purchased in the contract.
  - Click **View Details** to see the request usage breakdown between each license for the selected month.
- A ranked table displaying the percentage of selected application(s) usage compared to the total usage for the month.

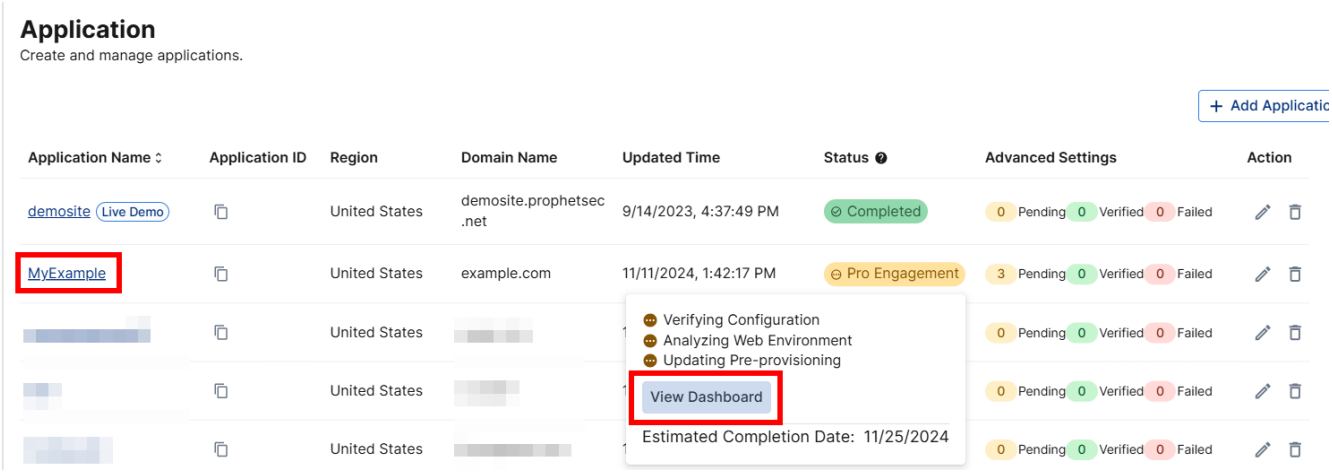
Traffic Insights

Traffic Insights is composed of different pages dedicated to helping you monitor the traffic activity on each application effectively.

This section covers the following:

- Dashboard on page 291
- Transactions on page 295
- Account Monitor on page 300
- Bot Monitor on page 302
- Exploration on page 305

To access these pages, go to **ABP > Application** and click on the desired **Application Name**, or click on the desired application's **Status** and click **View Dashboard**.

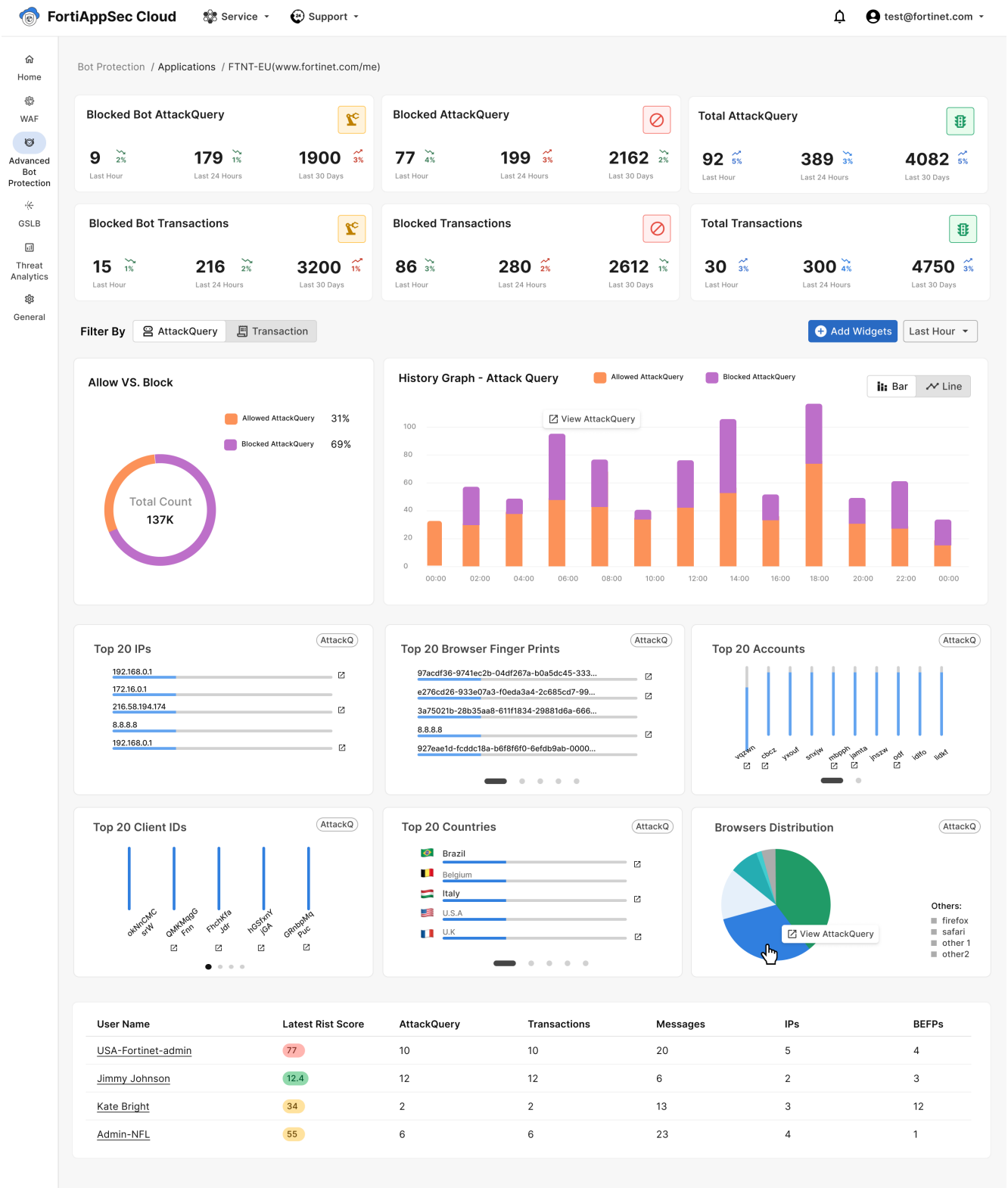


Dashboard

Extract valuable insights using tables and summary graphs that depict your application's traffic data.

Static Components

These components are fixed to your dashboard and cannot be edited or removed.

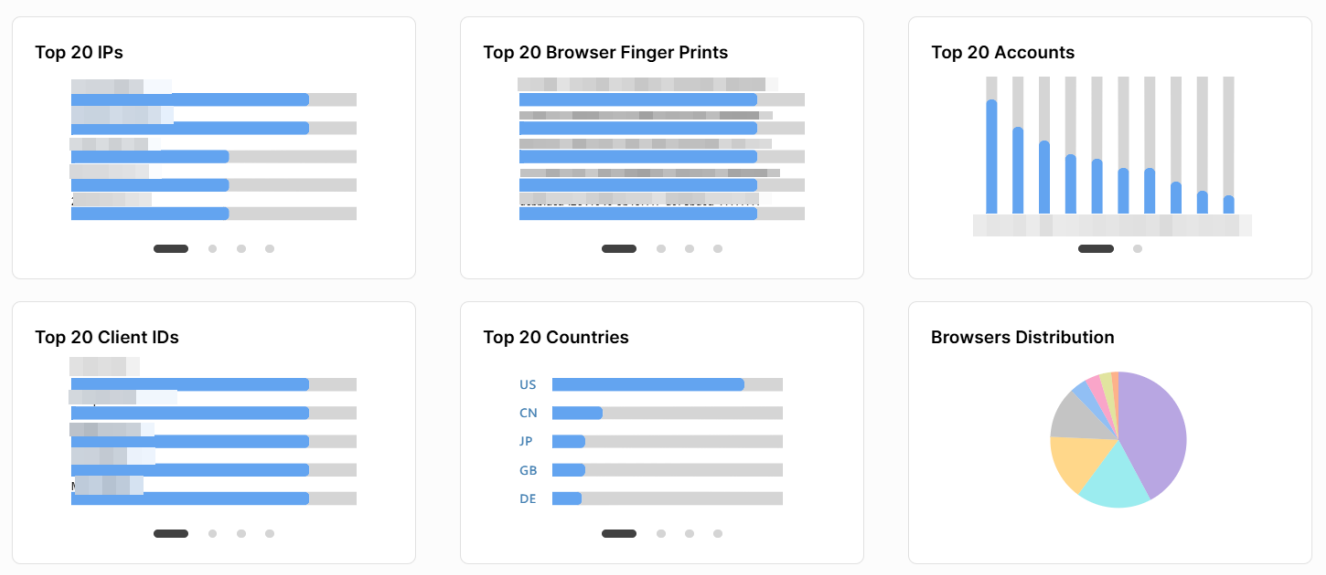


User Name	Latest Rist Score	AttackQuery	Transactions	Messages	IPs	BEFPs
USA-Fortinet-admin	77	10	10	20	5	4
Jimmy Johnson	12.4	12	12	6	2	3
Kate Bright	34	2	2	13	3	12
Admin-NFL	55	6	6	23	4	1

Static Component	Description
AttackQuery Count	The count of Blocked Bot AttackQueries, Blocked AttackQueries, and Total AttackQueries over the past hour, 24 hours, and 30 days. • **Total AttackQuery:** The number of queries exchanged between the ABP device and a FortiADC/FortiWeb device regarding user activity on the protected application. • **Blocked AttackQuery:** The number of times ABP suggested FortiADC/ FortiWeb/ WAF to block the action detailed in the AttackQuery. • **Blocked Bot AttackQuery:** The number of times ABP suggested FortiADC/ FortiWeb/ WAF to block the action detailed in the AttackQuery, due to detected malicious bot behavior.
Transactions Count	The count of Blocked Bot Transactions, Blocked Transactions, and Total Transactions over the past hour, 24 hours, and 30 days. • **Total Transactions:** Count of actions performed by users within your application, including logging in, completing payments, periods of inactivity, browsing behavior, and closing the browser. These activities may be initiated by either humans or bots, and characteristics of the transaction can aid in distinguishing between human and bot interactions. • **Blocked Transactions:** Transactions blocked by ABP • **Blocked Bot Transactions:** Transactions blocked by ABP due to bot activity. For more details, see Transactions on page 295
Allow VS Block	Displays the proportion of suggested action = Allow versus suggested action= block, within all AttackQueries or Transaction. Choose whether you want to see this display for attack queries or transactions. Use this pie chart to gain insight on the proportion of malicious bot traffic to benign human or bot traffic.
History bar graph	Click on the **Filter By** button to choose the data displayed in the graph. • **Transactions History:** Shows the number of regular and blocked transactions over the given time frame. • **AttackQuery History:** Shows the number of regular and blocked attack queries over the given time frame. Adjust the time range displayed on the graph by clicking the buttons labeled "last hour," "last 24 hours," and "last 30 days" above the chart.
Top Account List Under Threat	List displaying users of your applications ranked from the highest risk score to the lowest. Click on the username to access the account monitoring page for each user.

Widgets

Customize your dashboard by using widgets to display more information. Widgets present the chosen data in either bar or pie charts and when selected, are positioned between **Transactions History Graph** and **Top Account List Under Threat**. Hover your cursor over the charts to view the count associated with each bar or pie slice.



How to add widgets to your dashboard

1. Navigate to **TRAFFIC INSIGHTS > Dashboard**
2. Click the **Widgets** button located above the Transactions History Graph. This opens a drop-down menu.
3. Select the widget option(s) you would like displayed on your dashboard.

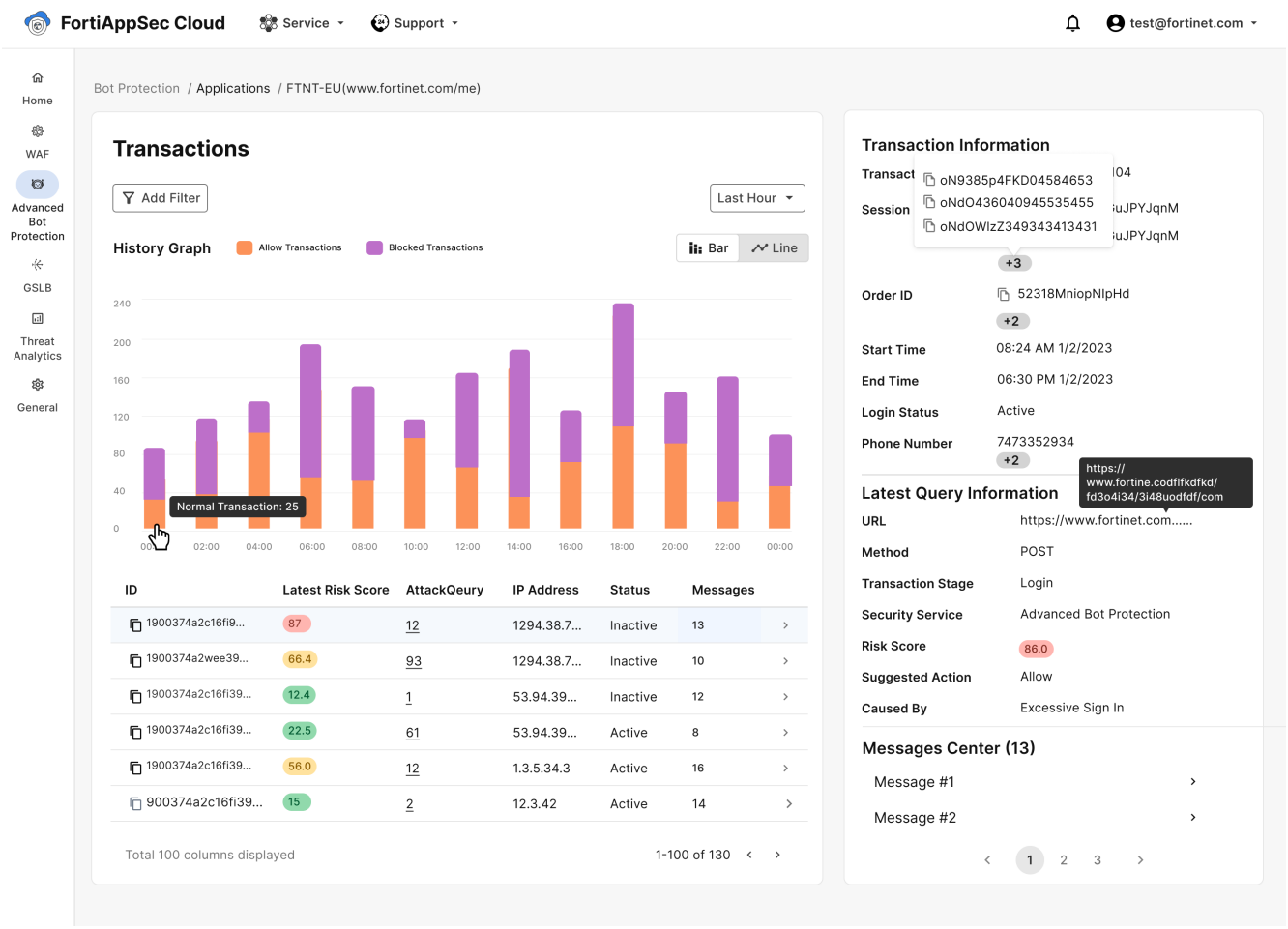
Widget name	Widget description
Top 20 IPs	20 IPs with the highest transaction counts.
Top 20 Browser Fingerprints	20 browser profiles with the highest transaction counts. Browser fingerprints identify repeat visitors to your website by cross-referencing various browser/device attributes. This includes crawler-specific attributes and browser/OS inconsistencies.
Top 20 Accounts	Usernames of 20 accounts with the highest transaction counts.
Top 20 Client ID	20 client IDs with the highest transaction counts. A client ID is a unique identifier for a user's web browser, generated from its configuration, including environment signals and HTTP transport layer information.
Top 20 Countries	20 countries with the highest transaction counts.
Browsers Distribution	Pie chart displaying the distribution of different browsers accessing your application. Hover over each pie slice to see the represented browser, along with the corresponding count (eg., Chrome: 58).
Top 20 UAs	20 user agents with the highest transaction counts.
OS Distribution	Pie chart illustrating the distribution of operating systems among devices accessing your application. Hover over each pie slice to see the represented operating system, along with the corresponding

Widget name	Widget description
	transaction count (e.g., Windows: 84).
Device Distribution	Pie chart illustrating the distribution of devices accessing your application. Hover over each pie slice to see the represented device type, along with the corresponding transaction count (e.g., Mac: 32).
Top 20 ASN	20 Autonomous System Numbers with the highest transaction counts.
Attacks Distribution	Pie chart illustrating the distribution of attacks on your application, as detected by FortiAppSec Cloud. Hover over each pie slice to see the represented attack type, along with the corresponding count (eg., Access from bad client: 2).
Top 20 Cities	20 cities with the highest transaction counts.
Top 20 Emails	The top 20 email addresses linked to the highest transaction counts.
Top 20 Phone Numbers	The top 20 phone numbers linked to the highest transaction counts.
Top 20 URLs	20 URLs on your application with the highest transaction counts.

Transactions

Transactions encompass all user activities within your application, such as login, payment outcomes, idle periods exceeding a specified duration, browsing, and browser closure.

The following attributes are displayed in **TRAFFIC INSIGHTS > Transactions**:



Attribute	Description
Transaction ID	Each transaction is assigned a unique, randomly generated ID. You can click on the Transaction ID in the table to open a modal window with more details on the selected transaction. See Transaction Information on page 297.
Latest Risk Score	Risk scores can range from 0-100. Higher scores indicate more bot-like behavior, while lower scores suggest human-like activity. For more information on the factors that go into calculating the Risk Score, please see this page.
Start Time	The local date and time when the transaction begins.
End Time	The local date time when the transaction ends.
Login Status	Whether the transaction was performed by a logged-in user.
Session ID	The unique, randomly generated ID associated with the session in which the transaction took place. A session begins when a user begins accessing your application, and ends when the user closes the tab or browser.

Attribute	Description
Order ID	This value identifies payment-related transactions, and is empty for all non-payment transactions.
Messages	The number of telemetry messages transmitted in the transaction. You can click on this value in the table to open a modal window with more details on the selected transaction. See Transaction Information on page 297.

Click Show Filter to filter for Transaction ID, Session ID, Risk Score, OrderID, or Login Status.

You can also filter for transactions that took place in the last hour, last 24 hours, or last 30 days by clicking the corresponding buttons.

Transaction Information

Transaction Information opens as a modal window when you click on a **Transaction ID** or **Messages** value.

Under Transaction Information, you can find detailed information on the latest query and telemetry messages of the selected transaction.

- **Latest Query Information** details the final data request before the transaction ended, offering insights into the transaction's nature and potential completion or blockage causes.

Latest Query Attribute	Description
URL	The URL at which the latest query took place on your application's domain.
Method	The HTTP method behind the latest query.
Transaction Stage	Describes the stage at which the last query took place. This value may provide insight into the nature of the transaction.
Risk Score	Risk scores can range from 0-100. Higher scores indicate more bot-like behavior, while lower scores suggest human-like activity. For more information on the factors that go into calculating the Risk Score, please see Overview on page 255.
Security Service	This value is determined by the terms of your license.
Suggested Action	The response FortiAppSec Cloud recommends based on the risk score.
Caused by	A brief explanation behind **Suggested Action**.

- The numbered messages under **Message** can be expanded to reveal the following details on the telemetry messages sent in the selected transaction.

Message Attribute	Description
IP	The IP address from which the telemetry message was sent.

Message Attribute	Description
User Agent	A software component that identifies and provides information about the device or application sending the telemetry message.
Country	The message's detected country of origin.
City	The message's detected city of origin.
User Name	If the telemetry message was sent during a logged-in session, the username of the user is included in this field.
Email	If the telemetry message was sent during a logged-in session, the registered email of the user is included in this field.
Order ID	This value identifies payment-related transactions, and is empty for all non-payment transactions.
Payment ID	This value identifies payment-related transactions, and is empty for all non-payment transactions.
Session ID	This value identifies the session in which the message was sent.
URL	The URL on your application's domain at which the message was sent.

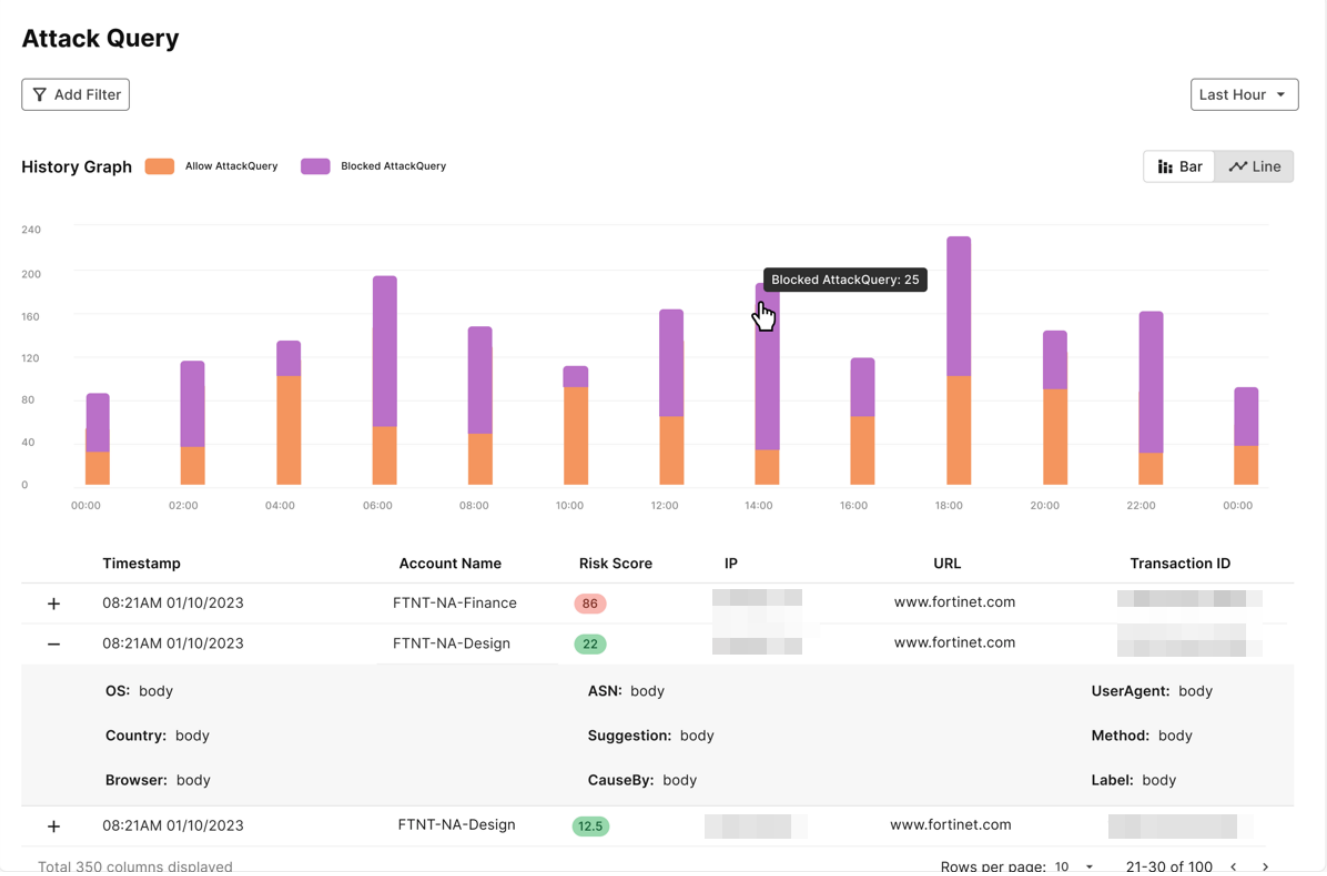
Attack Query

Attack Queries are exchanges between Advanced Bot Protection and WAF or a FortiADC/FortiWeb device, providing data on user activity within the protected application.

- **Blocked AttackQuery:** The number of times ABP suggested FortiADC/ FortiWeb/ WAF to block the action detailed in the AttackQuery.
- **Blocked Bot AttackQuery:** The number of times ABP suggested FortiADC/ FortiWeb/ WAF to block the action detailed in the AttackQuery, due to detected malicious bot behavior.

History graph

Hover over **History Graph** to view the value(s) corresponding to the area on the bar or line chart.



Attack Query Table

Table field	Description
Timestamp	The timestamp indicating when the Attack Query was triggered.
Account Name	The username collected by the Attack Query, representing the account name entered by the user in the browser during actions such as login, registration, or payment on the customer's website.
Risk Score	A numerical score (0–100) calculated by Advanced Bot Protection to indicate the likelihood that a user is a bot. For details on the calculation factors, refer to Advanced Bot Protection on page 254.
IP	The IP address associated with the user activity that triggered the attack query.
URL	The URL on your website where the user activity that triggered the Attack Query took place.
Transaction ID	Unique system-generated identifier.

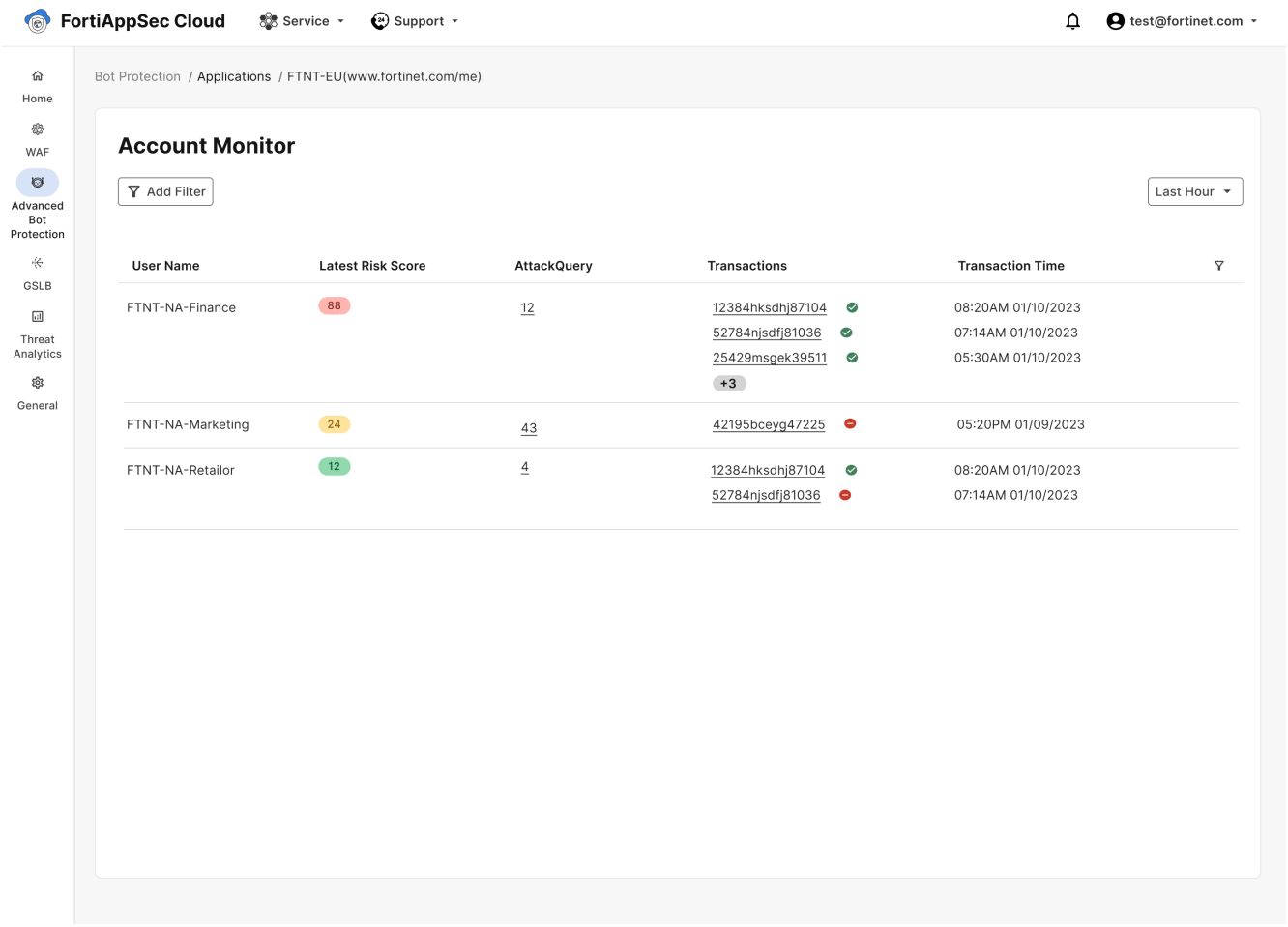
Clicking on an attack query in the table expands the following details:

Value	Description
OS	The client Operating System (OS) associated with the user activity that triggered the attack query.
Country	Country of Client IP associated with the user activity that triggered the attack query.
Browser	The browser associated with the user activity that triggered the attack query.
ASN	ASN (Autonomous System Numbers) of Client IP
Suggestion	Suggested action by FortiAppSec Cloud Advanced Bot Protection: **Block** or **Allow**.
CauseBy	Reason for the suggested action.
UserAgent	User Aagent in the HTTP request of the user activity that triggered the attack query.
Method	The HTTP request method, such as **GET**, **POST**, or **PUT**, used in the user activity that triggered the attack query.
Label	Request labels, such as **signin**, **payment**, or **signup**, associated with the user activity that triggered the attack query.

Account Monitor

Account Monitor aggregates the transaction information by individual accounts, and displays a risk score for each account. Accounts with risk score higher than 80 is considered as a bot.

The accounts are sorted by risk score. The one with the higher risk score will be ranked at top.



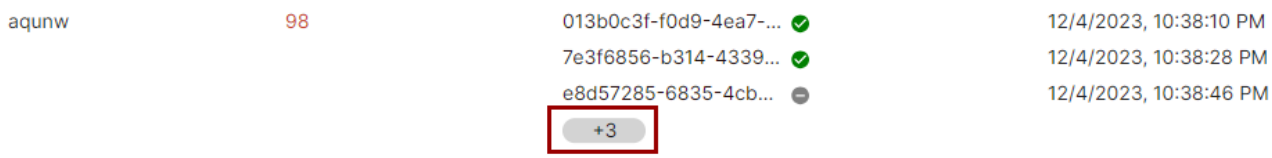
Filtering accounts

To tailor the displayed accounts according to specific criteria:

1. Go to **Traffic Insights > Account Monitor**.
2. Click **Show Filter**.
3. Enter values for **User name**, **Risk Score**, and **Transactions** to match the desired accounts.
4. Click **Apply Filters**.

Reading the transaction data of an account

All transactions associated with an account are visible in the **Transactions** column. Transactions exceeding three will be initially collapsed. To expand them, click the number icon at the bottom of each **Transaction** cell.



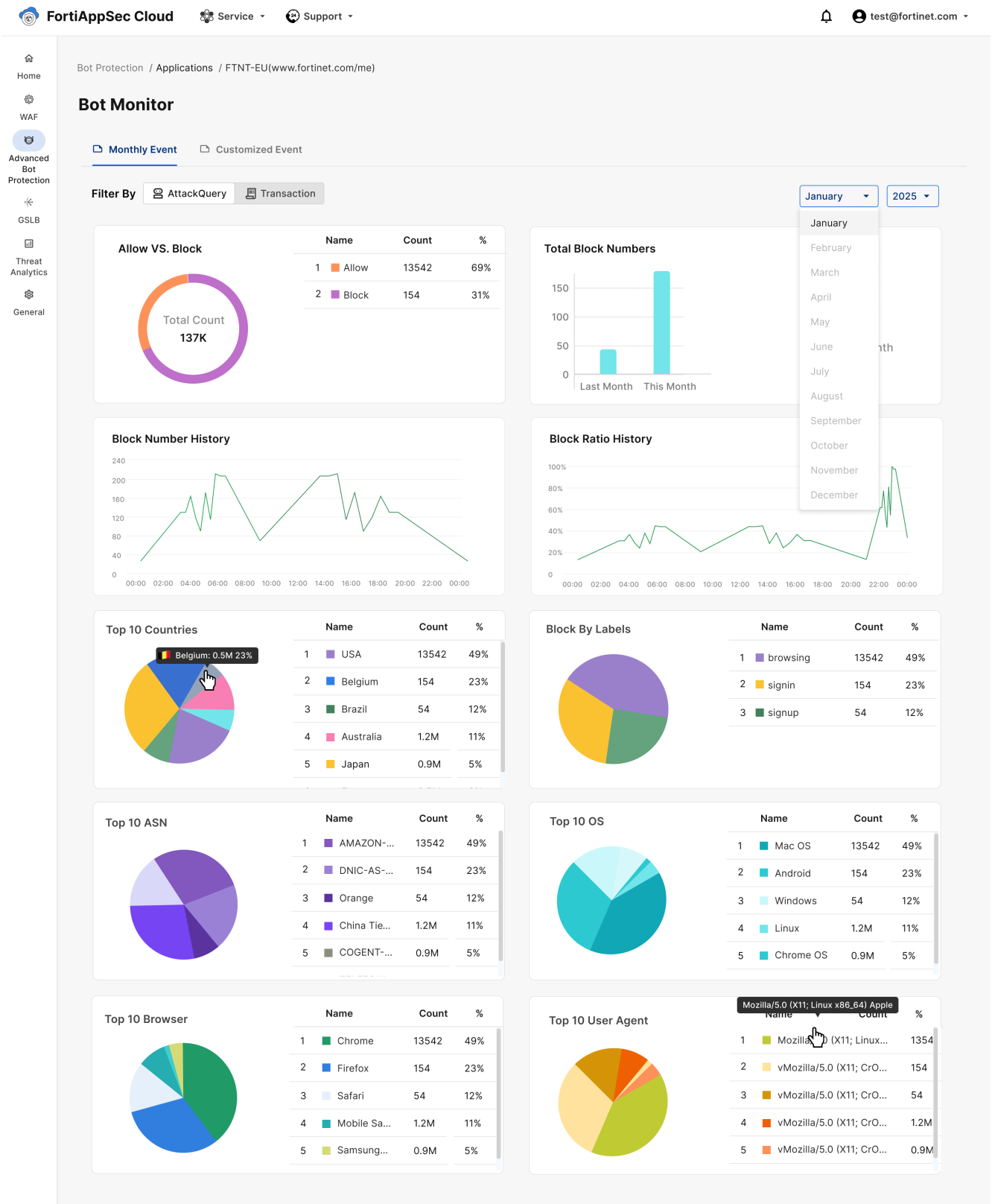
The transactions are marked with three Status:

Allow	The transaction is legitimate and is advised to let go.
Unknown	There is enough data to rate this transaction.
Block	The transaction is suspicious and is highly considered from a bot.

To access detailed information about a transaction, click on it. For more instructions on how to interpret a specific transaction, see Transactions on page 295

Bot Monitor

Track monthly bot activity or define special events to create reports on your application's activity during specific time frames.



Configure custom bot monitoring events:

1. Click **Event**.
2. Fill out the following fields:

Field	Description
Event Name	Name the event you would like to monitor (eg., product release day, New Year's Eve).
Start Time	Set the start time of the event
End Time	Optional; event is ongoing when empty.
URL	Optional; the URL(s) you would like to monitor. When empty, all of the URLs on your application's domain are monitored.
Description	Optional; enter a description that will help you keep track of the different events.

Bot Monitor

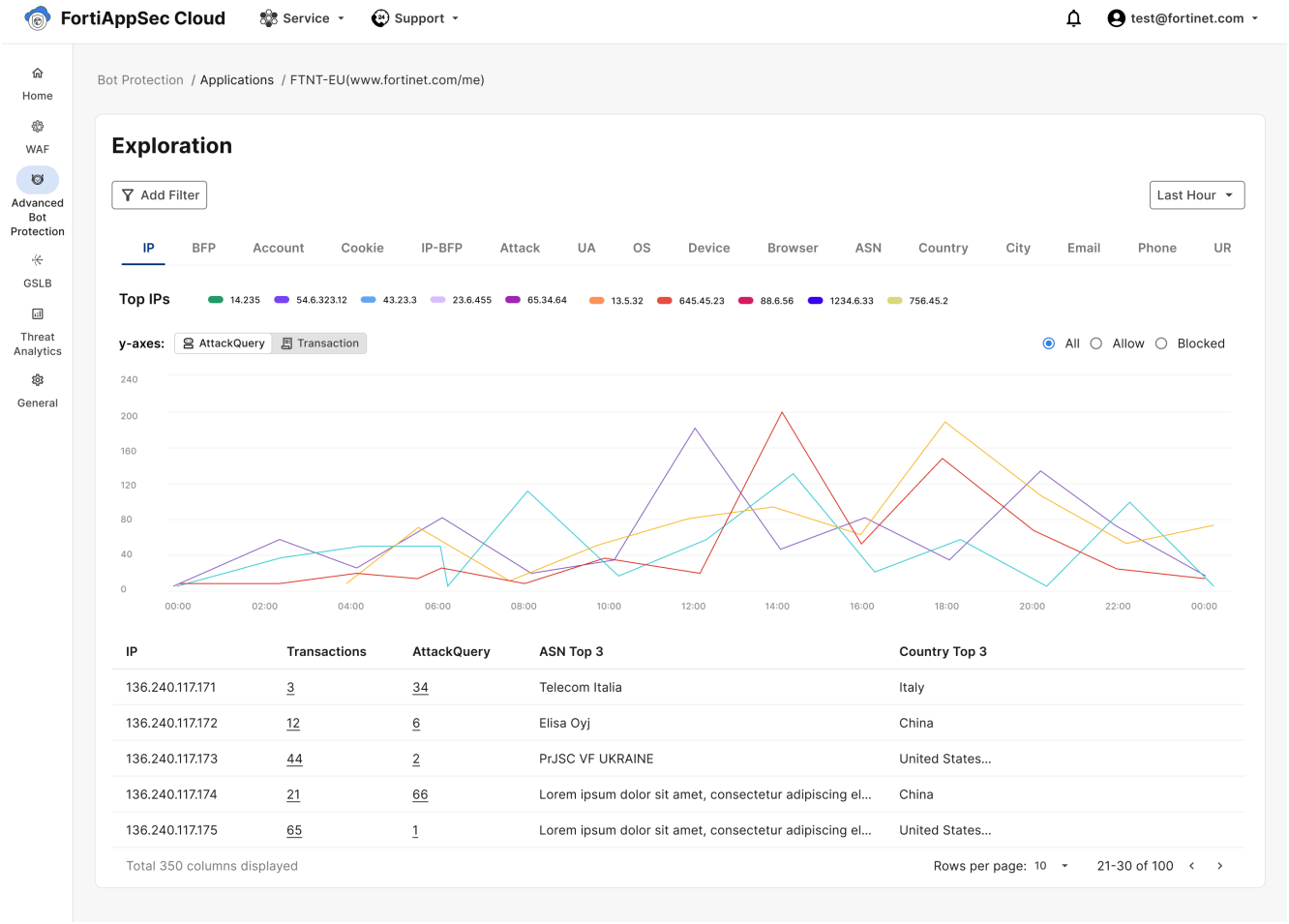
The Bot Monitor charts illustrate the following:

Static Component	Description
Allow VS Block	Displays the proportion of suggested **action = Allow** versus suggested **action = block**, within all AttackQueries or Transactions. Choose whether you want to see this display for attack queries or transactions. Use this pie chart to gain insight on the proportion of malicious bot traffic to benign human or bot traffic.
Total Block Numbers	Displays the block count for selected month and compares it to the previous month, highlighting the change.
Block Number History	Line charts show the number of blocks over 24 hours, allowing trend analysis throughout the day.
Block Ratio History	Line charts show the block ratio over 24 hours, allowing trend analysis throughout the day.
Category pie charts	Pie charts display the distribution of bot traffic across key categories: • **Country**: Geographic location of bot activity. • **Labels**: Describes activity types associated with blocked traffic. • **ASN (Autonomous System Number)**: Identifies the network from which bot traffic originates. • **OS (Operating System)**: The operating system used by the client, such as Windows, macOS, or Linux. • **Browser**: The browser type associated with the bot request • **User Agent:** A string in HTTP requests identifying the client software (browser, bot, or API client) to help classify traffic. Hover your cursor over the charts to view the count associated with each bar or pie slice.

Exploration

View traffic trends by common characteristics, including IP, User Agent, and Country.

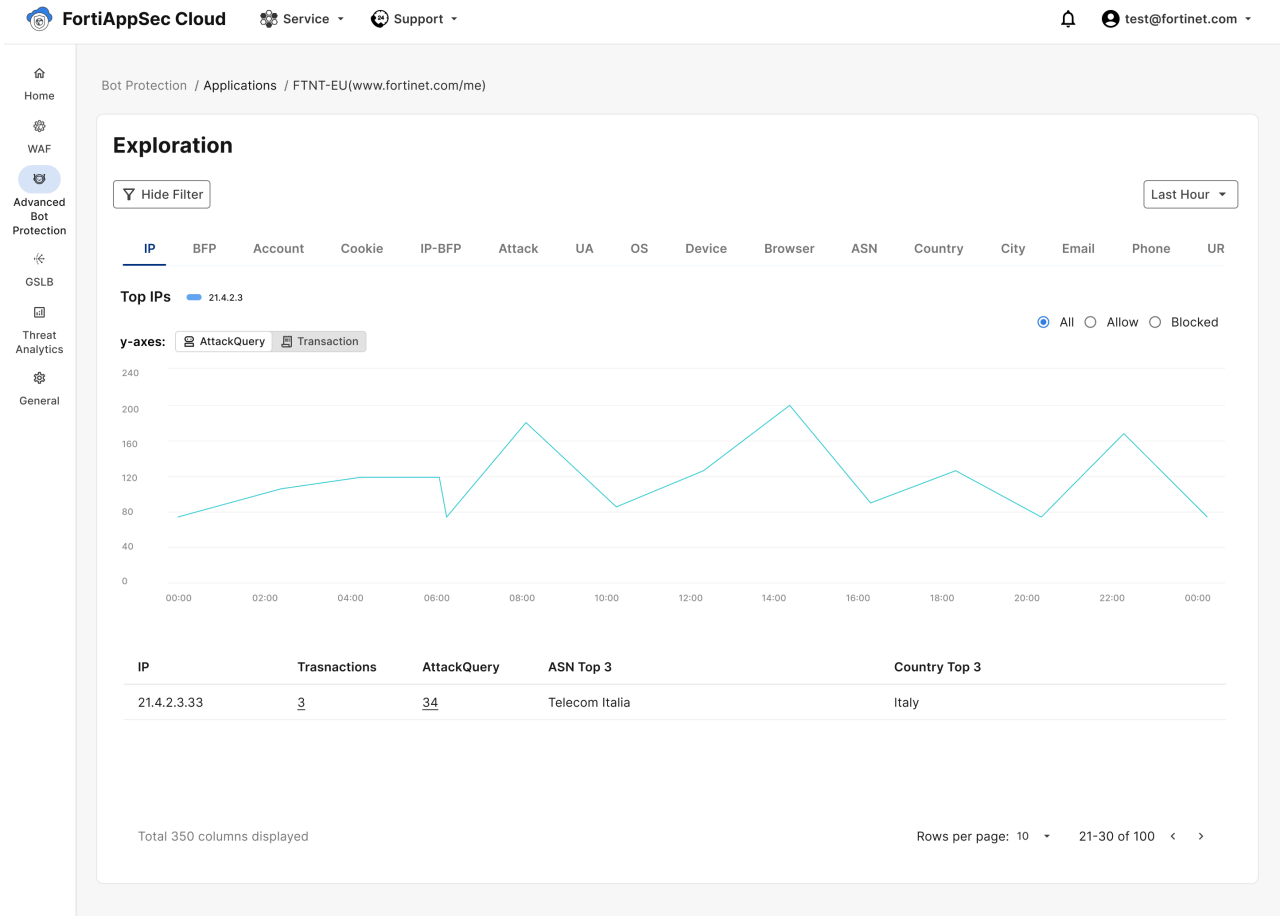
This page provides insights into telemetry messages, which capture real-time signals about user activity, such as session ID, device details, and behavioral patterns. Unlike transactions and attack queries that focus on specific request data, telemetry messages track broader activity trends and risk factors, enhancing bot classification and threat analysis.



To tailor the displayed accounts according to specific criteria:

1. Go to **Traffic Insights > Exploration**.
2. Click **Show Filter**.
3. Enter values for the criteria that you want to use to match certain traffic.

4. Click **Apply Filters**.



Message Attribute	Description
IP	The IP address from which the telemetry message was sent.
User Agent	A software component that identifies and provides information about the device or application sending the telemetry message.
Country	The message's detected country of origin.
City	The message's detected city of origin.
User Name	If the telemetry message was sent during a logged-in session, the username of the user is included in this field.
Email	If the telemetry message was sent during a logged-in session, the registered email of the user is included in this field.
Order ID	This value identifies payment-related transactions, and is empty for all non-payment transactions.
Payment ID	This value identifies payment-related transactions, and is empty for all non-payment transactions.
Session ID	This value identifies the session in which the telemetry message was

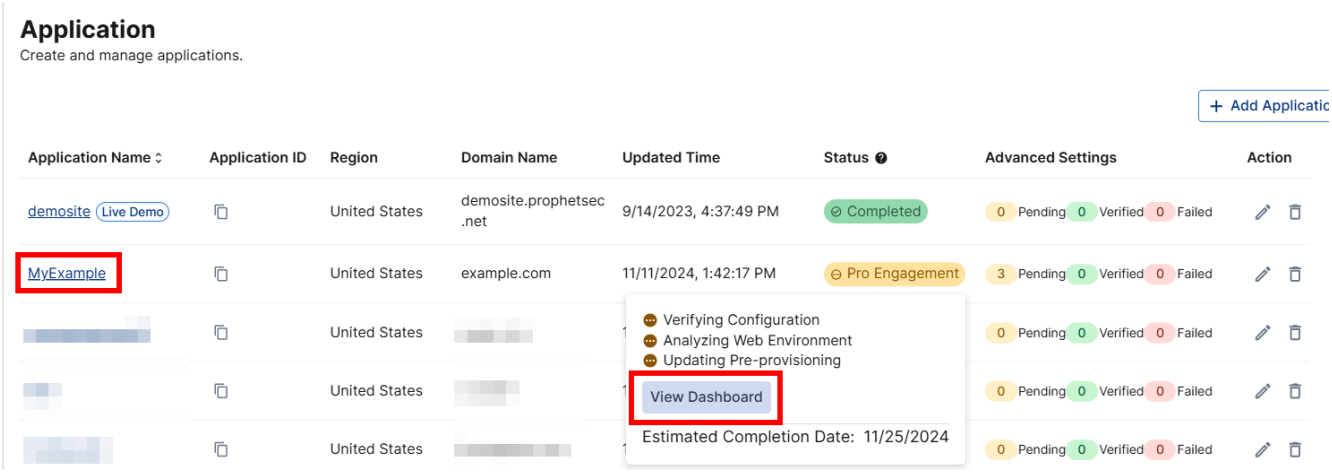
Message Attribute	Description
	sent.
URL	The URL on your application's domain at which the telemetry message was sent.

General

This section includes the following pages:

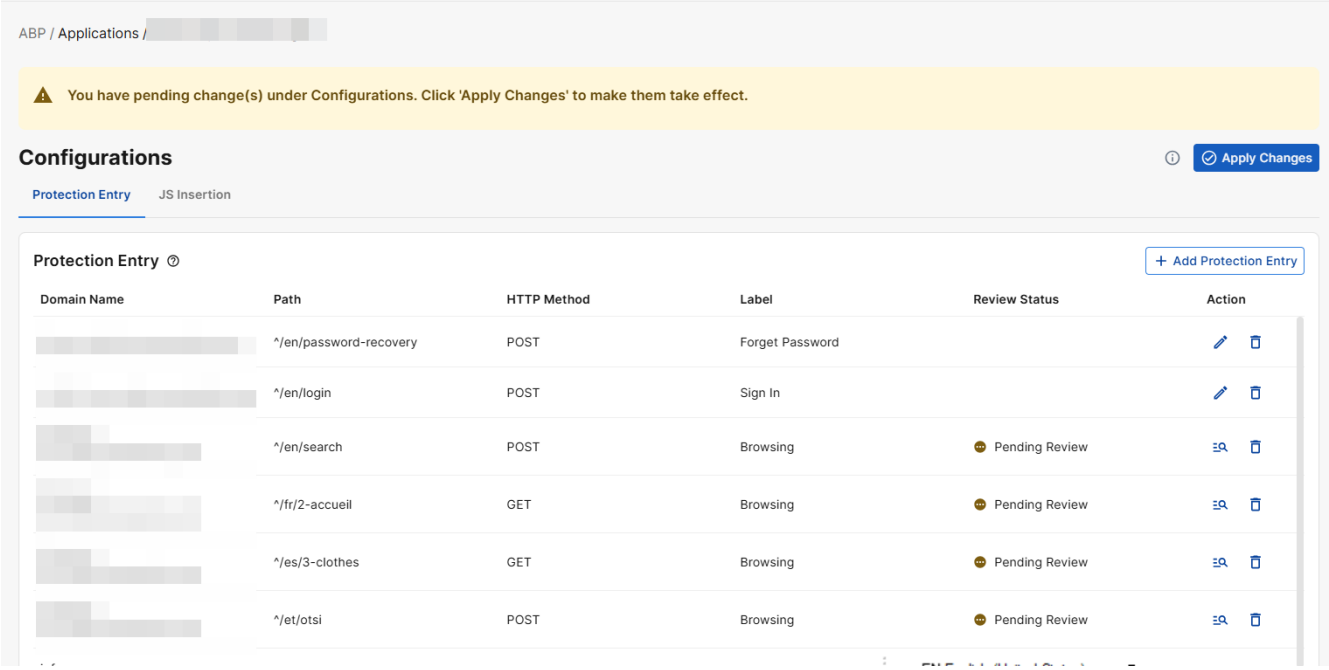
- Configurations on page 307
- Signals on page 310
- Connectors on page 311

To access these pages, go to **ABP > Application** and click on the desired **Application Name**, or click on the desired application's **Status** and click **View Dashboard**.



Configurations

The **Configurations** page contains the analyzed resources required to protect your application, which includes the protected URL entries and the locations where JavaScript is inserted through your connector devices to collect client information for bot detection.



Protection Entry

The **Protection Entry** table lists all the URL paths under your Application domain that ABP has identified should be protected.

Parameter	Description
Domain	Domain of the ABP Application to be protected.
Path	The URL path identified from the Application domain. Supports PCRE regex format.
HTTP Method	HTTP requests using any of the listed methods in the protected URL will initiate the attack query to the Advanced Bot Protection Cloud Service.
Label	The primary function of the page. • Sign In • Sign Up • Search • Forget Password • Browsing
Review Status	Indicates whether the protection entry must be reviewed before it can be applied. Manually added entries do not require review; only entries suggested by Auto Discovery trigger a review notification.
Action	The available actions to be taken on the protection entry. May include **Edit**, **Review**, and **Delete**.

Add Protection Entry

1. Click **Add Protection Entry**.
2. For detailed information on the configuration settings and their descriptions, refer to the Add ABP Application - Review Protected Entries section.

JS Insertion

The **Insert JS Entries** table lists all the locations ABP has identified in your Application domain that should be inserted with the JavaScript to collect client information.

By default, a custom JavaScript is automatically inserted into all pages that return HTTP 200 responses and have a text/html content type within the application's domains. This is essential for Advanced Bot Protection (ABP) to collect client information and secure your website.

JS Insertion Exclude

Temporarily exclude pages from JavaScript injection. Excluded pages will not be protected by Advanced Bot Protection.

Parameter	Description
Domain	The domain name of the ABP application to be protected.
URL	The path portion of the application's domain identified for this protection entry. Supports PCRE regex format.
Action	The available actions to be taken on the protection entry. Includes **Edit** and **Delete**.

Add JS Inertion Exclude

1. Click **Add JS Insertion Exclude**.
2. Enter the **Domain** and **URL** as per the descriptions above.

JS Insertion Special

Define custom injection rules for non-HTML content or non-200 responses to override the default behavior.

Parameter	Description
Domain	The domain name of the ABP application to be excluded from protection. If the port number is not 80 for HTTP or 443 for HTTPS, please include the custom port number in the Domain. Example input where the port number is 1111: `test.com:1111`
URL	The path portion of the application's domain to be excluded from protection. Supports PCRE regex format.
(Status) Code	The HTTP response status codes that this rule applies to. When a response matches one of these status codes, this custom injection rule overrides the default behavior.

Parameter	Description
	You can select one or more status codes from the drop-down list, or enter new ones to create them.
Content Type	Specify the HTTP `Content-Type` (MIME type) values that this injection rule applies to. The rule is evaluated only when a response's `Content-Type` matches one of the values you provide. Select one or more content types from the drop-down list, or enter new ones to create them.
Action	The available actions to be taken on the protection entry. Includes **Edit** and **Delete**.

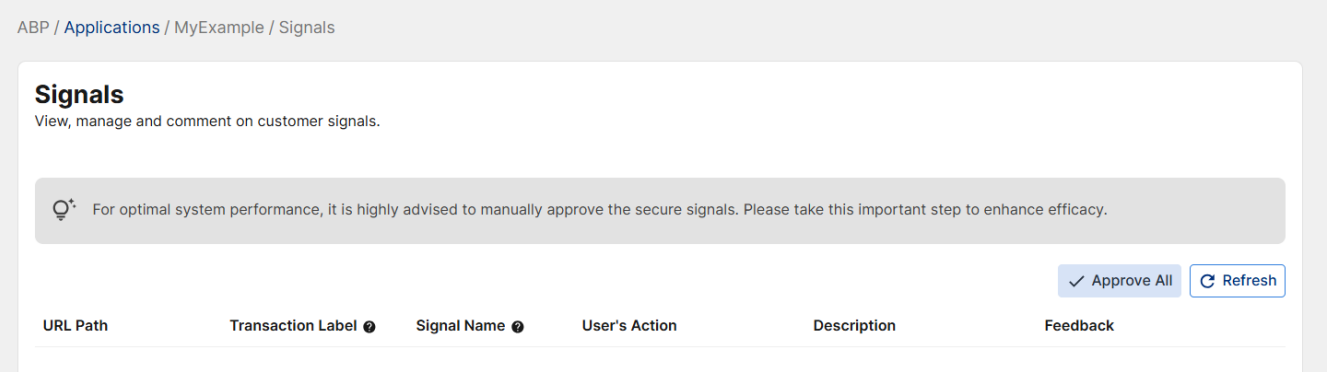
Add JS Insertion Special

1. Click **Add JS Insertion Special**.
2. Enter the **Domain**, **URL**, **Status Code**, and **Content Type** as per the descriptions above.

Signals

Detecting bot behaviors often relies on analyzing common characteristics such as IP addresses, User Agents, and mouse movements. However, uncovering more sophisticated bot activities requires additional insights, such as identifying patterns like rapid order placement across widely dispersed shipping addresses or unusually low transaction amounts (e.g., less than one cent).

To enable such advanced detection, you must authorize the system to collect data based on enhanced bot evaluation dimensions. This is essential for building a more comprehensive detection model capable of identifying deeply concealed bot activities.

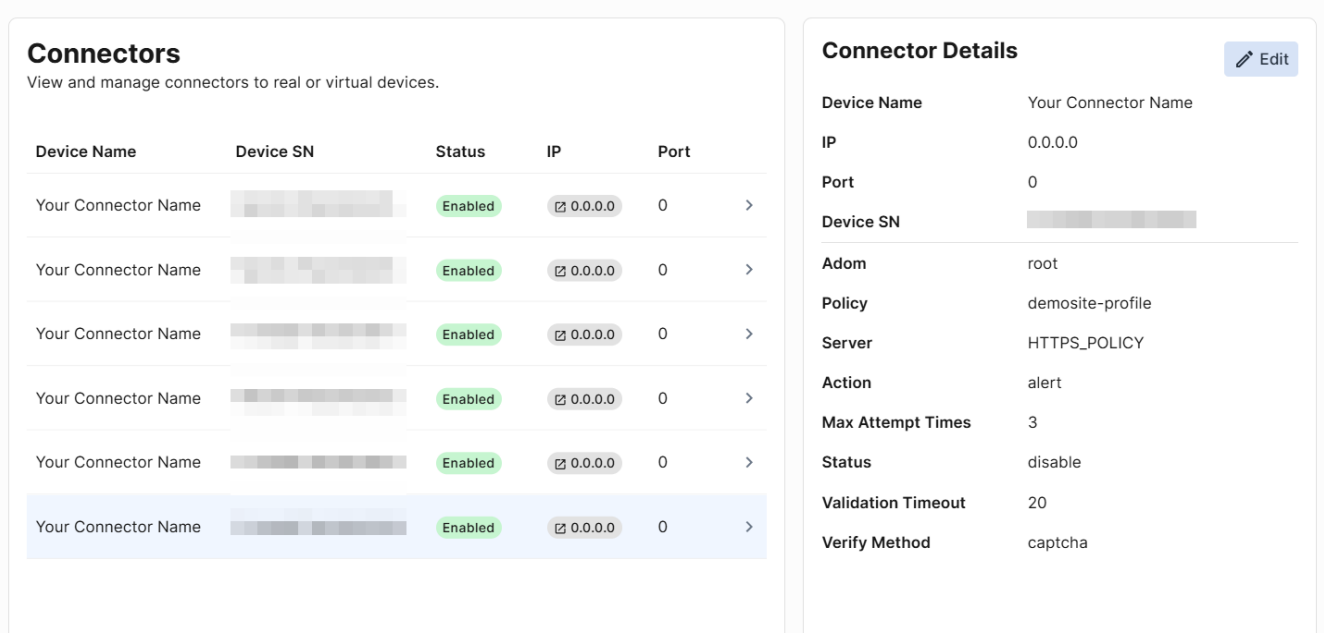


1. Go to the **Signals** page.
2. Locate the relevant URL path and the corresponding activities (Signal Name).
3. Click the **Approve** button to authorize the collection of additional data, enhancing the accuracy of bot detection. If you have concerns on collecting such data, please click **Comment** to explain your concern to FortiAppSec Cloud team.

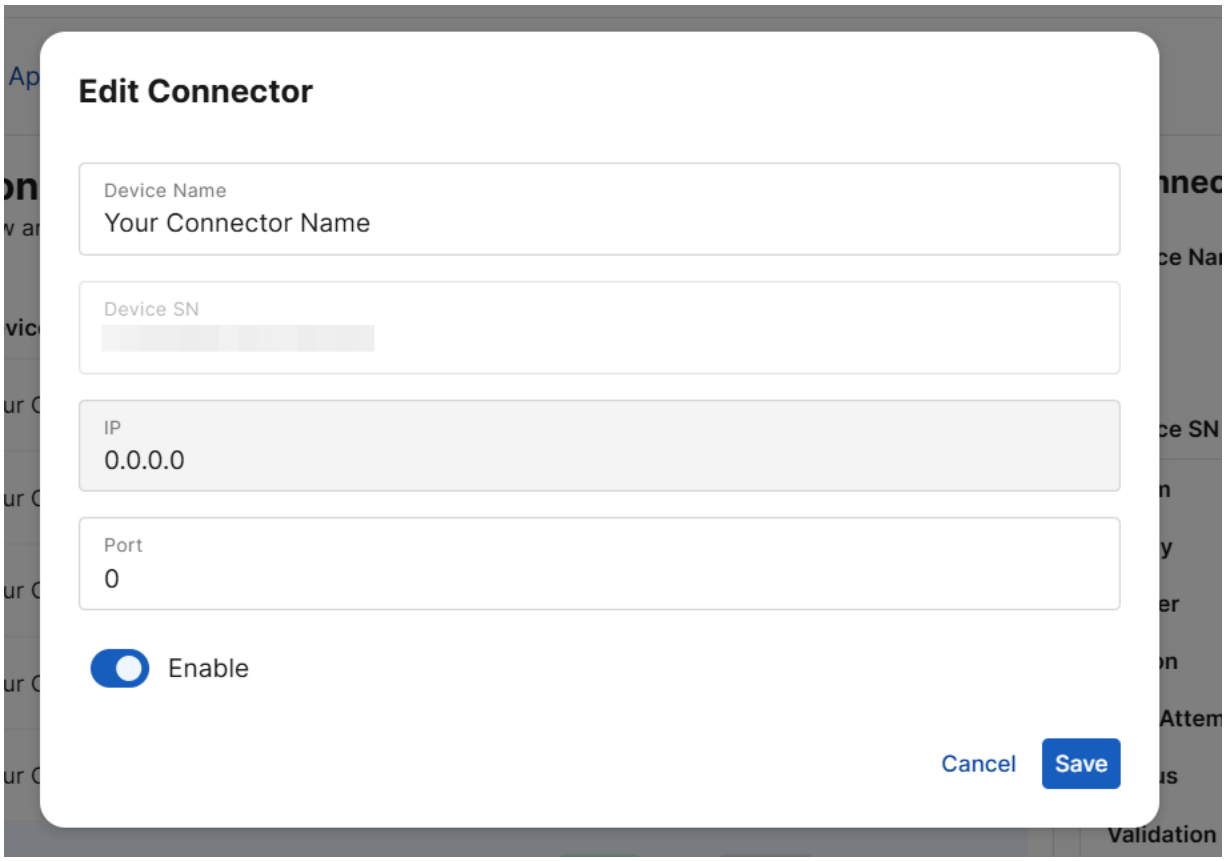
Connectors

From the **Connectors** page, you can view the Fabric devices connected to FortiAppSec Cloud. This page contains details of each connector device, including their device serial number, IP address, port number, and more.

In rare troubleshooting scenarios when ABP does not correctly fetch the device IP or Port, you may edit these fields. However, this does not affect the connection of ABP to the connector device.



You can edit connectors by selecting a connector in the list on the left, then clicking **Edit** under **Connector Details**.


Edit Connector
Device Name
Your Connector Name
Device SN
IP
0.0.0.0
Port
0
Enable
Cancel
Save

GSLB

Global Server Load Balancing (GSLB) is a DNS-based traffic management solution that ensures high availability and performance by distributing user requests across multiple servers or data centers globally. It provides redundancy and resilience by automatically directing traffic to the most optimal or available resources when a local deployment experiences unexpected downtime, spikes, or other disruptions.

GSLB supports EDNS Client Subnet (ECS) by default to improve geolocation accuracy during DNS resolution. When ECS data is available, the authoritative DNS server uses the client's subnet to make more precise routing decisions—especially for users behind public DNS resolvers. If ECS is absent, the query's source IP is used instead. No configuration is required.

GSLB objects are organized based on both physical and logical components on the network.

Physical Components:

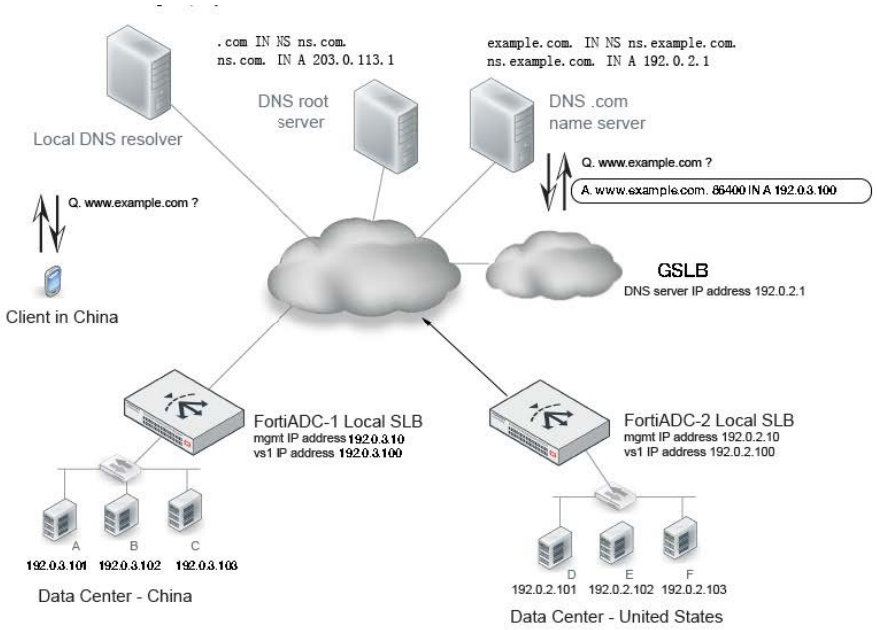
- Data Center: Represents a physical site where servers are hosted.
- Server: Refers to physical machines located in a data center.
- Location: A grouping of geographic areas that may include multiple data centers or servers.

Logical components:

- Virtual Server Pool: Represents a collection of virtual servers that distribute and manage traffic logically.
- FQDN Connector: Maps a fully-qualified domain name (FQDN) to a set of virtual servers for handling requests.

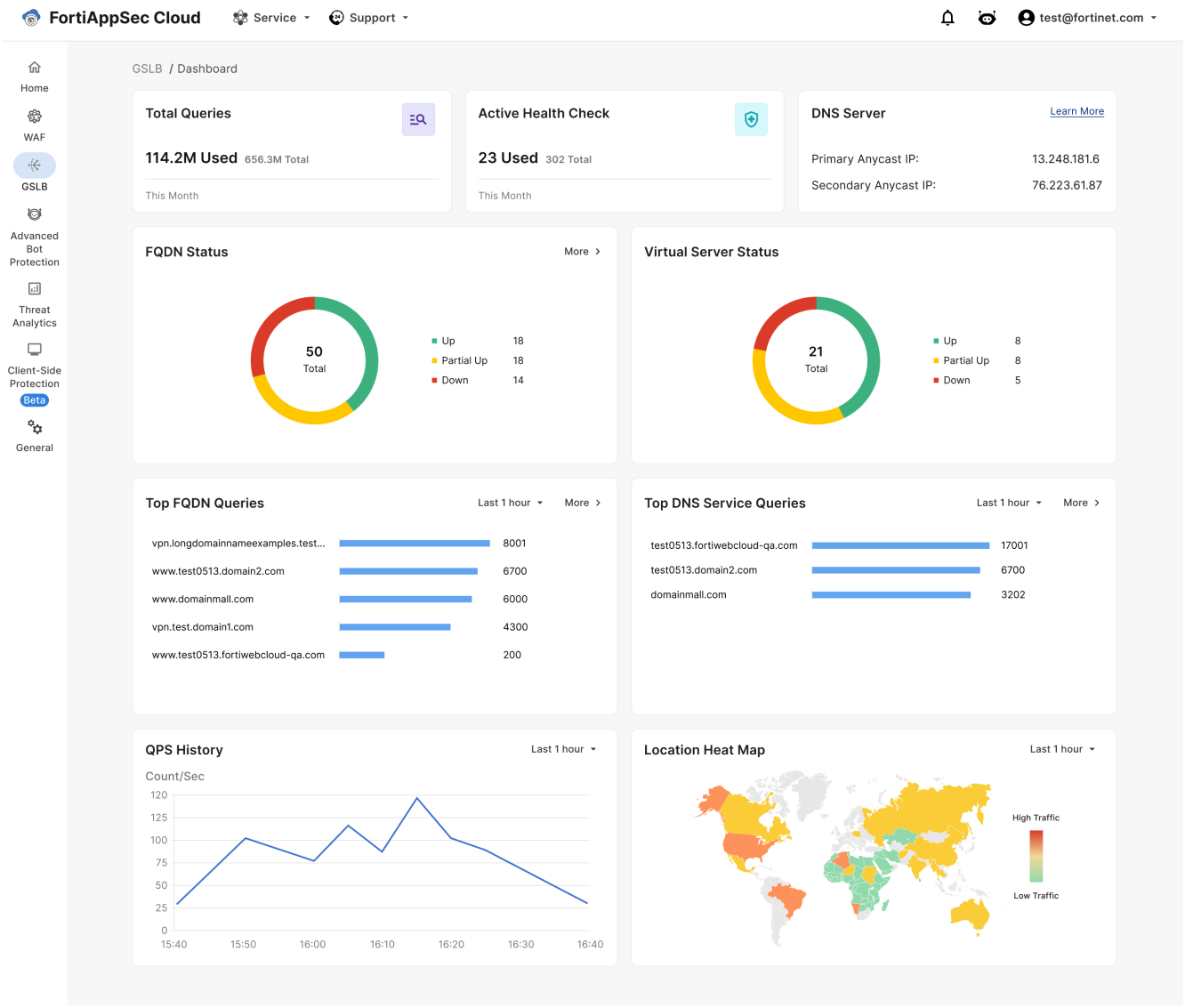
Mappings:

- The object data center corresponds to the physical data center.
- The object fabric connector relates to physical devices like FortiADC.
- The object location organizes geographical regions.
- The object pool represents a set of virtual servers.
- The object FQDN links a fully-qualified domain name to the virtual server pool for routing traffic.



GSLB Dashboard

The GSLB Dashboard provides real-time metrics on total queries, query per second (QPS) rates, load balancer health checks, fully qualified domain name (FQDN) status, and virtual server operational status.



FQDN status	Shows the status of the FQDN. Red is down; yellow is partially up; green is completely up.
Virtual server status	Shows the status of virtual servers. There are three statuses: up, down, and unknown.
Top FQDN Queries	The FQDNs receiving the highest number of queries over the selected time frame.
Top DNS Queries	The DNS domains that received the highest number of client queries over the selected time frame.
Queries per second (QPS) History	Queries per second over the selected time frame.
Total Queries	Total queries used by the account over the selected time frame.
Location Heat Map	A color-coded map showing the geographic origin of queries over time.

For comprehensive details regarding the functionalities within the GSLB services WebUI and its various pages, please see Service on page 337

Onboarding GSLB Applications

There are two ways to set up GSLB for your Application:

1. Topology Page: Set up GSLB settings in a more visual way, via Topology on page 334
2. Manual Configuration: Follow the steps below
   a. Configuring GSLB Objects on page 316 - This step entails setting up configurations within the FortiAppSec Cloud portal.
   b. Linking GSLB to domain register on page 318 - Once your application is configured on the FortiAppSec Cloud portal, this section demonstrates methods to implement your changes on the internet.



For those migrating a domain from another vendor to GSLB, it is crucial to configure the object on GSLB first. Otherwise, your domain could be temporarily out of service.

If you are setting up a brand new domain, the sequence of steps does not affect functionality.

Configuring GSLB Objects

Steps for configuration

Setting up an application for use with FortiAppSec Cloud involves two main steps:

1. Configure an FQDN for your application. This is done in *GSLB Services* > *Create FQDN*. See FQDN on page 338 for more information on configuration settings.

   Those using FortiADC, FortiGate, and FortiWeb can easily connect their services to GSLB with One-Click. One-Click enabled connectors automatically set up an FQDN. Therefore, if you choose to set up your application using the One-Click method, you don't need to perform this step manually.
2. Add your connector device to the FQDN created in the previous step. This is typically done in **Organization > Fabric Connectors**, but procedures vary for different kinds of connectors. Refer to Fabric connector on page 353 for detailed instructions on how to integrate your connector to GSLB.



Allow 1 to 2 minutes for GSLB to reload with the updated configurations.

Configuration example

The following is an example of how to set up GSLB with two devices: a Generic-Host connector and a FortiADC connector.

Scenario

The administrator manages the following devices:

- An HTTP service running on a FortiADC device in Oregon, USA
- An HTTP service running on a 3rd party device in Beijing, China

The administrator wants to achieve the following:

- The HTTP services should back up one another
  - DNS queries from China will be directed to the HTTP service IP address in Beijing, while queries from the United States will be directed to the HTTP service IP address in Oregon.
  - When the HTTP service in Oregon goes down, the HTTP service IP address in Beijing will respond.
    When the HTTP service in Beijing goes down, the HTTP service IP address in Oregon will respond.
    When both HTTP services go down, a default IP address will respond.

How to deploy this scenario

1. Enable One-Click on FortiADC, following the procedure for setting up FortiADC connectors.
2. Make sure the Connector FortiADC in Oregon is connected to GSLB.
   a. Go to *Fabric Connectors* > *Create Connector*
3. Make sure the FQDN is synced to GSLB.
   a. Navigate to *GSLB Services* and find the FQDN generated in step 2. Since this is a One-Click-enabled FQDN, its name typically follows the format OC_HostName_DomainName.

   b. Update Pool Select Method. See Virtual Server Pool on page 348 for more information on your configuration options.
      i. Click the pencil icon to edit the FQDN. The administrator's preferences outlined in the example scenario indicate that we should set the *Virtual Server Pool Selection Method* to *DNS-Query-Origin*.

   c. Update the location list for the existing pool created by One-Click.
      i. Scroll to the bottom of the *Edit FQDN* modal and locate the available member in the table. The name of this member should follow the format OCM_HostName.DomainName. Click the Edit icon.

      ii. Click *Create Location List* and add United States as a region. Click *Save* and go back to the member pool page.

      iii. Click *Save*. This brings you back to the *Edit FQDN* page. Save again to return to the FQDN service detail page.
4. Add the HTTP service in Beijing to FQDN.
   a. In the FQDN service detail page, click *Pool* and then click *Add pool*.
   b. Add a member pool for Beijing.

   c. Click *Create Location List* and add China as a region. Click *Save* and go back to the member pool page.
   d. Click *Create Virtual Server Pool* and create a pool for Beijing. Click *Save*.
   e. Click *Create Member* > *Create Virtual Server* > *Create Connector* and create a connector for Beijing.

   f. Click *Create Data Center* and create a China data center. Click *Save* and go back to the Create Connector page. Save the connector.

g. Go to the *Create Virtual Server* page and create a virtual server. Click *Save*. This brings you back to the *Edit Member Virtual Server* page.

h. Click *Save*. This brings you back to the *Create Pool* page.
i. Click *Save*. This brings you back to the *Add Member Pool* page.
j. Click *Save*. This brings you back to the *FQDN service detail* page.
k. The *Virtual Servers* table now displays that the HTTP service in Beijing has been added to FQDN.

Troubleshooting

1. Click on the left-most icon in the top right corner to see your Assigned DNS server addresses.
   The Primary Anycast IP refers to the IP address returned for the One Click GSLB Server. However, in all other aspects, the Primary and Secondary IP addresses are equivalent and either one can be used for domain management tools that only require one address.

2. Use the DNS tool dig to query the service with one of your IP addresses.

Linking GSLB to domain register

To leverage FortiAppSec Cloud's load balancing capabilities, you need to point your domain's name server to your FortiAppSec Cloud GSLB service. Configuring GSLB Objects on page 316

This section covers the following:

- General Procedures for directing your domain's name server to GSLB on page 318
- Configuration Examples on page 319
  - Modifying your domain registration with AWS Route 53 on page 319
  - Configuring a New GSLB Application: Network Solutions Use Case Example on page 321

General Procedures for directing your domain's name server to GSLB



For those migrating a domain from another vendor to GSLB, it is crucial to configure the object on GSLB before performing the steps on this page to avoid any temporary service interruptions.

If you are setting up a brand new domain, the sequence of steps does not affect functionality.



We recommend performing the following optional steps prior to setting up your domain:

1. Navigate to **GSLB > DNS** within the FortiAppSec Cloud GUI，and click the edit icon in the row of the desired application.
2. Ensure that the “Domain Name,” “Primary Server Name,” and “Primary Server Address matches the one on FortiAppSec Cloud.
3. It's recommended to set the “Primary Server Address” to match the assigned DNS Server IP.

These steps are recommended but not mandatory. If you skip these steps, GSLB will use default values for the domain settings.

Set Name Servers and Glue Records via Web Host:

1. `dig` from FortiAppSec Cloud to see your application's SOA records. Take note of your Name Severs and Glue Records.
2. Access your web host's settings.
3. Set the Name Servers and Glue Records using the SOA records directly provided by GSLB.

   Note: Changes to name servers may take time to propagate globally. The name server (NS) is specified in the Start of Authority (SOA) record, while the glue records are the IP addresses linked to the NS records.

Configuration Examples

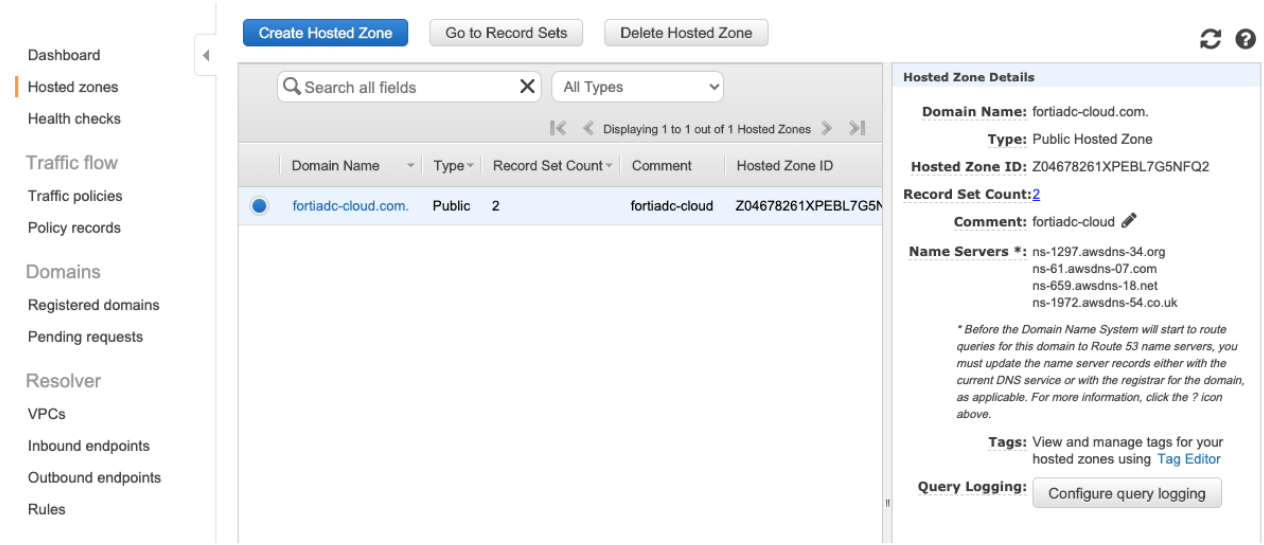
Typically, you can adjust your DNS records through your web host or the domain registrar from which you obtained your domain.

Here are procedures for AWS Route 53 and Network Solutions, both prominent domain registrars. However, keep in mind that other vendors like GoDaddy, Cloudflare, and local registrars may offer different processes.

Modifying your domain registration with AWS Route 53

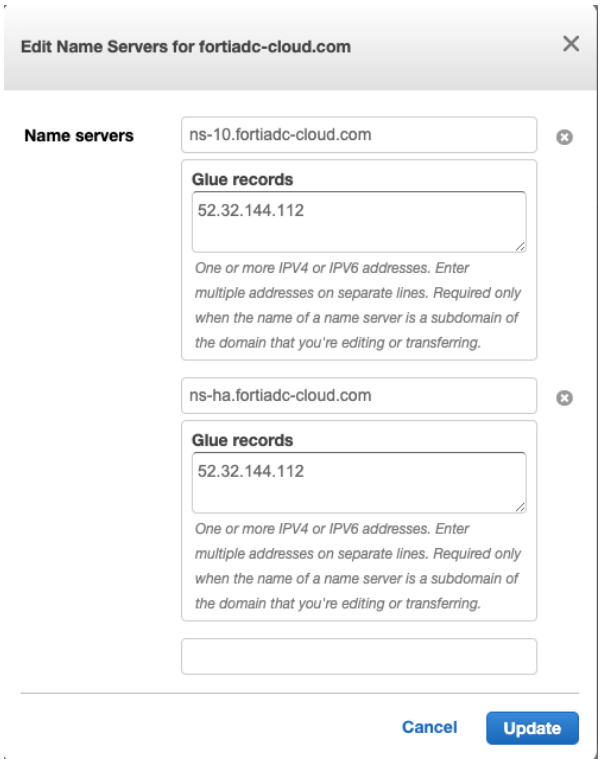
Below is the procedure for users who have registered their domain names through AWS Route 53.

1. Sign in to the AWS Management Console.
2. Go to *Registered domains* and click your *Domain Name*. Route 53 will display details of the domain. Click on *Manage DNS*.



3. Go to *Add or edit name servers* on the domain general information page. Set the Name servers and Glue records as SOA records directly taken from GSLB. Route 53 requires at least two name servers, so do not delete all other name servers.

   Note:Changes to Route 53 name servers may take time to propagate globally. The name server (NS) is specified in the Start of Authority (SOA) record, while the glue records are the IP addresses linked to the NS records.



Your domain SOA records should look something like the following when you `dig` from GSLB directly.

```
; <<>> DiG 9.10.6 <<>> @52.32.144.112 fortiadc-cloud.com. soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50204
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fortiadc-cloud.com.            IN      SOA

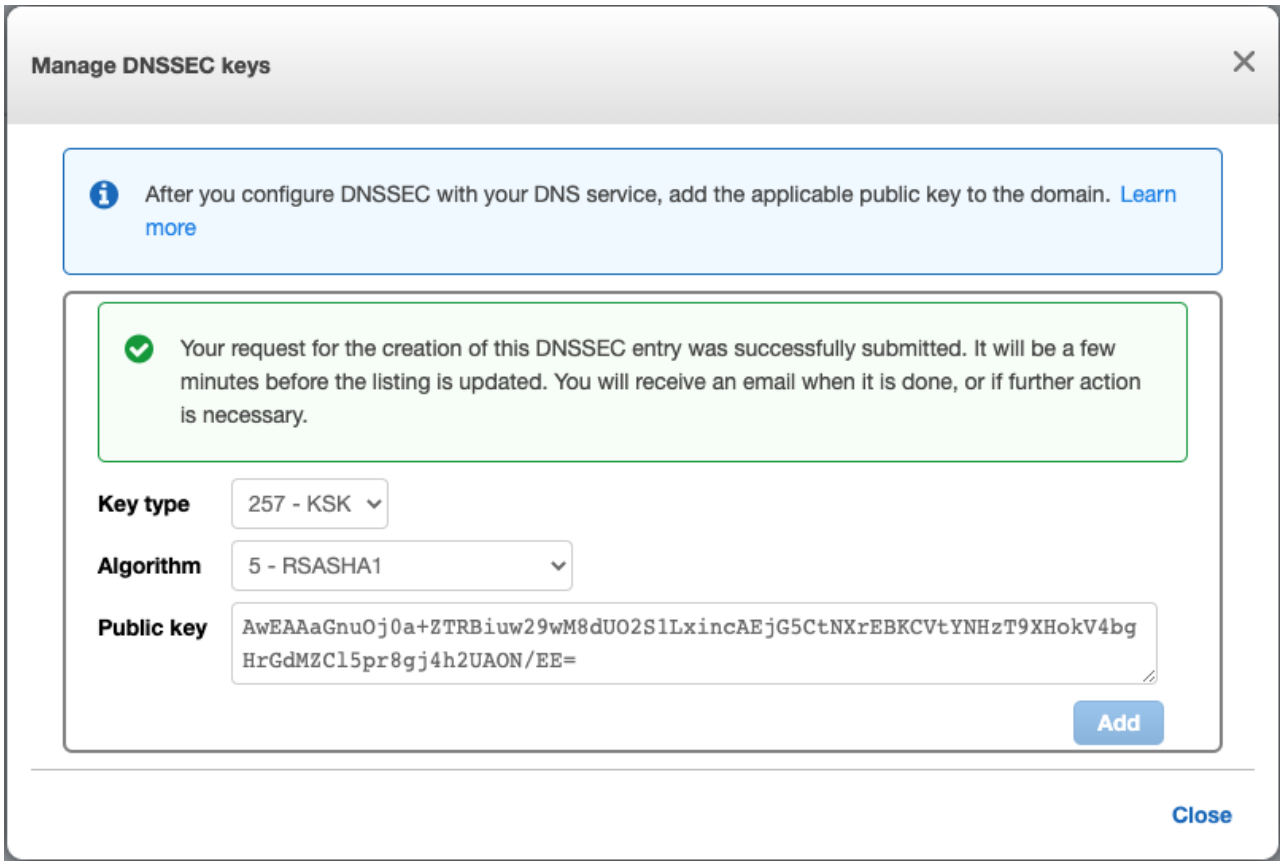
;; ANSWER SECTION:
fortiadc-cloud.com.     60      IN      SOA     ns-10.fortiadc-cloud.com. zhangwei.fortinet.com. 10004 3600 900 3600000
30

;; AUTHORITY SECTION:
fortiadc-cloud.com.     60      IN      NS      ns-10.fortiadc-cloud.com.

;; ADDITIONAL SECTION:
ns-10.fortiadc-cloud.com. 60    IN      A       52.32.144.112

;; Query time: 40 msec
;; SERVER: 52.32.144.112#53(52.32.144.112)
;; WHEN: Mon Jul 06 18:31:42 PDT 2020
;; MSG SIZE  rcvd: 137
```

4. If you enabled the DNSSEC for the domain, you can configure the DNSSEC by clicking **Manage Keys**. Select Key type and Algorithm, and paste the Public key without any spaces. Keys can be downloaded from the GSLB zone configuration page.

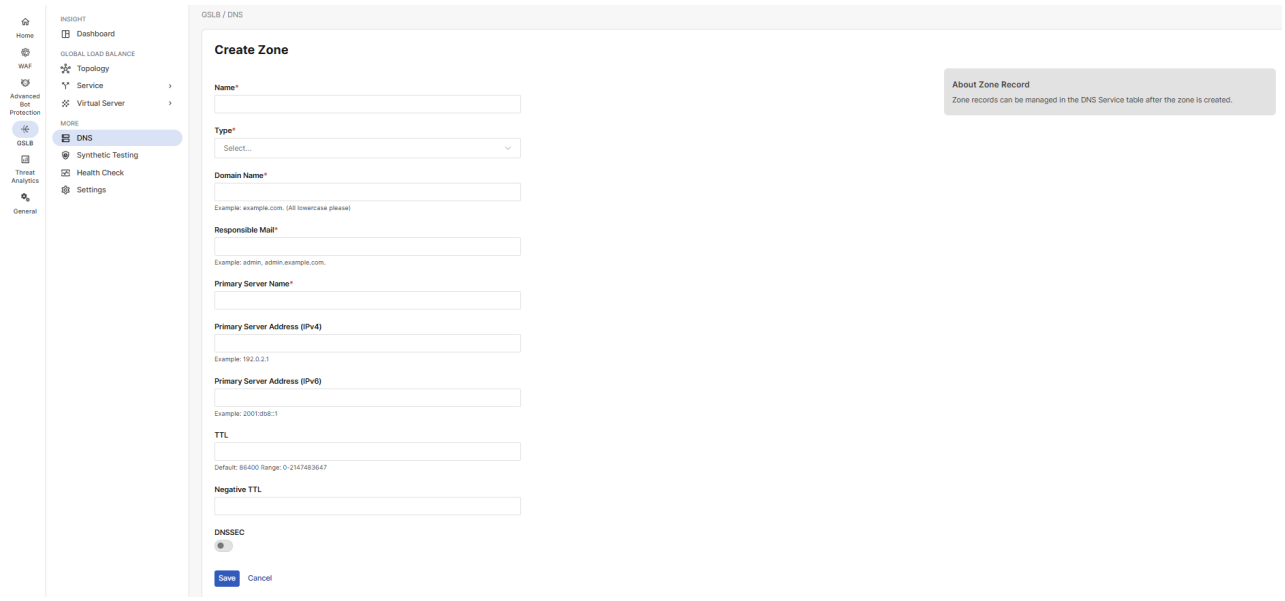


The following key file indicates that it is a key-signing key file and the algorithm is 5. Usually there will be two parts of the key, separated by a space. When you paste the key into Route 53 **Manage DNSSEC keys**, make sure to remove the space.

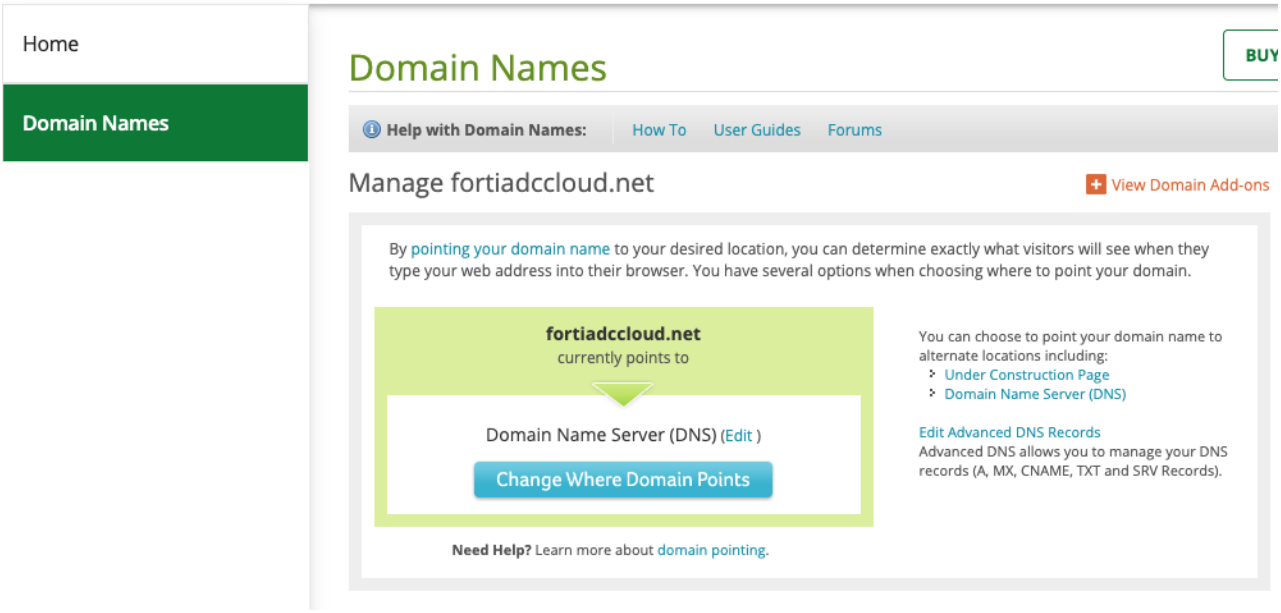
```
Shutings-iMac:dnssec shutingdong$ cat Kfortiadc-cloud.com.+005+25837.key
; This is a key-signing key, keyid 25837, for fortiadc-cloud.com.
; Created: 20200619182156 (Fri Jun 19 18:21:56 2020)
; Publish: 20200619182156 (Fri Jun 19 18:21:56 2020)
; Activate: 20200619182156 (Fri Jun 19 18:21:56 2020)
fortiadc-cloud.com. IN DNSKEY 257 3 5 AwEAAaGnuOj0a+ZTRBiuw29wM8dUO2S1LxincAEjG5CtNXrEBKCVtYNH zT9XHokV4bgHrGdMZCl5pr8gj
4h2UAON/EE=
```

Configuring a New GSLB Application: Network Solutions Use Case Example

1. To begin, prepare the domain within GSLB. Navigate to **GSLB> DNS** and configure the Zone service settings. Ensure to take note of the **Domain Name**, **Primary Server Name**, and **Primary Server Address** fields. We recommend setting the **Primary Server Address** to match the assigned DNS Server IP.

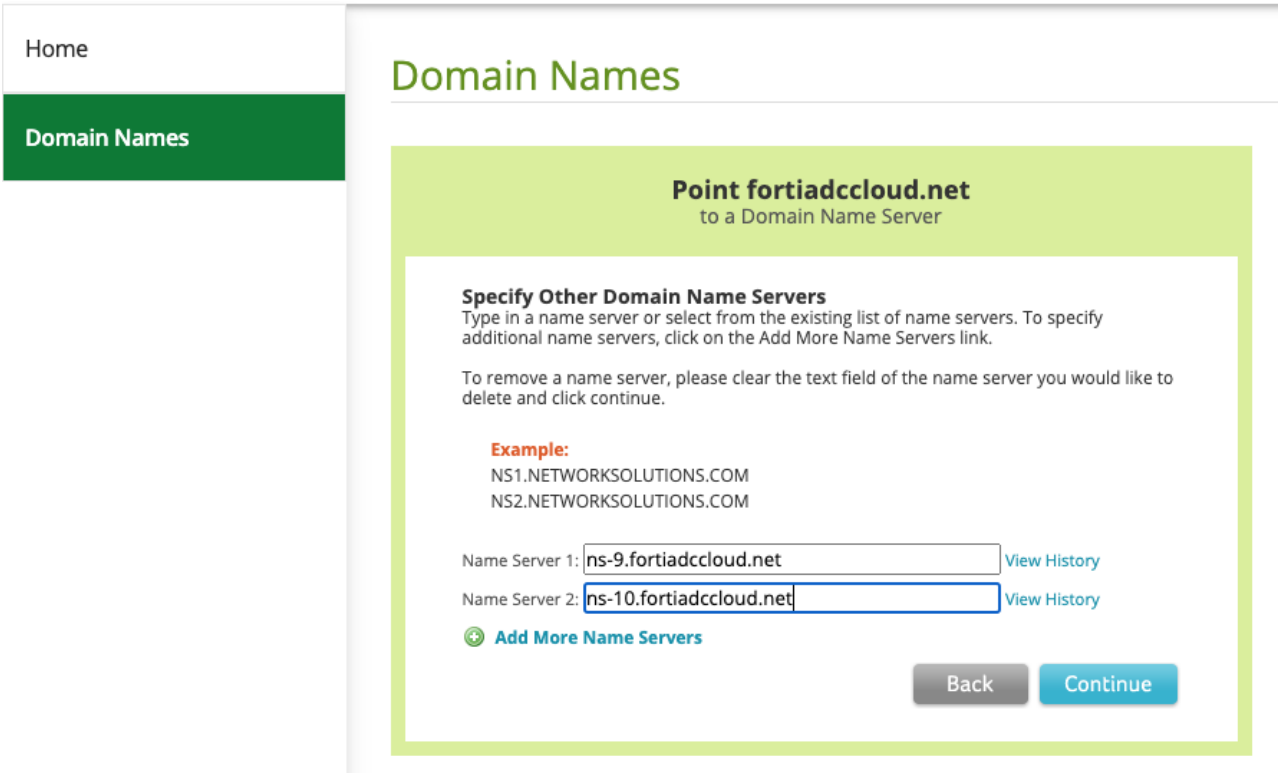


2. Register a domain. Once completed, you should see a window like the one below.

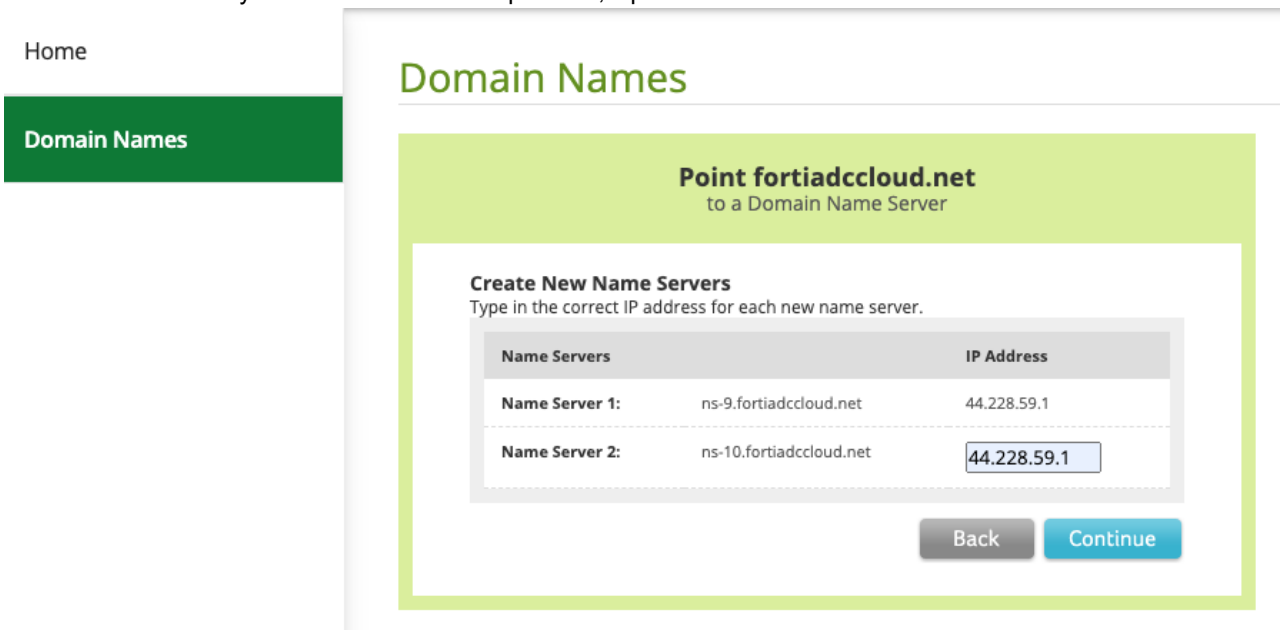


3. On your domain registrar, locate the page that allows you to change the destination of your domain.
In the Network Solutions example case, click **Change Where Domain Points**. In the **Domain Name Pointing Options** window, select the **Domain Name Server (DNS)** option and click **Continue.**
4. When configuring with Network Solutions, you need at least two name servers. Designate Name Server 1 as the primary server and Name Server 2 as the secondary. In the **Specify Other Domain Name Servers** section, enter the NS server for Name Server 1, which corresponds to the Primary Server Name and Domain Name from the GSLB Zone page. If you have a backup server, input its NS info for Name Server 2. Otherwise, provide alternative

information and proceed.



5. Under *Create New Name Servers*, input the IP address for Name Server 1 and input the backup server's IP address for Name Server 2. If you do not have a backup server, input the same IP as Name Server 1 and click **Continue**.



6. Double check the name server configuration and confirm the changes by clicking **Apply Changes**. It may take 24 - 48 hours for DNS changes take effect.
7. Click **Return to Domain Details**. After about 5 minutes, you will be able to `dig` the A record for this domain from the public DNS server.

Maintenance

To ensure the health and optimal performance of your GSLB service, we recommend staying up-to-date on the following:

- Migrate Legacy GSLB Organizations to FortiCloud Organizational Units (OU) on page 328
- Migrating Sub User to IAM user
- Migrate Legacy GSLB Organizations to FortiCloud Organizational Units (OU) on page 328

Anycast Migration for global DNS service

On September 8, 2023, the legacy FortiGSLB service transitioned to an Anycast DNS server to enable DNS service deployment across multiple regions. This Anycast DNS server remains in use in the updated FortiAppSec Cloud GSLB. If you have not yet updated your DNS server IP addresses, please add the current Anycast IP addresses promptly to ensure uninterrupted functionality.

Anycast is an IP network addressing method where requests from several physical destination servers can be combined under a single IP address. When a user makes a request, Anycast routers determine the optimal server in the network to handle the request based on factors like the user's location, the number of hops, shortest distance, lowest transit cost, and minimum latency. This optimization process prevents the need for the origin server to extend capacity and avoids service interruptions for clients seeking information from the origin server.

Once you set the Anycast IP address as the DNS server IP address, it automatically routes your DNS query results to the nearest FortiAppSec Cloud endpoint. This dynamic load-balancing reduces latency and improves response times for global queries.

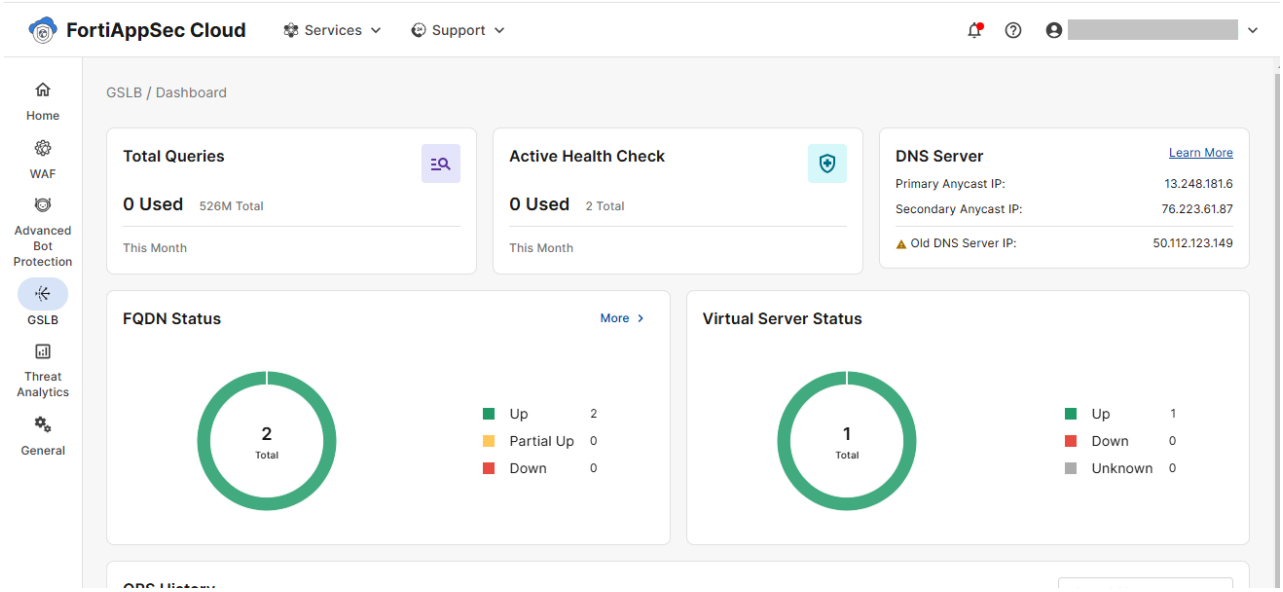
Changing the DNS IP (anycast) is not expected to cause service downtime. If you require any assistance, please see Contacting customer service.

How to migrate domains to Anycast

1. Log into the FortiAppSec Cloud portal.
2. Obtain the assigned Anycast IP address by navigating to GSLB > Dashboard. A yellow warning label will appear until you have successfully switched all of your domains to the new IP address(es).

   In the example below, the Anycast IP addresses are 13.248.181.6 and 76.223.61.87.

   Two Anycast IP addresses are provided as some domain management tools require each NS record to have two different IP addresses. The Primary Anycast IP refers to the IP address returned for the One Click GSLB Server. However, in all other aspects, the Primary and Secondary IP addresses are equivalent and either one can be used for domain management tools that only require one address.



3. Verify your domain works with the Anycast IP address by sending the DNS query traffic to Anycast DNS server directly. Here, your DNS query traffic still goes through the old DNS server.

   In our example, the test domain is *app.devdemo.GSLB-cloud.com*. You could use `dig` or `nslookup` to verify it.

```
hailin@ubuntu-hailin:~$ dig @13.248.181.6 app.devdemo.fortigslb-cloud.com.

; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> @13.248.181.6 app.devdemo.fortigslb-cloud.com.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44679
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;app.devdemo.fortigslb-cloud.com. IN    A

;; ANSWER SECTION:
app.devdemo.fortigslb-cloud.com. 5 IN   A       3.3.3.3
app.devdemo.fortigslb-cloud.com. 5 IN   A       6.6.6.6

;; AUTHORITY SECTION:
devdemo.fortigslb-cloud.com. 86400 IN   NS      defaultprimary.devdemo.fortigslb-cloud.com.

;; ADDITIONAL SECTION:
defaultprimary.devdemo.fortigslb-cloud.com. 86400 IN A 13.248.181.6

;; Query time: 25 msec
;; SERVER: 13.248.181.6#53(13.248.181.6)
;; WHEN: Fri Jul 28 21:39:51 PDT 2023
;; MSG SIZE  rcvd: 137
```

4. Confirm your current configuration management tools are connected correctly. This is important as the Anycast DNS server will connect to your existing domain management tool.

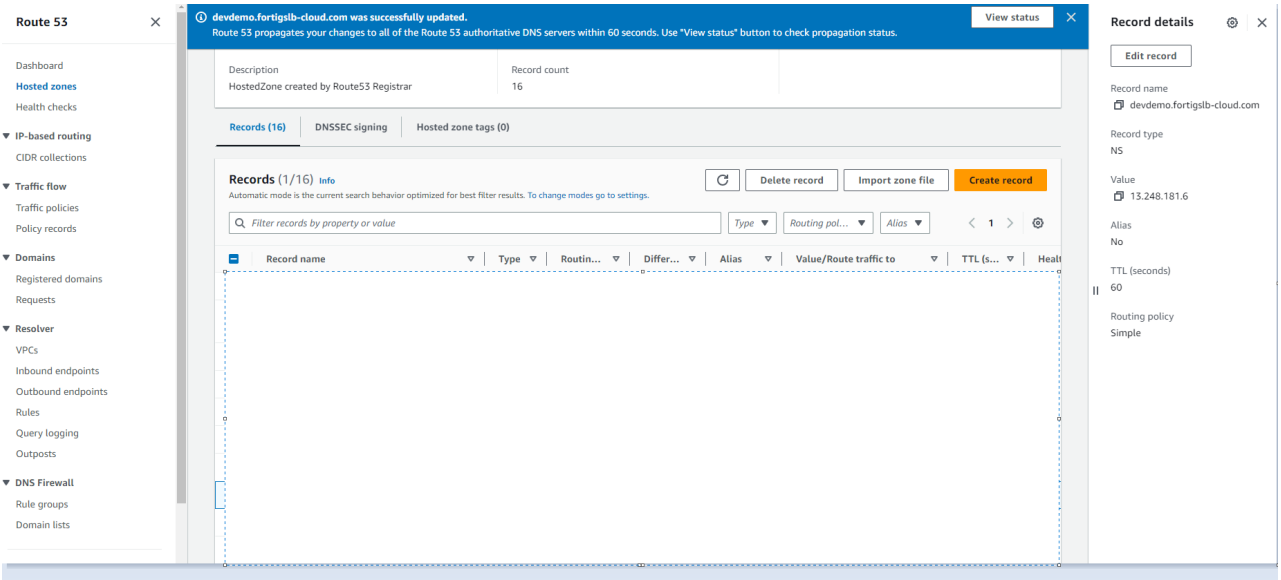
   In this example, we used `dig @8.8.8.8+trace` to verify the status.

```
devdemo.fortigslb-cloud.com. 60 IN      NS      50.112.123.149.
;; Received 88 bytes from [redacted] in 13 ms

app.devdemo.fortigslb-cloud.com. 5 IN   A       7.7.7.7
app.devdemo.fortigslb-cloud.com. 5 IN   A       78.22.1.1
devdemo.fortigslb-cloud.com. 86400 IN   NS      defaultprimary.devdemo.fortigslb-cloud.com.
;; Received 137 bytes from 50.112.123.149#53(50.112.123.149) in 27 ms
```

5. If you use a NS (Name Server) record to point your domain to GSLB, update the Anycast IP address to the NS record on your domain management tool.

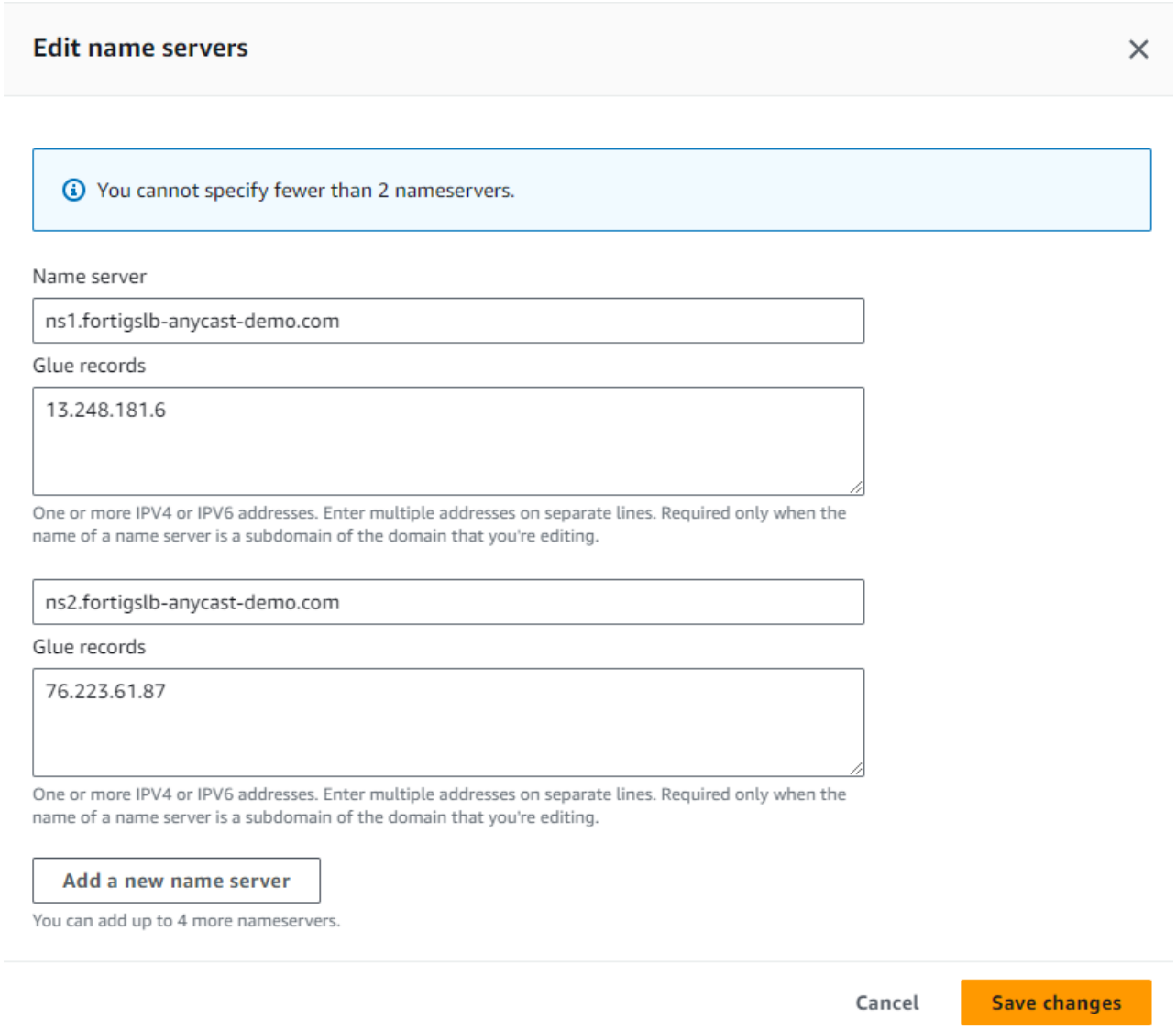
   In this example, the NS record is configured on Route 53 and the NS record value is updated to “13.248.181.6”.



   If you use a glue record to point your domain to GSLB, update the Anycast IP address to the glue record on your domain management tool.

   Pictured below is an example where the domain “GSLB-anycast-demo.com” is registered on AWS. Here, the domain will be configured under “Registered domains” in Route53 and the “Primary Anycast IP” and “Secondary Anycast IP” are updated to "Glue records".

   In this case, the DNS request is delegated to GSLB.



Please note, DNS changes can take several minutes to 48 hours to fully propagate throughout the internet. Please consult your domain management tool for more information.

6. To confirm the change is in effect, use dig or nslookup to verify the status of the newly configured IP address.

```
devdemo.fortigslb-cloud.com. 60 IN      NS      13.248.181.6.
;; Received 86 bytes from [redacted] in 13 ms

app.devdemo.fortigslb-cloud.com. 5 IN   A       3.3.3.3
app.devdemo.fortigslb-cloud.com. 5 IN   A       6.6.6.6
devdemo.fortigslb-cloud.com. 86400 IN   NS      defaultprimary.devdemo.fortigslb-cloud.com.
;; Received 137 bytes from 13.248.181.6#53(13.248.181.6) in 25 ms
```

The GUI will also reflect that all domains have been successfully changed to the Anycast server.

Migrate Legacy GSLB Organizations to FortiCloud Organizational Units (OU)

This section addresses the use case for migrating legacy organization assets to FortiCloud. It applies specifically to former FortiGSLB users with multiple legacy organizations that have not yet migrated to FortiCloud.

Legacy FortiGSLB Organizations are no longer supported. Migrating to FortiCloud enables asset management, role- and resource-based access controls, and hierarchical structures for efficient provisioning and consistent security.

For information on how FortiCloud Organizational Units (OU) works, please refer to this document outlining its key concepts.

- Key features of migration on page 328
- Migration prerequisites on page 328
- Migration steps on page 329
- Manage users after migration on page 334

After the migration, please refer to FortiCloud Organizational Units on page 453 for additional information on how to use FortiCloud with FortiAppSec Cloud.

Key features of migration

Benefits of migrating to FortiCloud OU include:

- **Comprehensive asset management:** view, organize, and manage assets with search options in one place, and organize assets into multi-depth hierarchies.
- **Secure user management:** delegate role-based and resource-based access controls.
- **Multitenancy Management:** use hierarchical structures for flexible, efficient resource provisioning and consistent security management.

Please note that after migrating to FortiAppSec Cloud:

- You will no longer be able to choose FortiGSLB legacy organizations.
- You will only see the resources in OneClick type FortiGSLB legacy organization.

For further details on FortiCloud OU use cases and benefits, please refer to the FortiCloud Organization Portal Online Help.

Migration prerequisites

- FortiCloud account



If you plan to enable **Contract Sharing Mode**, please register your service license to the root account, as all member accounts under FortiCloud OUs share the root account's license for calculations. Licenses registered under non-root accounts within an organization will not count toward the service.

You can view your current license type in the FortiAppSec Cloud web portal under **General > Contracts**.

Migration steps

1. Log in to FortiCloud.
2. Turn on the Organization feature.
   a. Access the Organizational portal. Go to **My Account > My Account (IAM version) > Account Preferences** and click **Enable Organization Feature**.
   b. Go to https://support.fortinet.com/organizations.
   c. Click **Create Organization** and follow the prompts to create the Organization. For more details on the Organization creation screens, please see Creating an Organization.
3. Add Organization Structure. There are two ways to do this:
   - **Option 1:** Upload Organization Structure. Choose this option if you would like to import your legacy service organization structure to FortiAppSec Cloud.
   - **Option 2:**Option 2: Input Organization Info. Choose this option if you would like to customize your FortiCloud OU structure by manually inputting OUs and member accounts.

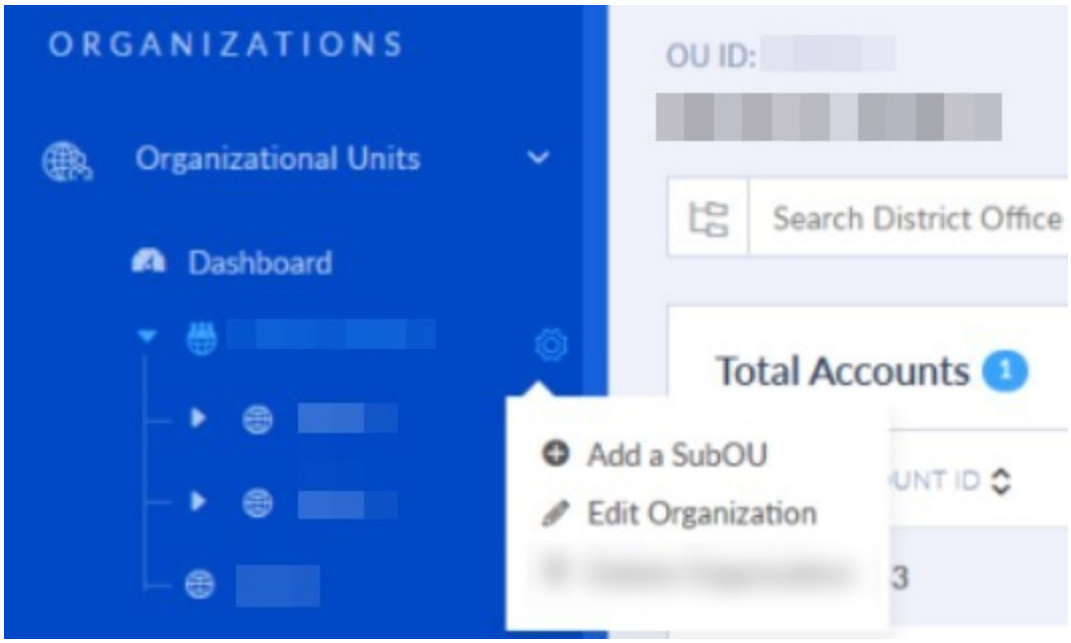
   Option 1: Upload Organization Structure
   a. Submit a ticket to request an **Organization Template** form with your legacy organization structure.
   b. Download the **Organization Template**.
   c. Edit the downloaded template, and update the values under **OU Path** to include the top-level organization's name, followed by a backslash.

   For example, if the top-level organization's name is "root_org," change the OU Path value "company1" to "root_org\company1."

   Similarly, update OU Paths with multiple values, changing "example-company\subgroup1" to "root_org\example-company\subgroup1."

	A	B	C	D
1	**OU Name ***	**OU Description**	**OU Path**	**OU ID**
2	default	default organization	root_org\default	
3	company1	company1	root_org\company1	
4	company2	company2	root_org\company2	
5				

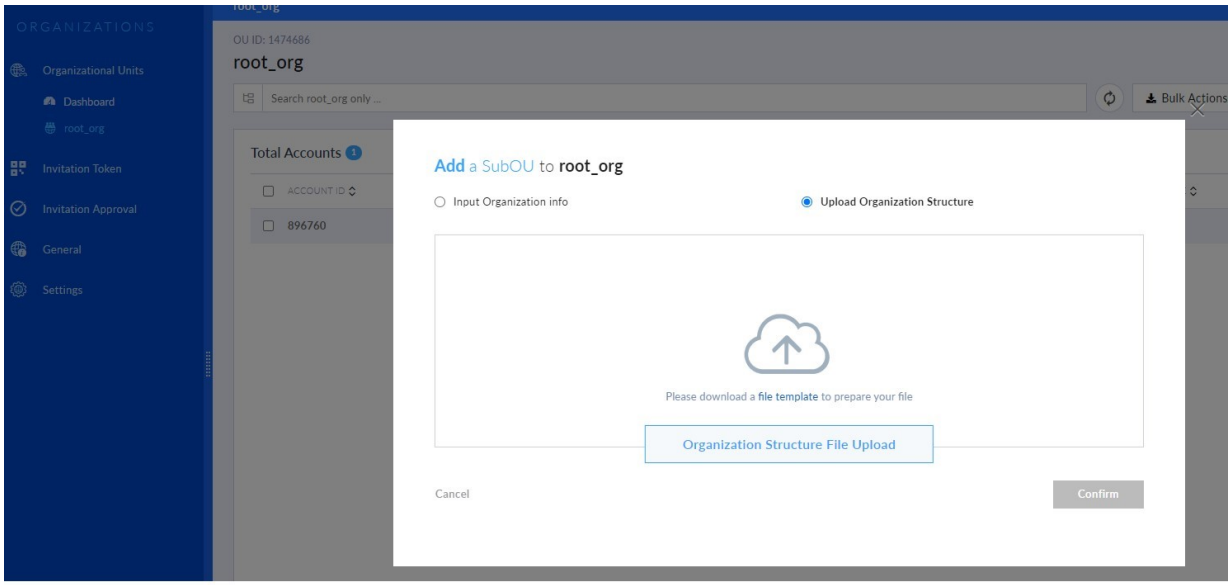
   d. Save the changes in your **Organization Template**.
   e. d. Return to FortiCloud. In the navigation menu, hover over your organization name and click the gear icon.

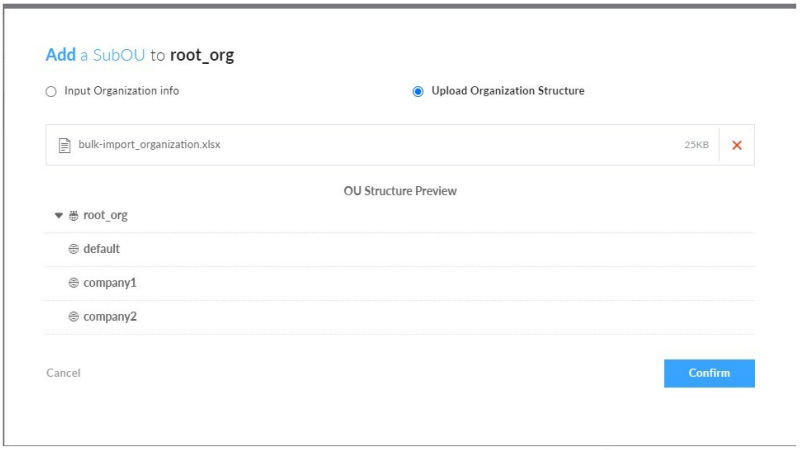


f. Click **Add a SubOU**. The **Add a SubOU to <org_name>** dialog opens.

g.

h. Select **Upload Organization Structure**, and upload the updated template from step **c**. This should auto-populate the **OU Structure Preview** window.

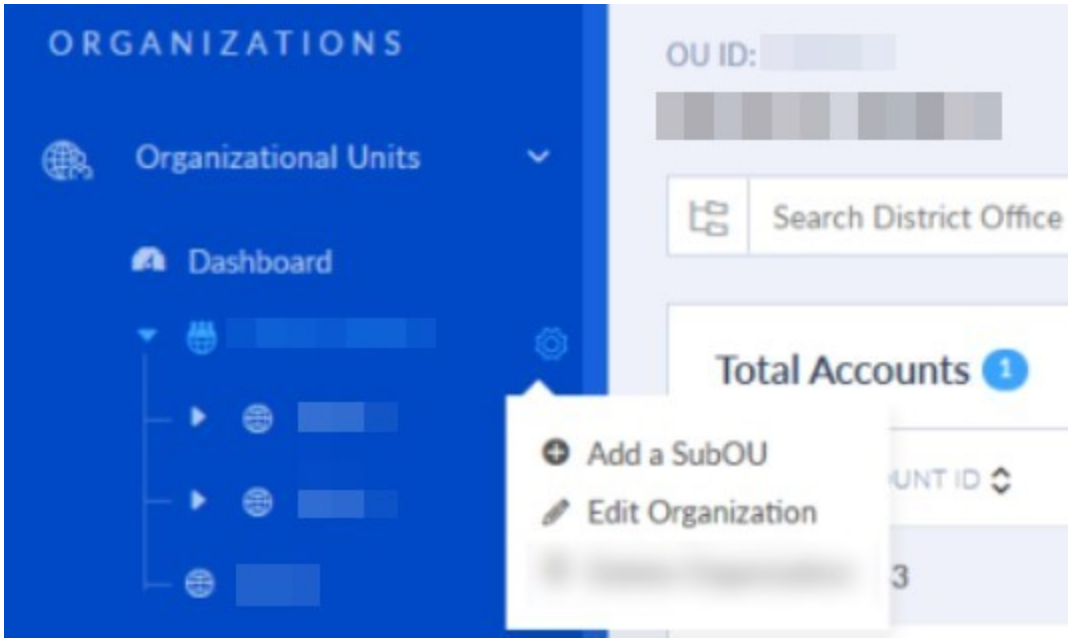




i. Click **Confirm**.

Option 2: Input Organization Info

a. In the **FortiCloud Organizations** navigation menu, hover over your organization name and click the gear icon.



b. Click **Add a SubOU**. The **Add a SubOU to <org_name>** dialog opens.

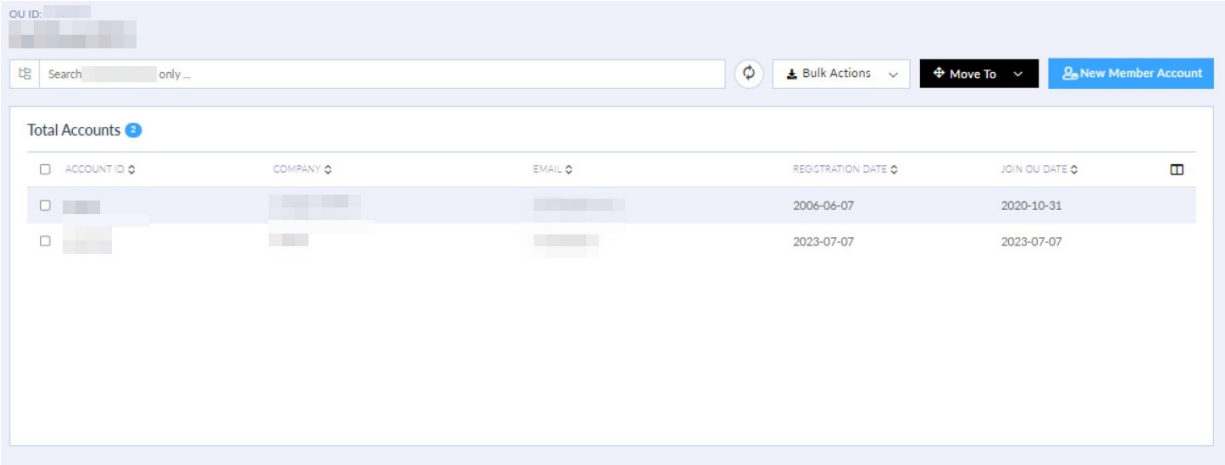
c. Enter the OU Name and OU Description, then click Confirm. The unit is added to the organization.

d. Repeat steps **a** and **b** until all organizations are added as desired.

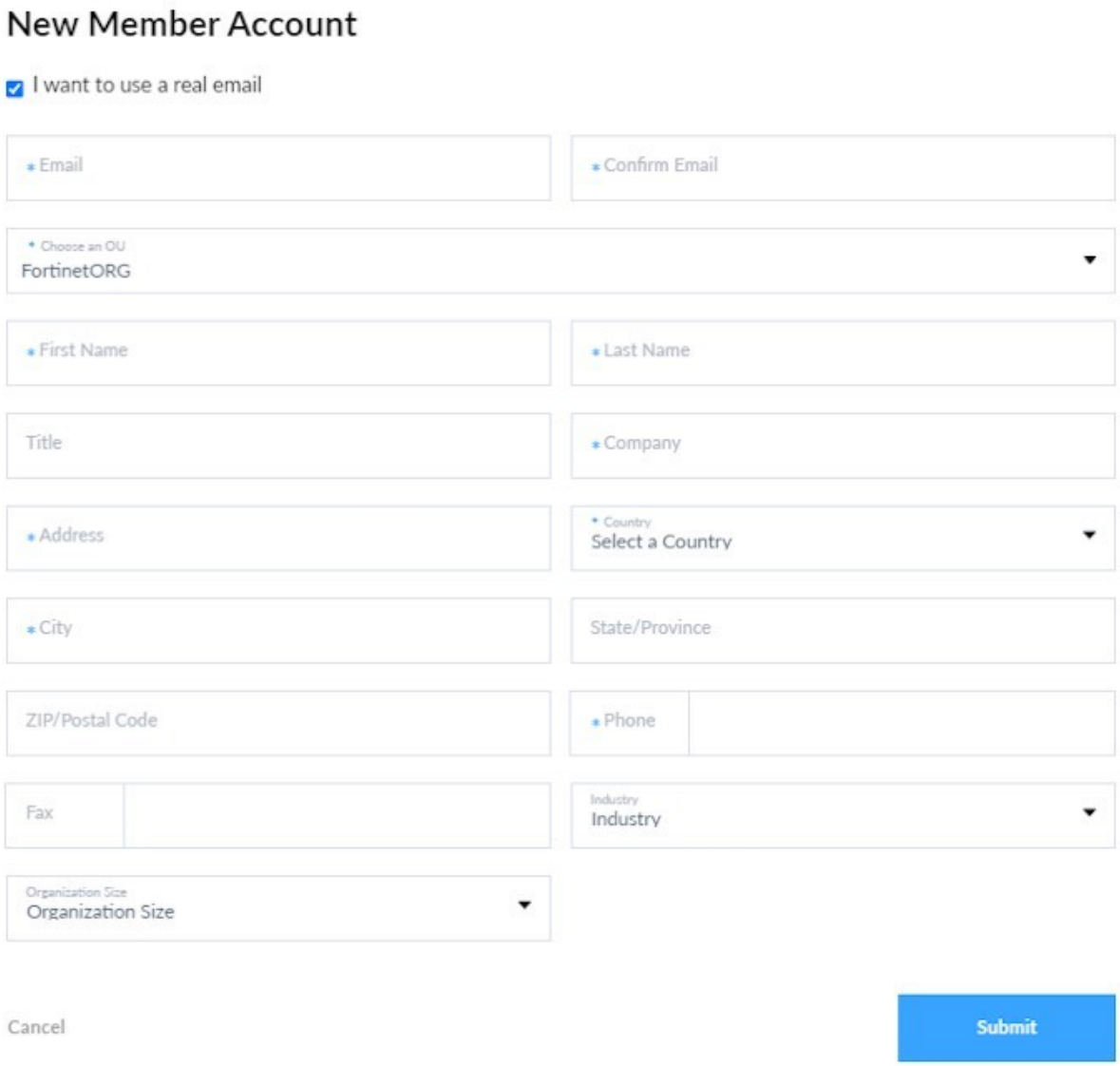
4. Create member accounts for each desired OU. For more detailed information beyond the steps below, please refer to Creating new Member Accounts.

   Since FortiAppSec Cloud resources are tied to member accounts, it is mandatory to create a member account for each desired Organizational Unit (OU).

   a. In the left navigation bar, click on the desired OU under **Dashboard** to navigate to the page shown below.

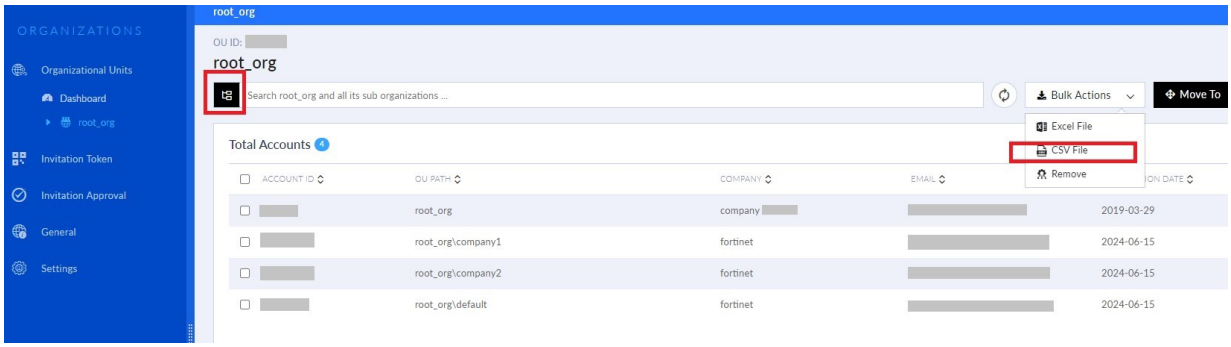


   b. Click **New Member Account**, fill out the **New Member Account** fields as required, and click **Submit**.

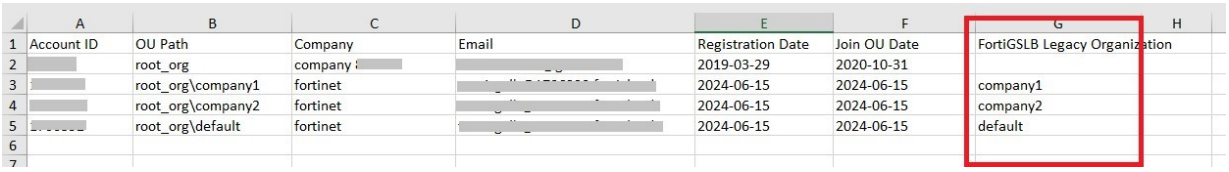


c. Repeat previous steps **a** and **b** until all desired OUs have corresponding member accounts.

5. Export OU structure.
   a. In the left navigation bar, click on the top-level organization.
   b. Click the hierarchy icon to ensure sub-organization units are selected. Then, from the Bulk Actions dropdown list, select **CSV File**.



c. Download the organization file and edit it to include a column specifying the legacy FortiGSLB organization associated with each member account. This ensures we can identify which assets to migrate to the corresponding new member accounts.



	A	B	C	D	E	F	G	H
1	Account ID	OU Path	Company	Email	Registration Date	Join OU Date	FortiGSLB Legacy Organization	
2		root_org	company		2019-03-29	2020-10-31		
3		root_org\company1	fortinet		2024-06-15	2024-06-15	company1	
4		root_org\company2	fortinet		2024-06-15	2024-06-15	company2	
5		root_org\default	fortinet		2024-06-15	2024-06-15	default	
6								
7								

6. If you would like to enable **Contract Sharing Mode**, go to **General > Settings** and enable **Contract Sharing Mode**.
7. Ensure all member accounts log in to the FortiAppSec Cloud portal. This step saves the account information needed for the next phase.
8. Submit a ticket requesting the FortiAppSec GSLB team to complete your migration to FortiCloud OU. Be sure to attach the OU Structure file downloaded and modified in Step 5.

   For guidance on submitting support tickets, please refer to Submitting support tickets on page 464

   Once the ticket is received, the GSLB team will synchronize the new member accounts and root account, binding the legacy FortiGSLB organizations to the corresponding new accounts as specified in the OU structure file.

If you would like to transfer your One-Click device to your new membership account, please wait to do so until the migration is complete.

You can check the status of the migration in the **Ticket Conversation** on FortiCare.

For more information on FortiCare tickets, see Ticket details.

Manage users after migration

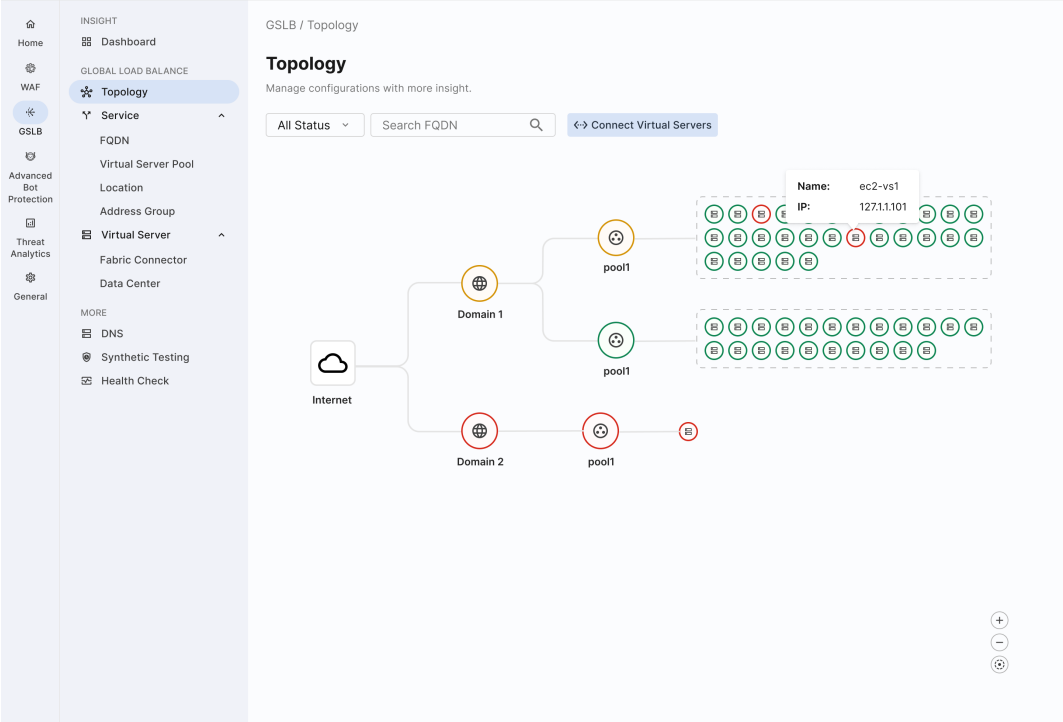
To manage IAM users' access to FortiAppSec Cloud GSLB resources under different member accounts, you can either edit an existing IAM user and set their Type to Organization, or create a new Organization type IAM user.

For details on advanced user management, please refer to FortiCloud Organizational Units on page 453

For instructions on creating a new IAM user, please refer to FortiCloud IAM on page 445

Topology

The **Topology** page provides a clear view of your configuration flow by displaying the relationships between your GSLB objects, helping you gain a deeper understanding of their connections. You can either create objects and their relationships on this page, or individually create each component by following the instructions on Onboarding GSLB Applications on page 316.



Configure Topology

1. **Add Fabric connectors and Virtual Servers**

   If you have a physical Fortinet device (e.g., FortiGate) and want to start with server management, begin with this step. If you prefer to focus on network identity and are familiar with DNS, proceed to the next step to set up your FQDN.

   a. Click **Connect Virtual Servers** to configure fabric connectors and virtual servers.

      Connectors in GSLB are linked to a physical device at the data center which houses virtual servers, from which the cloud can fetch all the virtual servers running information.

      For more information on the configuration options on this page, please refer to Fabric connector on page 353.

2. **Add FQDN**

   An FQDN object maps a fully qualified domain name (FQDN) to a set of virtual servers (pool). For additional details on FQDNs, please refer to FQDN on page 338.

   a. Return to the **Topology** page, and right-click **Assigned DNS Server**.

   b. Click **Add FQDN**.

      For more information on the configuration options for this object, please refer to FQDN on page 338.

   c. Click **Save** to return to the **Topology** page.

3. **Add Virtual Server Pool**

   a. On the **Topology** page, right-click the FQDN you added in the previous step.

   b. Click **New Virtual Server Pool**.

      For more information on the configuration options for this object, please refer to Virtual Server Pool on page 348.

      Click **Save** to return to the **Topology** page.

4. **Add Virtual Server to Virtual Server Pool**

a. On the **Topology** page, click **Connect Virtual Servers**.
b. Add the desired Virtual Servers you configured in step 1 to the Virtual Server Pool(s) you created in step 3. We recommend placing virtual servers with similar functions or locations into the same pool.

Edit Topology

To edit the relationship between objects in your Topology, click and edit an object to remove or add a child object in Topology tree.

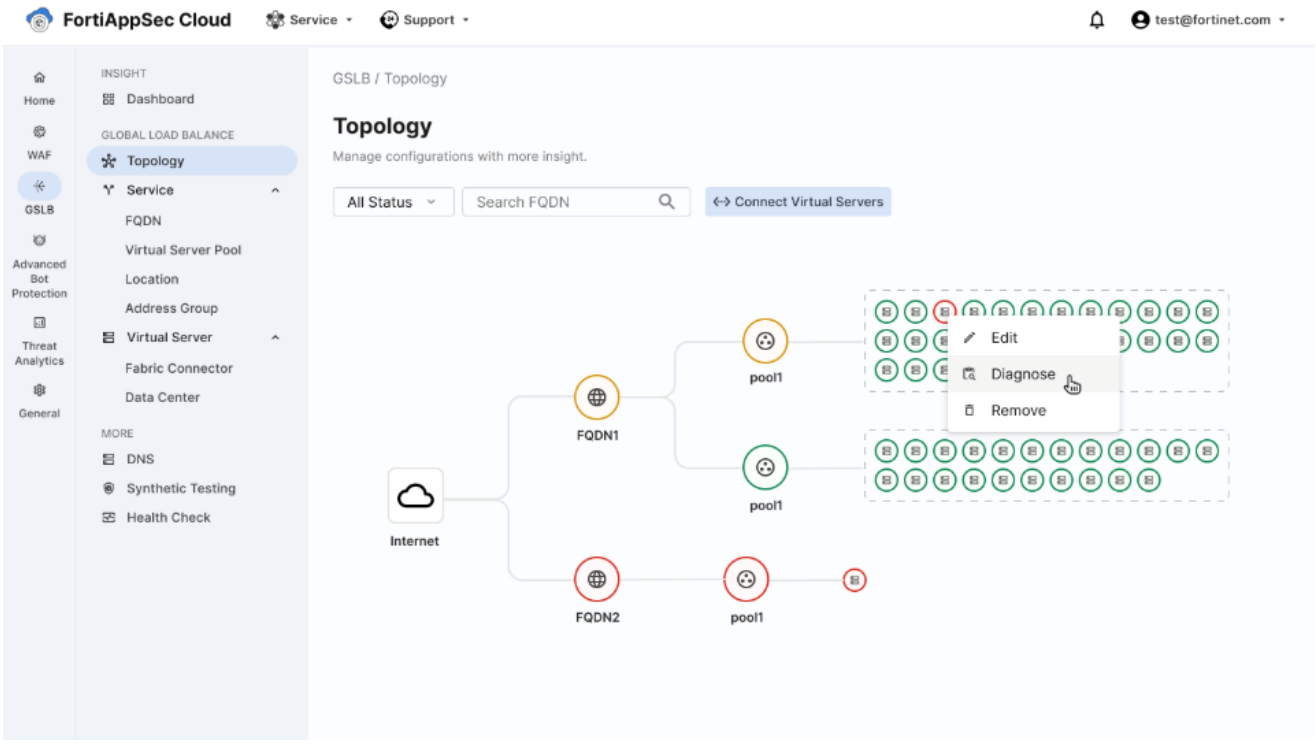
To edit settings on individual objects:

1. Right-click the object you would like to edit.
2. Click **Edit** to open a modal window with configuration options for the selected object.
3. Make the desired changes.
4. Click **Save**.

Run Diagnostics

Run diagnostics on Virtual Servers, Fabric Connectors, and Health Checks directly from the GSLB Topology view by right-clicking the item and selecting **Diagnose**.

This displays further details on its status such as associated health check, region, and error message if applicable.

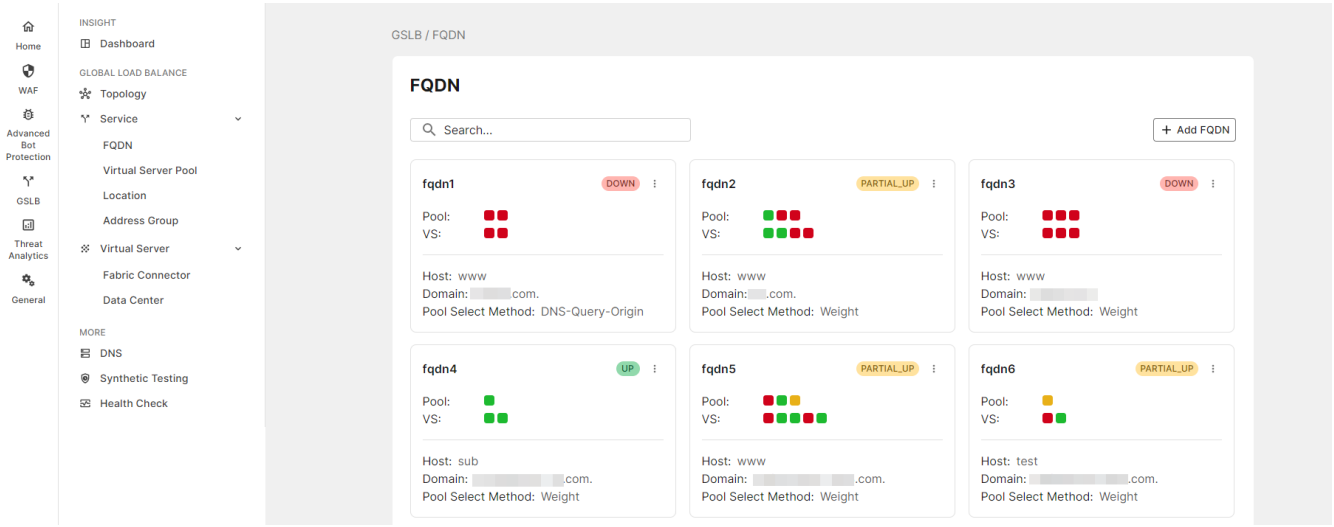


Service

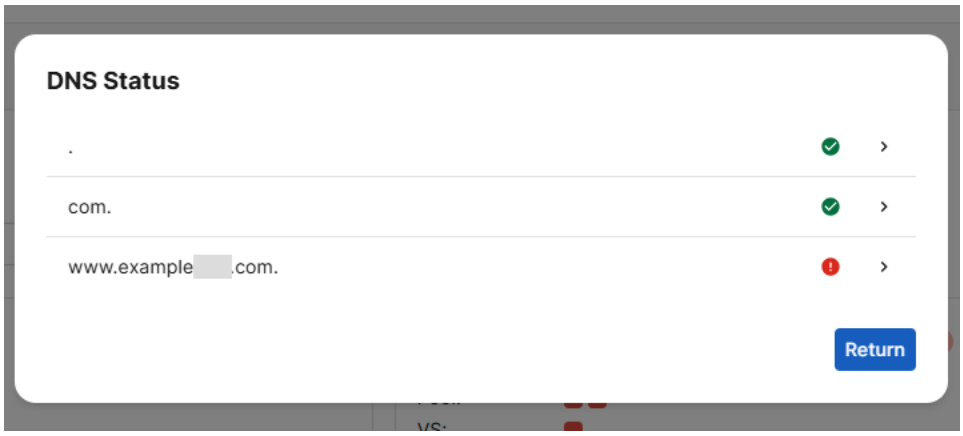
- FQDN
- Virtual Server Pool on page 348
- Synthetic testing on page 371
- Location on page 351
- Address group on page 353

FQDN

The FQDN object is a GSLB Service. An FQDN object will map a fully-qualified domain name (FQDN) to a set of virtual servers (pool). Administrators can set a global geographic policy in this object. After the administrator has defined the pool objects and the location objects, a pool object can bind a location object as a member for the FQDN object, and the FQDN object can define multiple members. When the DNS queries are trying to reach the GSLB, it will do the first level load balance according the virtual server pool selection method. Then, the DNS queries will be forwarded to a pool and the virtual servers will respond according to the pool's preferred schedule methods for the queries.



To view the DNS status of an FQDN, click the three-dot menu next on an FQDN object, then select **Check DNS Status**.



Creating an FQDN

1. Click **Add FQDN**.
2. Enter the following:
3.

Settings	Guidelines
Name	The name of the FQDN. This cannot be modified after the FQDN is created.

Settings	Guidelines
Host Name	The hostname part of the FQDN, such as www. Note: You can specify the @ symbol to denote the zone root. The value substituted for @ is the preceding $ORIGIN directive.
Domain Name	The domain name must end with a period. For example: example.com. This cannot be modified after FQDN is created.
Respond Single Record	Enable/disable an option to send only the top record in response to a query. Disabled by default. By default, the response is an ordered list of records.
Virtual Server Pool Selection Method	Virtual Server Pool Selection Method: Weight: DNS queries will be load balanced to pool by weight, and the virtual server will respond according to the pool's preferred schedule methods. DNS-Query-Origin: DNS queries will be load balanced to the pool with the same geographic information as the local DNS address, and the virtual server will respond according to the pool's preferred schedule methods. Global-Availability: DNS queries will be load balanced to the first available pool in the FQDN pool member list, and the virtual server will respond according to the pool's preferred schedule methods.
Default Feedback IPv4	Specify an IP address to return in the DNS answer if no virtual servers are available.
Default Feedback IPv6	Specify an IPv6 address to return in the DNS answer if no virtual servers are available.

Configuring FQDN members text field

Settings	Guidelines
Name	The name of the member
Virtual server pool	Specify a pool for this FQDN.
Weight	Assign a weight. Valid values range from 1 to 255.
Location List	Bind a location for the pool. A location list configuration consists of a list of locations you select. **Note**: The **any** location object is a default configuration that includes all regions in the database. When the **any** location list is applied, all traffic that do not match the other locations will then match to any other region that has not been specified.
Address Group	Bind an address group for the pool. An address group configuration consists of a list of IP/Netmasks or IP ranges. **Note**: IP/Netmasks: 0.0.0.0/0 indicates all IPv4 IP addresses.

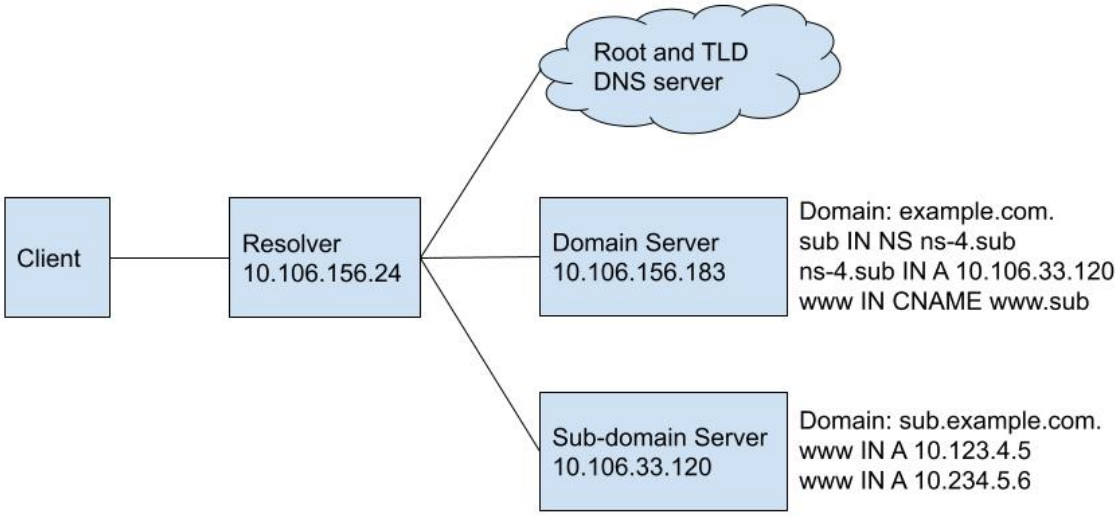
FQDN service logs

Refer to FQDN Logs for more information.

How to make an existing FQDN work with GSLB

Example: You have an existing domain ‘example.com’ running on a DNS server that does not support global app load balance. Your FQDN ‘www.example.com' pointed to a single host 10.123.4.5. When business grew, you brought in another server 10.234.5.6 also have this service.

Now you would like to have global app load balancing for the FQDN. However, you still want your other FQDNs running on your existing DNS server. To do this, change the A record for ‘www.example.com’ to a CNAME record, and point it to ‘www.sub.example.com’. Add ‘sub.example.com’ as a sub-domain. Then configure ‘www.sub.example.com’ global app load balance service on GSLB.



Steps

1. Configure the GSLB for sub-domain 'sub.example.com'.
   a. Go to *DNS Services* and click *Create DNS Services* or *Create New*. Add a DNS service for the sub-domain and name the Primary Server Name as ns-4. The DNS server address in this example is 10.106.33.120.
   b. Add a FQDN service for 'www.sub.example.com'. For detailed instructions, see Setting up an FQDN with Generic-Host connector on page 379.
2. Configure the ‘sub.example.com’ as a sub-domain of ‘example.com’ by adding a NS record in the domain configuration. You may need a NS record that points ‘sub.example.com’ to ‘ns-4.sub.example.com’, and another A record that points ‘ns-4.sub.example.com’ to 10.106.33.120.
   The following is an example from FortiADC. The FortiADC will automatically create these two records according to the configuration settings.
3. Remove the old A record for 'www.example.com' and replace it with a CNAME record. Alias 'www.example.com.' to the Target Name 'www.sub.example.com.'.
   CNAME Record example from FortiADC
4. Verify the configuration by querying the resolver 10.106.156.24 using any of the following methods. We recommend using `dig` for Linux, and `nslookup` or `Resolve-DnsName` for Windows.
   The expected query output is as follows:
   Linux - `dig`
   Windows - `nslookup`
   Windows - `Resolve-DnsName`

If you configure steps 1 – 3 correctly, your host should now be able to load balance between two data centers. You can test this by querying the pubic DNS resolver 8.8.8.8 multiple times and seeing the order of the two IP address change when the TTL counts down.

Debugging

If verification fails, the user will need to debug according to the steps below:

1. Test the sub-domain A record by querying the sub-domain DNS server 10.106.33.120 directly.
   Linux - `dig`

```
[root@localhost ~]# dig @10.106.33.120 www.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.33.120 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44587
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    5       IN      A       10.234.5.6
www.sub.example.com.    5       IN      A       10.123.4.5

;; AUTHORITY SECTION:
sub.example.com.        120     IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   120     IN      A       10.106.33.120

;; Query time: 3 msec
;; SERVER: 10.106.33.120#53(10.106.33.120)
;; WHEN: Thu Jun 17 17:08:08 EDT 2021
;; MSG SIZE  rcvd: 115
```

Windows - `nslookup`

```
C:\Users\ [redacted] >nslookup www.sub.example.com 10.106.33.120
Server:  UnKnown
Address:  10.106.33.120

Name:    www.sub.example.com
Addresses:  10.123.4.5
          10.234.5.6
```

Windows - `Resolve-DnsName`

```
PS C:\Users\        > Resolve-DnsName -Server 10.106.33.120 -Name www.sub.example.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.sub.example.com                            A      5     Answer     10.234.5.6
www.sub.example.com                            A      5     Answer     10.123.4.5

Name       : sub.example.com
QueryType  : NS
TTL        : 120
Section    : Authority
NameHost   : ns-4.sub.example.com

ns-4.sub.example.com                           A      120   Additional 10.106.33.120
```

a. If the test fails, remove all other records from Zone service and try again. The Zone service may take a minute to reload after the configuration changes.

2. Test the NS record by querying the domain server 10.106.156.183.

Linux - `dig`

```
[root@localhost ~]# dig @10.106.156.183 sub.example.com ns

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.183 sub.example.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23956
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.example.com.               IN      NS

;; ANSWER SECTION:
sub.example.com.        90      IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   100     IN      A       10.106.33.120

;; Query time: 1 msec
;; SERVER: 10.106.156.183#53(10.106.156.183)
;; WHEN: Thu Jun 17 17:17:48 EDT 2021
;; MSG SIZE  rcvd: 79
```

Windows - `nslookup`

```
C:\Users\          >nslookup -q=NS sub.example.com  10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

Non-authoritative answer:
sub.example.com nameserver = ns-4.sub.example.com

ns-4.sub.example.com    internet address = 10.106.33.120
```

Windows - `Resolve-DnsName`

```
PS C:\Users\          > Resolve-DnsName -Server 10.106.156.183 -Name sub.example.com -Type NS

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
sub.example.com                NS     53    Answer     ns-4.sub.example.com

Name       : ns-4.sub.example.com
QueryType  : A
TTL        : 53
Section    : Additional
IP4Address : 10.106.33.120
```

a. If the test fails, check to see if the NS record conflicts with any other records in the Zone configuration.

3. Test the CNAME record by query the Domain DNS server 10.106.156.183.

Linux - `dig`

```
[root@localhost ~]# dig @10.106.156.24 www.example.com cname

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 www.example.com cname
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43925
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      CNAME

;; ANSWER SECTION:
www.example.com.        34      IN      CNAME   www.sub.example.com.

;; Query time: 2 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Tue Jul 06 21:03:37 EDT 2021
;; MSG SIZE  rcvd: 66
```

Windows - `nslookup`

```
C:\Users\[redacted]>nslookup -q=cname www.example.com 10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

www.example.com canonical name = www.sub.example.com
example.com     nameserver = ns.example.com
ns.example.com  internet address = 10.106.156.183
```

Windows - `Resolve-DnsName`

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.183 -Name www.example.com -Type CNAME

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
www.example.com                CNAME  180   Answer     www.sub.example.com
example.com                    NS     180   Authority  ns.example.com

Name       : ns.example.com
QueryType  : A
TTL        : 180
Section    : Additional
IP4Address : 10.106.156.183
```

a. If the test fails, check to see if the CNAME record conflicts with any other records in the Zone configuration.

How to add generic SD-WAN device to GSLB

Follow the steps to add the generic SD-WAN device to GSLB.

1. Create FQDN in **GSLB Services > Create FQDN Member > Create new Virtual Server Pool > Create new generic connector > Create new connector member** (add Generic SD-WAN device IP).
2. The virtual server from the generic SD-WAN connector will be added into Pool and Connector directly and will work in GSLB Services.

Example solution

This example assumes the following:

- You have two ISP routers.
- The generic SD-WAN has two members for each ISP. The SD-WAN will do the out-going load balance for App1 (as shown on the right side of the diagram). But sometimes,the incoming traffic may come always from ISP2, which means that the ISP2 link is very busy while ISP1 link is very free.
- The GSLB can load balance the incoming traffic to ISP1 link and ISP2 link from the DNS level, thus solving this issue.

Steps:

1. Create FQDN App1-www.fsdwan.com in GSLB services.

2. Create FQDN member > Create new Virtual Server Pool ISP1-pool > Create new generic connector sdwandevice > Create new Connector member VIP1-ISP1. Add generic SD-WAN device Virtual IP App1 ISP1 Public IP 202.0.20.21 and enable health check Default_HLTHCK_HTTP.
3. Create FQDN member > Create new Virtual Server Pool ISP2-pool > Select Connector sdwandevice > Create new Connector member VIP2-ISP2. Add generic SD-WAN device Virtual IP App1 ISP2 Public IP 54.20.0.22 and enable health check Default_HLTHCK_HTTP).
4. The virtual server from the generic SD-WAN device will be added into Pool and Connector directly and will work in GSLB services.

Sample topology view of GSLB

We have added 2 pools to perform the load balancing and each pool has a VIP.

After completing these steps, the customer can monitor the App1 status for both ISP1 link and ISP2 link on the FQDN service detail page. The GSLB will load balance the traffic to two links. If one of the links is down, the GSLB will direct the traffic to the available link. If both of the links are down, the GSLB will direct the traffic to the App1 default server.

How to load-balance by geolocation

The **GEO** load balancing method directs traffic based on the geographic location of the client, typically using the source IP address. This method helps route users to the nearest or most appropriate regional endpoint, improving performance and supporting data residency compliance.

Geolocation matching is based on the source IP address relative to the data center location specified in the connector associated with the virtual server. The matching follows this order:

1. Region (e.g., state or province)
2. If no region match, fall back to country
3. If no country match, fall back to continent
4. If no continent match, use Weighted Round Robin

Example: One virtual server is configured in US–California.

- A query from a source IP in Canada will also match this virtual server if no other virtual server exists anywhere in the US.
- A query from a source IP in US–Oregon will match this virtual server if no other virtual server exists in US–Oregon.

Configure load balancing by geolocation

1. Create FQDN in GSLB Services and create an FQDN member.



If your deployment requires strict geographical matching, we recommend enabling the **Respond Single Record** option under FQDN settings.

2. Create a new Virtual Server Pool and use **GEO** preferred method in Pool.
3. Choose existing virtual servers for Pool. You can also create several new connectors with different Data Centers. Create new Connector member (Virtual Server) into Connectors.
4. The FQDN will respond to the DNS query according to the virtual server's location in Connectors and the DNS query's source IP.

How to set up the load balance method DNS-Query-Origin

Perform the following steps to setup the load balance method DNS-Query-Origin.

1. Create FQDN in GSLB Services and choose DNS-Query-Origin as the Virtual Server Pool Selection Method.
2. Create multiple FQDN members.
   a. Click *Create Member* in FQDN and choose Virtual Server Pool.
   b. Click *Create Location List* and add location(s) to list (if needed).
   c. Click *Create Address Group* and then add the IP/Netmasks or IP ranges as address members (if needed).
   Create second Virtual Server Pool with other location(s) using the steps above.
3. Add the virtual servers into Virtual Server Pool. The FQDN will respond to the DNS query according to the Virtual Server Pool's listed location(s) and DNS query's source IP.

Note: If you want to use DNS-Query-Origin for matching Virtual Server Pool, all query source IP locations should be added to the location list or all corresponding IP/Netmasks or IP ranges should be added to the address group. Otherwise it uses Weight Round Robin method.

Example 1: Use only Location list

- Define one Location: *United_States*
- Assign Location United_States to virtual server pool: *Virtual_Server_Pool_US*
- Define second Location: *Germany*
- Assign Location Germany to virtual server pool: *Virtual_Server_Pool_Germany*

Result:

Queries from the United States will get replied from Virtual_Server_Pool_US, queries from Germany will get replied from Virtual_Server_Pool_Germany, queries other than these two countries will use Weight Round Robin between those two virtual server pools.

Example 2: Use Location list together with Address Group

Following the scenario set in *Example 1*, after having run the configuration for a while, you are finding that some particular source IP from the United States (here we are using 8.8.8.8 and 8.8.4.4 as an example) is not always getting replies from the Virtual_Server_Pool_US.

- Define an Address Group: *United_States_IPs* and add AddressNet 8.8.8.8/32 and AddressRange 8.8.4.4-8.8.4.4 as the members
- Assign Address Group *United_States_IPs* to virtual server pool *Virtual_Server_Pool_US*

Result:

Queries from 8.8.8.8 and 8.8.4.4 will also get replied from *Virtual_Server_Pool_US*.

Example 3: Use only Address Group

- Define one Address Group: *Google_Resolvers*
- Add AddressNet 8.8.8.8/32 and AddressRange 8.8.4.4-8.8.4.4 as the members
- Assign Address Group *Google_Resolvers* to virtual server pool *Pool_for_Google*
- Define another Address Group: *any_IP*
- Add AddressNet 0.0.0.0/0 as the member
- Assign Address Group *any_IP* to virtual server pool *Pool_General*

Result:

Queries from 8.8.8.8 and 8.8.4.4 will get replied from virtual server pool Pool_for_Google. Queries from other IP addresses will get replied from virtual server pool Pool_General.

Note: Although 8.8.8.8 and 8.8.4.4 are also included in the Address Group *any_IP*, the GSLB service is matching the virtual server pool by the sequence they are in the FQDN configuration. They will match the Address Group *Google_Resolvers* first, and get replied from *Pool_for_Google*.

Example 4: Use city-level location list

- Define one Location: *CA_Sunnyvale*
- Assign Location *CA_Sunnyvale* to virtual server pool *Virtual_Server_Pool_CA_Sunnyvale*
- Define second Location: *CA_ Sacramento*
- Assign Location *CA_ Sacramento* to virtual server pool *Virtual_Server_Pool_CA_Sacramento*

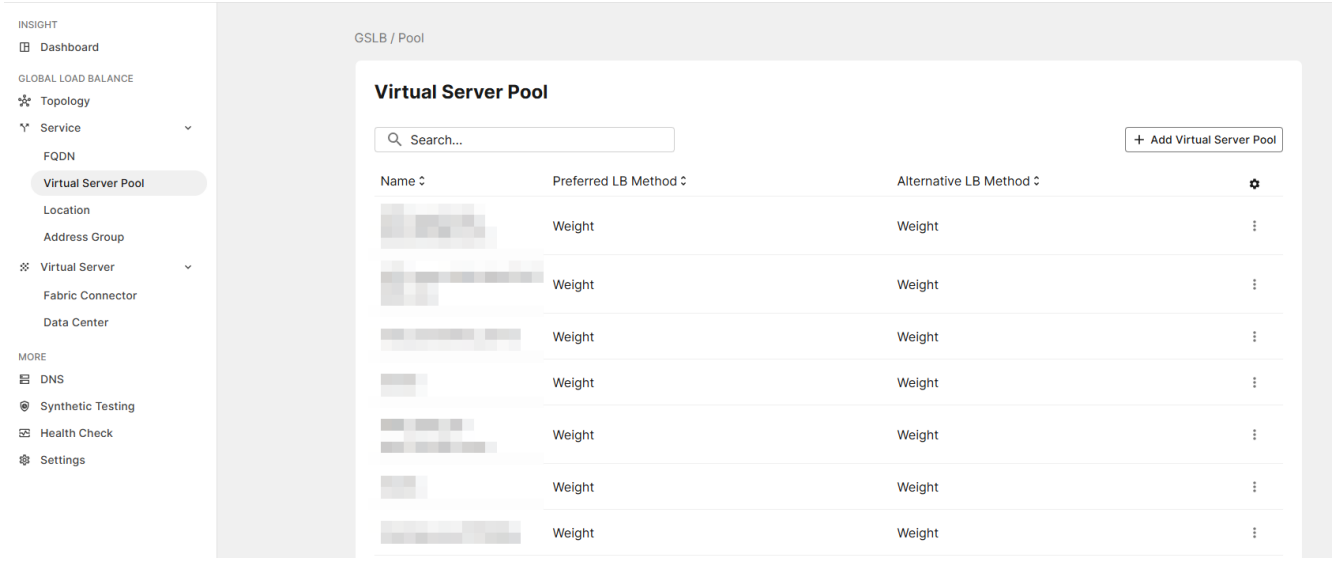
Result:

Queries from Sunnyvale will get replied from Virtual_Server_Pool_CA_Sunnvayle, queries from Sacramento will get replied from Virtual_Server_Pool_CA_Sacramento.

Virtual Server Pool

The Virtual Server Pool is a group of virtual servers that perform the same role on the network. The administrator puts the virtual servers with the same role in a pool. The administrator can also divide a pool into several sub pools based on geographic location.

For more information on virtual servers, please see Virtual Server on page 353.



Add Virtual Server Pool

1. Click **Add Virtual Server Pool**.
2. Enter the following:

Settings	Guidelines
Name	Name of the pool
Preferred LB Method	The preferred Load Balancing (LB) method determines how traffic is distributed among virtual servers associated with a specific FQDN. **WEIGHT**: GSLB distributes traffic using the weighted round-robin method, directing more requests to resources with higher assigned weights. **GEO**: GSLB performs load balancing according the request's source geographic location. **Least-Connection** (FortiADC): GSLB will load balance the traffic to the virtual server which has the least connections. **Connection-Limit** (FortiADC): GSLB will perform load balancing according to the virtual servers' connection limit determined by the virtual servers' weight: the greater the weight of a virtual server, the more responses it will get. **Bytes-Per-Second** (FortiADC): GSLB will load balance the traffic to the virtual server which has the least BPS. **Server-Performance** (FortiADC/FortiGate): GSLB will load balance the traffic to the server which has the lowest load (memory and CPU). Virtual servers with better server-performance in the CPU or Memory (whichever one you give more weight to) will respond. **SDWAN-InBandwidth** (FortiGate): GSLB load balances the traffic to the virtual server which has the lowest InBandwidth for the related SD-WAN gateway.

Settings	Guidelines
	SDWAN-OutBandwidth (FortiGate): GSLB load balances the traffic to the virtual server which has the lowest OutBandwidth for the related SD-WAN gateway. **SDWAN-BiBandwidth** (FortiGate): GSLB load balances the traffic to the virtual server which has the lowest sum of InBandwidth and OutBandwidth for the related SD-WAN gateway.
Alternate	Enable this option to specify a load balancing method to use as a backup if the primary method becomes unavailable or fails to meet required conditions, such as health check failures. If the alternative method is unable to select a server, the system defaults to the **WEIGHT** method. Refer to **Preferred LB Method** above for a complete list of load balancing methods and their descriptions. **Note**: This option is not supported when **WEIGHT** is selected as the preferred load balancing method. **Example use case:** An organization operates two virtual servers, one in the United States and one in Singapore. The preferred method is **GEO**, and the alternative method is set to **Least-Connection**. • Queries originating from the United States or Singapore are routed geographically to the corresponding local servers, as determined by the preferred method. • Queries originating from other locations are routed using the alternative **Least-Connection** method, directing traffic to the server with the fewest active connections. • If both servers have the same number of connections, traffic from outside the United States and Singapore is distributed using Weighted Round-Robin (**WEIGHT**), alternating requests based on each server's assigned weight.
Check Virtual Server Status	Enable/disable checks on whether the status of the virtual servers in the virtual server list is known. Virtual servers with unknown status are not selected for DNS answers.

3. Click **Add Virtual Server**. This opens a modal window.

Settings	Guidelines
Virtual Server	Select a virtual server that you have created to add it to this Pool. For information on how to configure Virtual Servers, please refer to
TTL	The Time to Live of the Resource Records, which defines how long DNS servers cache the server's details before refreshing. Lower TTL values allow quicker updates, while higher values reduce lookup frequency and improve caching efficiency. Default: 5; Range: -1 to 2147483647. When this value is -1, it means the virtual server will use the zone level TTL.

Settings	Guidelines
Weight	Assigns relative preference among virtual servers—higher values are more preferred and are assigned connections more frequently. The default is 1. The valid range is 1-255.
Backup	Enable to designate the member as a backup. Backup members are inactive until all main members are down.

4. Click **Save** to save the Virtual Server.
5. Click **Save** to save the Virtual Server Pool.

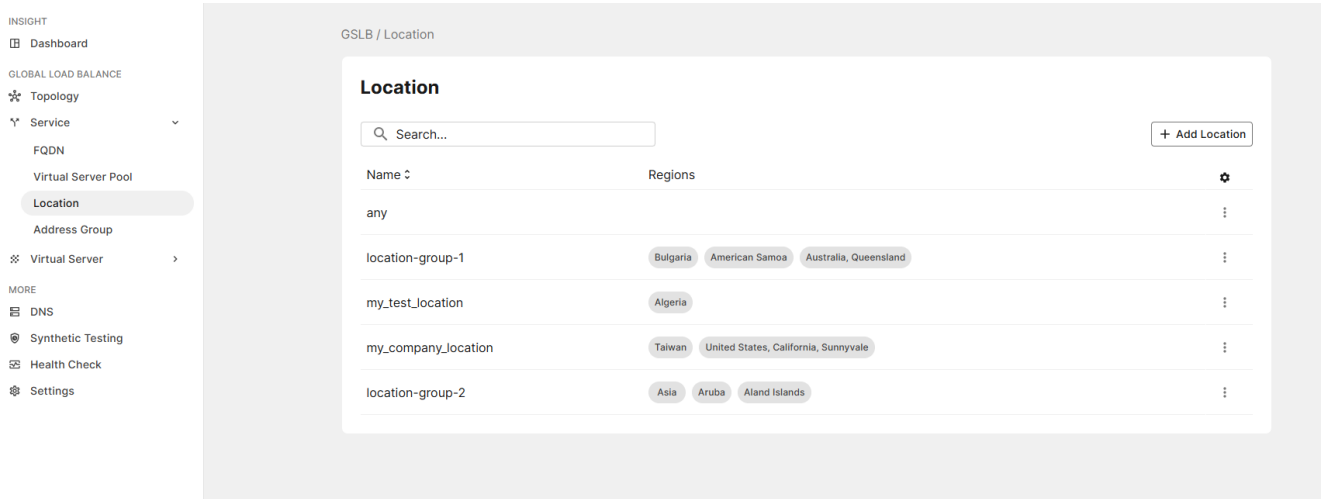
Location

The location object is a group of GeoIP regions. GSLB is able to detect requests from all countries and regions in the world and is accurate to the city level of G20 countries.

Each location object must contain at least one location record, with a maximum of 50 location records supported per location object.

When configuring multiple location records, ensure that each record specifies distinct GeoIP regions that do not overlap, otherwise it results in an invalid configuration. For example, if one record specifies the continent as Asia, and another record specifies the country as Japan; these two GeoIP regions would overlap as Japan is already a part of Asia, resulting in an invalid Location configuration.

After you have configured the location object, you can then use it as the location list in GSLB services. For more information, see FQDN on page 338.

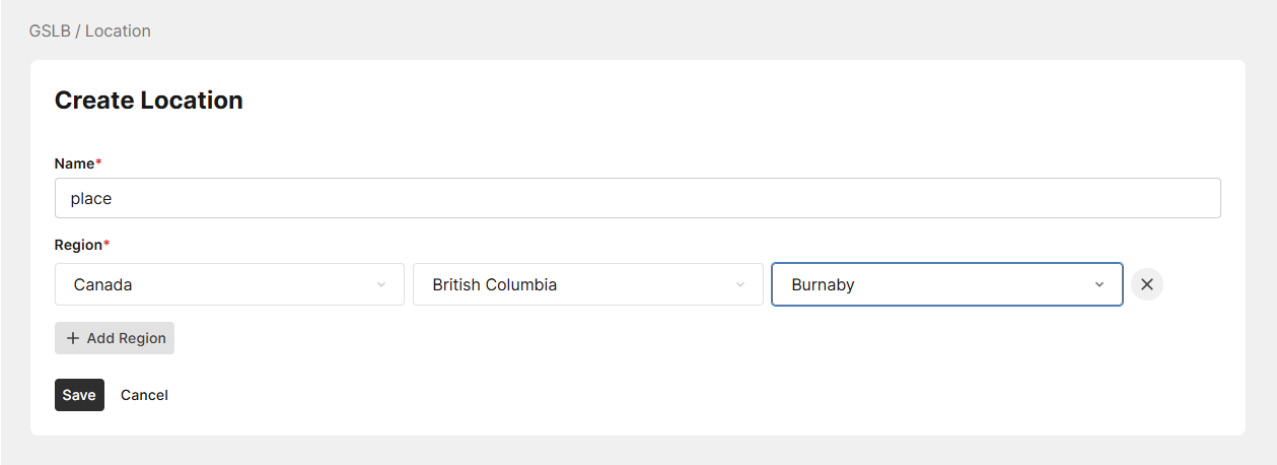


Note: **any** is a predefined location object that includes all regions in the database by default.

To configure a location object:

1. Go to **GSLB > Service > Location**.
2. Click **Add Location** to display the configuration editor.

3. In the **Name** field, specify a unique name for the location configuration.
   Valid characters are `A-Z`, `a-z`, `0-9`, `_`, and `-`. No spaces. After you initially save the configuration, you cannot edit the name.
4. Click **Add Region** to add a location record.
   At least one **Region** must be added for a location object.



5. Configure the following Location settings:

Setting	Description
Continent/Country	Specify the continent or country to include in the GeoIP region. The *Continent/Country* selection determines the availability of the *State* and *City* options. *ALL* is the default option, which specifies that all continents/countries is included in this GeoIP region. **Note**: At minimum, a continent or country must be selected for a location record to be valid.
State/Province	Specify the state to include in the GeoIP region. The availability of *State* options is dependent on the selected *Continent/Country*. *ALL* is the default option, which specifies that all states under the specified continent/country is included in this GeoIP region.
City	Specify the city to include in the GeoIP region. The availability of *City* options is dependent on the selected *Continent/Country* and *State*. *ALL* is the default option, which specifies that all cities under the specified state is included in this GeoIP region.

6. Optionally, you can add multiple location records under the same location object, with up to 50 location records supported per single location object. However, a Location configuration becomes invalid if multiple location records share the same GeoIP region specification.
   Beware of the following scenarios that can result in this type of configuration conflict:
   - When separate location records specify regions that overlap, such as when both Asia and Japan are selected as the **Continent/Country**. As Japan is a part of Asia, the two GeoIP regions overlap.
   - When one of the location records is set as **ALL** for **Continent/Country**, **State**, and **City** levels. If the **Continent/Country** is set to **ALL**, then it would naturally overlap with any other location record that specifies a continent or country. However, by default, a location record is already invalid if **ALL** is set for **Continent/Country**.

7. Click **Save**.
   The new location object will be listed on the Location page.

Address group

The address group object is a group of IP intervals in the form of IP/Netmasks or IP ranges.

Create Address Group

1. Click Add Address Group
2. Enter the **Name** of the address group.
3. Click **Add Address Group member**. This opens a modal panel for configuring the Address Group Member's settings.
4. Select the Address Type, and enter the Net or Range.

   Address Net refers to an entire subnet or network of IP addresses, defined by a network address and a subnet mask.

   An example of an **Address Net** entry would be 10.0.0.0/24

   Address Range specifies a continuous range of IP addresses, usually defined by a starting and ending IP address.

   An example of an **Address Range** entry would be: **Address Range Start:** 10.0.0.0, **Address Range End:** 10.0.0.255

Virtual Server

Manage connections between your FQDNs and external resources, such as fabric connectors and data centers.

There are two types of virtual servers:

- Fabric connector on page 353
- Data center on page 357

Fabric connector

Connectors in GSLB are linked to a physical device at the data center which houses virtual servers, from which the cloud can fetch all the virtual servers running information.

You can either create a connector manually in the FortiAppSec Cloud GUI, or enable a One-Click DNS service on a FortiADC/FortiGate/FortiWeb appliance, which will automatically create the connector and GSLB service.

Create Connector manually

1. Go to **Virtual Servers > Fabric Connectors** and click **Create Connector**.
2. Create a connector according to the following configuration.

Settings	Guidelines
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	GSLB can support three types of connectors: **1.** FortiGate The FortiGate Connector is for a FortiGate device. The administrator can edit the FortiGate Management IP address or FQDN, port, API version, sync control and authentication for the connector. Once the Fortigate Connector is configured, GSLB will sync the Virtual Server and SD-WAN configuration and run information from the FortiGate host periodically through RestAPI and update automatically. The administrator can specify the SD-WAN member name with the virtual server. The administrator can also create the virtual server manually or specify the health check for the virtual server. **2.** FortiADC A FortiADC instance that has enabled GSLB. The FortiADC type connetor is the FortiADC device that runs GSLB service. Once the device connects to the cloud, it will actively connect to the cloud. Then the connector object will be generated automatically, and the administrator will define the Virtual Servers' domains and hosts at the connector side in just one step. FortiADC will send the Virtual Servers' domains, hosts, running information to the cloud periodically, while the cloud will perform global servers load balancing automatically. The administrator can also create the virtual server manually or specify the health check for the virtual server. **3.** Generic-Host A third party FortiADC connector. The Generic-Host type connector is a third party host system that cannot communicate with the cloud directly. The administrator can add the host IP address on this server, and the administrator cloud can also specify the health check for the host. The cloud will detect the remote host automatically, then the administrator can configure the pool, the GSLB service. **4.** FortiWeb A FortiWeb instance that has enabled one-click GSLB service. The FortiWeb type connector is the FortiWeb device that enable GSLB service as fabric connector. Once the device connects to the GSLB, it will publish the polices with hosts and domains to GSLB, and GSLB will create connector object and GSLB service automatically. **5.** AWS The Fabric Connector is for AWS. The administrator can create a connector and virtual servers from a specified AWS region with the provided *Access Key* and *Access Secret.* **6.** AZURE The Fabric Connector is for AZURE. The administrator can create a connector and virtual servers from a resource group in a specified AZURE location using the provided *Tenant ID*, *Client ID*, *Client Secret* and *Subscription ID*.

Settings	Guidelines
Data center	Select a data center configuration object. The data center indicates the physical geography location of the connector.
Address type	IPv4 or FQDN
Address IPv4	FortiGate management IPv4 address
Address	FQDN address
Port	FortiGate administrative access port for HTTPS. Default: 443, Range: 1-65535
API version	The restful API version that GSLB can use when access FortiGate . Currently only v2 is supported
Sync control	User can configure to sync SD-WAN and/or Virtual Server configuration and running information from FortiGate. Default: SD-WAN. **Note:** The name of the synced SD-WAN and Virtual Server will use VDOM name as prefix, such as root-xxxx.
Auth type	The authentication method that GSLB can use when access FortiGate. Currently, Auth-Verify and Token authentication are supported. When Auth-Verify is chosen, user needs to provide username and password info; when Token is chosen, user needs to provide the RestAPI Key generated from FortiGate

3. After the FortiGate Connector is created, the Virtual Servers and SD-WAN member should be synced to GSLB within a couple minutes.

Notes & limitations:

- FortiGate Connector supports FortiGate hosts that run FortiOS version 6.2.5 or higher, due to the supported RestAPIs on FortiGate.
- FortiGate Connector supports Rest API version v2, this is the same Rest API version that FortiGate host currently supports. If in the future, FortiGate supports additional versions, FortiGate Connector will extend to support additional versions as well
- The FortiGate API token needed in FortiGate Connector token authentication can be generated on FortiGate using CLI. Below is an example of how to config an api-user and generate API key:

```
config system api-user
   edit "g-api-rw-user"
      set api-key ENC SH2SHFEtfJQ9OsfH/keh4kdULAp3V4ps7HkxBuDIzpR4Cmsckaa9wJ6kw28dFQ=
      set accprofile "super_admin"
      set vdom "root"
      config trusthost
         edit 1
            set ipv4-trusthost 10.6.30.0 255.255.255.0
         next
      end
   next
end
execute api-user generate-key g-api-rw-user
```

- If Virtual Domains(VDOM) are enabled on FortiGate host, the RestAPI administrator configured for FortiGate Connector access should have access to all the VDOMs

Create a Generic-Host type connector

1. Go to **Fabric Connectors** and click **Create Connector**.
2. Create a connector according to the following configuration. For Type, select Generic-Host.

Settings	Guidelines
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	GSLB can support three types of connectors. Refer to the table under Create Connector manually on page 354 for details. For Generic-Host type, select "Generic-Host"
Data center	Select a data center configuration object. The data center indicates the physical geography location of the server.

3. Input a meaningful name for the connector, and select the Data Center or create a new one. Don't forget to save. Then, configure virtual servers according to Configuring virtual servers for connectors on page 356.



It is recommended to create only one Connector for each Data Center, unless you have a lot of services and IP addresses for this Data Center (which means you will have a lot of virtual servers, hundreds). In this case, you may need multiple Connectors. For easy management, it is recommended to create a Connector for each hardware device or a set of devices that running the similar service, or a set of devices that for one domain.

Note: The FortiADC type connector is automatically generated and available to use in GSLB once the user enables GSLB service on the FortiADC device. The user does not need to manually create this type of connector.

Configuring virtual servers for connectors

In the edit connector window, click "Create Member" to create a virtual server.

To configure the virtual server, input a virtual server name, and IP address. Enable the health check if needed. Virtual Server is allowed to enable multiple health checks for each virtual server with a simple and/or relationship.

Refer to the table below for details on virtual server configuration settings.

Settings	Guidelines
Name	Virtual server name Note: Usually, the service name or FQDN name is used for ease of identification. You may still edit it after you initially save the configuration.
Address Type	IPv4 or IPv6.
IP Address	Virtual server IP address.
Health Check Control	Enable health checking for the virtual server. Note: you must enable this option to configure the Health Check Relationship and Health Check List fields below.

Settings	Guidelines
Health Check Relationship	• AND—All of the specified health checks must pass for the virtual server to be considered available. • OR—One of the specified health checks must pass for the virtual server to be considered available.
Health Check List	Specify one or more health check configuration objects.
SD-WAN Link Name	Specify the SD-WAN member name for the virtual server, applicable to FortiGate type connector only. **Notes:** • The SD-WAN member should be in the same VDOM as the virtual server if the virtual server is synced from FortiGate • For a virtual server that is synced from a FortiADC or FortiGate, the synced attributes, such as name, ip address, and etc are not allowed to modify in GSLB.



It is recommended that you reuse the same Virtual Server for different GSLB services if they share the same IP. However, it is also reasonable to have multiple Virtual Servers with the same IP, which then may use different health check for different GSLB services.

Data center

The data center object is defined as the physical data center on the network, and its location item tells the cloud where the data center is located. Using the data center location information, the cloud can then perform proximity load balancing to direct all requests from the specified region to the data center.

To configure a data center object:

1. Go to **Virtual Server > Data Center**.
2. Click **Add Data Center** to display the configuration editor.

3. Configure the following Data Center settings:

Setting	Description
Name	Specify a unique name for the data center configuration. Valid characters are `A-Z`, `a-z`, `0-9`, `_`, and `-`. No spaces. After you initially save the configuration, you cannot edit the name.
Description	Optionally, describe the purpose of the configuration, to help you and other administrators more easily identify its use.
Region	

Setting	Description
Continent/Country	Select the continent or country in which the data center is located. The *Continent/Country* selection determines the availability of the *State* and *City* options. To set the data center as a *country-level data center*, you can select the *Continent/Country*, and then set *State* and *City* as *ALL*. All requests from the specified continent or country will then be directed to this data center location. **Note**: Antarctica is the only continent selection that allows for *ALL* as an option for *State* and *City*.
State	Select the state in which the data center is located. The availability of *State* options is dependent on the selected *Continent/Country*. To set the data center as a *state-level data center*, you can select the *State*, and then set *City* as *ALL*. All requests from the specified state will then be directed to this data center location. Alternatively, you can select *ALL* to specify that requests from all states under the specified continent or country will be directed to this data center location, making this a *country-level data center*.
City	Select the city in which the data center is located. The availability of *City* options is dependent on the selected *Continent/Country* and *State*. Select a city to set the data center as a *city-level data center*. All requests from the specified city will then be directed to this data center location. Alternatively, you can select *ALL* to specify that requests from all cities under the specified state will be directed to this data center location, making this a *state-level data center*.

4. Click *Save*.
   The new data center object will be listed on the Data Center page.

DNS service

This section covers the DNS services offered by FortiAppSec Cloud.

- DNS Resource Types on page 362
- How to create a DNS record on page 366
- How to enable DNSSEC on GSLB on page 366
- How to add GSLB as sub-domain on page 369

GSLB, functioning as a DNS Service, can support both standard DNS zones and primary type zones.

Adding a DNS Zone

1. Click **Add Service**
2. Configure the following:

Settings	Guidelines
Name	Name of the zone.
Type	Primary—The configuration contains the “primary” copy of data for the zone and is the authoritative server for it.
Domain name	The domain name must end with a period. For example: example.com.
Responsible Mail	Username of the person responsible for this zone, such as `admin.example.com`. **Note**: Format is mailbox-name.domain.com. (remember the trailing dot). The format uses a dot, not the @ sign used in email addresses because @ has other uses in the zone file. Email, however, is sent to admin@example.com.
Primary server name	Sets the server name in the SOA record.
Primary server address (IPv4)	The IPv4 address of the primary server. Note: The address will append on the 'ADDITIONAL SECTION' of the query reply. In most cases is the GSLB DNS server IP address.
Primary Server Address (IPv6)	The IPv6 address of the primary server. Note: The IPv6 address will append on the 'ADDITIONAL SECTION' of the IPv6 type query reply. If you have another DNS server hosting the same domain and it supports IPv6, then put that IPv6 address, otherwise leave it empty.
TTL	The `$TTL`(Time-To-Live) is the length of time or “hops” that a packet may move through a network before being discarded by a router, or how long content or a query is retained in DNS and CDN caching. This entry sets a default TTL that applies to all resource records (RRs) in the file unless they explicitly define their own TTL. If unconfigured, the default TTL is 86,400. The valid range is 0 to 2,147,483,647.
Negative TTL	The last field in the SOA—the negative caching TTL. This informs other servers how long to cache no-such-domain (NXDOMAIN) responses from you. The default is 3600 seconds. The valid range is 0 to 2,147,483,647.
DNSSEC	Only enable DNSSEC when necessary. Click the **DNSSEC** toggle switch to enable DNSSEC, and then click **Save**. For detailed instructions on enabling DNSSEC on GSLB, please refer to How to enable DNSSEC on GSLB on page 366. **Note**: DNSSEC works with A/AAAA, CNAME, CAA, NS, MX, TXT, SRV and PTR records created in the Zone. It can also work with FQDN-generated A records, with the limitation that only one record will reply to the client for FQDN services.

3. If you have enabled **DNSSEC**, please see the following. If you have not enabled DNSSEC, feel free to skip this section.

   The **DSSET** (Delegation Signer Set) keys are used in DNSSEC to securely sign and validate the integrity of DNS records for domains, including those under sub-domains.

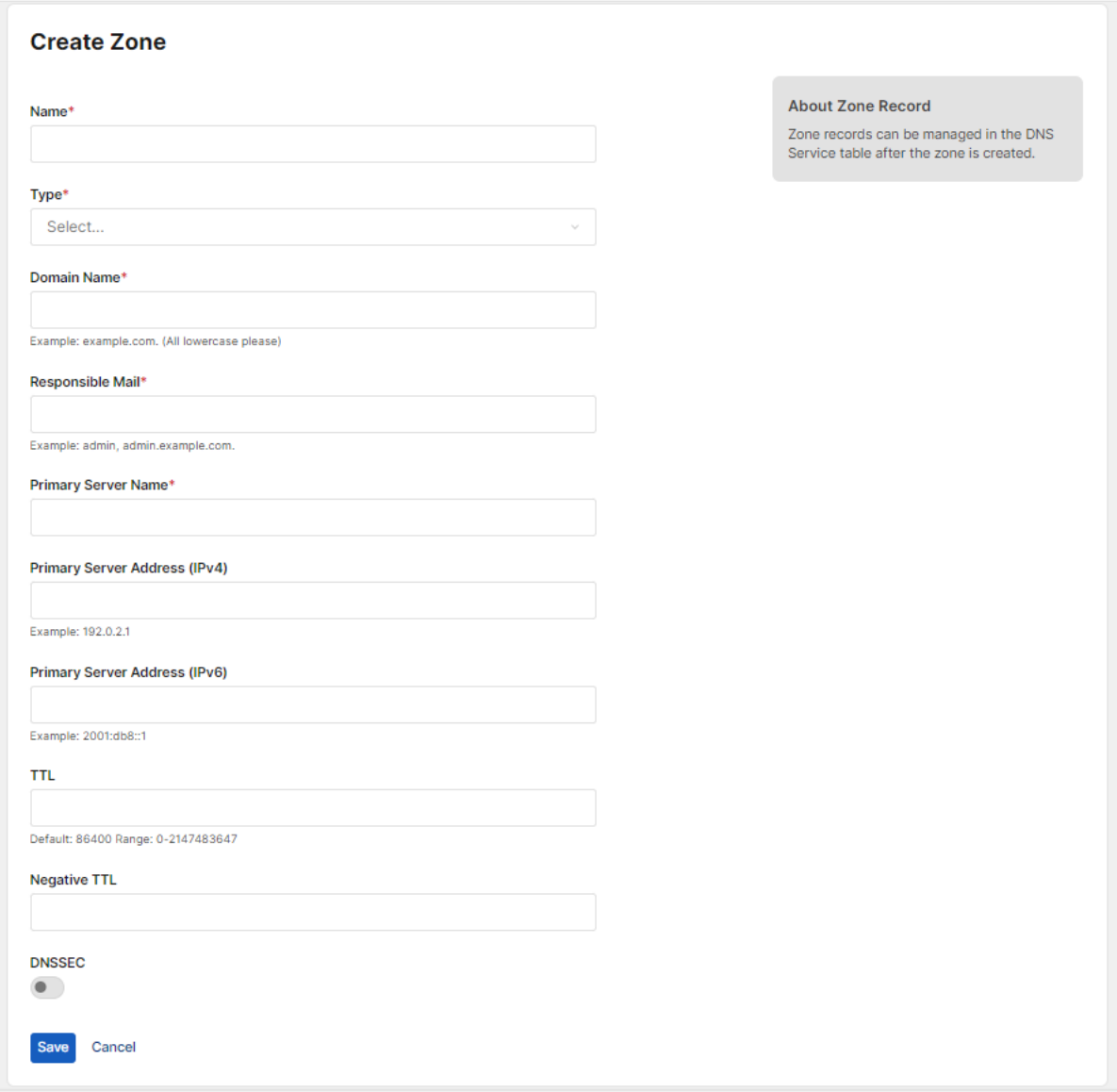
Note: Corresponding NS record should already exist, when add a dsset. And key content must be valid. Failed to do so will result in the Zone reload fail and not respond to any query request.

To configure DSSet, click **Add DSSet** and enter the following:

Settings	Guidelines
Name	Key name

Key	Paste the DSset file content. The content of DSset files is similar to the following:
	`dns.example.com. IN DS 21961 5 1 6E6C2D5EBF440DB2C71A8191FF2772F58A434175`
	`dns.example.com. IN DS 21961 5 2 1B000131FCC68FF34441A710ACACDFD67350CF962260F47309321F8D0551DADF`

Importing zone configuration files



Before importing a zone file in GSLB's DNS Services, ensure proper zone configuration.

Consider the following guidelines:

- Zone file must comply with RFC standards and BIND format.
- Record domain names in the zone file must match the hosted zone's name.
- GSLB ignores SOA records in the zone file.
- NS records and their corresponding A records for the configured zone domain are disregarded.
- The imported zone file must not duplicate any records already present in the hosted zone, or the import process will fail.
- Duplicate records in the imported zone file will also cause the import process to fail.
- You can import up to 1024 records.

Below is a sample zone file:

```
$TTL 86400
example.com. IN SOA ns1 admin (
   10004 ; serial
   3600 ; refresh
   900 ; retry
   3600000 ; expiry
   3600 ; minimum
)
example.com. IN NS ns1
$ORIGIN example.com.
ns1 86400 IN A 1.2.3.4
mail 86400 IN A 192.0.2.2
www 86400 IN A 192.0.2.1
www.example.com 86400 IN CNAME example.com.
sub.example.com 86400 IN MX 10 mail
```

DNS Resource Types

Select Resource Types

This section details resource types supported by GSLB:

- A/AAAA record on page 362
- CNAME record on page 363
- NS record on page 363
- MX record on page 363
- TXT record on page 364
- SRV record on page 364
- PTR record on page 365
- CAA Record on page 365

In the future, secondary type zones should be available.

A/AAAA record

A host IPv4 or IPv6 address.

Configuring the A/AAAA record

Settings	Guidelines
hostname	The hostname part of the FQDN, such as www. **Note**: You can specify the @ symbol to denote the zone root. The value substituted for @ is the preceding $ORIGIN directive.
Address type	IPv4 / IPv6
Address	Specify the IP address of the virtual server.
TTL	The time-to-live of the **Resource Records**

Settings	Guidelines
Weight	Assigns relative preference among members—higher values are preferred and are assigned connections more frequently. The default is 1. The valid range is 1-255.

CNAME record

Identifies the canonical name of an alias. Described in RFC 1035.

Configuring the CNAME record

Settings	Guidelines
Alias	An alias name to another true or canonical domainname (the target). For instance, www.example.com is an alias for example.com. **Note**: Alias should not be the same as other records, nor should there be duplicate aliases for the same domain.
target	The true or canonical domain name. For instance, example.com.
TTL	The time-to-live of the **Resource Records**

NS record

The authoritative name server for the domain. Described in RFC 1035.

Configuring the NS record

Settings	Guidelines
Domain name	The domain for which the name server has authoritative answers, such as example.com. Note: FortiAppSec Cloud supports third-party domain names.
Host name	The hostname part of the FQDN, such as ns.
TTL	The time-to-live of the **Resource Records**
Address Type	IPv4 / IPv6
Address	Specify the IP address of the name server.

MX record

Identifies a mail exchange for the domain with a 16-bit preference value (lower is better) followed by the host name of the mail exchange. Described in RFC 974, RFC 1035.

Configuring the MX record

Settings	Guidelines
Domain name	The domain of the mail exchange server.
Hostname	The hostname part of the FQDN for a mail exchange server, such as mail.
TTL	The time-to-live of the **Resource Records**
Priority	Preference given to this RR among others at the same owner. Lower values have greater priority.
Address type	IPv4 / IPv6
Address	Specify the IP address.

TXT record

Described in RFC 1035.

Configuring TXT record / NS record

Settings	Guidelines
name	Hostname. TXT records are name-value pairs that contain human readable information about a host. The most common use for TXT records is to store SPF records.
text	Comma-separated list of name/value pairs. An example SPF record has the following form: `v=spf1 +mx a:colo.example.com/28 -all` If you complete the entry from the Web UI, do not put the string in quotes. (If you complete the entry from the CLI, you do put the string in quotes.)
TTL	The time-to-live of the **Resource Records**

SRV record

Information about well-known network services (replaces WKS). Described in RFC 2782.

Configuring the SRV record

Settings	Guidelines
Hostname	The host name part of the FQDN, e.g., www.
TTL	The time-to-live of the **Resource Records**
Priority	A priority assigned to the target host: the lower the value, the higher the priority.
Weight	A relative weight assigned to a record among records of the same priority: the greater the value, the more weight it carries.
Port	The TCP or UDP port on which the service is provided.
Target name	The canonical name of the machine providing the service.

PTR record

Resolves an IP address to a fully-qualified domain name.

Configuring the PTR record

Settings	Guidelines
PTR address	A PTR address, such as 10.168.192.in-addr.arpa. or 1. **Note**: If you use the number, the domain name is in the format "x.x.x.in-addr.arpa."
FQDN	A fully qualified domain name, such as "www.example.com".

CAA Record

A Certificate Authority Authorization (CAA) record is a type of DNS record that specifies which Certificate Authorities (CAs) are authorized to issue certificates for a specific domain. It acts as an additional layer of control to prevent unauthorized certificate issuance.

A Certificate Authority (CA) sends a Certificate Authority Authorization (CAA) request to a DNS server during the domain validation process. This typically happens when:

- **A Certificate is Requested:** When a user or entity requests an SSL/TLS certificate for a domain, the CA must verify that it is authorized to issue a certificate for that domain.
- **CAA Record Check is Performed:** As part of the validation process, the CA performs a CAA lookup by querying the domain's DNS. This is done to check if the domain's DNS records include a CAA policy that specifies which CAs are authorized to issue certificates for the domain.
- **Before Certificate Issuance:** The CA queries the DNS for the CAA record using a standard DNS query. If a CAA record is found, the CA ensures that it is listed as an authorized CA. If no CAA record exists, the CA assumes it is authorized to issue the certificate by default (as per current industry standards).

If the DNS server returns a CAA record that does not authorize the CA to issue certificates for the domain, the CA will deny the certificate request.

Configuring the CAA record

Settings	Guidelines
Hostname	The domain or subdomain to which the policy applies. If the zone record is `example.com.`, you can use a subdomain (e.g., `www`, `sub`) as the **Hostname** to add a CAA record for that subdomain. To add a CAA record for the root domain, use `@` as the hostname.
Flags	**Default**:No special enforcement—certificate requests proceed as usual. **Critical**: If the CA does not understand the record, it must reject the certificate request, preventing issuance.
Tag	A label that specifies the type of policy being defined. • **issue**: Specifies which CAs are authorized to issue certificates for the domain. • **issuewild**: Specifies which CAs are authorized to issue wildcard certificates

Settings	Guidelines
	for the domain. • **iodef**: Specifies a URL where certificate mis-issuance reports should be sent.
Value	The value associated with the tag. • For **issue** and **issuewild**, enter the domain name of the Certificate Authority (CA) authorized to issue certificates (e.g., letsencrypt.org). The maximum length is 253 characters. • For **iodef**, enter a URL where mis-issuance reports should be sent (e.g., mailto:admin@example.com or https://example.com/report). While there is no strict length limit, it is recommended to keep it within 253 characters.

How to create a DNS record

1. Configure the Zone for the SOA record.
   a. *Primary Server Name*: Name for the primary server. You will need this name when creating the NS record of your domain. If you use '@', this means the server name is exactly the same as the domain name. Make sure to add a '.' at the end of the name if you would like to name it with a different domain name, such as in 'example.com.'. If there is no '.' at the end, our server will append the domain name automatically as the server name.
   b. *Responsible Mail*: Use '.' to replace the '@' for the email address. If there is no '.' at the end of the mail, the DNS server will automatically append the domain name. For example, an input of 'dns_admin' would be automatically interpreted as 'dns_admin@sub.example.com'. Be sure to add a '.' at the end of the email address if a different domain name is used (e.g. 'dns_admin.example.com.').
2. Configure NS record
   a. Without '.' at the end of the Hostname: Requires an IP for the sub-domain. DNS will append the domain name automatically.
   b. With '.' at the end of the Hostname: No IP needed. Usually only used for redirecting to another domain.
3. Configure CNAME record
   CNAME Alias cannot conflict with any other record in the same domain. Otherwise, the DNS service will fail.
   a. Without '.' at the end of the Target: This means CNAME is within the same domain and the DNS server will append the domain automatically. TTL=-1 indicates use of the same TTL as the Zone configuration.
   If there is a valid A record for 'ms.sub.example.com'
   b. Without '.' at the end of the Target: CNAME will redirect to an A record in another domain.
   If there is a valid A record for 'mail.sub1.zw120.com' exists, then request from resolver '10.106.156.24'.

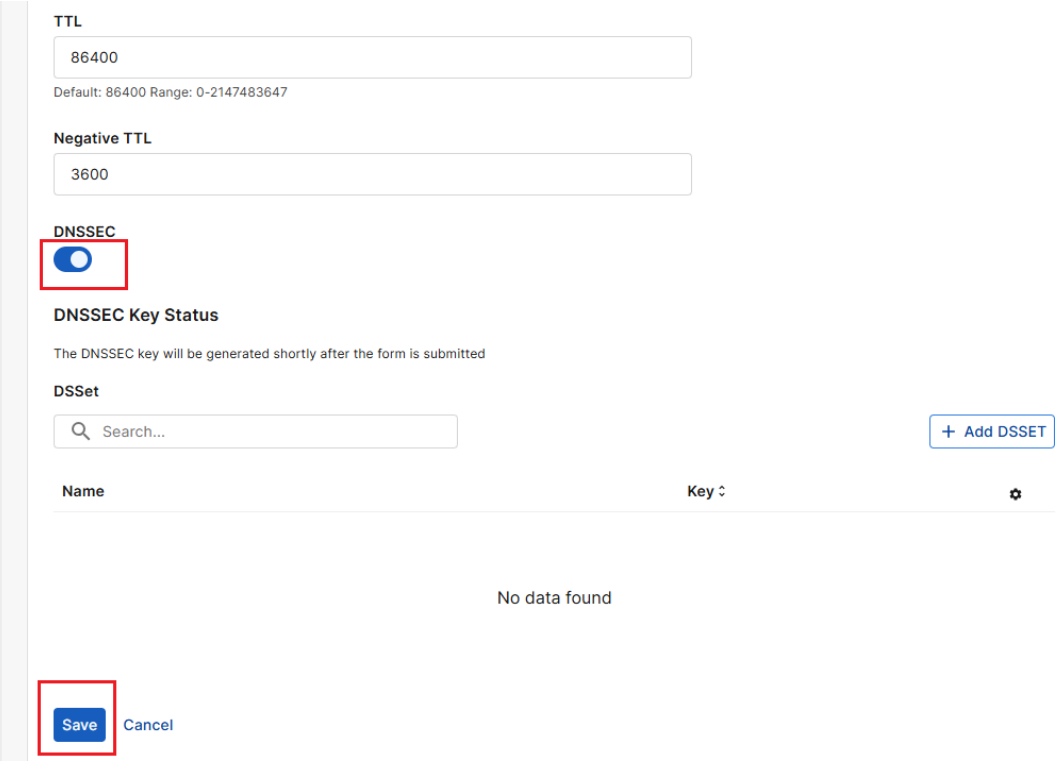
How to enable DNSSEC on GSLB

Prerequisites:

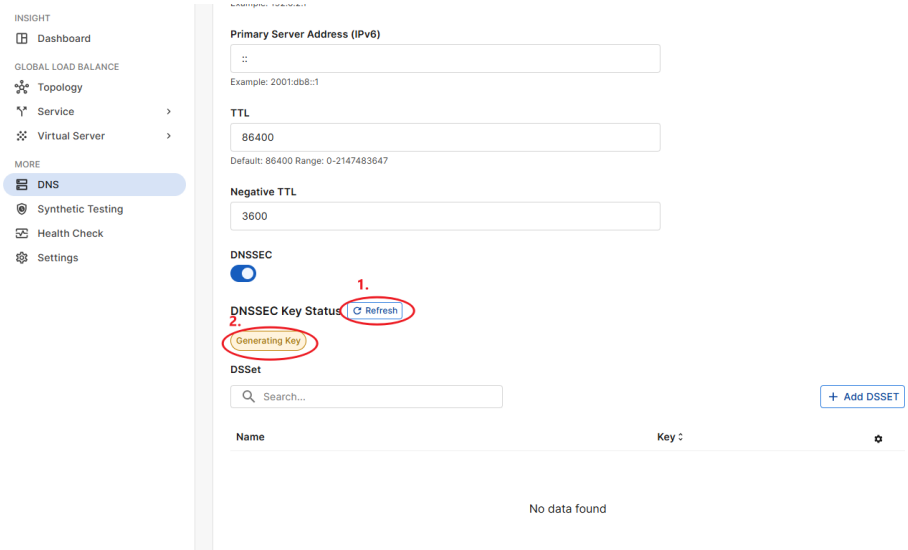
- Ensure your top-level domain (TLD) supports DNSSEC.

Steps:

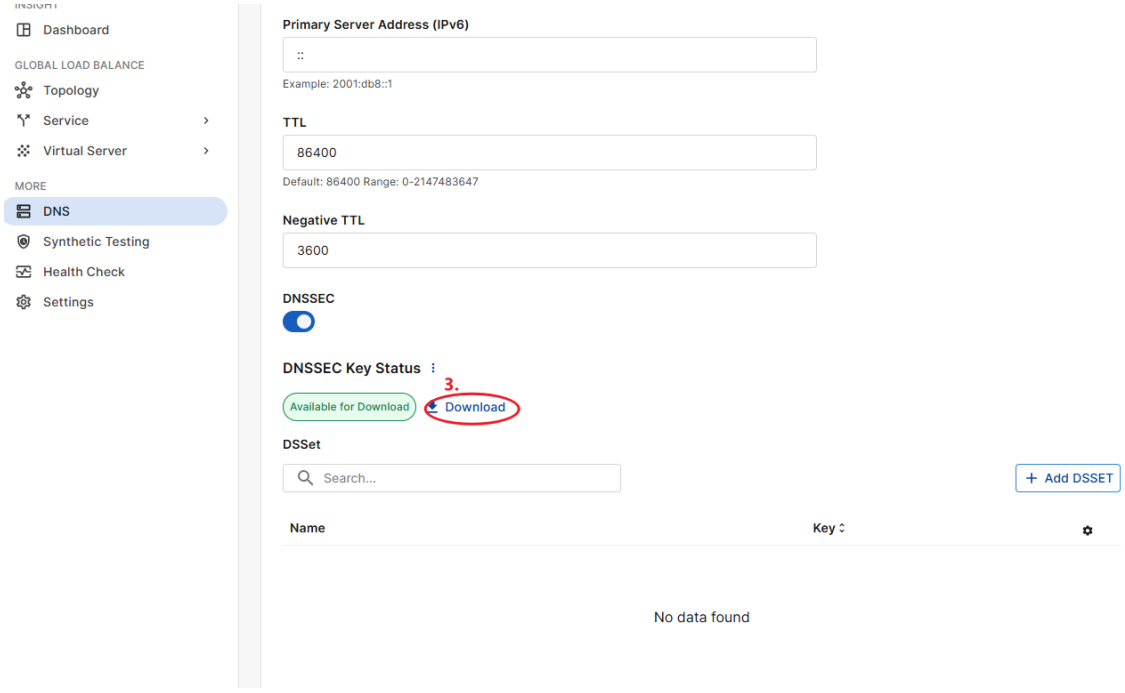
1. Navigate to **GSLB > DNS**, and create a new Zone or edit an existing Zone.
   If you are creating this for an existing FQDN service, you need to create a Zone service with the same Domain Name.
2. Toggle **DNSSEC** on to enable it, then save the configuration. The DNSSEC key will be generated shortly after submission.



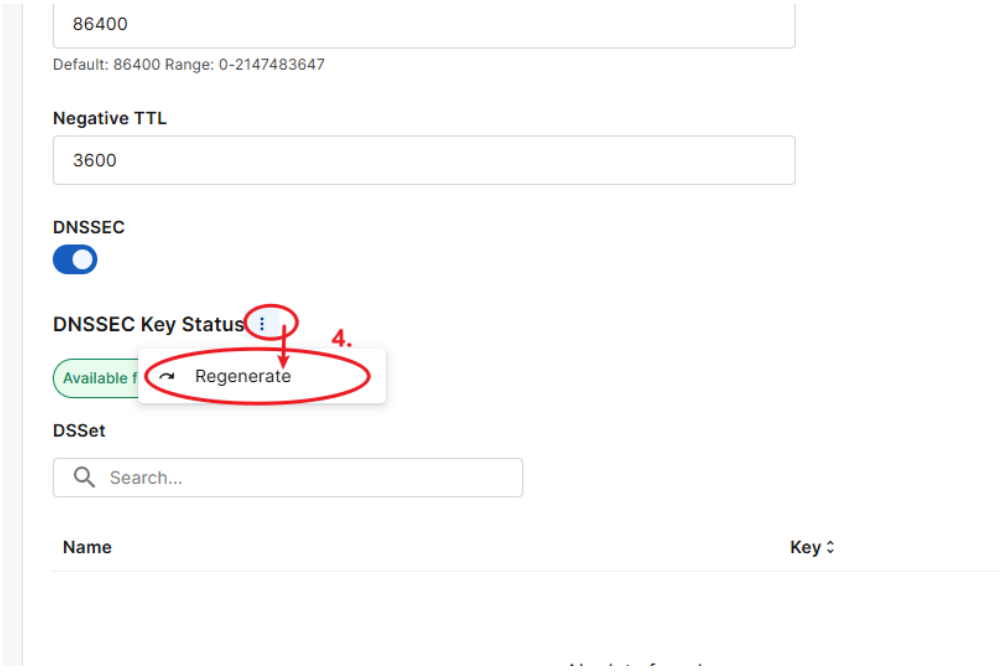
3. Click **Edit** for this Zone service. You may see the **Refresh** button and the **DNSSEC Key status** indicator under DNSSEC.



4. Click the **Refresh** button until the **DNSSEC** status changes from **Generating key** to **Available to download**, and the **Download** button appears. The key-generation process should take less than one minute.

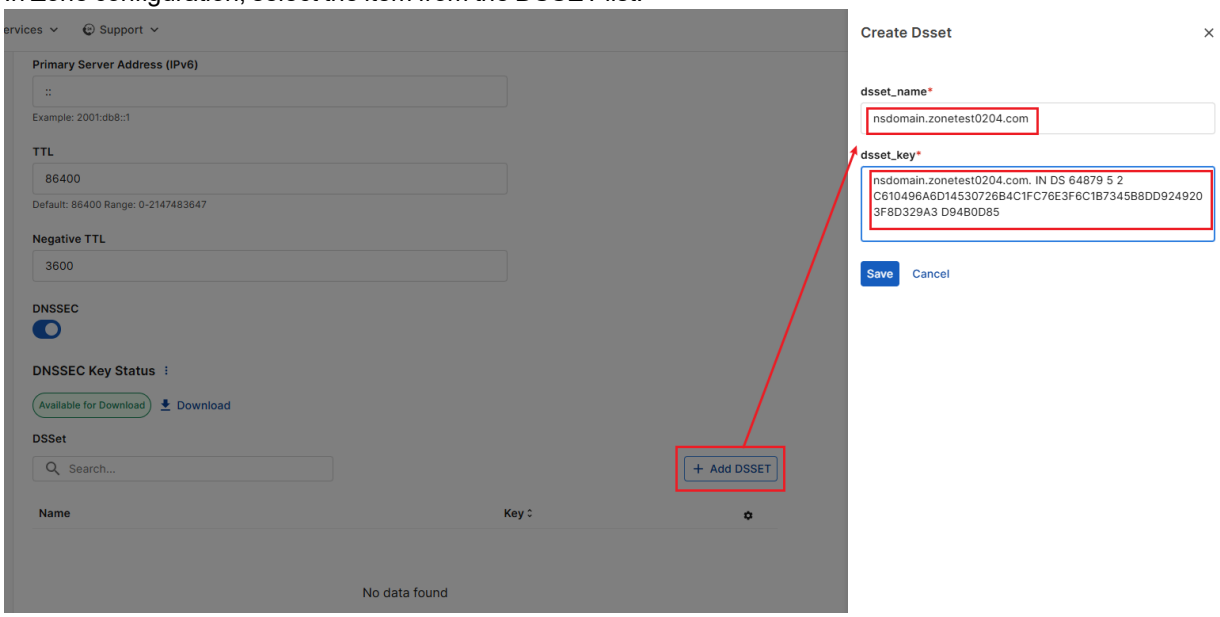


If you suspect your DNSSEC key has been compromised, click the three dots next to **DNSSEC Key Status**, then select **Regenerate**. Repeat Step 4 to download the new key before proceeding.



5. Click the Download button to download the **DNSSEC Key** files.

6. Unzip the downloaded key files, and open the file name that begins with "dsset". You may need this for your top-level domain (TLD).
   a. Add the opened file to the DSSET list
   b. In Zone configuration, select the item from the DSSET list.



7. You should now be able to query the domain records via CLI with the DNSSEC flag. The resulting output contains a RRSIG record and a DS reccord.

   Linux - `dig`

   Windows - `Resolve-DnsName`
8. Add the DNSSEC key downloaded in Step 5 to your domain registrar.
   - To avoid DNS resolution issues, do not delete the old DNSSEC key until its TTL (Time to Live) has expired and the new key has fully propagated.
   - We recommend verifying propagation of the new DNSSEC key using public DNS resolvers such as Google, Cloudflare, or TLD-specific resolvers.
   - GSLB DNS servers will retain the old DNSSEC key for 14 days after a new key is generated to ensure uninterrupted service. After this period, DNS requests signed with the old key will be rejected.
   - To ensure continuity, delete the old DNSSEC key from your domain registrar within the 14-day window, once propagation of the new key is confirmed.

Debugging

Please see the Debugging on page 370.

How to add GSLB as sub-domain

Example: You have a domain configured on a FortiADC as 'example.com'. You want the sub-domain "sub.example.com' to be configured on GSLB with the name of this sub-domain's primary server name to be 'ns-4.sub.example.com'. The resolver address is '10.106.156.24' and the FortiADC DNS server address is '10.106.156.183'. The sub-domain DNS server address provided by GSLB is '10.106.33.120'.

Steps

1. To configure the sub-domain on GSLB, go to *DNS Services* and *Click Create DNS services* or *Create New*.
   a. *Domain Name*: full sub-domain name with '.' at the end
   b. *Primary Server Name*: primary server name without domain name at the end
   c. *Primary Server Address*: DNS server address

   d. Add an A record for testing. In this example, a 'www' A record is configured with IP '10.107.9.81'

2. To configure an NS record on FortiADC, go to *Global Load Balance* > *Zone Tools* > *Zone*. Click on the zone to edit. Click Create New and select NS Record.
   a. *Domain Name*: The sub-domain name without 'example.com.'
   b. *Host Name*: The sub-domain's Primary Server Name without 'example.com'
   c. *Address*: The IP address of the sub-domain's DNS server

3. Verify the configuration by querying the resolver '10.106.156.24'.
   Recommendation: `dig` for Linux; `nslookup` or `Resolve-DnsName` for Windows.
   If done correctly, the output should look like the following:

   At this point, you should be able to get the A record resolved from the Google resolver '8.8.8.8'

Debugging

If verification fails, the user will need to debug according to the steps below:

Debugging on Linux

1. Try querying the sub-domain DNS server ‘10.106.33.120’ directly for the A record.
   a. If the query fails, you may need to reconfigure your sub-domain Zone. Try deleting some of the other records and query again. **Note**: The configure changes may take a few minutes to take effect.
2. Try querying the domain NS server '10.106.156.183' for the NS record.
   a. If the query fails, double check your FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.
3. Double check the domain NS record and Zone configuration. They should match with the query results.
4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.
   Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

Debugging on Windows using `nslookup`

1. Try querying the sub-domain DNS server '10.106.33.120' directly for the A record.
   a. If the query fails, you may need to reconfigure your sub-domain zone. Try deleting some of the other records and querying again. **Note**: The configure changes may take a few minutes to take effect.

2. Try querying the domain DNS server '10.106.156.183' for the NS record.
   a. If the query fails, double check the FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.
3. Double check the domain NS record and Zone configuration. You can also check the SOA record from the sub-domain DNS server and NS record from the domain DNS server.
4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.
   Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

Debugging on Windows using `Resolve-DnsName`

1. Try querying the sub-domain DNS server '10.106.33.120' directly for the A record.
   a. If the query fails, you may need to reconfigure your sub-domain zone. Try deleting some of the other records and querying again. **Note**: The configure changes may take a few minutes to take effect.
2. Try querying the domain DNS server '10.106.156.183' for the NS record.
   a. If the query fails, double check the FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.
3. Double check the domain NS record and Zone configuration. They should match with the query results.
4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.
   Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

Synthetic testing

Synthetic testing checks applications availability by sending probes to applications from GSLB. It can be used to monitor application website services or application endpoints at various network layer, and the results of these tests can provide valuable information on application up/down time, availability, and regional performance issues.

Synthetic testing types

Synthetic testing supports ICMP, HTTP, HTTPS, DNS, TCP, UDP and TCP Echo testing. It utilizes the health check object configured under *Profiles* > *Health Check*.

Configuring application

Go to *Synthetic testing* and click *Create New*. Create an application according to the following configuration settings:

Setting	Description
Name	Application name

Setting	Description
Address Type	IPv4 or FQDN
IP Address	Application IP address
Address	FQDN address
Region	The physical location of the application
Health Check Control	Enable health checking for the application. **Note**: you must enable this option to configure the Health Check Relationship and Health Check List fields below.
Health Check Relationship	AND—All of the specified health checks must pass for the application to be considered available. OR—One of the specified health checks must pass for the application to be considered available.
Health Check List	Specify one or more health check configuration objects.

Viewing testing results

Synthetic testing is activated within 1 minute after the testing is setup. The time needed for results to become available depends on your health check configures (for instance, Up Retry, Down Retry, Timeout and Interval). You can refresh and view Synthetic testing results in the GUI as a Map or as a List by selecting the desired view at the top left. You can also view testing related activities and logs in *Recent Activities*.

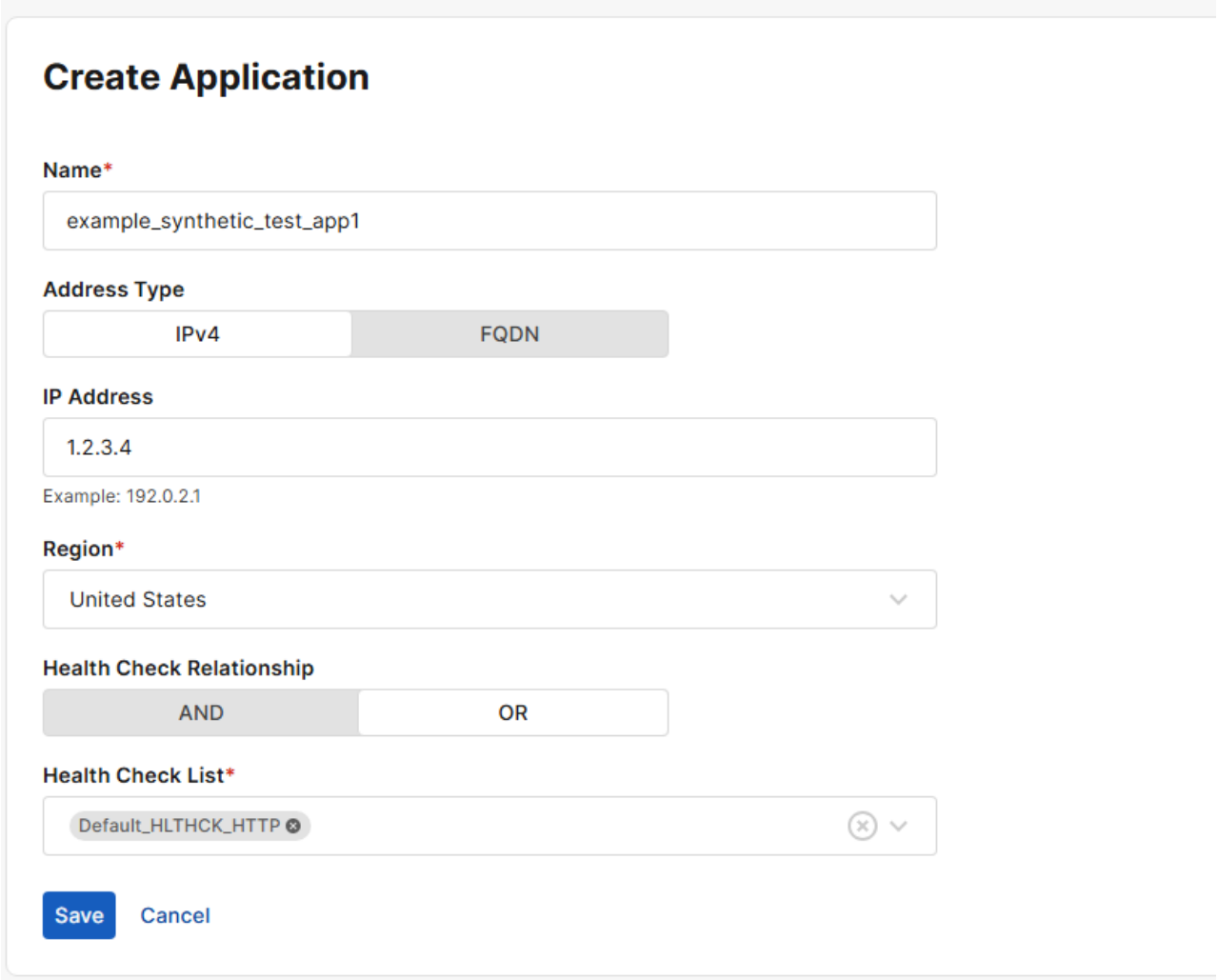
In *Map* view, get detailed application info for specific regions by hovering over the region or clicking the region icon.

How to set up synthetic testing for multisite applications

Scenario: The client has web service applications located in several different regions (United States, Arizona; Italy, Enna; etc). The client wants to proactively monitor the web services in all these regions and check whether the web services are responding to requests. They also want to manage the web services reachability issue from a region perspective. To achieve this goal, the client can set up HTTP synthetic testing on their applications.

Steps

1. Go to *Profile* > *Health Check* and create a HTTP type health check.
2. From *Synthetic Testing*, click *Create New* to create an application. Specify the name, IP address of the application, and region. Enable health check and then select the health check configured in step 1. Applications in other regions can be created in similar steps.



3. You can view the testing result as a *Map* or as a *List* by selecting the desired view at the top left. Region location and status data can be conveniently viewed from *Map* view. You can get testing activities and logs from *Recent Activities*.

Health check

View, create, and manage your health check configurations.

In Global Server Load Balance (GSLB) deployments, health checks are used to poll virtual servers to determine their availability. A health check profile can include results from multiple checks. For example, you can configure an HTTP health check test and a TCP health check test.

- Before you begin on page 374
- Configure health check on page 374
- Add Health Check to a Virtual Server on page 376

Predefined health check configuration objects

Predefined health check configuration objects are available to help you get started. These can be used as-is or serve as templates for creating custom health check objects.

Predefined	Description
Default_HLTHCK_HTTP	Sends a HEAD request to the server port 80. Expects the server to return an HTTP 200.
Default_HLTHCK_HTTPS	Sends a HEAD request to the server port 443. Expects the server to return an HTTP 200.
Default_HLTHCK_ICMP	Pings the server.
Default_HLTHCK_TCP_ECHO	Sends a TCP echo to server port 7. Expects the server to respond with the corresponding TCP echo.

Before you begin

- You should have a solid understanding of TCP/IP and global load balancing concepts.
  - You must know the IP address, port, and configuration details of the local load balancing servers.
- For certain protocol checks, valid user credentials are required.
  - You must have **Read-Write** permission for Load Balance settings.
- Health checks will be performed from the following IP addresses. To avoid disruptions caused by misidentification as DDoS attacks, please add the following IPs to your application's allowlist:
  - USA: 44.231.37.61
  - Europe: 18.195.172.168 (new)
  - Asia Pacific: 52.77.144.83 (new)

Configure health check

1. Go to Health Check, click **Create New** to display the configuration editor.
2. Select one of the following options:
   - ICMP
   - TCP Echo
   - TCP
   - HTTP
   - HTTPS
   - UDP
   - DNS
3. Complete the configuration as described in Health check configuration.
4. Save the configuration.

Setting	Guidelines
Name	Configuration name. Valid characters are A-Z, a-z, 0-9, _, and -. No spaces. After you initially save the configuration, you cannot edit the name.
Type	Select a type of health check.
General	
Destination Address Type	IPv4
IPv4 Address	The IPv4 address to send health check traffic. If you do not specify an IPv4 address, the virtual server IPv4 address is used.
Interval	Seconds between each health check. Should be more than the timeout to prevent overlapping health checks. The default is 30.
Timeout	Seconds to wait for a reply before assuming that the health check has failed. The default is 10.
Area	Select the geographical areas(s) where the health check will be performed.
Healthy Area Threshold	Specifies the number of areas that must be healthy for the health check to be considered a pass.
Up Retry	Attempts to retry the health check to see if a down server has become available. The default is 1.
Down Retry	Attempts to retry the health check to see if an up server has become unavailable. The default is 3.
Specifics	
TCP / UDP	
Port	Listening port number of the virtual server.
HTTP / HTTPS	
Port	Listening port number of the virtual server. Usually HTTP is 80, HTTPS is 443. If testing an HTTP proxy server, specify the proxy port.
SSL Ciphers	For HTTPS only. Default selections are recommended.
Local Cert	For HTTPS only. Paste the local SSL Health Check Client certificate into the blank.
HTTP CONNECT	Specify an HTTP CONNECT option: • Local CONNECT—Use HTTP CONNECT to test the tunnel connection through the proxy to the remote server. The virtual server is deemed available if the request returns status code 200 (OK). • Remote CONNECT—Use HTTP CONNECT to test both the proxy server response and remote server application availability. If you select this option, you can configure an HTTP request within the tunnel. For example, you can configure an HTTP GET/HEAD request to the specified URL and the expected response. • No CONNECT—Do not use the HTTP CONNECT method. This option is the default. The HTTP CONNECT option is useful to test the availability of proxy servers only.

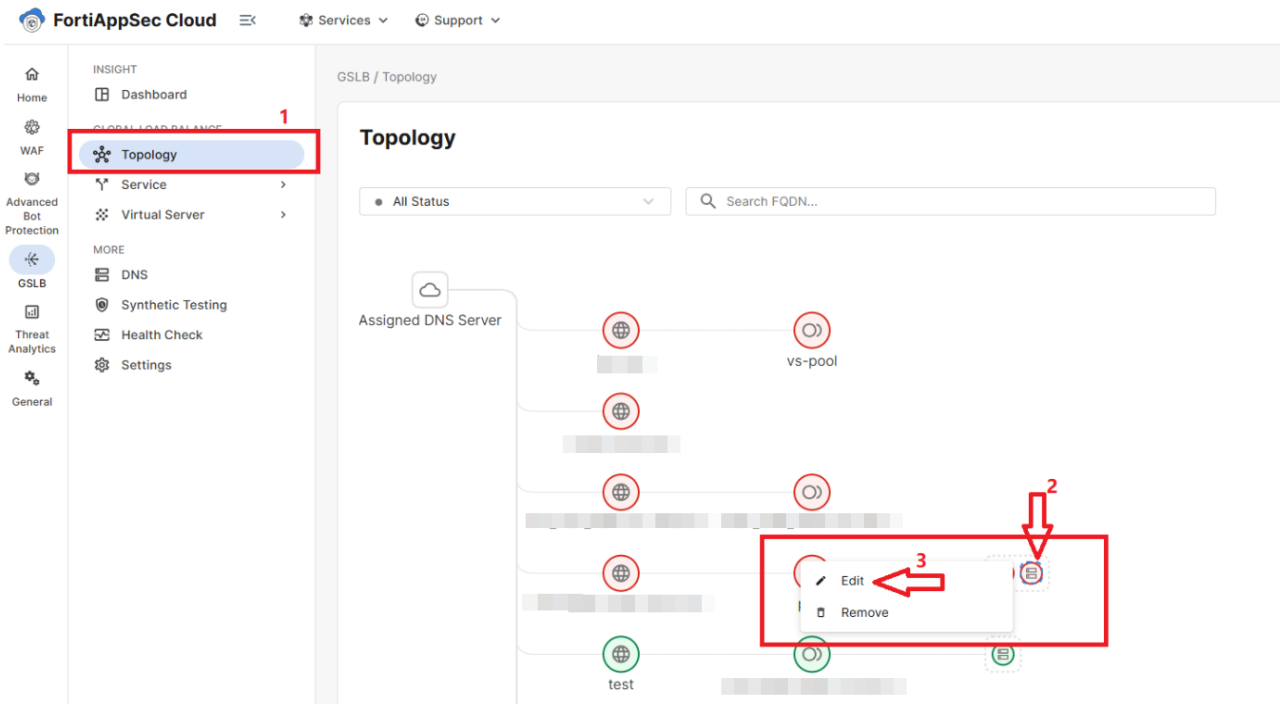
Setting	Guidelines
Remote Host	If you use HTTP CONNECT to test proxy servers, specify the remote server IP address.
Remote Port	If you use HTTP CONNECT to test proxy servers, specify the remote server port.
Method Type	HTTP method for the test traffic: • HTTP GET—Send an HTTP GET request to the server. A response to an HTTP GET request includes HTTP headers and HTTP body. • HTTP HEAD—Send an HTTP HEAD request. A response to an HTTP HEAD request includes HTTP headers only.
Send String	The request URL, such as /contact.php.
Receive String	A string expected in return when the HTTP GET request is successful.
Status Code	The health check sends an HTTP request to the server. Specify the HTTP status code in the server reply that indicates a successful test. Typically, you use status code 200 (OK). Other status codes indicate errors.
Match Type	What determines a failed health check? • Match String • Match Status • Match All (match both string and status) Not applicable when using HTTP HEAD. HTTP HEAD requests test status code only.
DNS	
Domain Name	The FQDN, such as www.example.com, to use in the DNS A/AAAA record health check.
Address Type	IPv4
Host Address	IP address that matches the FQDN, indicating a successful health check.

Add Health Check to a Virtual Server

There are two methods to add health checks to virtual servers:

Add Health Check to Virtual Server via Topology Page

1. Navigate to **GSLB >Topology**.
2. Right-click the virtual server and select **Edit**. This opens the **Edit Virtual Server** side panel.



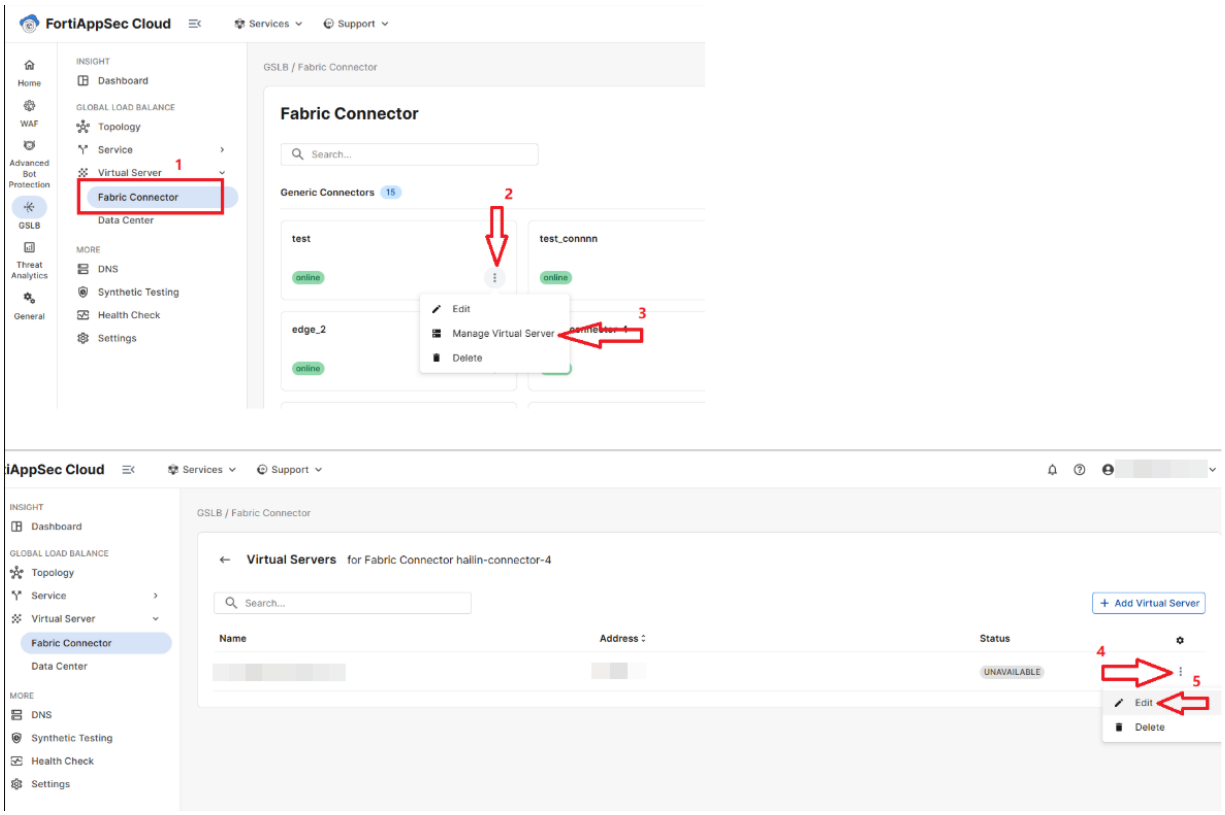
3. Enable **Health Check**, then select the **Health Check Relationship** and applicable health checks from the **Health Check list**.

   Health Check Relationship:

   - AND — All of the specified health checks must pass for the virtual server to be considered available.
   - OR — One of the specified health checks must pass for the virtual server to be considered available.

Add Health Check to Virtual Server via Fabric Connector page

1. Navigate to **GSLB > Virtual Server > Fabric Connector**.
2. Click the three-dot menu on the connector card and select **Manage Virtual Server**. This opens the **Edit Virtual Server** side panel.



3. **a.** Enable **Health Check**, then select the **Health Check Relationship** and applicable health checks from the **Health Check list**.

   Health Check Relationship:

   - AND — All of the specified health checks must pass for the virtual server to be considered available.
   - OR — One of the specified health checks must pass for the virtual server to be considered available.

Integrating GSLB into the Fortinet Security Fabric

This section details the following use cases for GSLB.

For information on connectors, see Fabric connector on page 353

- Setting up an FQDN with Generic-Host connector on page 379
- FortiADC Integration with One-Click GSLB on page 380
- FortiGate Integration on page 385
- FortiWeb Integration with One-Click GSLB
- Fabric connectors with AWS and Azure on page 395

Setting up an FQDN with Generic-Host connector

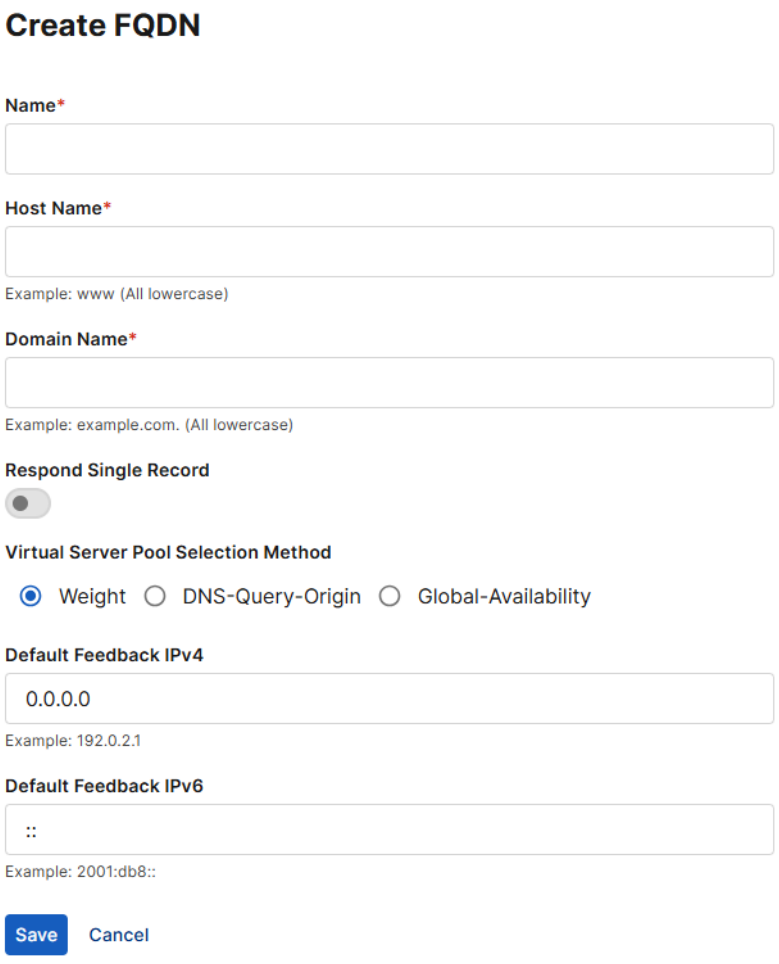
The Generic-Host type connector is a third party host system that cannot communicate with the cloud directly.

The administrator can add the host IP address on this server and specify the health check for the host. The cloud will automatically detect the remote host, after which the administrator can configure the pool and the GSLB service.

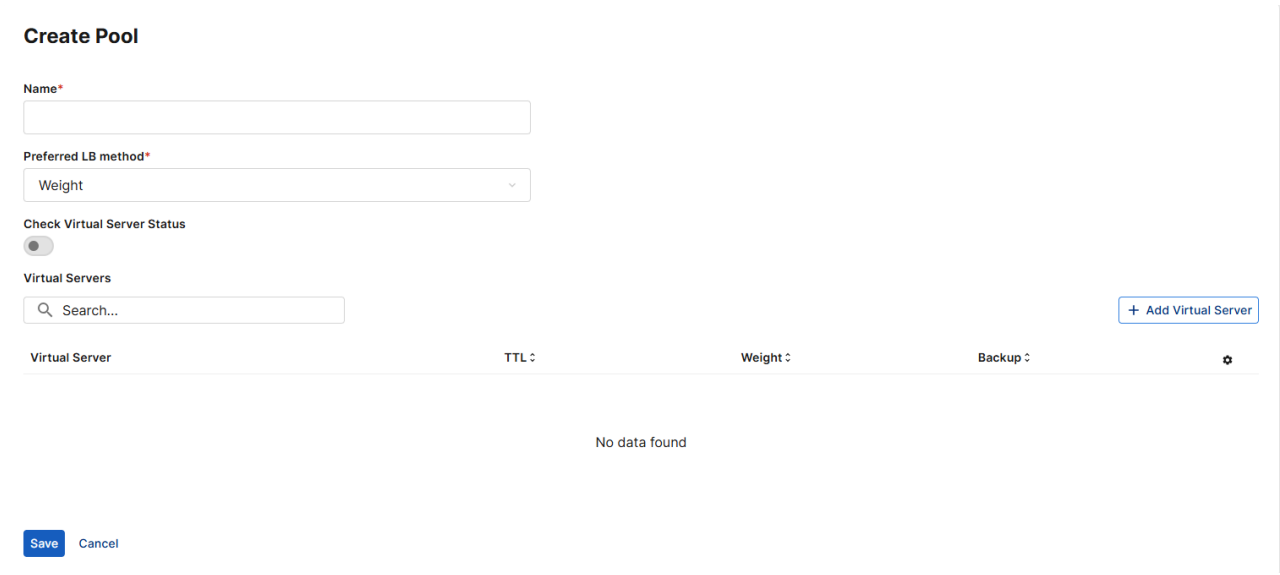
Configuration Steps

Perform the following steps to add an FQDN with generic-host connector.

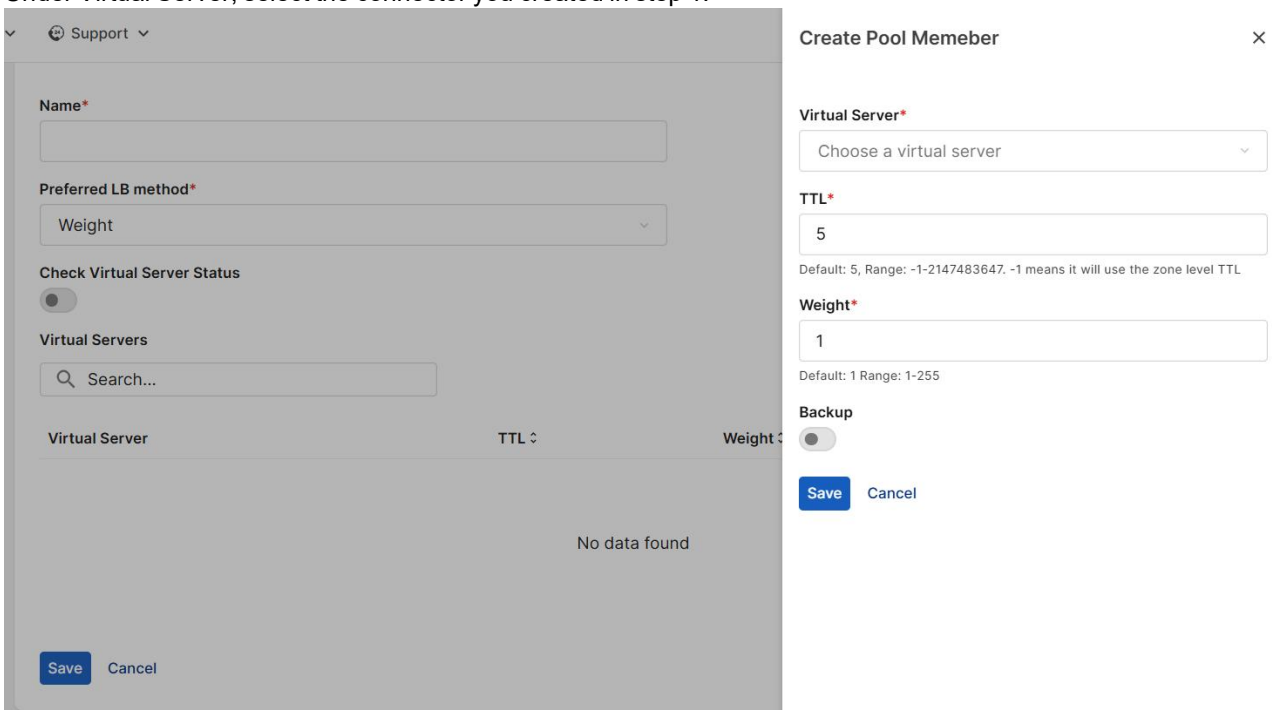
1. Navigate to **GSLB > Virtual Server > Fabric Connector**, and click **Add Connector**. For detailed configuration information, please see Create a Generic-Host type connector on page 356.
2. Navigate to **Service > FQDN** and click **Add FQDN**. Enter FQDN information and save. For detailed configuration information, please see Creating an FQDN on page 338.



3. Go to **Server > Virtual Server Pool** to create a new Virtual Server Pool. For detailed configuration instructions, please seeAdd Virtual Server Pool on page 349



4. After saving the Pool, create a member (virtual server) into Pool.
5. Click **Create Virtual Server**.
6. Under Virtual Server, select the connector you created in step 1.



7. The virtual server should be added successfully into Pool. Click **Save**. The Virtual Server Pool is also added successfully into FQDN.

FortiADC Integration with One-Click GSLB

Perform the following steps to configure GSLB. This section is split into two parts:

- New customers on page 381—for customers who are new to GSLB.
- Returning customers on page 383—assumes you already know how to enable GSLB.

New customers

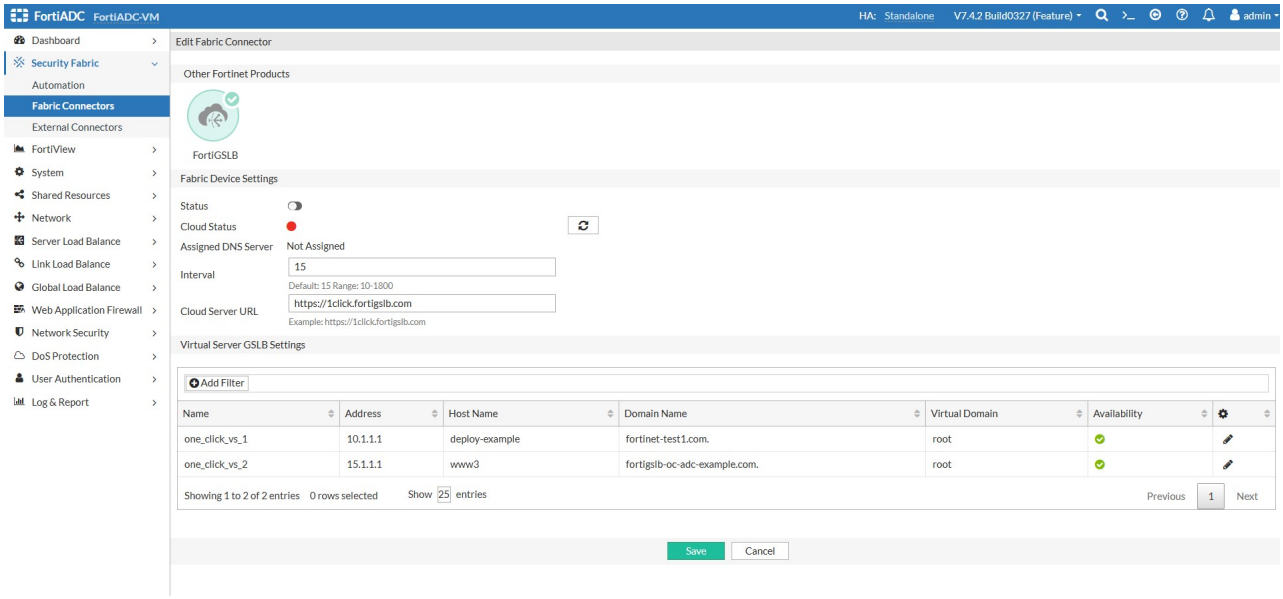
Follow the steps to set up GSLB for the first time.

Link the FortiADC to GSLB

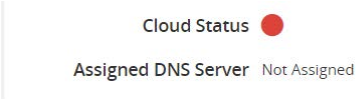


The FortiADC device must be registered. Check this under **FortiADC > System > FortiGuard > Support Contract > Registration**.

1. Log into FortiADC.
2. Navigate to **Security Fabric > Fabric Connectors > GSLB**) Click **edit** on the far right. Here you will connect FortiADC to GSLB.



3. Configure basic settings.
   a. Set **status** to on - on/off (enable/disable GSLB service)
   b. Set the **interval** to the default (15) - How often the FortiADC will attempt to connect to the One-Click Cloud Server.
   c. Set the **Cloud Server URL** to the default (https://1click.fortigslb.com) - URL of the One-Click Cloud Server.
4. Click **Save**.

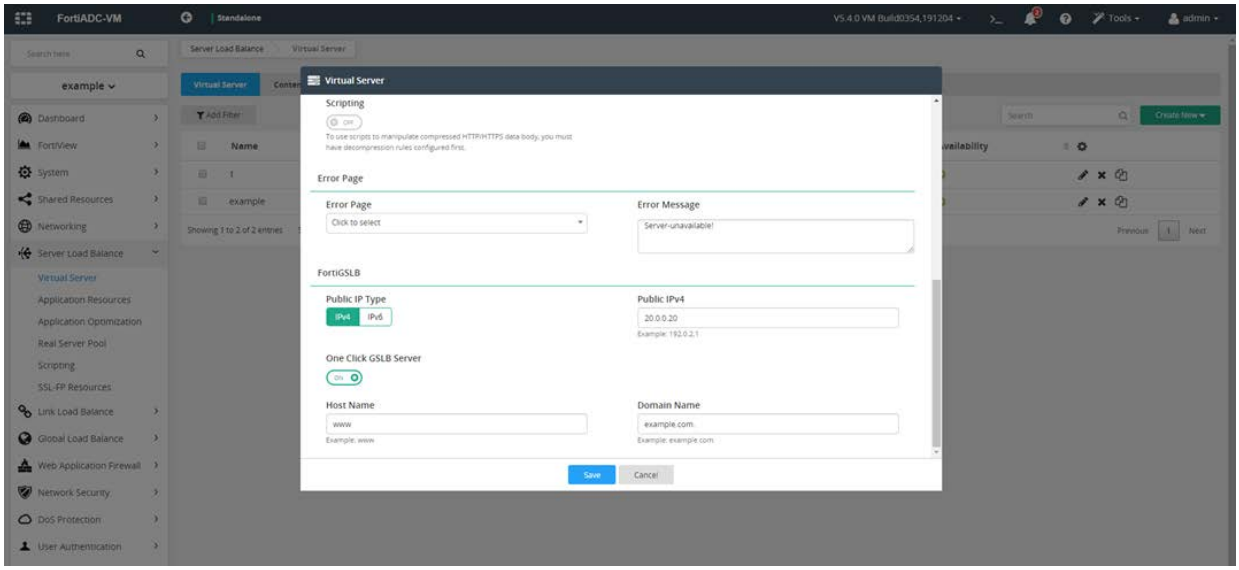


Ensure the Cloud Status on the top is green. Green means the connection has succeeded, whereas red indicates failure. The Assigned DNS Server shows the DNS server address. "Not assigned" means the DNS Server is not assigned.

If it is red, moving the cursor onto it will result in an error message showing up.

There may be some lag time. Refresh if necessary.

5. In a second browser tab/window, log into FortiAppSec Cloud, and navigate to GSLB. Refresh the page to check if your organization now appears on the Management Console dashboard. The default organization is labeled 'Default.' For details on the current dashboard, refer to the GUI Dashboards section.
6. Return to **FortiADC > root > Server Load Balance > Virtual Server**. Create a virtual server with GSLB enabled and set the Host/Domain name. Go to **General** and enable the One Click GSLB Server. This will reveal the Host Name and Domain Name.



7. After you save, the virtual server's information will show in **WAF > System > Settings > GSLB** (or **WAF > Security Fabric > Fabric Connectors > GSLB** for FortiADC releases 6.0 and above). Your virtual servers should show up at the bottom under Virtual Server. If configured correctly, the FortiADC will send the IP addresses, host name and domain name to GSLB, which will then load-balance with these virtual servers.

If over 50 virtual servers have enabled GSLB, we recommend using at least 30 seconds as GSLB's interval.

View virtual servers in GSLB

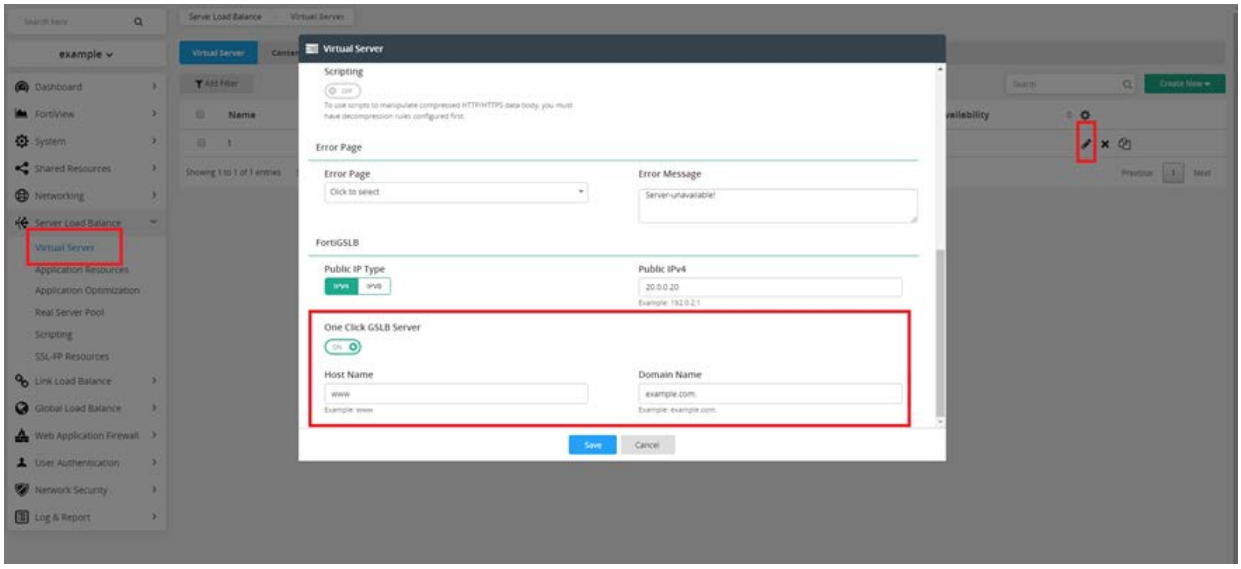
1. Go to GSLB and click into individual organization. In this example we are selecting the default organization, "default". We will see the virtual servers in GSLB.
2. In the individual organization, go to **Fabric Connectors**. The name is the FortiADC serial number. The type is FortiADC. The data center is the default or the first data center you already configured in Cloud. Click **edit** and you will see your virtual servers. **Note:** The load balancing may take a little while to start when the "green" is lit in the FortiADC.
3. In **Profiles > Pool** you will see the automatically generated virtual server pools that the Cloud has done for you. Click **edit** on the far right to see the IP addresses of the virtual servers. They are pooled according to your PREFERRED method. See the Virtual Server Pool on page 348 section for more information.

Returning customers

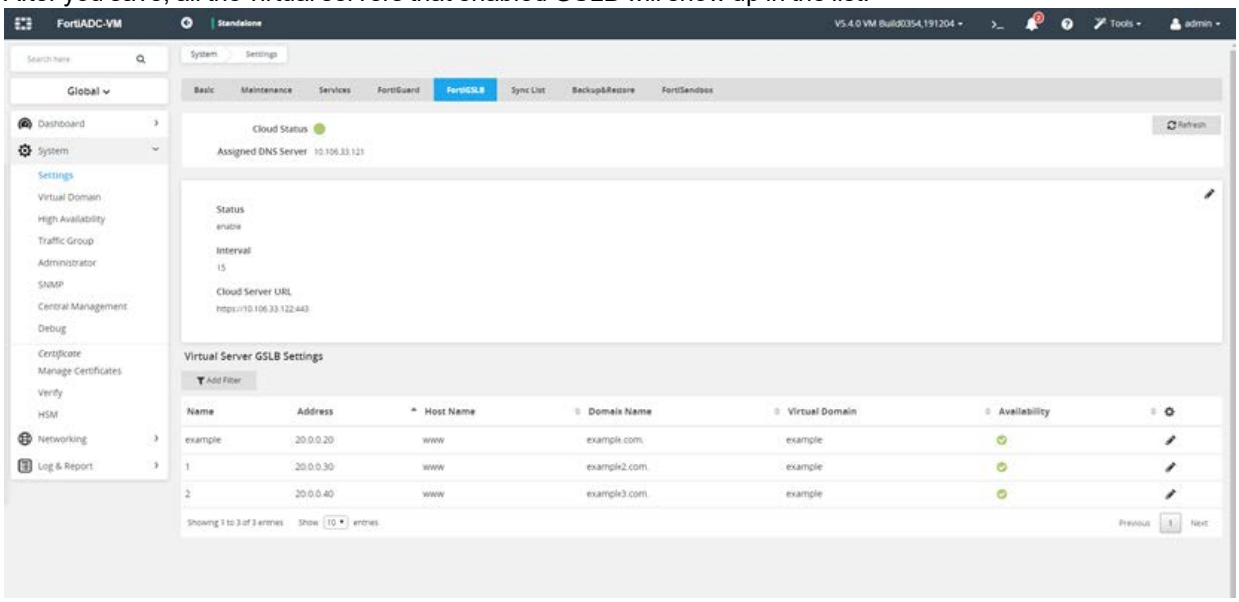
This section assumes that you have already enabled GSLB and know how to create new virtual servers with GSLB enabled.

To add more virtual servers into GSLB and support certain services:

1. Go to **FortiADC > Server Load Balance > Virtual Server > edit Virtual Server > General > Enable One Click GSLB Server** and enter Host/Domain Name.



2. After you save, all the virtual servers that enabled GSLB will show up in the list.



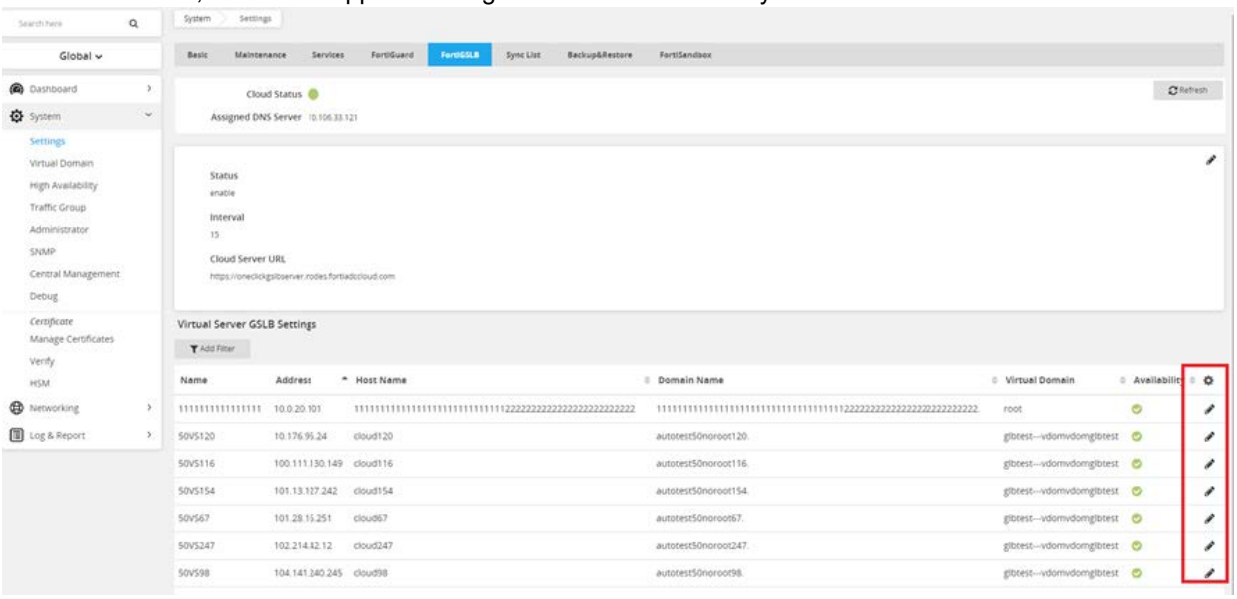
Further steps for modifications:

If you want to modify FQDN host/domain name or disable Virtual Server GSLB function, there are two ways.

Method 1

Go to GSLB to edit the virtual server that has already enabled GSLB.

From GSLB 2.0.0, FortiADC supports editing the virtual server directly inside the FortiADC GSLB module.



You can edit the Virtual Server and modify One Click GSLB-related parameters. To do so, disable One Click GSLB server. The virtual server will disappear from GSLB list afterwards.

Method 2

Go to **FortiADC > Server Load Balance > Virtual Server > edit Virtual Server > General**. You can modify the FQDN host/domain name or disable Virtual Server GSLB function here.

How to transform FortiADC GSLB to FortiAppSec Cloud GSLB

Object type	FortiADC location	FortiAppSec Cloud location
Data Center	Global Load Balance > Global Object > Data Center	GSLB > Virtual Server > Data Center
Server	Global Load Balance > Global Object > Server	GSLB > Virtual Server > Fabric Connectors
Location	Global Load Balance > FQDN Settings > Location List	GSLB > Service > Location
Virtual Server Pool	Global Load Balance > FQDN Settings > Virtual Server Pool	GSLB > Service > Virtual Server Pool
FQDN	Global Load Balance > FQDN Settings > Host	GSLB > Service > FQDN
Zone	Global Load Balance > Zone Tools > Zone	GSLB > DNS
Health Check	Shared Resources > Health Check > Health Check	GSLB > Health Check

Add FQDN with FortiADC

Perform the following steps to add an FQDN with FortiADC.

1. Create FQDN in GSLB services.
2. Create FQDN member and create new Virtual Server Pool. Then choose the virtual server from FortiADC into Pool. The virtual server from FortiADC will now work in GSLB services.
3. FortiADC virtual servers are synced with the Cloud, so please make sure to select the correct virtual server when adding it to the Pool

FortiGate Integration

This section covers all the use cases for using FortiAppSec Cloud with FortiGate.

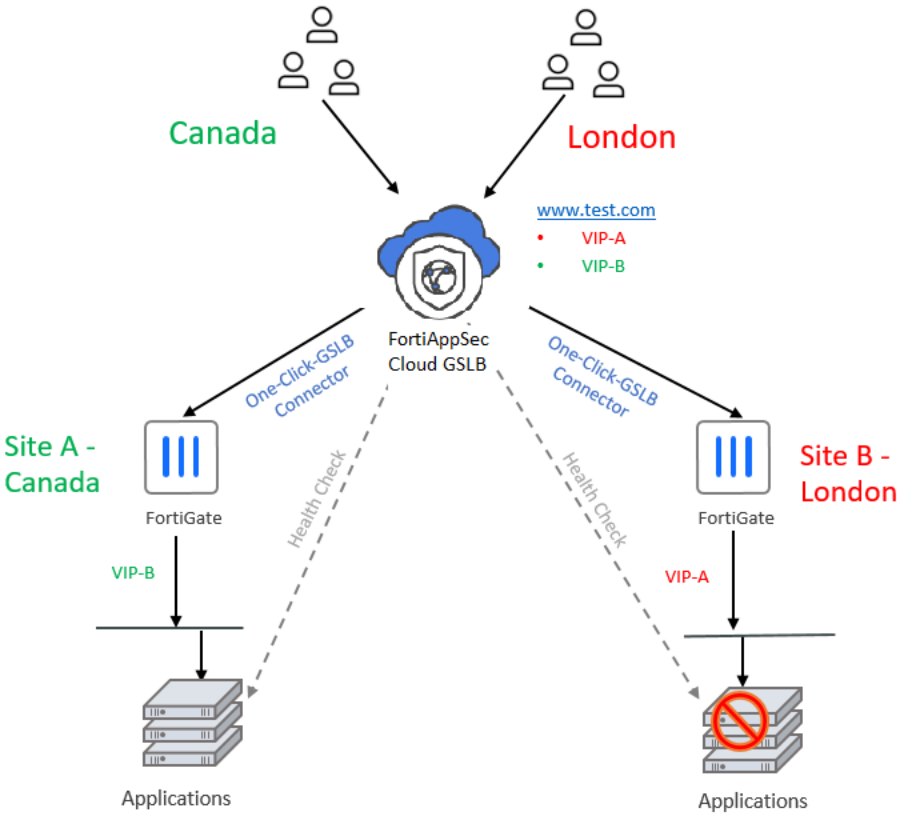
- FortiWeb Integration with One-Click GSLB
- Load balance FortiGate VPN servers to GSLB on page 390
- How to add FortiGate SD-WAN Inbound Load Balancing to GSLB on page 392
- How to add multisite LB (FortiGate) to GSLB on page 393

FortiGate Integration with One-Click GSLB

GSLB seamlessly integrates with FortiGate through the use of One-Click GSLB, streamlining server connections for enhanced efficiency. This section covers the following:

- Packet Flow on page 386
- Configuration prerequisites on page 386
- Configuration steps on page 386
- How to check the status of the FQDN on FortiAppSec Cloud GSLB on page 387
- How to view/edit FortiGate connector via GSLB after integration on page 388
- How to load balance traffic based on geolocation on page 389

By enabling One-Click GSLB, FortiGate synchronizes the Fully Qualified Domain Name (FQDN) configuration with Virtual IP (VIP) or Zero Trust Network Access (ZTNA) server features. This is beneficial for FortiGate customers that would like to load-balance an application across multiple data centers, based on factors such as availability or geographical location. In such cases, you can publish this application using a single FQDN on FortiAppSec Cloud using one-click GSLB. The result is a single domain with multiple unique IP addresses corresponding to the different FortiGates.



Please note that this feature is currently only available through the command line (CLI) and does not support web GUI configuration.

Packet Flow

1. The client sends a DNS query to the GSLB (www.test.com)
2. GSLB will redirect the user (based on the application Health Check) to the most available application according to the Geolocation, load, proximity, and service availability.

Configuration prerequisites

- The account of FortiGate's license should have a valid GSLB QPS license as well as a valid HC license.
- To enable a connector, the account license for FortiGate must match that of GSLB.
- This feature is supported by FortiGate version 7.4.2.

Configuration steps



To ensure uninterrupted connectivity, update your configuration to redirect all outbound connections to 44.241.230.143

1. Enable GSLB connector from FortiGate.
   a. **CLI:**
   ```
   config system global
      set fortigslb-integration enable
   end
   ```
2. Configure the ZTNA/VIP policy and add the FQDN (hostname + domain) to the policy.
   a. **CLI:**

   Example VIP configuration:

   ```
   config firewall vip
      edit www-test-com
         set type server-load-balance
         set extip 13.2.211.56
         set extintf any
         set server-type ip
         set one-click-gslb-server enable
         set gslb-hostname "www"
         set gslb-domain-name "test.com."
      next
   end
   ```

   commands for setting up One-Click GSLB

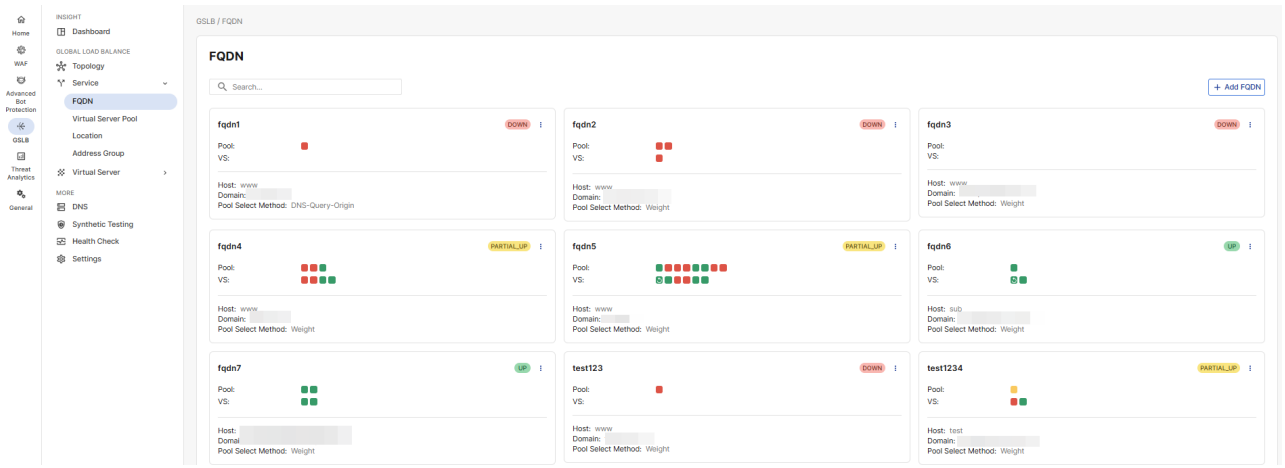
   Example ZTNA configuration:

   ```
   config firewall vip
      edit mail-oc-test-com
         set type access-proxy
         set extip 54.1.2.1
         set extintf port2
         set server-type https
         set one-click-gslb-server enable
         set gslb-hostname "mail"
         set gslb-domain-name "oc-test.com."
         set extport 25
         set ssl-certificate "Fortinet_SSL"
      next
   end
   ```

   commands for setting up One-Click GSLB
3. The FortiGate syncs the ZTNA/VIP configuration (along with the FQDN) to the GSLB via the One-Click GSLB connector.
4. You can always edit the VIP/domain/hostname on the FortiGate, which will automatically change on the GSLB.
5. Go to **Profiles > Health Check** and click **Create New** to set up a health check for your newly added FQDN. For more information and full descriptions of each field, see Health check on page 373.

How to check the status of the FQDN on FortiAppSec Cloud GSLB

1. Login to FortiAppSec Cloud and navigate to **GSLB > Service > FQDN**. This page shows all FQDNs in your account, including their status and the status of the associated virtual servers and pools.



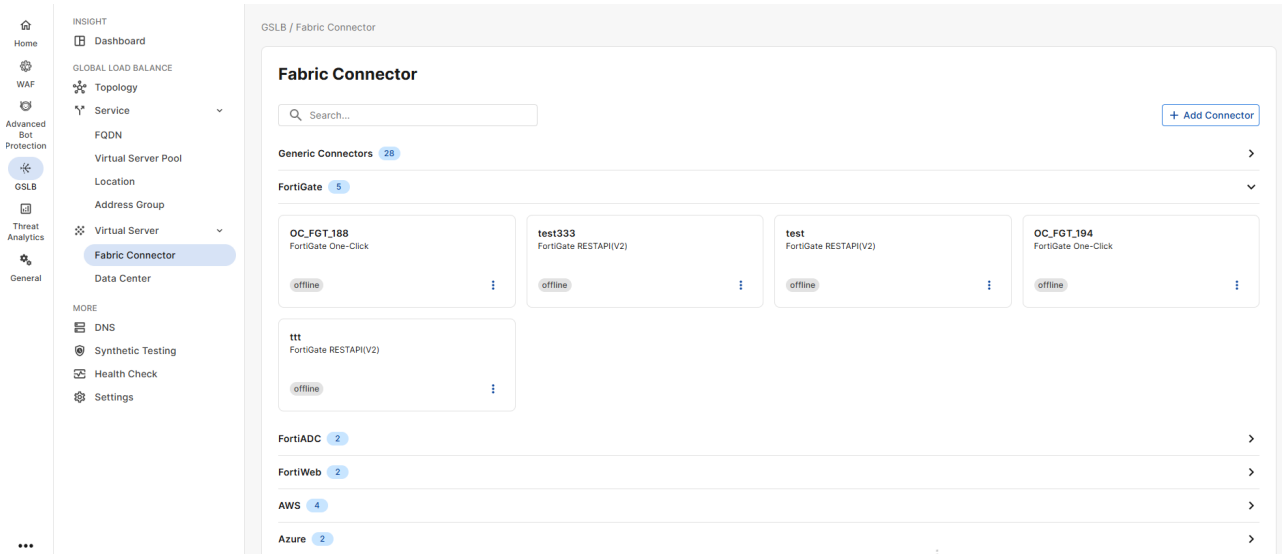
2.

If your FQDN does not appear in **GSLB Services** on the GSLB GUI, it could be due to the External IP (ExtIP) in the VIP/ZTNA being a private IP address. In other words, this refers to an IP reserved for use within private networks and is not routable on the public internet. In such instances, consider configuring the corresponding public IP address using `config gslb-public-ips` in the CLI.

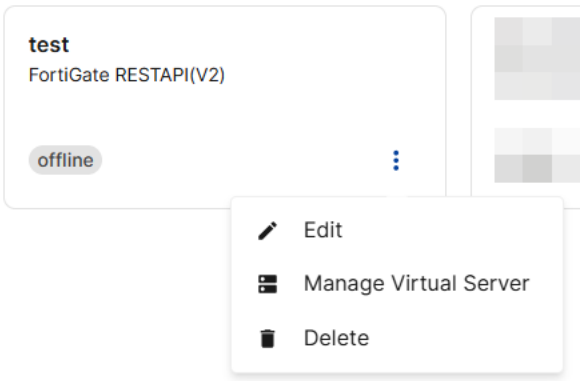
3. Once your health check is set up, you can also see the status of your servers in **Profiles > Health Check**. For more information and full descriptions of each field, see Health check on page 373.

How to view/edit FortiGate connector via GSLB after integration

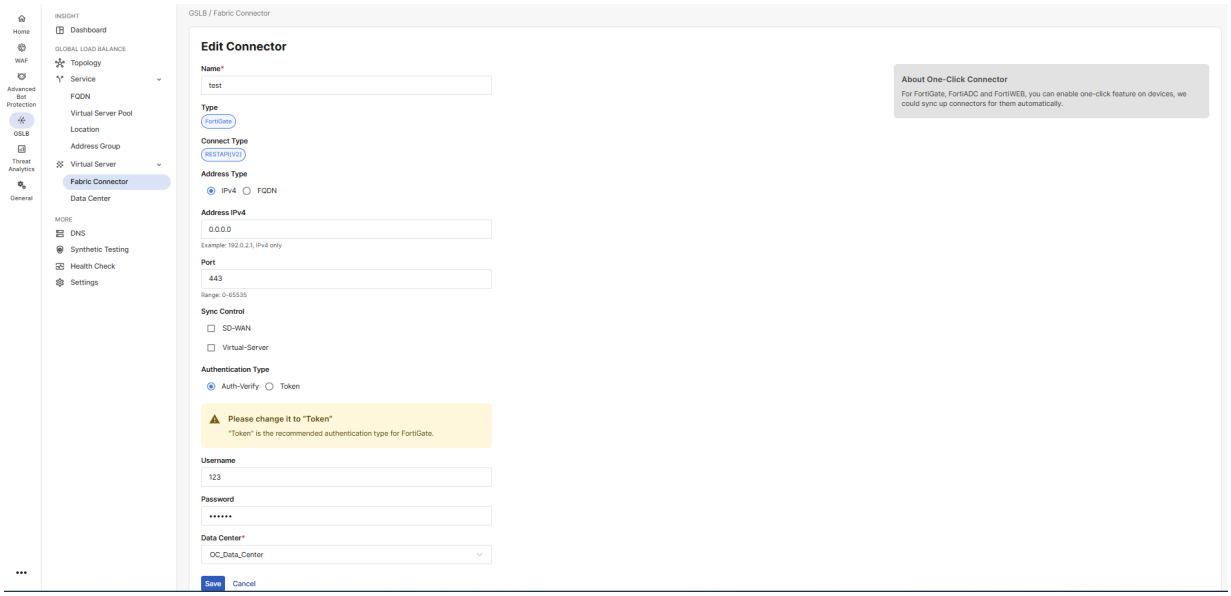
1. Navigate to **GSLB > Virtual Server > Fabric Connector** and locate the relevant FortiGate involved in this process to check its status.



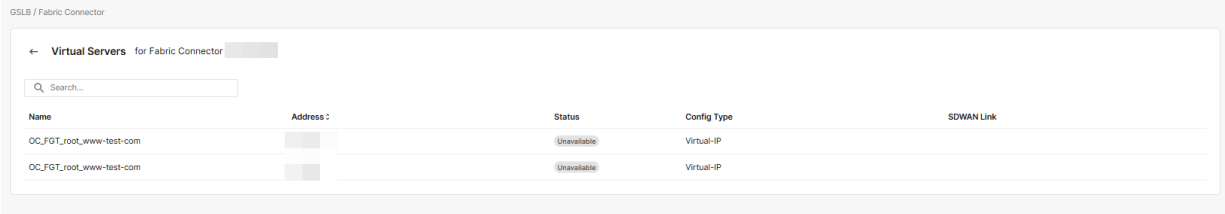
2. Expand the **Actions** by clicking the three dots in the top right corner of the desired connector.



a. To change connector configurations, click **Edit**.

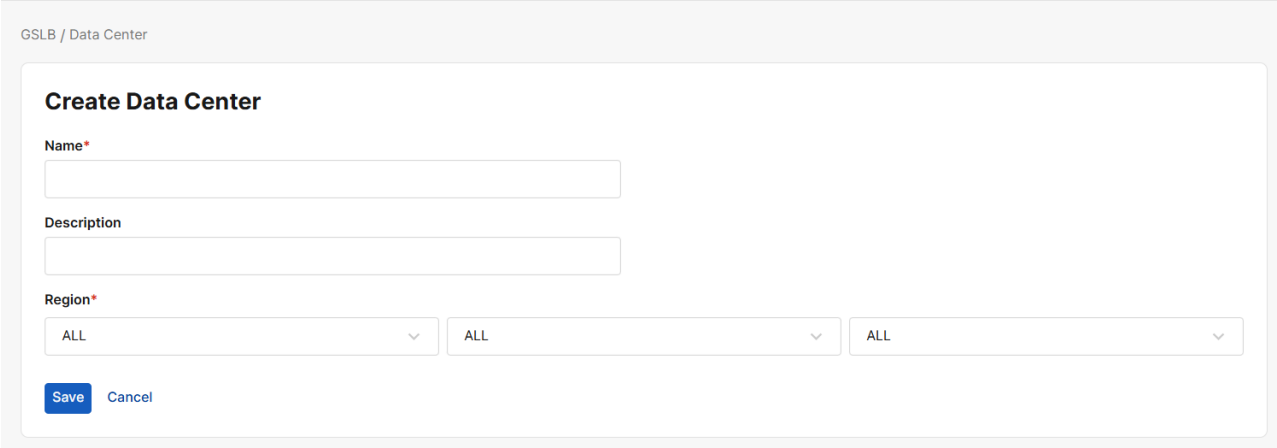


b. To view virtual servers, click **Manage Virtual Server**.



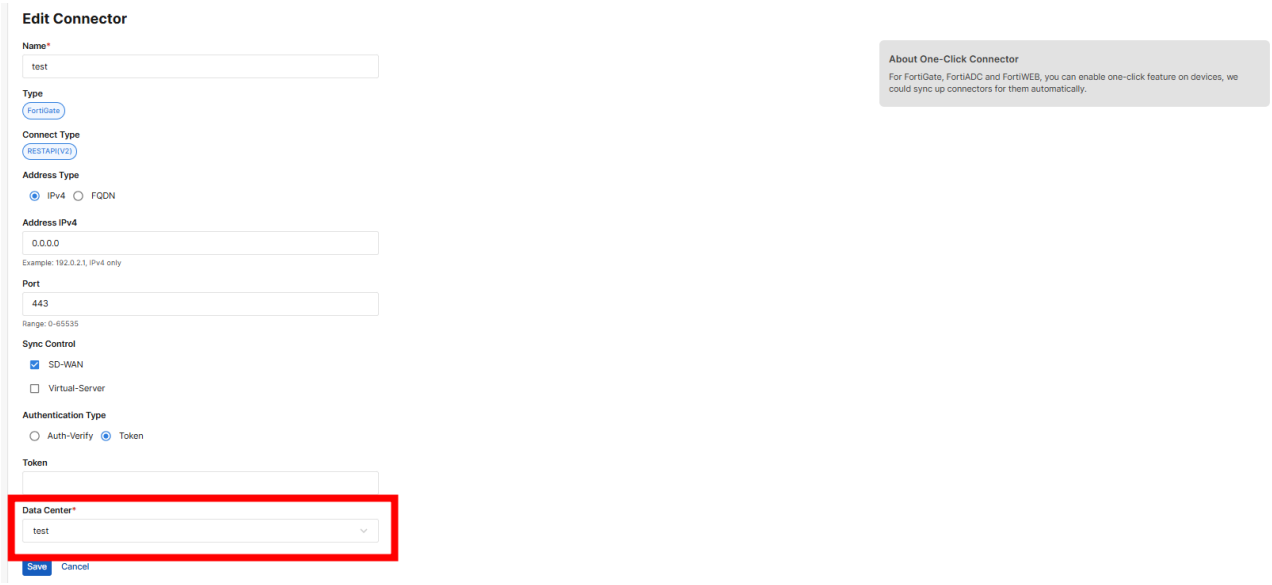
How to load balance traffic based on geolocation

1. Go to **Virtual Server > Data Center**
2. Click **Add Data Center** to create the data center for the connector. The default data center for One-Click GSLB is set the United States, but you can set your region to any option in the drop-down lists under **Region.**



3. Navigate to **Virtual Server > Fabric Connector** and click the edit icon next to the desired connector.

   In **Edit Connector**, open the drop-down list under Data Center and select the data center you created in the previous step.



4. Go **Service > Virtual Server Pool**, locate the desired Virtual Server Pool and click its corresponding **edit** icon.

   In **Edit Pool**, change the **Preferred LB Method** to **GEO**.

Load balance FortiGate VPN servers to GSLB

FortiAppSec Cloud enables clients to automatically connect to the most optimal FortiGate VPN server, ensuring efficient, high-speed access and reliable connectivity regardless of their location.

This section covers the following:

- Configuration Prerequisites on page 391
- Example Use case on page 391
- Configuration Steps on page 391

Configuration Prerequisites

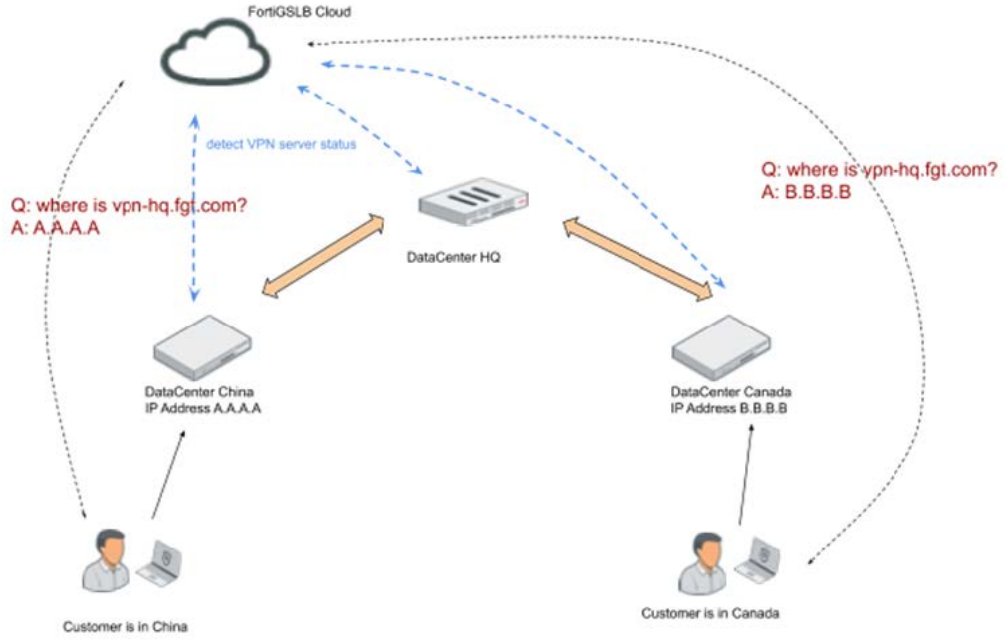
- A valid GSLB QPS license
- A valid HealthCheck license
- Allow the GSLB source IP addresses to access the FortiGate's restAPI. The source IP could be found at

Example Use case

In the following scenario, you have FortiGate VPN servers in two locations, each supporting a VPN service that connects to the company HQ.
GSLB manages these servers within a single pool, allowing for geographic load balancing of incoming traffic and real-time monitoring of the VPN servers' status.

If traffic originates from one location, GSLB directs it to the nearest available server. If that server becomes unavailable, the traffic is automatically redirected to the next available VPN server.

This setup ensures that clients from any location can enjoy optimal VPN performance and a fast connection to the company HQ, even while traveling.



Example solution

The diagram below illustrates the solution for when all the client's incoming traffic comes from one location.

Configuration Steps

To ensure uninterrupted connectivity, update your configuration to redirect all outbound connections to 44.241.230.143

1. Create a new FQDN for your FortiGate VPN in **GSLB Services**.
   a. For this example, the name of the FQDN will be 'VPN-hq.fgt.com'.
   b. For details on creating an FQDN, refer to Configuring GSLB Objects on page 316.

2. FQDN Member and Virtual Server Setup.
   a. Click *Create Member*. This option appears when you save the parent record from the previous step.

   b. Create a new virtual server. In this example, we will call it 'Pool1'.

      i. If you would like to load balance based on physical location, select *GEO* as the preferred method.

      ii. Click *Save*.
3. Create a pool member, a FortiGate connector, and a new connector member
   a. Create a pool member for 'Pool1' and create a new FortiGate Connector. We will refer to this connector as 'fgt-VPN1'.

   b. Create a new Data Center and create a new connector member. We can refer to this member as 'VPN1-DC1'.
   c. Add FortiGate 'VPN IP VPN1-DC1' Public IP and enable health check of your choice. In this case, we have enabled 'Default_HLTHCK_ICMP'.
4. Repeat step 3 for all additional Virtual Servers.

Note: The virtual server from the FortiGate Connector will be added into Pool and Connector directly and will work in GSLB services.

Sample topology view in GSLB

We have added each FortiGate VPN server into the GSLB pool. GSLB will load balance client traffic geographically using connector locations.

After completing these steps, the customer can monitor the VPN service status from both Location DC1 and Location DC2 on the GSLB Service detail page. The GSLB will load balance the traffic to the connector that have the nearest location. If the nearest location VPN server is down, the GSLB will direct the traffic to other available location. If both VPN service servers are not available, the GSLB will direct traffic to the default VPN server.

Note: The virtual servers from the FortiGate connector will be added into Pool and Connector directly and will work in GSLB Services.

How to add FortiGate SD-WAN Inbound Load Balancing to GSLB

Integrating FortiGate SD-WAN inbound load balancing with GSLB ensures high availability and optimized performance for an application by distributing traffic across multiple links and providing automatic failover to the default server when necessary.

This section covers the following:

- Example solution on page 393
- Configuration Steps on page 393

Example solution

This example illustrates the solution for when all the incoming traffic comes from one ISP.

The example assumes that the customer has three ISP routers. The FortiGate SD-WAN has three members for each ISP. The SD-WAN will do the out-going load balance for App1, but in some cases the incoming traffic will keep coming from ISP1 and ISP2, which causes the ISP1 and ISP2 links to be very busy and leaves ISP3 link very free.

To solve this issue, GSLB can load balance the incoming traffic to ISPs from the DNS level.

Configuration Steps



To ensure uninterrupted connectivity, update your configuration to redirect all outbound connections to 44.241.230.143

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use an existing Virtual Server.
2. Create FortiGate connector in **Fabric Connectors** and wait few seconds to sync virtual servers.
3. Bind SD-WAN link with virtual servers in FortiGate Connector.
4. Create FQDN for your SD-WAN application in GSLB services.
5. **Create FQDN member > Create new Virtual Server Pool**. Select Connector member *ISP1/ISP2/ISP3*, enable health check Default_HLTHCK_HTTP, and choose SDWAN-InBandwidth as the preferred method.
6. The virtual server from the FortiGate Connector will be added into the Pool and will work in GSLB services.

Sample topology view in FortiAppSec Cloud GSLB

After completing these steps, the customer will be able to monitor the App1 status for all ISPs on the GSLB service detail page. The GSLB will load balance the traffic to three links. If one of the links is down, the GSLB will direct the traffic to the available link. If all of the links are down, the GSLB will direct the traffic to the App1 default server.

How to add multisite LB (FortiGate) to GSLB

This use case describes multisite LB in cases of connector failure/busy. For customers who hold multiple datacenters with FortiGate and want to make sure the service is always on, GSLB can check FortiGate service availability and redirect users to the nearest available site.



To ensure uninterrupted connectivity, update your configuration to redirect all outbound connections to 44.241.230.143

Perform the following steps to add multisite LB (FortiGate) to GSLB:

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use the existing Virtual Servers.
2. Create two FortiGate connectors in **Fabric Connectors > Create Connector > Create data center**. Enable Virtual Server in Sync Control and enter FortiGate information. Wait a few seconds for the Virtual Servers to sync.
3. Navigate to **GSLB Services > Create FQDN**. Create an FQDN member and Create a new Virtual server Pool. Select GEO as the preferred method.
4. **Create pool member** and select Virtual Servers that synced from the two FortiGates.
5. The virtual servers from the multisite FortiGate connectors will be added into Pool and work in GSLB Services.

Example solution

This example illustrates the solution for the situation when all the incoming traffic comes from one data center.

This example assumes the following:

- You have two FortiGate connectors from different data centers.
- Every FortiGate has one member that supports App2 service.

Sometimes, the incoming traffic that comes from data center1, or from places close to data center1, will go to the connector (FortiGate) located in data center2, which is far away from the client, thus possibly causing long time latency and resource waste.

The GSLB can load balance the incoming traffic to the nearest available site according to the incoming traffic location and redirect to another site if that one is not available.

Also, GSLB will load balance the traffic by weight if no FortiGate service site matches the location.

Perform the following steps:

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use the existing Virtual Server.
2. Create FQDN App2-www.fgtdc.com in GSLB Services.
3. Create two FortiGate connectors with different Data Centers.
   a. Create a new FortiGate connector 'fgt-server1' and Create a new Data Center 'DC1'.
   b. Enter FortiGate1's IP/Auth and enable Sync Control for the virtual server.
   c. Wait a few seconds before refreshing to check that the virtual server has synced.
4. **Create FQDN member > Create new Virtual Server Pool** and use GEO preferred method
5. **Create pool member** and select FortiGate fgt-server1 Virtual Server APP2 DC1 Public IP 202.0.20.22 and enable health check Default_HLTHCK_HTTP.
6. **Create pool member** and select FortiGate fgt-server2 Virtual Server APP2 DC2 Public IP 54.20.0.23 and enable health check Default_HLTHCK_HTTP).

Sample topology view at GSLB

We have added two pool members to do the load balancing and each member belongs to one data center.

After completing these steps, the customer can monitor the App2 service status from both DC1 and DC2 on the FQDN service detail page. The GSLB will load balance the traffic to the service site that have the nearest data center. If the nearest data center is down, the GSLB will direct the traffic to other available data center. If both service sites are not available, the GSLB will direct the App2 default server.

Fabric connectors with AWS and Azure

The AWS and Azure connectors for GSLB provide seamless integration with AWS EC2, and Azure virtual machine and load balancer environments; enabling comprehensive load balancing and visibility for your cloud-based servers. This solution leverages the full configuration from AWS and Azure, ensuring optimal distribution of traffic and enhanced performance for your applications.

This section covers the following:

- Example Use Case on page 395
- How to configure a fabric connector with AWS on page 396
- How to configure a fabric connector with Azure on page 397
- Virtual Server Status on page 398
- Running Instances with Dynamic IPs on page 398

Key Features of AWS and Azure connectors

1. Automated Discovery and Configuration: Automatically integrate AWS EC2 instances and Azure VMs into GSLB, simplifying configuration management.
2. Intelligent Load Balancing: Distribute traffic across cloud instances based on health and performance metrics for optimal routing.
3. Enhanced Visibility and Monitoring: Gain insights into server performance and traffic patterns through detailed analytics and reporting.
4. Scalability and Flexibility: Easily scale application infrastructure and manage resources across AWS and Azure from a single interface.

Example Use Case

Scenario

A multinational e-commerce enterprise requires continuous availability and optimal performance for its web applications across multiple regions. The enterprise uses AWS EC2 instances in North America and Azure virtual machines in Europe to host its application servers.

Solution

1. Integration
   - GSLB connects to the enterprise's AWS and Azure environments, automatically discovering all EC2 instances and VMs.
   - The configuration details, including instance types, IP addresses, and region information, are imported into GSLB.
2. Load Balancing
   - GSLB distributes incoming traffic based on server health and load, ensuring that no single server is overwhelmed.
   - Real-time health checks are performed to dynamically adjust traffic flow, directing users to the best-performing servers.
3. Visibility
   - Detailed dashboards provide insights into server performance, traffic distribution, and user access patterns.
   - Alerts and notifications are set up for any performance issues or downtime, enabling proactive management.

4. Scalability
   - Automatically integrate additional instances during peak times, optimizing costs during off-peak times.

Benefits of AWS and Azure connectors

- Improved Performance: Ensures users are directed to the best-performing servers, reducing latency and enhancing user experience.
- High Availability: Maintains application uptime by distributing traffic across multiple cloud instances and regions.
- Comprehensive Monitoring: Provides deep visibility into server health and performance for informed decision-making.

How to configure a fabric connector with AWS



If you already have an AWS user with the necessary permissions and an *Access key* and *Secret access key*, you can skip to the last step.

1. Log into your AWS account, then go to *IAM* > *Users* and create a new user.
   Assign the *AmazonEC2FullAccess* and *AmazonEKSClusterPolicy* permissions to the user.
2. Generate Access Keys:
   a. Select the newly created user and generate a new pair of *Access key* and *Secret access key* where needed.
   b. For *User Case*, choose *Third-party service*.
3. Log into FortiAppSec Cloud, go to *Fabric Connectors* and click *Create Connector.*
   Enter the following fields on this page:

Field	Description
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	Select the type of connector you are creating. In this case, choose AWS. For more details on the different options, refer to Fabric connector on page 353.
AWS Access Key	Paste the *Access Key* from AWS.
AWS Access Secret	Paste the *Secret Access Key* from AWS.
Region	Eligible resources in the selected region will be synced to GSLB. For guidance on factors to consider when choosing a region, refer to the AWS documentation.

Once you click *Save*, the following should now be synchronized to FortiAppSec Cloud:

- EC2 instances that are running, regardless of whether their IP addresses are dynamically assigned.
- EC2 instances that are shut down but have an elastic IP assigned.
- Load Balancers

Keep in mind the following for IPv6 Addresses:

- EC2 instances or VMs with only IPv6 addresses will be synced, whether they are running or shut down.
- EC2 instances or VMs with multiple IPv6 addresses will have each address treated as a separate virtual server in GSLB.



Starting in version 25.2, the AWS connector supports both EC2 instances (IP-based) and Load Balancers (domain name–based) as endpoints.

For EC2 instances, the connector continues to use **A/AAAA** Record Types in both the FQDN and Virtual Server Pool (VSP).

For Load Balancers, the connector uses **CNAME** Record Types for the FQDN and VSP.

How to configure a fabric connector with Azure



If you already have an Azure user with the necessary permissions and a *Tenant ID, Client ID, Client Secret,* and *Subscription ID*, you can skip to the last step.

1. Create a New Application:
   a. Log into your Azure account and go to *App Registration* > *New registration* to create a new application.
   b. In the new application, create *Client credentials.*
   c. The tenant ID can be found on the application overview page.
2. Assign Role to the Application:
   a. Go to *Subscriptions* > *Access control (IAM)* > *Add role assignment*.
   b. Search and select *Virtual Machine Contributor* > *Next.*
   c. Select members, then search and select the new application created in step 1.
   d. Review and assign. The subscription ID can be found on the *Subscriptions* overview page.
3. Enter required information to FortiAppSec Cloud:

Field	Description
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	Select the type of connector you are creating. In this case, choose Azure. For more details on the different options, refer to Fabric connector on page 353.
Tenant ID	Copy and paste the Tenant ID from Azure.
Client ID	Copy and paste the Client ID from Azure.
Client Secret	Copy and paste the Client Secret from Azure.
Subscription ID	Copy and paste the Subscription ID from Azure.
Resource Group	The resource group of your virtual server(s). For more information on resource groups and how to manage them, please refer to Azure documentation.
Location	Select the region of your virtual server(s) from the drop-down list. For more information on Azure regions, please refer to Azure documentation.

a. Click **Save**. The following should be synchronized to FortiAppSec Cloud:
   - Virtual Machines that are running, regardless of whether their IP addresses are dynamically assigned.
   - Virtual Machines that are shut down but have a static IP assigned.
   - Load Balancers.

Please note the following for Load Balancers:

- A running VM added to a load balancer will be removed from the “Virtual Machines” list.
- Load balancers will be synced even without any virtual machines.
- If a VM is part of a Load Balancer, both its IPv4 and IPv6 addresses will not appear under “Virtual Machines.” If this VM is added to a pool, its virtual server status will be shown as down in “Virtual Machines.”

Virtual Server Status

When your AWS or Azure credentials have successfully connected to GSLB, you will be able to see the EC2 instances, Virtual Machines, and Load Balancers from your AWS or Azure account.

To view your virtual servers, navigate to the edit connector page by going to *Fabric Connectors* and clicking on the edit icon corresponding to the connector you want to view.

The colored dots to the right of each virtual server indicate its status, as follows:

- Green: The virtual server is “AVAILABLE.”
- Red: The virtual server is “UNAVAILABLE,” which occurs when the EC2 or VM is down or when the key and credentials are deactivated.
- Grey: The virtual server is "UNKNOWN".

  This occurs when an EC2 instance with both IPv4 and IPv6 addresses changes only one IPv4 address after rebooting. If the virtual server is part of a pool, it must be manually deleted and re-added.

  If an EC2 or VM has a single IPv4 address, it updates automatically after changes.

  A stopped VM with a detached static IPv4 address will show as grey.

  Updating credentials without access permission will also result in a grey status.

Running Instances with Dynamic IPs

Please note the following for running instances with Dynamic IPs:

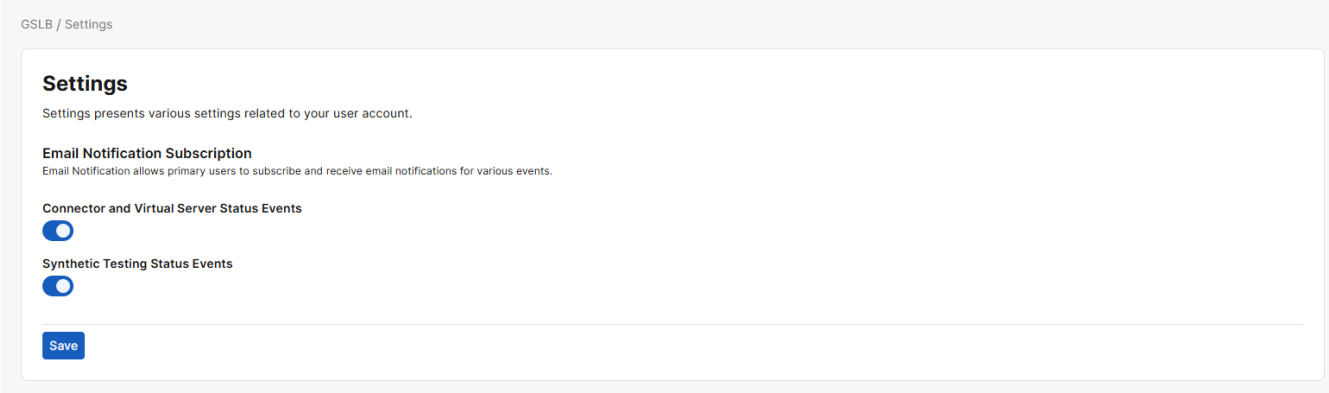
- If not added to a virtual server pool, the virtual server will be deleted if it is shut down.
- If added to a virtual server pool, the virtual server will **not** be deleted if it is shut down.

GSLB Settings

Email Notification Subscription

Subscribe or unsubscribe from email notifications for the following events. Notification emails will be sent to your registered email address.

- Connector and Virtual Server Status Events
- Synthetic Testing status events


GSLB / Settings
Settings
Settings presents various settings related to your user account.
Email Notification Subscription
Email Notification allows primary users to subscribe and receive email notifications for various events.
Connector and Virtual Server Status Events
Synthetic Testing Status Events
Save

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.

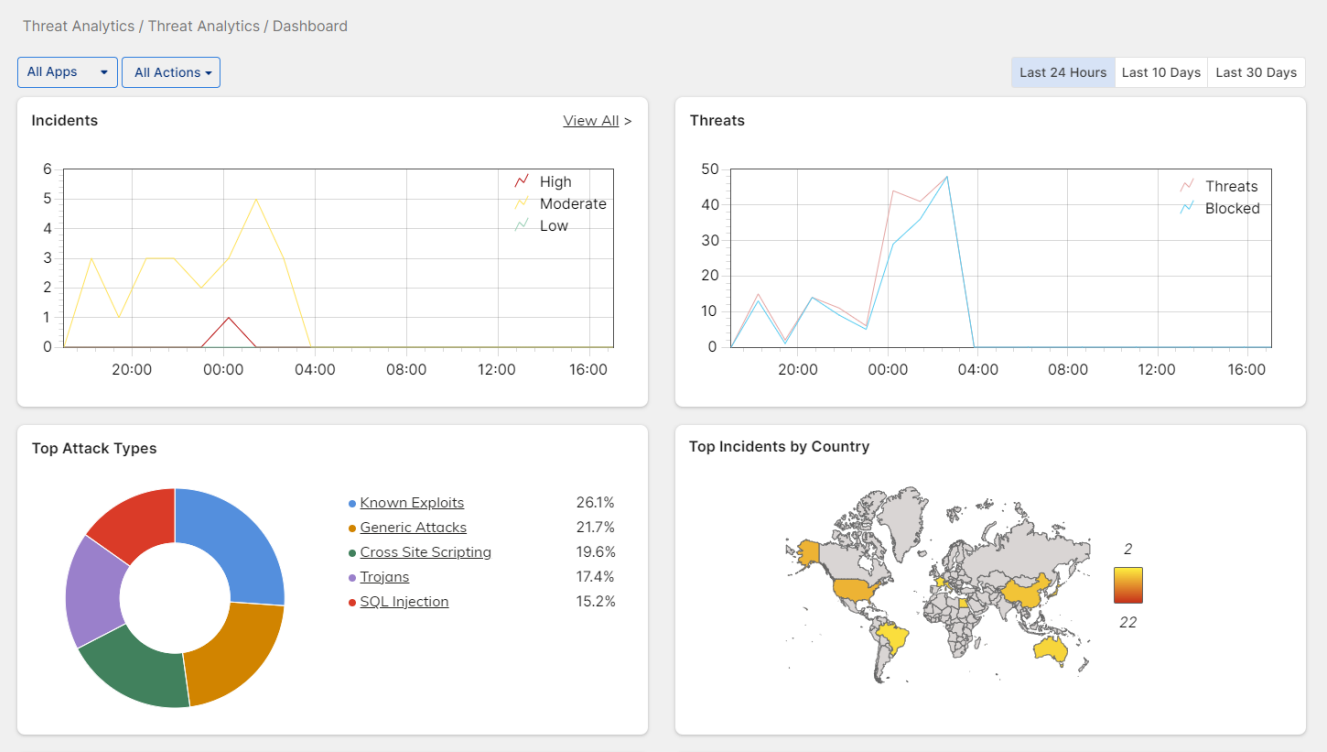
- Threat Analytics Dashboard on page 400
- Incidents
- Insights
- Settings
- Attack logs on page 412
- Gateways on page 423
- Security Operations Center-as-a-Service (SOCaaS) on page 423

Threat Analytics Dashboard

The default **Threat Analytics Dashboard** page opens when you click on **Threat Analytics** in the side navigation bar.

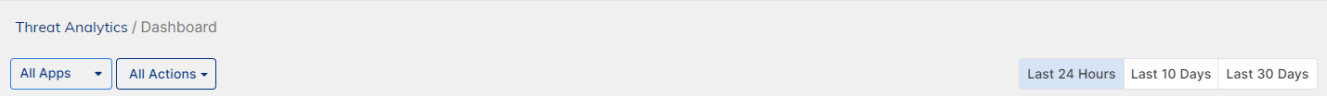
This section covers the following:

- Filter on page 401
- Widgets on page 401



Filter

You can narrow down the scope of these visualizations by specifying the desired application(s), attack types, and time frame of the attacks shown.



To filter by application, click on **All Apps** to expand the list of all applications on your account.

To filter by action, such as **Monitor** or **Block**, click on **All Actions** to expand list of options.

- When you select **Monitor**, the widgets on this page only reflect attacks that have been logged, but not interrupted.
- When you select **Block**, the widgets on this page only reflect attacks that have been stopped from reaching your application.

To filter by time frame, select one of the three options on the right side of the page:

- Last 24 hours
- Last 10 days
- Last 30 days

Widgets

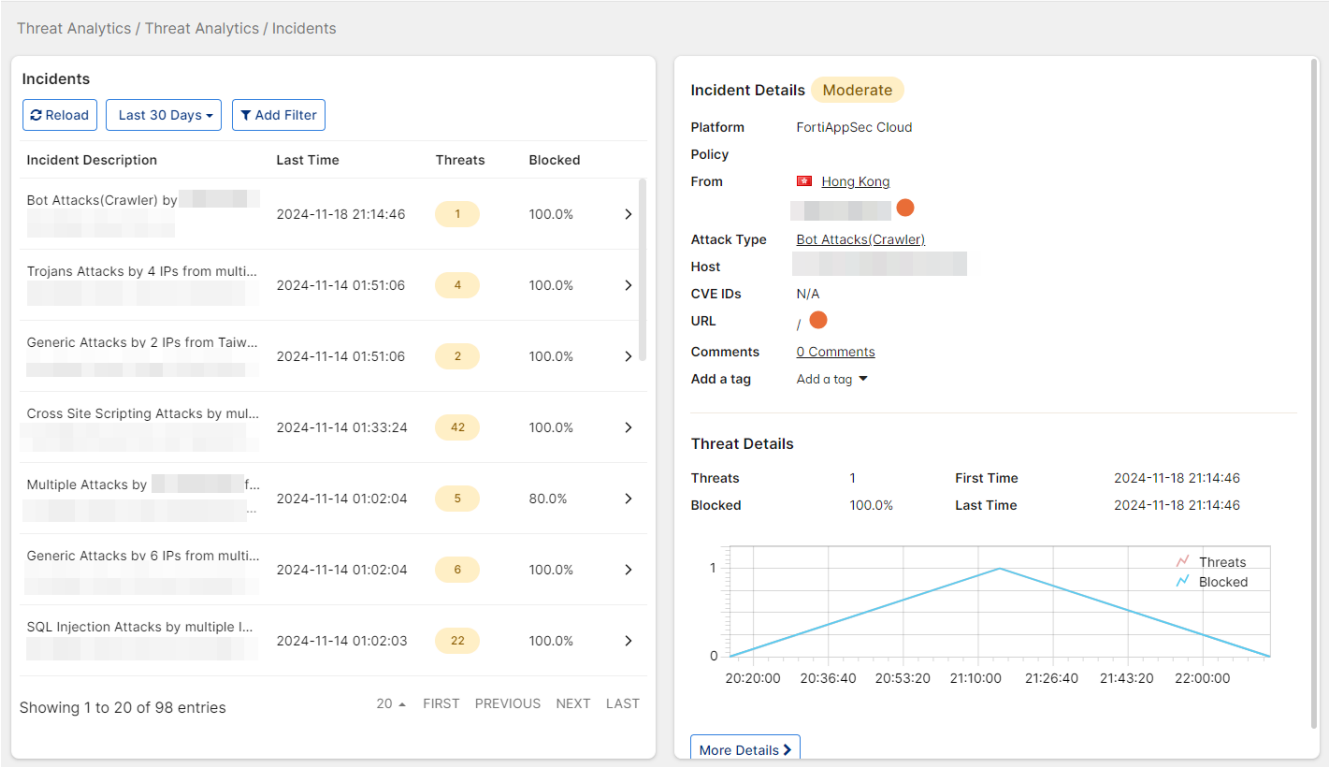
The **Threat Analytics Dashboard** displays widgets that provide insights to the attack traffic detected on your applications.

The following table highlights the information contained in each of the widgets:

Widget	Description
Incidents	Three lines that depict the number of notable incidents over the selected time frame. Each line represents a different level of severity. Hover over a line to see the number of incidents of the selected severity at the selected time.
Threats	Two lines that depict the number of threats, and the number of blocked interactions over the selected time frame. Hover over a line to see the number of threats or blocked interactions at the selected time.
Top Attack Types	Displays the pie chart distribution and percentage of most common attack types on your application.
Top Incidents by Country	A map displaying the geographical locations with the highest incidence of incidents.
Top Attacked Resources	A ranked table of applications on your platform with the highest number of threats, showing their platform and the Block/Monitor ratio for each.
Top Incidents by Severity	Displays the highest-severity activity on your applications.
Top Attacks by CVE ID	Displays the distribution and percentage of most common attacks by CVE ID. A CVE (Common Vulnerabilities and Exposures) is a publicly disclosed cybersecurity vulnerability or exposure that has been assigned a unique identifier, allowing it to be tracked and managed across different platforms and security systems.

Incidents

Attack events are aggregated into incidents based on common characteristics, allowing you to quickly identify frequent attack types, the most malicious source IP addresses, and more.

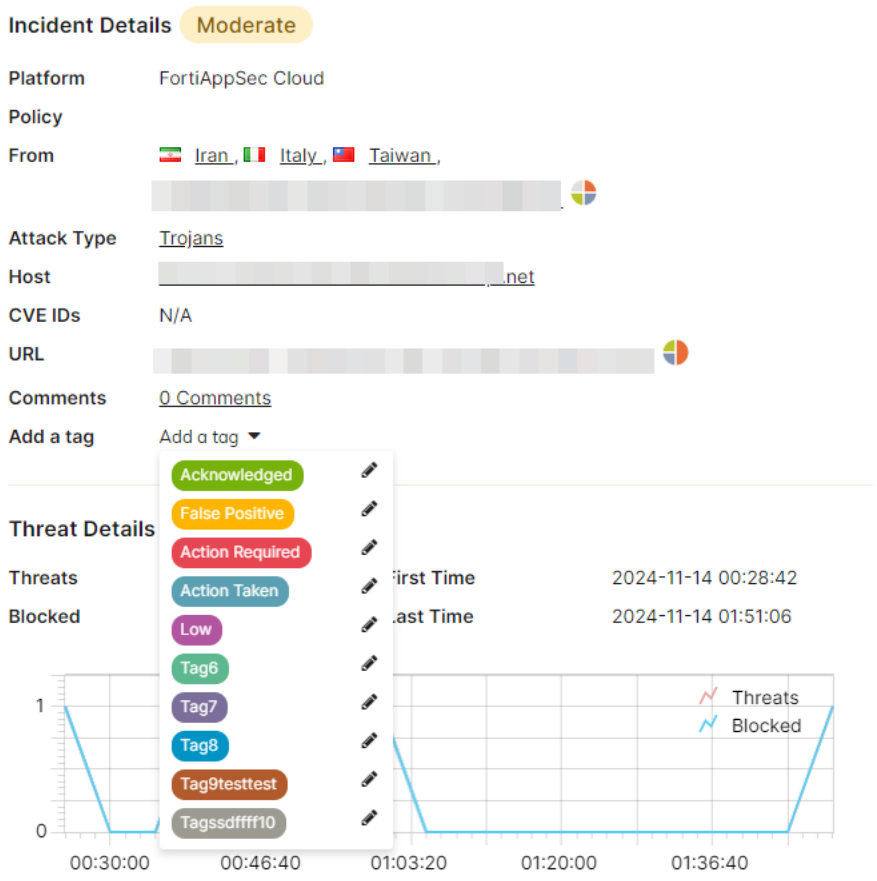


Selecting an incident reveals details such as the attack type, target application, and source IPs.

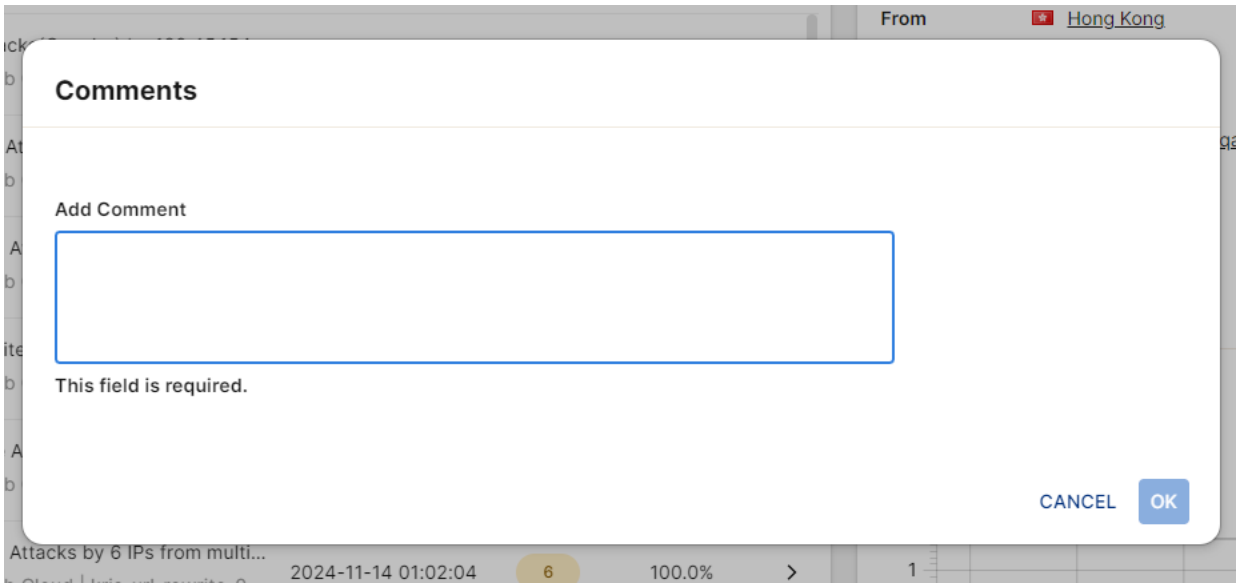
You can filter the displayed Incidents by the Last detected time, App Name, Attack Type, CVE ID, Device, Host, Incident ID, Source Country, Source IP, and Tag.

Incident Organization

You can add tags with predefined labels to mark incidents, which updates their status icons for easier tracking. These labels are for your reference only and do not affect the system's threat detection but help with organizing incidents for sorting, filtering, and acknowledgment. Tag names can also be edited to suit your needs.

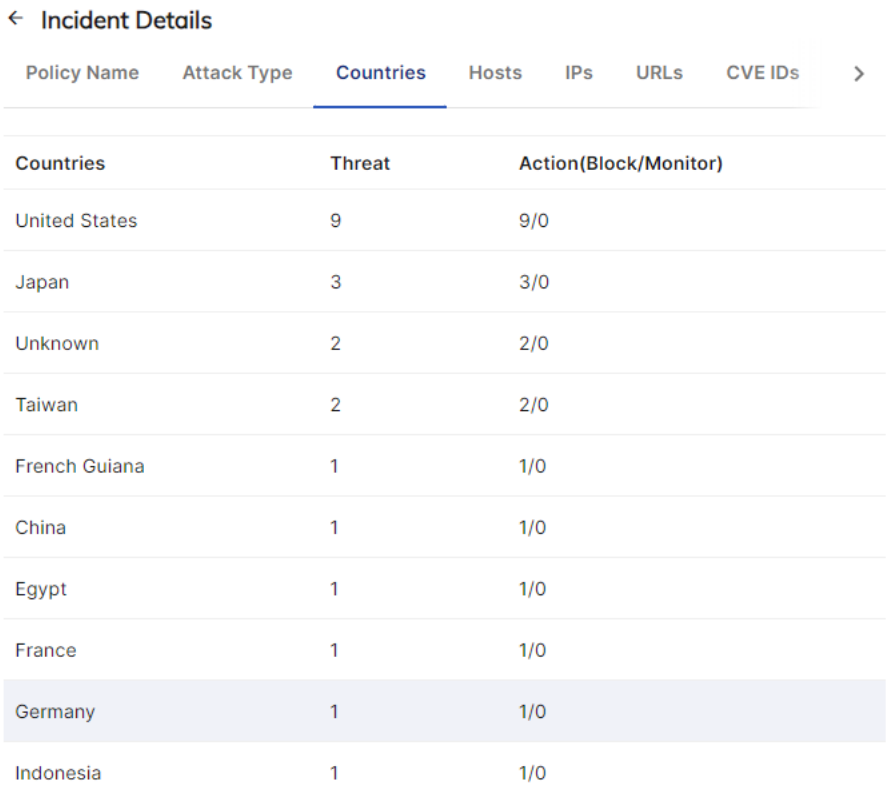


Additionally, you can use the **Comments** link under **Incident Details** to add notes to an incident.



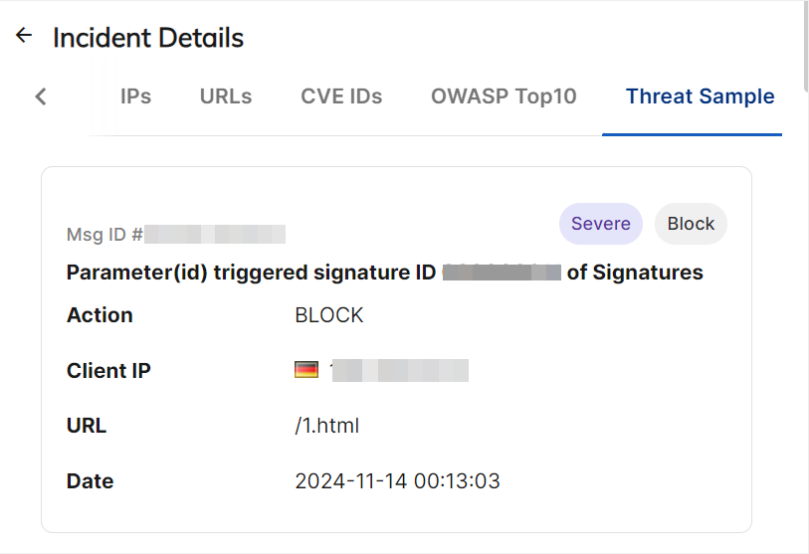
Additional Incident Details

You can access additional information on the selected incident by scrolling down **Incident Details** clicking **More Details**.



When you click on any detail category on this page (except for Threat Sample), a table is displayed showing the information described below, along with the corresponding threat count and block/monitor ratio. The block count indicates how many transactions were blocked, while the monitor count represents the total number of transactions detected for this incident.

Detail Category	Descripion
Policy Name	The name of the afflicted application.
Attack Type	The type of attack(s) detected by Threat Analytics. Examples include SQL Injections, Cross-Site Scripting, and Trojans Attacks.
Countries	The countrie(s) from which attacks in the recorded incident originate.
Hosts	The host(s) of the afflicted application.

Detail Category	Descripion
IPs	The Client IP address(es) from which the attack came from.
URLs	The URL(s) on your domain where the attacks occurred.
CVE IDs	The CVE ID(s) associated with the incident. CVE IDs are unique identifiers for tracking publicly disclosed cybersecurity vulnerabilities. They follow the format CVE-YYYY-NNNNN (e.g., CVE-2023-12345) and are managed by the CVE Program, overseen by MITRE. If no CVE ID is associated with this attack, this will display as N/A.
OWASP Top 10	The OWASP Top 10 risk(s) associated with the incident. The OWASP Top 10 is a list of the most critical security risks to web applications, published by the Open Web Application Security Project (OWASP).
Threat Sample	This page lists out each detected transaction within the incident and lists out its description, Action, Client IP address, URL, and date detected. 

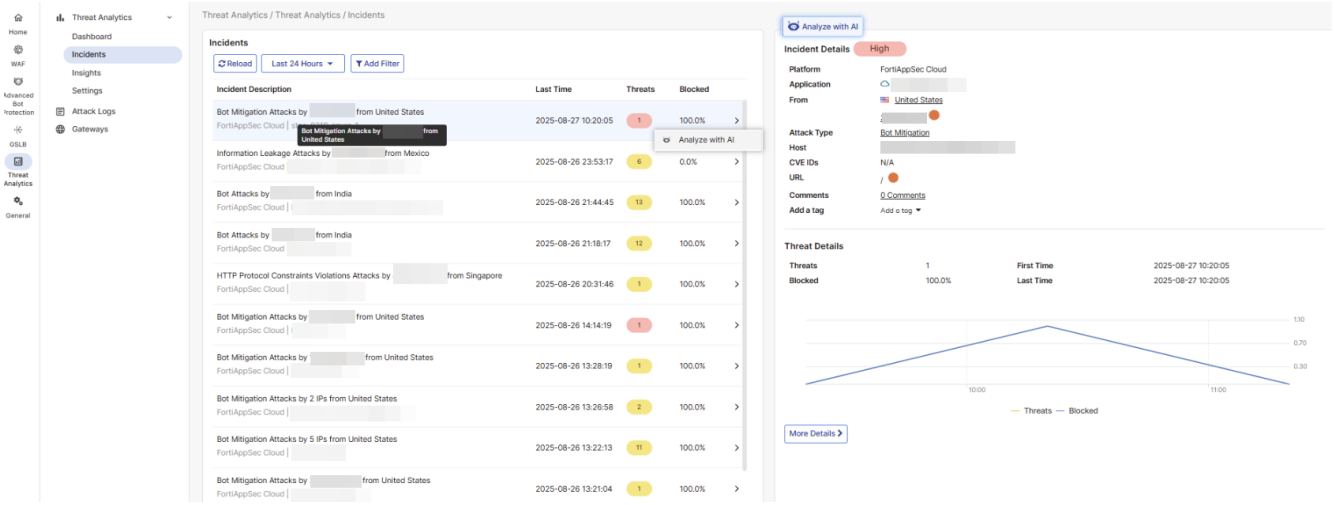
Analyze with AI

Click **Analyze with AI** to see AI-generated summaries and insights for Threat Analytics (TA) incidents, streamlining incident review and decision-making.

- **Contextual Summaries**: Generates a summary for each TA incident, including type, severity, risk level, affected resources, timeline, source IP, geolocation, false positive status, acknowledgment, and recommended next steps.
- **Natural Language Queries**: Submit plain-language queries to filter incidents; the system retrieves matching incidents and displays an AI-generated summary or trend overview.

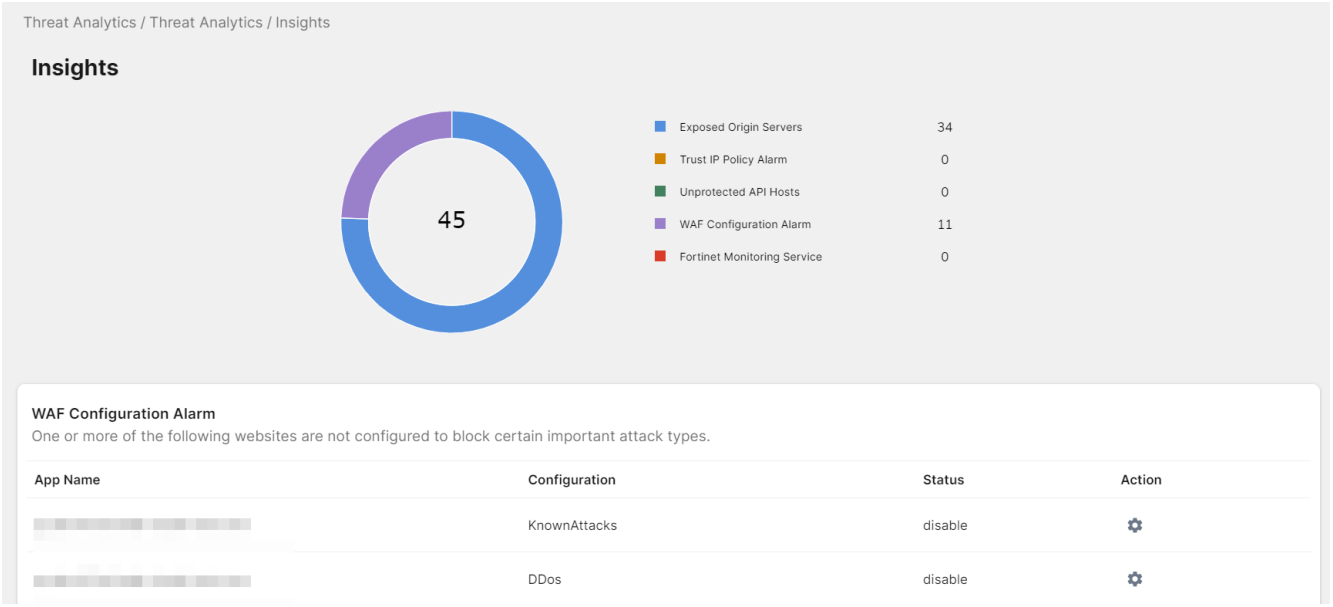
  Prompt examples:
  - "Summarize all bot-related incidents in TA which is come from US IPs in the past week"
  - "What are the top 5 attacks by CVE ID over the past month?"

  - "What are the trends in attacks coming from the United States over the past week?"
- **Validation & Access**: Only authenticated users can access summaries; queries must use supported schema dimensions, and results include only relevant fields.
- **Error Handling**: Displays fallback messages if summaries cannot be generated, queries fail, or no incidents match; provides suggestions or examples as needed.
- **Feedback & Guidance**: Shows loading status, result counts, and options to view or export; includes tooltips and inline help for queries.



Insights

The Insights page adds another level of incident analysis and provides recommendations to enhance your security posture.



The pie chart on this page shows the highest security risk factors in your application, along with the number of violations detected for each risk factor across your applications.

Clicking on one of the listed threats next to the pie chart will modify the table below the chart to show information specific to the selected threat, along with information for suggested actions.

Threat	Description
Exposed Origin Servers	This refers to situations where parts of your application expose the address of the physical or virtual machine hosting the application and/or database software. Examples include when the Origin Server IP is directly accessible through HTTP/HTTPS requests or is visible in public DNS records.
Trust IP Policy Alarm	This threat occurs when your account's **Trust IP** list contains IPs with a bad reputation that have been identified as malicious. We recommend removing these IPs immediately from the **Trust IP** list in **Access Rules > IP Protection**.
Unprotected API Hosts	This threat occurs when one of the hosts in your account is not protected by API security. When this occurs, we recommend enabling **ML based API Protection** to automatically discover and protect all API endpoints.
WAF Configuration Alarm	This refers to when one or more websites on your account are not configured to block important attack types. To better protect your application, please find the suggested page under **Configuration** in the table below, and navigate to said page under **WAF**.
Fortinet Monitoring Service	This includes threats detected by engineers through Fortinet's managed services, such as SOCaaS.

Settings

Attack logs Export

Attack logs provide detailed insights for individual applications, helping track and analyze security events.

Export attack logs to a log server

Please note, you can configure up to five log servers for attack log export at one time.

1. Navigate to **Threat Analytics > Settings**.
2. Click **Add Log Server**.
3. Select move applicable WAF Applications from the **Available** list to the **Selected** list.
   - » Moves all applications from the **Available** to the **Selected** list.
   - › Moves selected applications from the **Available** to the **Selected** list.

- « Moves all applications from the **Selected** list to the **Available** list.
- ‹ Moves selected applications from the **Selected** list to the **Available** list.

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 FortiAnalyzer, FortiSIEM, Syslog, and ElasticSearch.

- If you selected **FortiAnalyzer**, configure the following.

  FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides centralized logging and analysis, plus end-to-end visibility.



- FortiAnalyzer is supported. However, FortiAnalyzer Cloud is not.
- When configuring the corresponding ADOM on FortiAnalyzer, please set the **Type** to **FortiWeb**.
- FortiAnalyzer supports assigning devices to different ADOMs, provided that each OU's master account is associated with a distinct contract (i.e., a unique serial number).

  However, if the organization has enabled Contract Sharing Mode, all OU accounts share the same contract and serial number. In this case, FortiAnalyzer treats them as a single device, which prevents assigning them to different ADOMs.
- When configuring FortiAnalyzer as the log server, supported versions depend on the FortiAppSec Cloud serial number prefix and contract type. Refer to the table below for the corresponding FortiAnalyzer versions.

Serial Number Prefix	Contract Type	Supported FortiAnalyzer Versions
UCAPFW	Fortinet Contacts	7.4.7, 7.6.2
UCAPFE	FortiFlex Contracts (Pre-Paid)	7.6.5
UCAPFM	FortiFlex Contracts (Post-Paid)	
FUCAPP	Fortinet Private Cloud Contracts	
APPSEC	Public Cloud Subscription	

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	This option is only available when you select **SSL** under **Protocol**. 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.

- If you selected **FortiSIEM**, configure the following:

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	This option is only available when you select **SSL** under **Protocol**. When enabled, the system will enforces server certificate verification before it sends attack logs to the log server.
Log Format	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.

- If you selected **Syslog**, configure the following:

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:**FortiAppSec Cloud automatically retrieves the SSL certificate used to encrypt the HTTPS connections between the log server and FortiAppSec 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. See Custom Log Fields on page 411 • **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.

- If you selected **ElasticSearch**, configure the following.

  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.

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 FortiAppSec Cloud. The source IPs are as follows:

- 3.226.2.163
- 3.123.68.65

Custom Log Fields

Below is a list of all supported log fields when **Log Format** is set to **Custom**.

Field Name	Placeholder	Example
Date and Time	dt	2025-02-19T19:34:05-05:00
Date	date	2025-02-27
Time	tm	19:34:05
Time Zone	tz	-05:00
UTC Date	utc	2025-02-20T00:34:05
Timestamp	ts	1740011645000
Log Type ID	li	20000007
Message ID	mid	098765432123
Application ID	eid	1234567890
Application Name	an	ftnt-app1
Application Domain	ed	docs.fortinet.com

Field Name	Placeholder	Example
Template Name	tn	My Template
Source IP	si	0.00.000.00
Source Port	sp	80
Destination IP	ds	123.456.789.0
Destination Port	dp	443
Source Country	sc	Canada
Service	svc	https/tls1.3
Login User	lu	Unknown
Main Type of Threat	mt	Known Attacks
Sub Type of Threat	st	Cross Site Scripting
Threat Level	tl	Severe
Threat Weight	tw	10
Action	act	Block
HTTP Host	hh	fortinet.com
HTTP URL	hu	/ContactUs.aspx
HTTP Version	hv	1.x
HTTP Method	hm	POST
HTTP Agent	ha	gp-vcloud-director
HTTP Refer	hr	none
Signature ID	sid	010000009
Signature CVE ID	sci	N/A
OWASP Top10	ott	A03:2021-Injection
Message	msg	Parameter(emailID) triggered signature ID 010000009 of Signatures
Packet	pkt	"packet string"

Attack logs

The Attack Logs display logs from all applications. You can click on an entry to view detailed threat information or use the Add Filter option to filter threats as needed. Click Reload to refresh the page and load any new logs recorded since the last time it was accessed.

Unlike FortiView, which organizes threat data into different categories, the Threat Analytics **Attack Logs** page lists all threats in a single table.

A maximum of 10,000 logs will be displayed per filter, and FortiAppSec Cloud retains attack logs for two months before they are deleted.

Please note that the number of attacks displayed in Attack Logs, FortiView Threat View , 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, FortiAppSec Cloud only logs the first request in Attack Logs and FortiView Threat View , 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, FortiAppSec 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 Threat View 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 FortiAppSec 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
20000010	Brute Force Login
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

Attack ID	Security Rule
20000018	GEO IP
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
20000033	Timeout Session
20000035	FTP File Security
20000036	FTPS Connection Failure
20000037	Machine Learning
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
20000051	Known Bots Detection
20000052	Client Management
20000053	Allow Only IP List

Attack ID	Security Rule
20000054	Web Shell Detection
20000055	Zero trust access
20000056	GRPC Security

Add Exception

If you know that a specific URL or parameter consistently triggers false positives by matching an attack signature during normal use, you can create an **exception** for that signature ID by clicking the three dots icon on the right side of any log entry, and clicking **Add Exception**. This prevents matching traffic from being flagged as an attack.

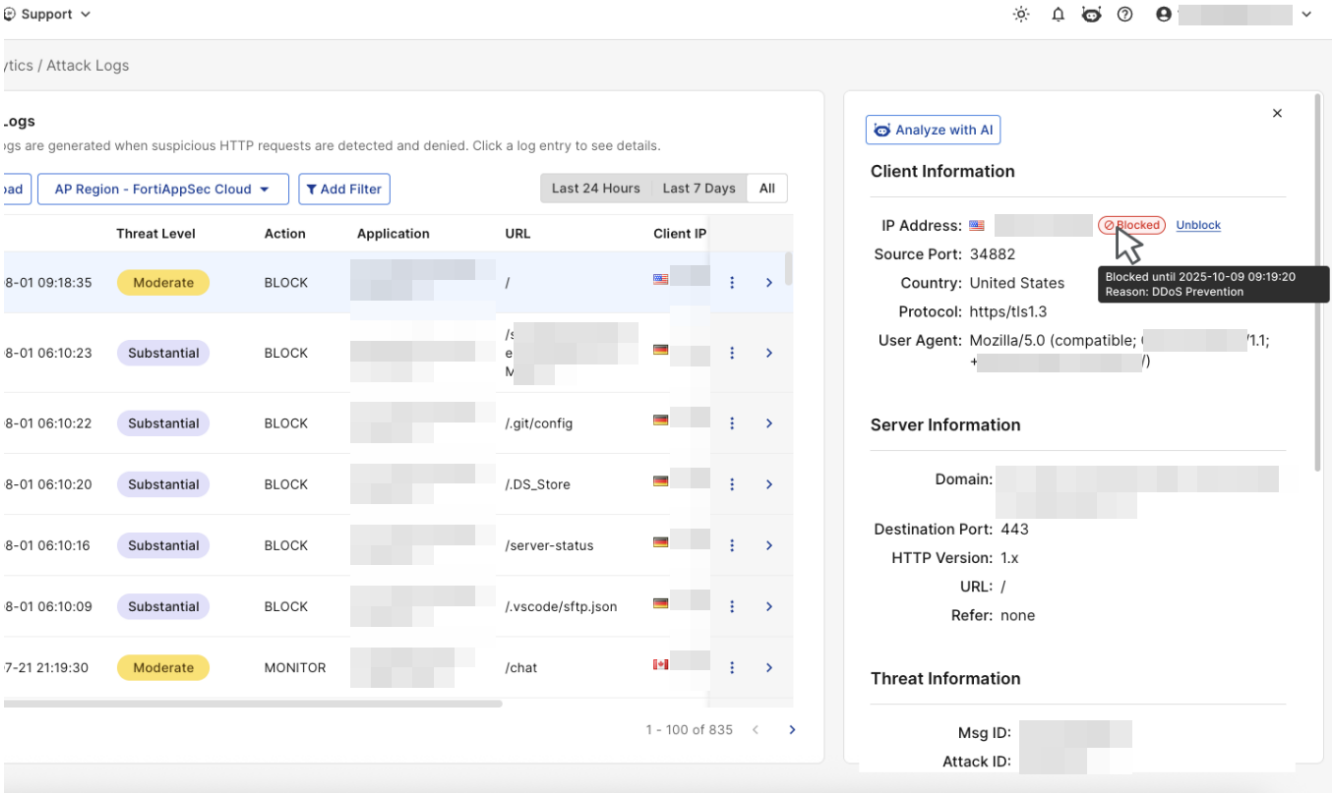
Please note, this feature is only available when the **main type** of an attack is **Known Attack**.

Request Host	Specify the host value (domain name) to match. For example, `www.test.com` or `api.test.com`. • If **String Match** is selected, is selected, enter the host name directly. Wildcards are supported (e.g., `*.test.com`). • If **Regular Expression Match** is selected, you can define a regex pattern to match one or more hostnames. For details, see Frequently used regular expressions on page 243.
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 243. 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 243.
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.

View Blocked Attack Details or Unblock

When an attack has been blocked, select the attack to open its details. Under **Client Information**, the **Blocked** tag and **Unblock** option are displayed.

- View block details: Hover over the **Blocked** tag to see the block duration and reason.
- Unblock the source IP: Click **Unblock** to allow the source IP to resume access to your application.



Forwarding FortiADC attack logs to Threat Analytics

Through the FortiADC integration with FortiAppSec Cloud Threat Analytics, you can forward FortiADC attack logs to FortiAppSec 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.

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

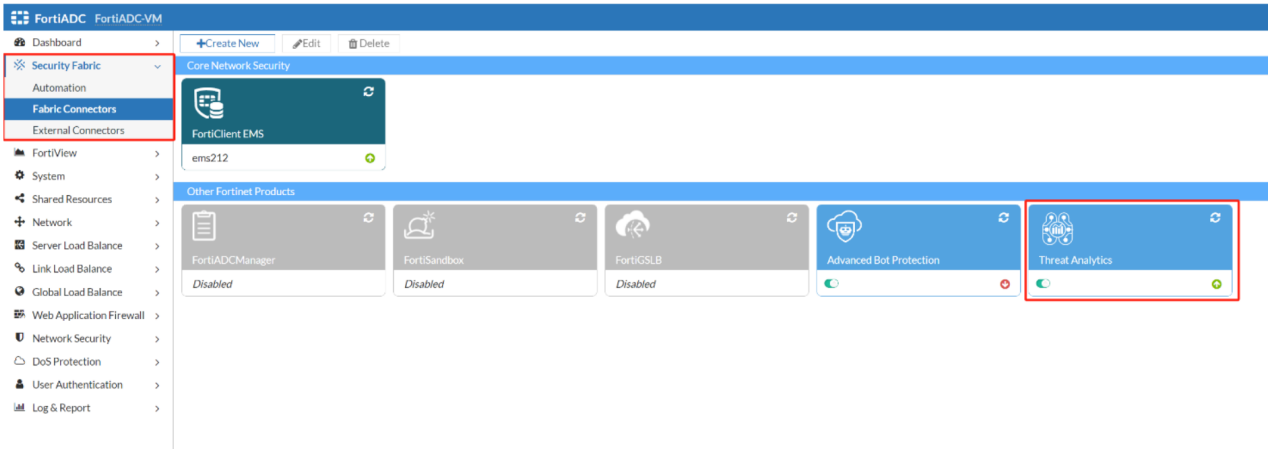
A 14-day Evaluation license is offered to customers who would want to evaluate the Threat Analytics service. This 14-day Evaluation license can only be used once. To activate the 14-day Evaluation license, enable Threat Analytics connector from **Security Fabric > Fabric Connectors**. During this 14-day 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. Log in to https://support.fortinet.com/ register the serial number for your FortiAppSec Cloud license. For details, please see Registering Assets.
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
```

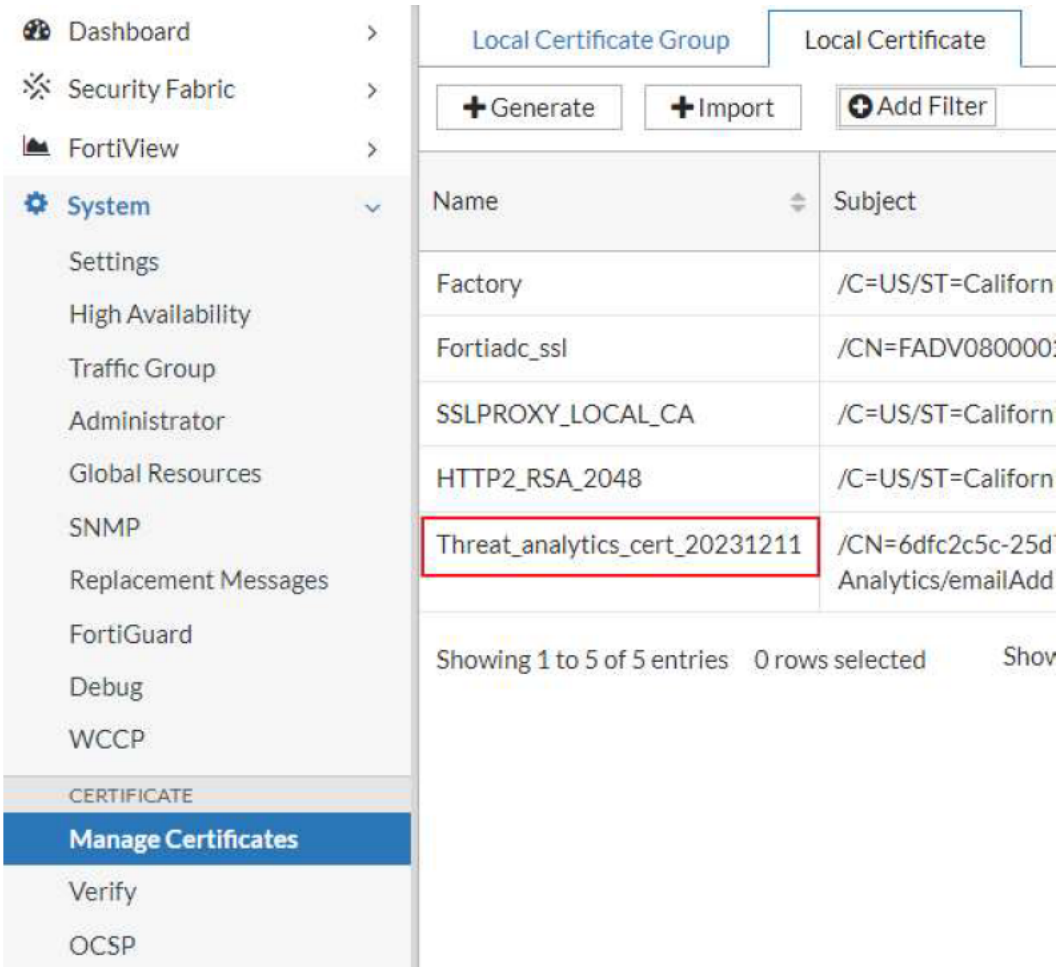
   If you do not have an active Threat Analytics contract, you will receive the following message:

```
FortiADC-VM # conf sys global

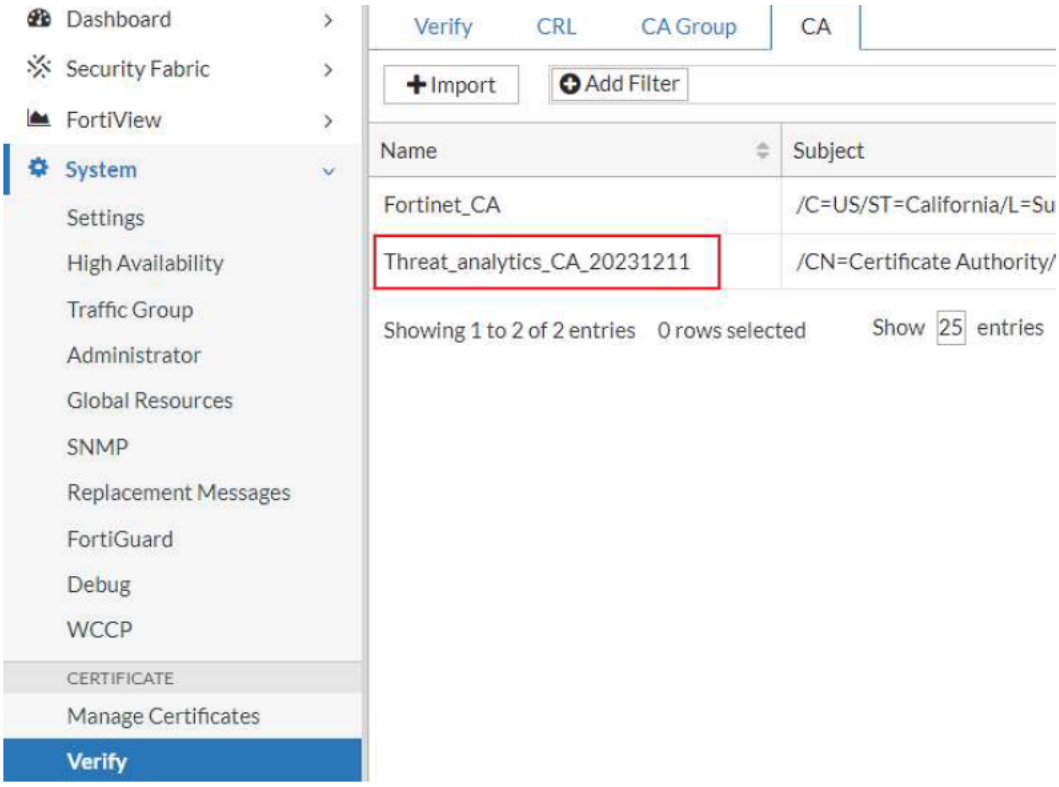
FortiADC-VM (global) # set threat-analytics enable

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 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>*.



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



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 FortiAppSec Cloud.
8. Log In to FortiAppSec Cloud with the account you used when registering your license on the Fortinet Support site.

Do not delete or modify the syslog remote and certificate/CA entry. Threat Analytics cannot function 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 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 FortiAppSec Cloud at the same time. As only the primary node is connected to FortiAppSec 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 FortiAppSec Cloud and performs several integral functions when Threat Analytics is enabled. This includes the following:

Command	Guidelines
	• Establishing a web socket connection with the FortiAppSec 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 FortiAppSec Cloud with FortiADC configuration changes, such as HA status changes, member updates, or mode modification. • Updating device certificates received from the FortiAppSec Cloud. Ifwassd registered to the FortiAppSec 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 FortiAppSec Cloud again with the latest CA issue date. • Starting the forwarding of FortiADC attack logs to FortiAppSec Cloud. If wassd has successfully registered to FortiAppSec 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

Forwarding FortiWeb attack logs to Threat Analytics

Attack logs on FortiWeb can be forwarded to FortiAppSec 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:

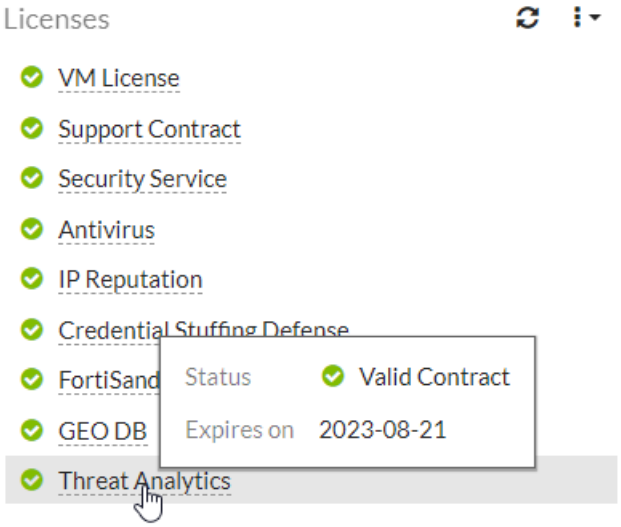
- You have a valid Threat Analytics service license.
- Threat Analytics service is enabled in FortiWeb.

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

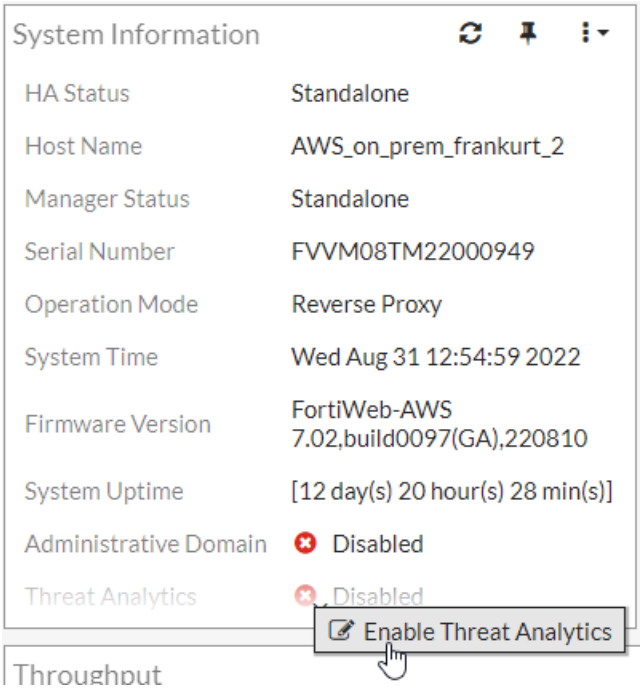
To enable Threat Analytics:

1. Log in to FortiWeb.

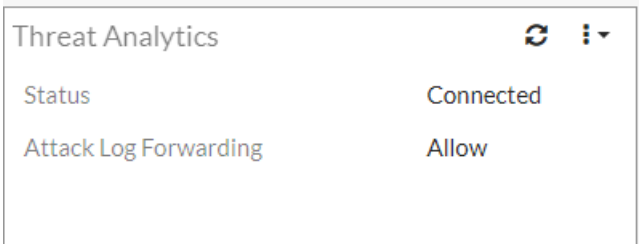
2. Check the status of Threat Analytics in the **Licenses** widget in **Dashboard > Status**. It should be displayed as Valid.



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



4. Make sure **Enable Attack Log** is switched on in **Log&Report > Log Config > Other Log Settings**.
5. 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 FortiAppSec Cloud and whether the attack logs are being forwarded.



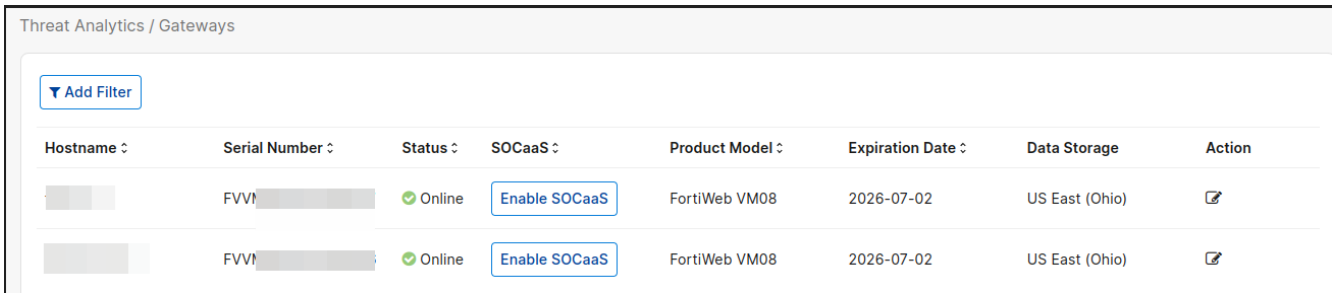
6. Wait for FortiWeb to generate attack logs.
7. Log in to FortiAppSec Cloud with the account you used when registering your license on Fortinet Support site.

Gateways

Use **Gateways** to integrate Threat Analytics with FortiWeb and FortiADC appliances. This allows you to collect attack logs from all your FortiWeb and FortiADC platforms and apply threat analytics across your entire web infrastructure.

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

The devices connected to Threat Analytics are displayed in the web portal GUI under **Threat Analytics > Gateways**.



Security Operations Center-as-a-Service (SOCaaS)

This page outlines instructions for enabling SOCaaS for Gateways.

For instructions on enabling SOCaaS for WAF applications, please refer to WAF Settings on page 204.

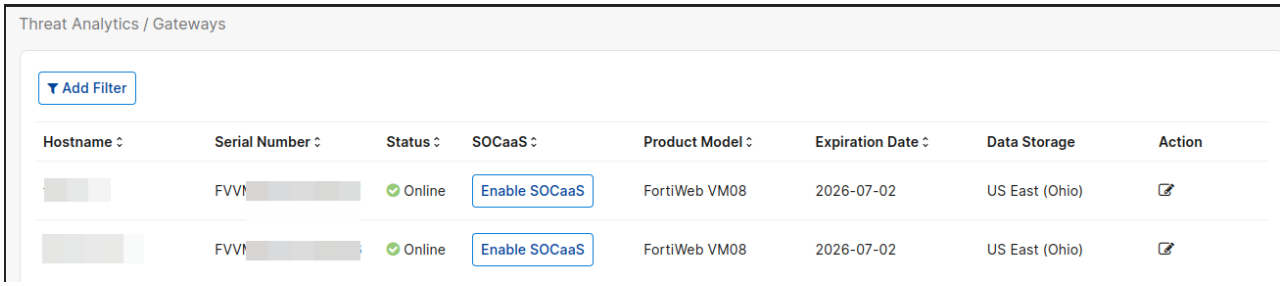
Fortinet Security Operations Center-as-a-Service (SOCaaS) offers a cloud-based security monitoring service that analyzes security events generated from your FortiAppSec Cloud, performs alert triage, and escalates confirmed threat notifications. Its key services include:

- Real-time web application and API security monitoring
- Clear Call to Action on detected Web Attacks
- Noise reduction of False Positives and Information alerts
- Weekly FortiAppSec Cloud executive and threat protection report

To allow the SOCaaS team to perform essential security operations, grant them access to retrieve attack logs from Threat Analytics on FortiCloud.

Enable SOCaaS

1. Navigate to **Threat Analytics > Gateways**.
2. Click **Enable SOCaaS** for the desired device. This should open the SOCaaS portal.

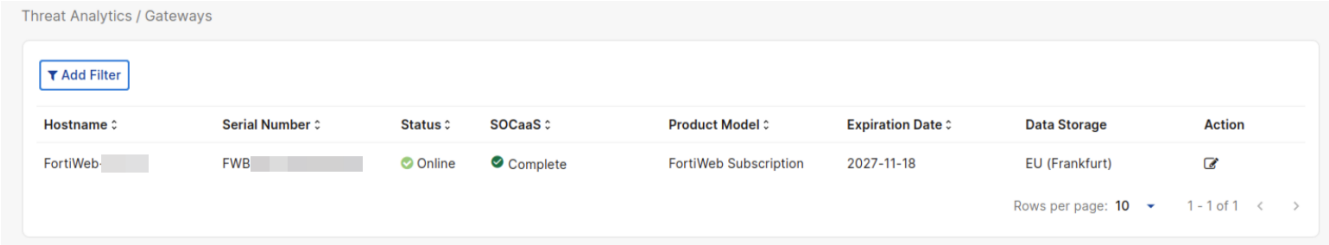


3. Onboard your device on the SOCaaS portal. For detailed instructions, please refer to the following article: Onboarding FortiWeb or FortiAppSec Cloud.

After onboarding

After you onboard your device through the SOCaaS portal, there is a short waiting period while configuration and service setup complete.

The Gateways page displays the SOCaaS onboarding status.



Once SOCaaS is ready for your device, hover over the **SOCaaS** status field to view the FortiAnalyzer server settings (address and port) that logs are forwarded to.

General

This section covers information that applies to all services of your account, covering account-wide settings and logs collected from each service.

- Settings on page 426
- Asset Groups on page 429
- Audit Logs on page 431
- Contracts on page 433
- Usage on page 436
- Reports on page 440
- Notifications on page 441
- Organization on page 445

Settings

Audit Logs Export

Enable this option to export system-level events, such as user logins and server creation, to specified log servers for individual accounts.

Exporting logs that span the entire organizational unit is not supported.

Server Type	Select the destination server for exporting audit logs. See the following instructions for FortiAnalyzer, FortiSIEM, SysLog and ElasticSearch.
FortiAnalyzer FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides centralized logging and analysis, plus end-to-end visibility. Please note the following: • FortiAnalyzer is supported; however, FortiAnalyzer Cloud is not. • When configuring the corresponding ADOM on FortiAnalyzer, please set the **Type** to **FortiWeb**. • FortiAnalyzer supports assigning devices to different ADOMs, provided that each OU's master account is associated with a distinct contract (i.e., a unique serial number). However, if the organization has enabled Contract Sharing Mode, all OU accounts share the same contract and serial number. In this case, FortiAnalyzer treats them as a single device, which prevents assigning them to different ADOMs.	
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 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 FortiSIEM is an advanced Security Information and Event Management (SIEM) solution that combines advanced log and traffic analysis with performance/availability monitoring, change analysis, and accurate knowledge of the infrastructure to provide accurate threat detection, remediation, incident response and compliance reporting.	
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	This box shows a preview of the log format, and is not editable.
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.
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:**FortiAppSec Cloud automatically retrieves the SSL certificate used to encrypt the HTTPS connections between the log server and FortiAppSec 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.

Contract Sharing Mode

When Contract Sharing Mode is enabled, all accounts within your organization will use the license from the root account, regardless of any license(s) under member accounts. This feature is ideal for Large Enterprises and Fully Managed MSSPs, allowing them to manage applications and permissions effectively through sub-member accounts.

Please note, this feature is only available for licenses purchased directly from Fortinet. It is not supported for FortiFlex or public cloud marketplace contracts.

API Key

FortiAppSec 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 an API key.

Please note, the API key's permissions are bound to the user who created it.

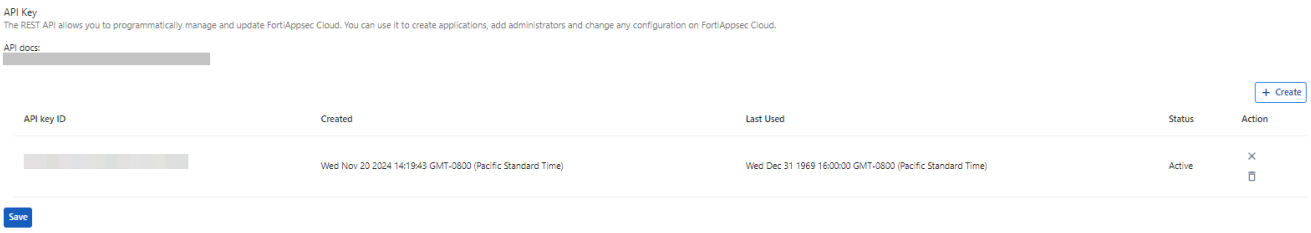
For API documentation, see the FortiAppSec Cloud RESTful API Reference.

Generating API Key

1. Log into your FortiAppSec Cloud account through the Web UI.
2. Go to **General > Settings**.
3. Scroll down to **API Key**.
4. Click **Create**. This will generate an API key ID and API key secret.



You only have **one** chance to view the API key secret, so make sure you save it in a secure location. The key secret will not be stored at the back-end server.



In the API Key table, you can see the API key ID, creation and last usage timestamps, as well as its active or deactivated status. If you encounter any security issues with the key, you have the option to deactivate it. Please note that if your API Key is leaked, we might deactivate it as a precautionary measure. Each user is limited to creating only one API key at a time. If needed, you can delete an existing API key before generating a new one.

When using this API key, add it to the HTTP authentication header as below:

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

Please note, exceeding the limit of failed attempts (3 times) will result in a 30-minute cool down period for further requests. Failed attempts can accumulate due to the following four scenarios:

1. Cannot find the corresponding user on FortiCloud.
2. The API key is illegal.
3. Do not have any valid licenses.
4. Using a deactivated API key.

We have implemented rate limiting, allowing a maximum of 200 requests per minute. This limit applies to both IP addresses and API keys.

Asset Groups

Manage administrative permissions by organizing applications into asset groups, and assigning users to those groups.

This system replaces the older Custom Application Permissions feature, while providing similar capabilities with improved flexibility.

- Key Concepts on page 429
- View Asset Groups on page 430
- Create Asset Group on page 431

To use this feature, go to **General > Settings** and enable **Asset Groups**. This feature is only supported for IAM users. It is not supported for users authenticated through an external identity provider (IdP).



When **Asset Groups** is enabled:

- When onboarding a new WAF application, you must select an Asset Group for the application.
- IAM users will not be able to see applications unless they are added to the Global Asset Group by the Master user.

Key Concepts

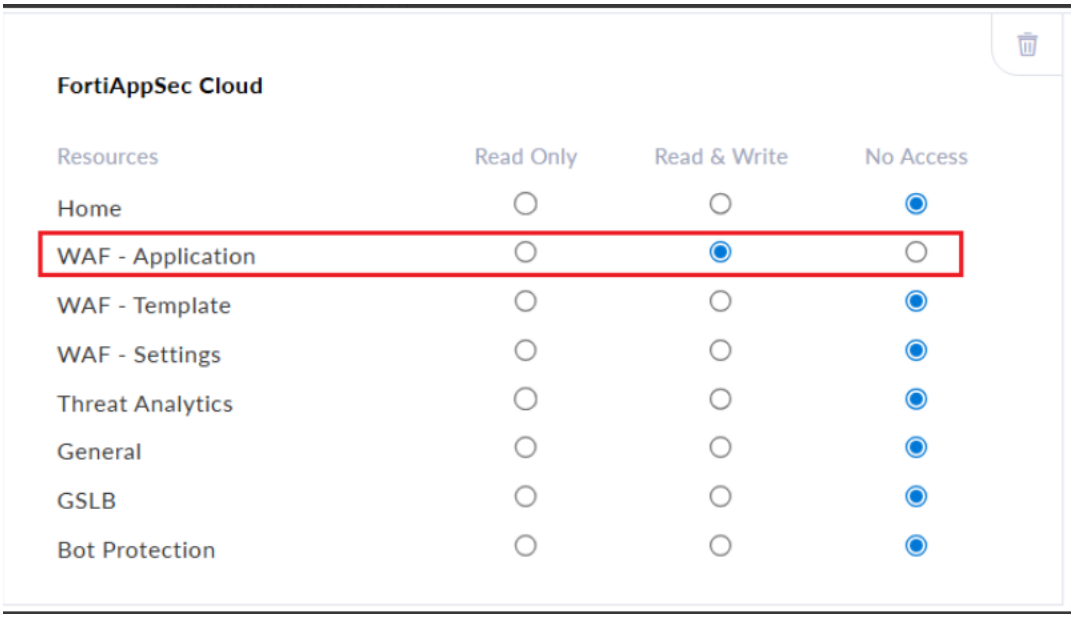
- **Asset**: Each WAF application is treated as a separate asset. Ownership of the asset remains with the account, but management rights can be delegated to users.
- **Default Access**:IAM users have management rights to zero assets by default. Master users and OU admins have access to all assets, and can grant access to IAM users by assigning them to asset groups.
- **Access Restrictions**: Users can only view or manage applications—and their related data such as attack logs, event logs, security incidents, insights, and reports—if they are granted management rights through an asset group.
- **Asset Groups**: These act as an intermediary between users and assets. You cannot assign assets directly to users. Instead, use asset groups to efficiently grant permissions for multiple assets to one or more users.
- **Global Asset Group**: This is a default group that contains all assets in your account. You can configure account-wide settings here that apply to all WAF applications.
  - It is listed first on the Asset Groups page.
  - It is managed by the Master user and OU Admins by default.
  - IAM users can be added as administrators for the Global Asset Group.

Relationship Summary

- Assets → Asset Groups: Many-to-one
  Each asset belongs to only one asset group aside from the **Global Asset Group**.
- Asset Groups ↔ Users: Many-to-many
  A group can have many users, and a user can be assigned to multiple groups.

Interaction with FortiCloud IAM permission profiles

Permission control continues to follow the access levels defined in the IAM Portal. For example, if a user is granted **Read & Write** permissions for the resource in the IAM portal, they will have **Read & Write** access to all applications they are assigned through Asset Groups.

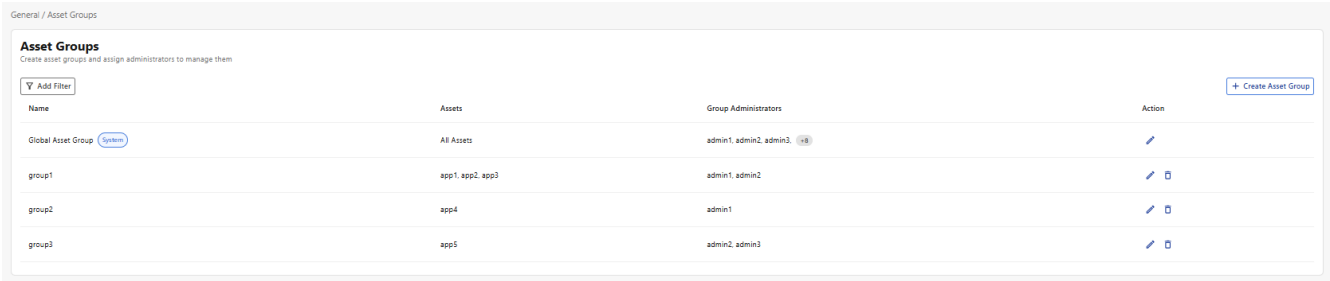


We recommend setting the IAM permission profile for non-master users and non-OU admins to **Read Only** or **No Access** for the **FortiAppSec Cloud > General** resource. This ensures these users will not be able to overwrite General configurations, even if they are assigned as Asset Group Administrators.

This ensures consistent and conflict-free permission enforcement between FortiAppSec Cloud and IAM.

View Asset Groups

On the **Asset Group**s page, you can view all created asset groups.



Edit or Delete Asset Groups

You can edit or delete an Asset Group by clicking the corresponding icons in the **Action** column.

Create Asset Group

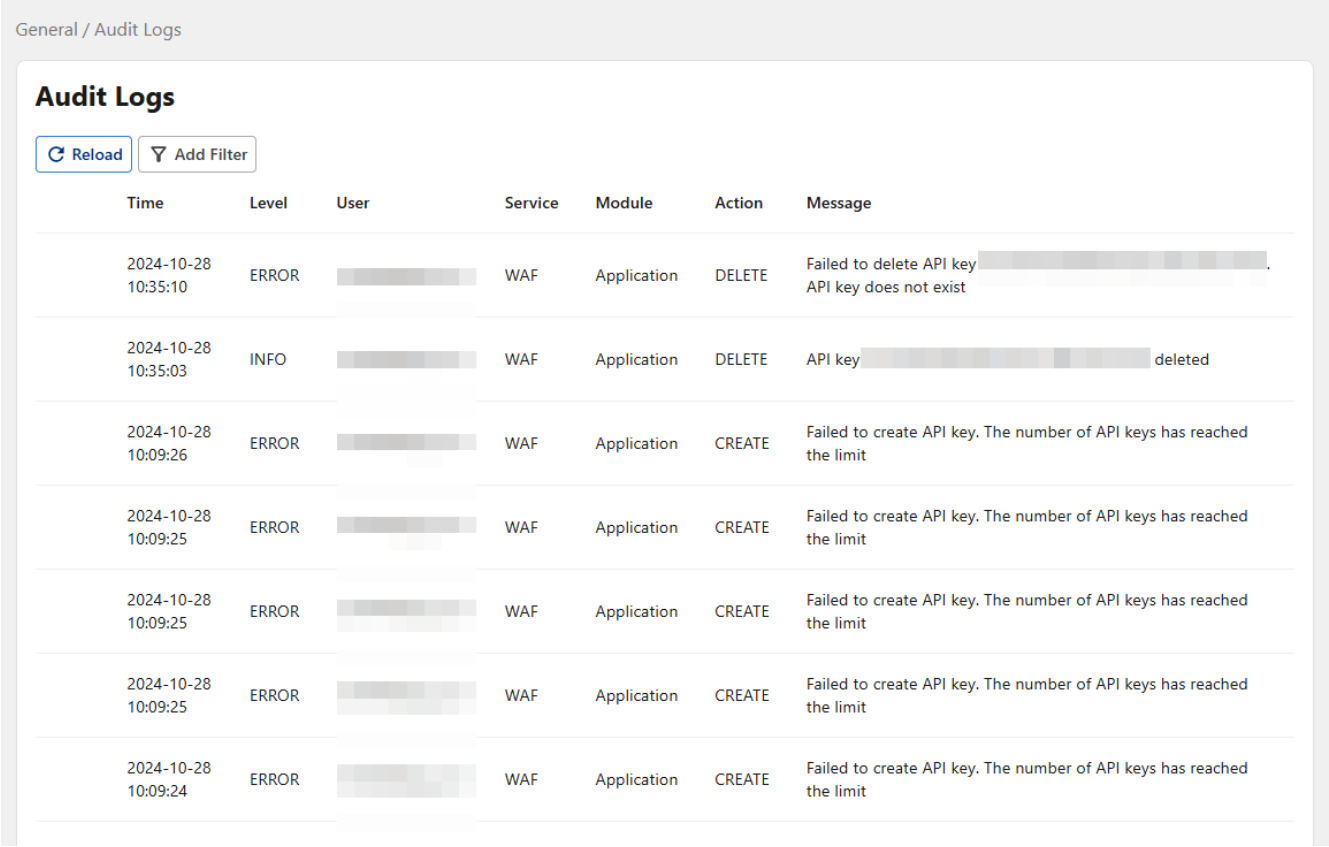
Each account can have up to 32 Asset Groups.

1. Click **Create Asset Group**.
2. Enter a name for your Asset Group.
3. Move desired WAF Assets in from the **Available** list to the **Selected** list using the following buttons.
   All items under the **Selected** list will be added to the Asset Group. Each group can contain up to 500 Assets.
   - Moves all assets from the **Available** to the **Selected** list.
   - Moves selected assets from the **Available** to the **Selected** list.
   - Moves all assets from the **Selected** list to the **Available** list.
   - Moves selected assets from the **Selected** list to the **Available** list.
4. Move desired group administrators in from the **Available Users** list to the **Selected Users** list using the following buttons.
   All items under the **Selected Users** list will be added to the Asset Group. Each group can have up to 10 admin users, and each user can be assigned as administrators of up to 10 Asset groups.
   - Moves all users from the **Available Users** to the **Selected Users** list.
   - Moves selected users from the **Available Users** to the **Selected Users** list.
   - Moves all users from the **Selected Users** list to the **Available Users** list.
   - Moves selected users from the **Selected Users** list to the **Available Users** list.
5. Click **Save** to create the Asset Group.

Audit Logs

The audit log records system activities such as user login and logout, and issues warnings for personal licenses. It triggers reminders in the log if a license is due to expire within 1, 3, or 15 days. Additionally, it notifies when all query license capacities are exhausted.

Primary users can access all audit logs, while sub-users can only view their own audit logs.

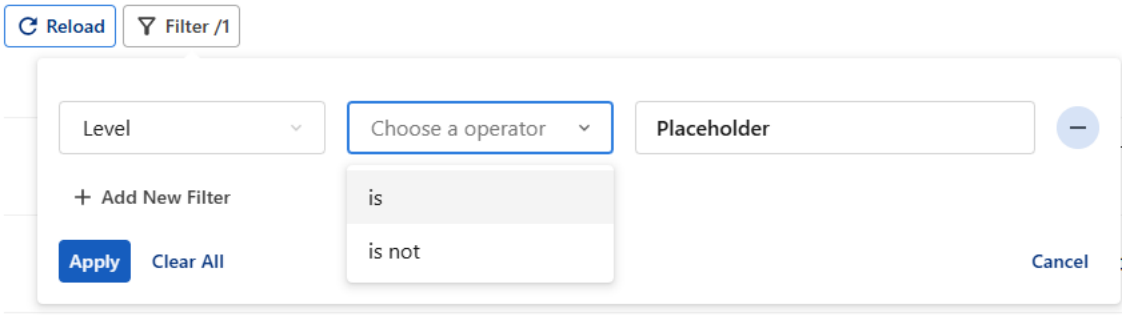


Field	Description
Time	The local time when the event occurred.
Level	The system's assessment of the urgency level for this logged event. **Emergency**: This is the most severe level, indicating a catastrophic failure or situation that requires immediate attention and action. **Alert**: This level indicates a critical situation where immediate action is required from the customer. **Critical**: This level denotes a severe error or failure that affects the system's functionality. **Warning**: This level signifies a potential problem or issue that the customer should be aware of and investigate further. **Notice**: This level provides insight into the cause of an error or an unusual event. **Info**: This level conveys general informational messages that are useful for tracking system activities or providing updates. **Debug**: This level is used for detailed debugging information.
User	If the event pertains to a user in your organization, their username will be displayed in this field; otherwise, it will show as **None**.
Service	The service that detected this event.
Module	This field describes the nature of the log.

Field	Description
	system: Tracks system events like licensing changes and user logins. **config**: Configuration events, such as a newly configured FQDN **health_check**: Monitors system health through tests and alerts for issues like overloads or status changes. **connector**: Keeps tabs on the health and function of connectors, essential for data flow and system connections.
Action	This field specifies the action recorded in this audit log, offering more detail than the **Type** field.
Status	The outcome of the event, indicating success or failure.
Message	Details regarding the event as gathered from the system.

Filters

Customize your log views by specifying a date range and by adding filters (by Time, Level, Message, Service, User, and Action).

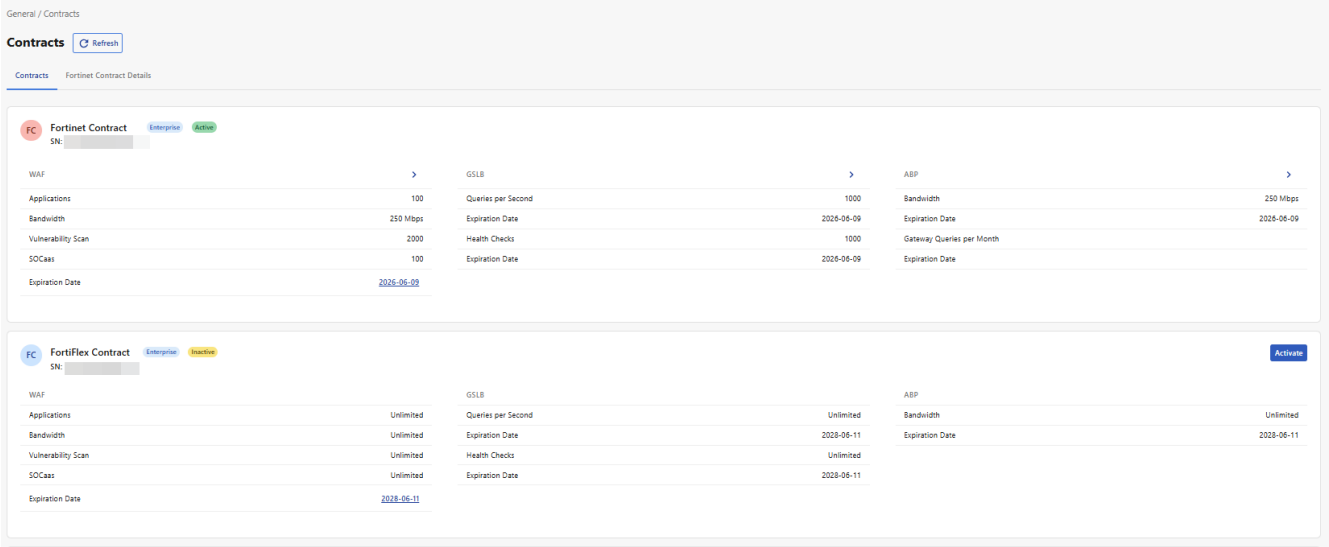


Contracts

On this page, you can view your active licenses, license history, and query usage.

For information on different types of contract options and instructions on purchasing the different license types, please refer to License & Contract on page 21.

View contracts



The values on this page correspond to the maximum allowances in each category defined in the purchased contract.

Applications	Maximum number of WAF Applications allowed under this account.
Bandwidth	Maximum bandwidth used by the applicable service.
Queries per second	Maximum number of queries per second.
Health Checks	Maximum number of health checks used.
Vulnerability Scan	Maximum number of vulnerability scan assets, calculated based on the WAF application seats. Each application can have up to 10 domains, and each domain is scanned on 2 ports (HTTP/HTTPS). Therefore, the number of vulnerability scan assets = *the number of applications* × 10 × 2.
SOCaaS	Maximum number of applications you can use the SOCaaS on. This number should match the **Applications** value.

Change Contract

1. Purchase a FortiAppSec Cloud contract by contacting your Fortinet reseller.
2. After purchasing the new contract, please log into your FortiAppSec Cloud portal and navigate to **General > Contracts**.

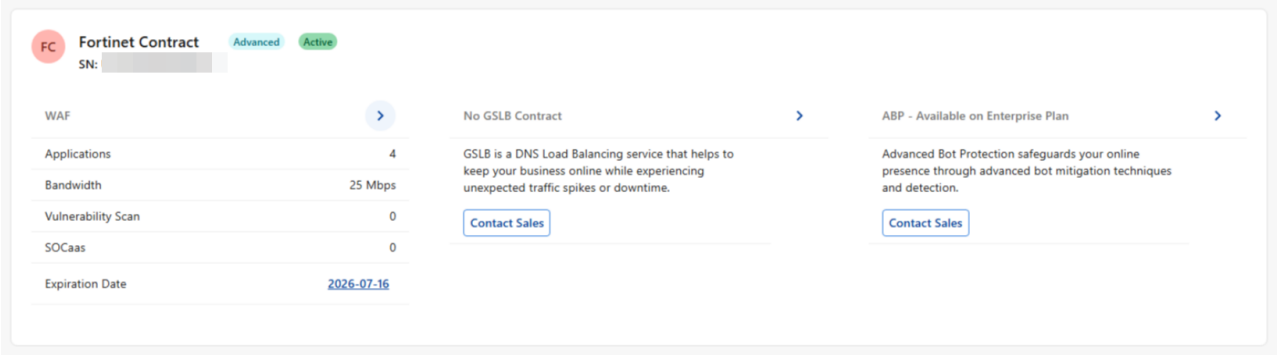
   Only one contract can be active at a time. Before activating your new contract, your previous contract will remain active.
3. Click **Activate** in the new contract to activate it.

Upgrade or downgrade plan

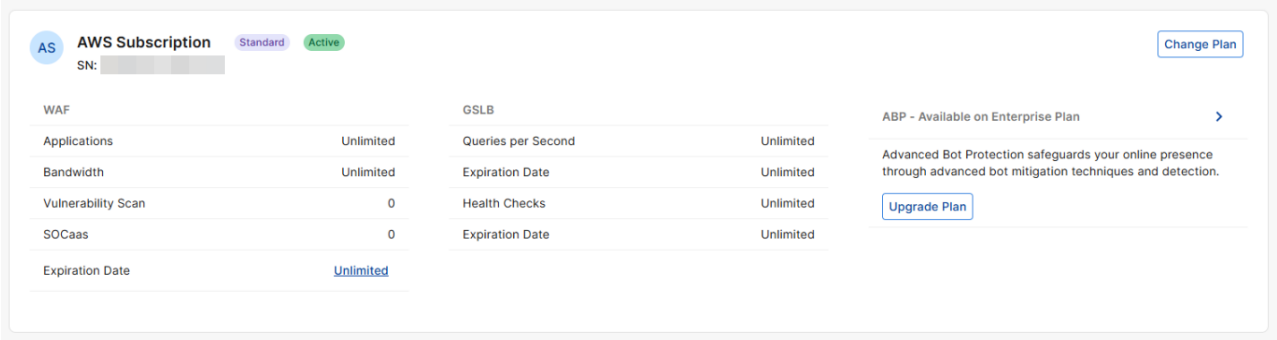
To switch between Standard, Advanced, and Enterprise plan options for your existing contract, the process depends on your contract type.

To see the differences between Standard, Advanced, and Enterprise plan feature offerings, please refer to License & Contract on page 21.

- If you are using a license purchased from Fortinet, you must contact Fortinet Sales.



- If you are using a Public Cloud marketplace subscription, you have options to upgrade and downgrade your plan from the FortiAppSec Cloud web portal.

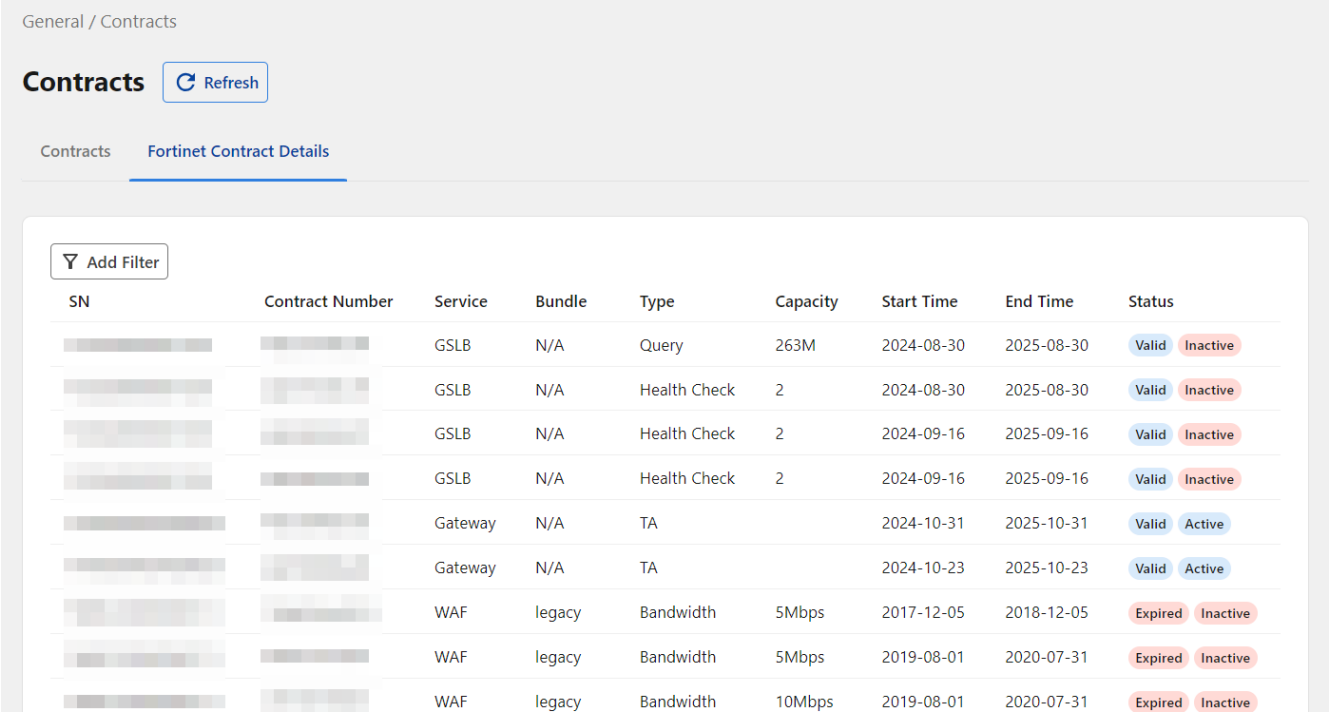


- If you are using a FortiFlex subscription, you can make changes to your plan via the FortiFlex portal.
- If you are using a Legacy Contract, you do not have the option to make changes to your plan. Please purchase a FortiAppSec Cloud Plan.

For details on the offerings available for your contract type, please refer to its dedicated page.

Fortinet Contract Details

View the serial numbers, contract numbers, capacity, and additional details for all individual services associated with your license.



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.

The information displayed on this page vary based on the billing structure of your active license.

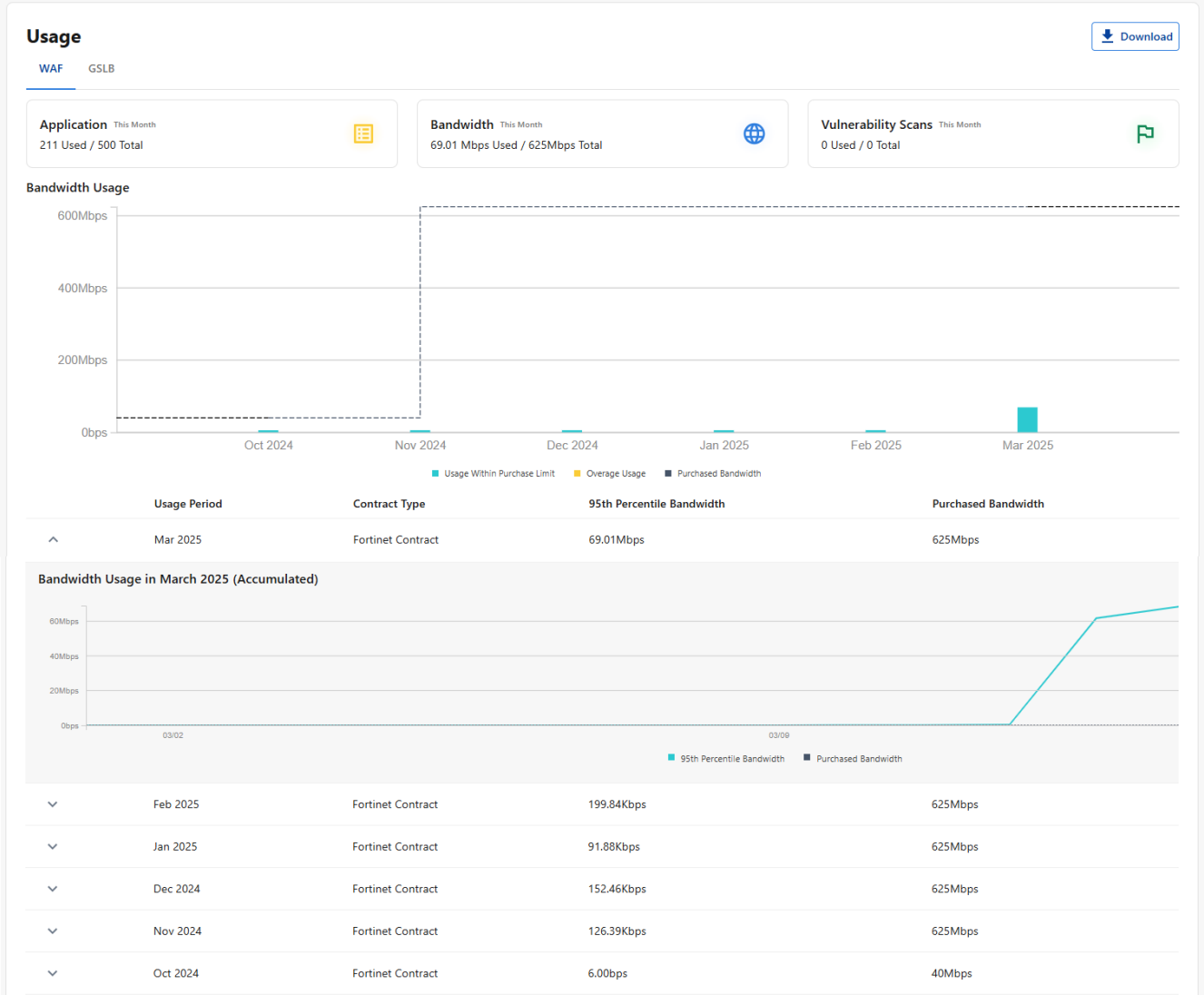


Some services have a minimum billable usage, regardless of actual traffic.

For example, if a WAF application is deployed, a minimum of 25 Mbps per day of WAF bandwidth will be billed, even if the application receives no traffic.

Contract-based usage

When you are using a license purchased from Fortinet, this page displays usage statistics at the top, tailored to the selected service, showing how much of each resource has been used relative to its limits.



- **WAF**
  - **Application**- the number of applications onboarded to WAF
  - **Bandwidth**- the amount of data transmitted between your applications and FortiAppSec Cloud for protection and security filtering. This includes data traffic that is analyzed and monitored for threats such as attacks, malicious requests, and other security risks.
  - **Vulnerability Scans**- the number of times the Vulnerability Scan feature was triggered.
- **GSLB**
  - **Queries** - the number of queries exchanged between your GSLB service and WAF/FortiADC/FortiWeb regarding user activity on the protected application.
  - **Health Checks**- the total number of health checks utilized by your service.
- **Advanced Bot Protection**
  - **Queries**- the number of queries exchanged between your ABP service and WAF/FortiADC/FortiWeb regarding user activity on the protected application.

The following display for all services:

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

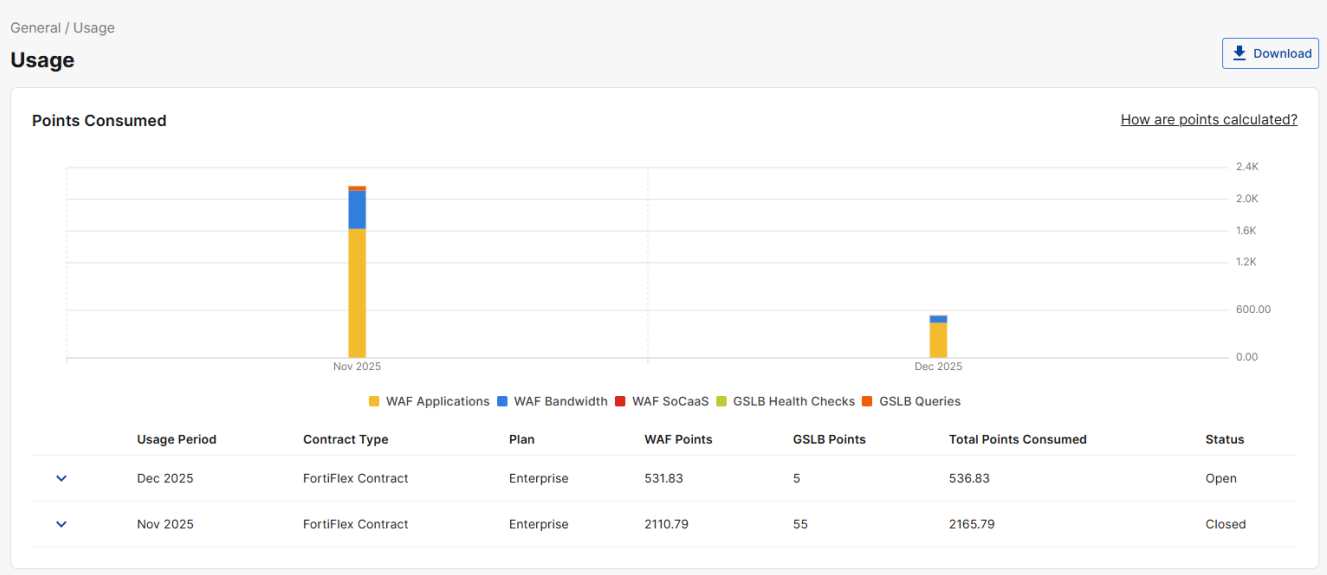
Points-based usage

When you are using an AWS/GCP/Azure marketplace or FortiFlex contract, this page displays the number of points consumed by your application, split by bandwidth, WAF applications, GSLB Queries, and GSLB Health checks.



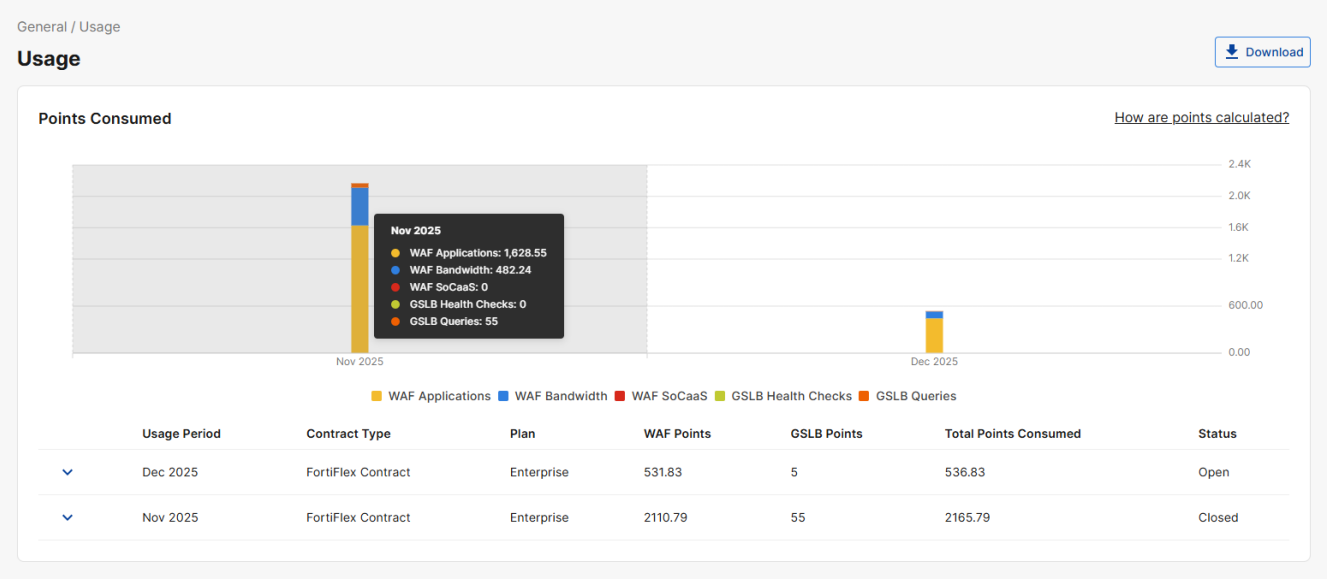
For a cost estimate based on manual entry of your usage information:

- If you are using a AWS/Azure/GCP contract, please visit the FortiAppSec Cost Calculator.
- If you are using a FortiFlex contract, please visit the FortiFlex Cost Calculator.



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 the table below the stacked bar chart to expand the usage details of each month.





The application-level 95th-percentile bandwidth usage is not displayed in the web portal. You can retrieve this data through the API using: `GET /v2/general/reports/waf_app_usage/{month}?ep_id={ep_id}`

For more information, please refer to the FortiAppSec Cloud API documentation.

Reports

In addition to the application-level threat data displayed on **Dashboard**, **FortiView** and **Logs** pages, you can you can schedule customized reports that summarize threat activity across all applications in your account. These reports can be automatically emailed to specified recipients.

For each report entry, you can use **Add Filter** to filter out reports based on the recipients or report names.

1. Click **Create Report** in **WAF > 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.
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.
At	Specify when the report is generated, based on the selected **Schedule** value. For example, if **Weekly** is chosen, enter the day and time the report should be sent (e.g., Monday, 13:00)
Recipients	Specify the email addresses that will receive the weekly report. Separate multiple email addresses with ",". A maximum of 10 email addresses are supported.
Service	The FortiAppSec Cloud service associated with the report. • WAF • CSP
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

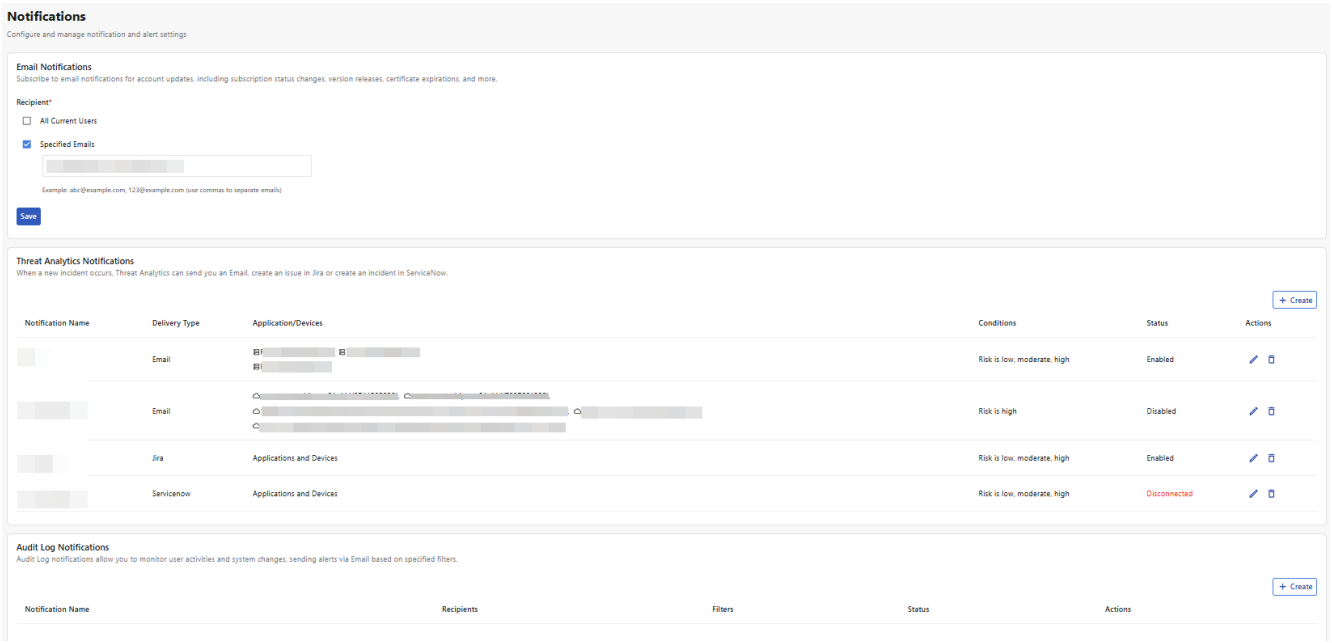
	• Applications Traffic Summary
Applications	Define the applications that you want to generate the weekly report for or not. You can add or remove all applications once.

3. Click **OK**.

Notifications

Manage notification settings, including which events trigger notifications and the destinations where they are delivered.

- Email Notifications on page 441
- Threat Analytics Notifications on page 442
- Audit Log Notifications on page 444



Email Notifications

Configure recipients for account-related email notifications, such as subscription changes, version releases, and certificate expirations.

Note: These recipients receive only general account notifications. Other notification modules manage their own recipient settings separately.

1. Select any of the following options:

Recipient	Description
All Current Users	Select to send email notifications to all users associated with this account.
Specified Emails	Select to input email addresses to receive these notifications. Separate email addresses with commas.

2. Click **Save** to apply changes.

Threat Analytics Notifications

Receive notifications for selected applications and devices when activity reaches the specified risk level.

1. Click **Create**.
2. Configure the following:
3.

Setting	Description
Notification Name	The internal name by which this set of notification rules is displayed.
Enable Notification	Enable to receive notifications for this configuration set. You can disable it later to pause notifications without losing your configurations.
Scope	• **All Applications and Devices**: Select this option if you want to apply this set of configurations to all applications and devices under your account. • **Customized**: Select this option to move applications and devices to the selected list to receive notifications for them.

4. Click **Next**.
5. Configure the following:

Setting	Description
Notify me when	Set the lowest risk level you want to receive notifications for. • **Low**: Receive notifications for all threat analytics events. • **Moderate**: Receive notifications for **Moderate** and **High** risk events. • **High**: Receive notifications for **High** risk events.
Type	Select how you would like to receive notifications. • **Email** • **Jira** • **ServiceNow**

- If you selected **Email**, configure the following:

Setting	Description	Input Example
Recipient	Enter up to 10 email addresses to receive these notifications, separated by commas.	user@a.com,user@b.com
Subject	Enter the subject line for this email notification. You can include keywords to help with email filtering. Use **%%** to indicate placeholders, such as **%%RISK%%**, **%%DESCRIPTION%%**, or **%%HOST_DESC%%**.	[%%RISK%%] Alert on %%HOST_DESC%% – %%DESCRIPTION%%

- If you selected **Jira**, configure the following:

Setting	Description
Jira URL	Enter the URL of the Jira instance to which notifications should be sent.
Account (Email)	Enter the email address of the Jira user account that FortiAppSec Cloud will use to send notifications. This account is used to authenticate with your Jira instance and post issues or comments on your behalf.
Token	Enter the API token associated with the Jira account provided in the **Account (Email)** field. This token is used to authenticate FortiAppSec Cloud with your Jira instance securely. To access this token: **1.** Generate the token in Jira for the user account you entered. **2.** Ensure the token has the required permissions to create or update issues. **3.** The token allows FortiAppSec Cloud to send notifications without storing the Jira password.

- If you selected **ServiceNow**, configure the following:

Setting	Description
ServiceNow URL	The web address of your ServiceNow instance where FortiAppSec Cloud will send notifications.
Client ID	The unique identifier for the OAuth application in ServiceNow. This identifies FortiAppSec Cloud as a trusted client for sending requests.
Client Secret	A confidential key associated with the Client ID. It is used to authenticate FortiAppSec Cloud with ServiceNow. Keep it secure.
Refresh Token	A token used to obtain a new access token when the current one expires, allowing FortiAppSec Cloud to maintain a continuous connection with ServiceNow without requiring repeated authentication.

6. Click **Save** to apply changes.

Audit Log Notifications

Receive email notifications for user activities and system changes based on specified conditions.

1. Click **Create**.
2. Configure the following basic settings:

Setting	Description
Notification Name	The internal name by which this set of notification rules is displayed.
Recipients	Input email addresses to receive these notifications. Separate email addresses with commas.
Enable Notifications	Enable to receive notifications for this configuration set. You can disable it later to pause notifications without losing your configurations.

3. Configure **Notifications Conditions**.
   From the dropdown list, select the category of events for which you want to receive notifications:
   - Custom
   - WAF Health Check Events
   - WAF DNS Status Events
   - Automatic Certificate Failures
   - WAF Module Updates

   If you select any category other than **Custom**, the system automatically applies the predefined notification settings for that category.
4. Add and/or edit **Notification Conditions**. This is optional if you selected any category other than **Custom** in the previous step.

Settings	Description
Field	The **Field** specifies the attribute of an event you want to filter. The available options correspond to the columns in the Audit Logs table. Depending on the selected **Field**, you can set an **Operator** and **Value** to determine which audit log entries trigger notifications. • **Level**: The system's assessment of the urgency level for this logged event. • **Message**: Details regarding the event as gathered from the system. • **Service**: The service that detected this event. • **User**: If the event pertains to a user in your organization, their username will be displayed in this field; otherwise, it will show as **None**. • **Action**: This field specifies the action recorded in this audit log. • **Module**: This field describes the nature of the log. For more details, including the meaning of values for each field, please refer to Audit Logs.
Operator	Select how the field value should be matched: • **Is**

Settings	Description
	• **Is not**
Value	Depending on the selected **Field**, clicking the input box for Value will display a dropdown list of valid options that appear in your Audit Logs. You can: • Begin typing to filter the suggestions and select the desired value. • Enter a custom value not listed in the dropdown. Note that custom entries may not be effective.

5. Click **Save** to apply changes.

Organization

User management for FortiAppSec Cloudis handled through FortiCloud, where you can add or delete users.

- FortiCloud IAM on page 445
- FortiCloud Organizational Units on page 453

FortiCloud IAM

IAM (Identity and Access Management) users are assigned permission types and permission profiles, facilitating controlled access to FortiCloud resources and services.

Before creating an IAM user to use with FortiAppSec Cloud, you must first create a FortiAppSec Cloud portal Permission Profile.

- IAM User permission Types on page 445
- IAM permission profiles on page 446
  - WAF - Application Management, WAF - Application Network, and WAF - Application Security on page 447
- Create a new FortiAppSec Cloud portal permission profile on page 448
- Add an IAM User to FortiAppSec Cloud on page 450
- Manage IAM users on page 453

IAM User permission Types

Permission Type is assigned when creating a permission profile or an IAM user. It defines the scope of access a user has in terms of asset folders or OU hierarchy.

- **Local:** Default type, limited to the selected account's asset folders.
- **Organization:** Advanced settings for assigning IAM users, user groups, and permissions to OUs and member accounts. Only IAM users with this type can be assigned as an OU admin.



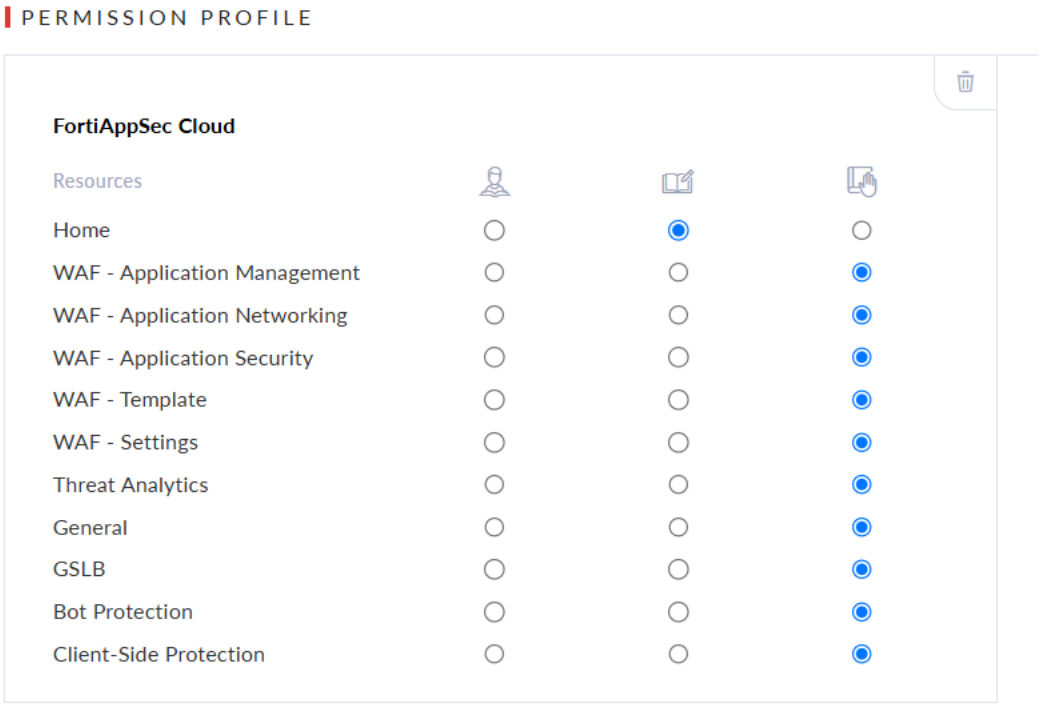
Assigning IAM users with a local type to an organization on the GSLB organization page will no longer be effective if the organization is associated with a member or root account.

IAM users from the member or root account will always be able to manage resources under the account, provided their permission profile allows it.

Permission scope can be defined as Local or Organization when a permission profile is being created. The Local type is automatically assigned to all permission profiles when OU access is not enabled. However, if a login user does have OU access enabled, the scope can be set to either the Local or Organization type. Once selected, permission scope can then be based on hierarchical OU (Organization type) or asset folder (Local type) paths in the Organization portal and Asset Management portal, respectively.

IAM permission profiles

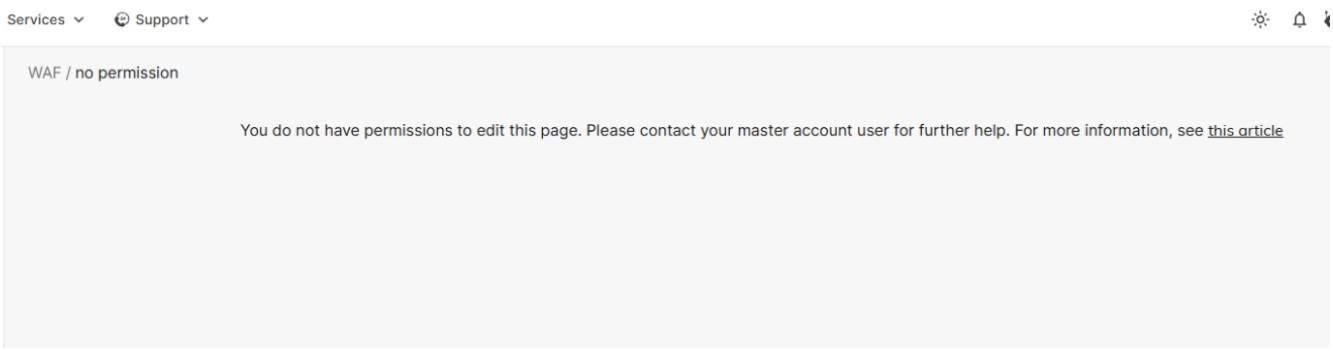
Permission profiles define the scope of access that users have across different Fortinet services. Each **permission profile** includes **Portals** for the various Fortinet services. Within each **Portal**, you can specify which features or modules the profile grants access to.



The FortiAppSec Cloud portal displays information on each page according to the user's access level.

- Read Only
- Read & Write
- No Access

When a permission profile has a resource set to No Access, an IAM user assigned to that profile will see a No Permission page when attempting to access the corresponding resource. When set to Read Only, the user can view the page but cannot edit any of its settings.



WAF - Application Management, WAF - Application Network, and WAF - Application Security

In the version 25.4 update, the **WAF - Application** resource is split into **WAF - Application Management**, **WAF - Application Network**, and **WAF - Application Security**.

For all existing Permission Profiles that were created prior to this change, the permissions for **WAF - Application** will be automatically cloned into each new resource to maintain backward compatibility.

WAF - Application Management

Manages the application lifecycle, dashboard, and monitoring:

- List Applications
- Create or Delete Applications
- Modify basic application information (name, region, block/monitor mode)
- View Application Dashboard
- Configure Application Log Settings
- Add Modules to Applications

WAF - Application Network

Manages application network configuration:

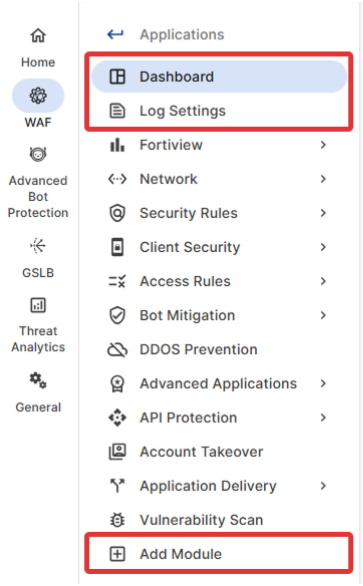
- Endpoints
  - Origin Servers
  - Content Routing
  - Diagnostics

WAF - Application Security

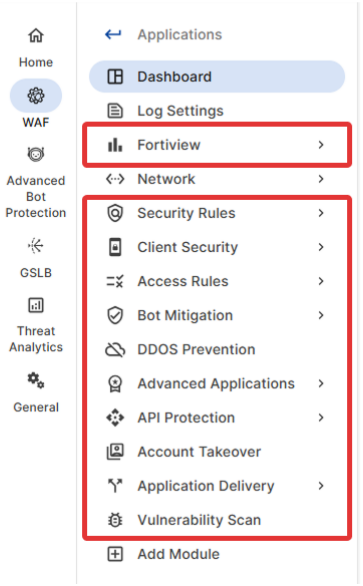
Manages application FortiView and security module configuration:

- FortiView (including Threat and Traffic views)
- All WAF Modules

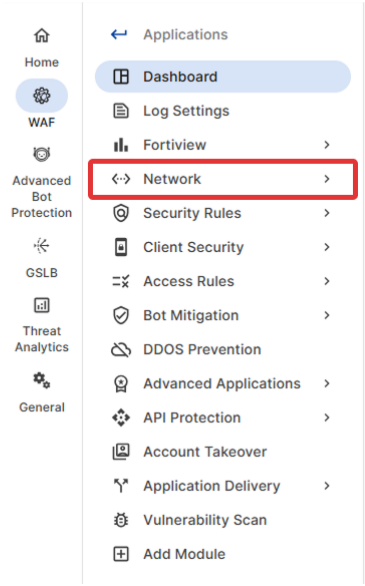
WAF - Application Management



WAF - Application Security

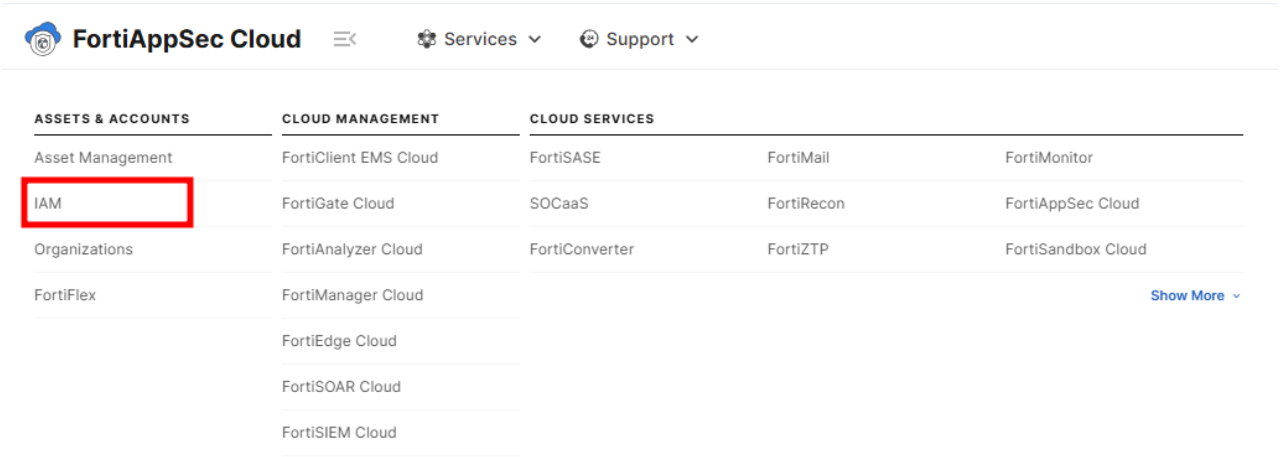


WAF - Application Network

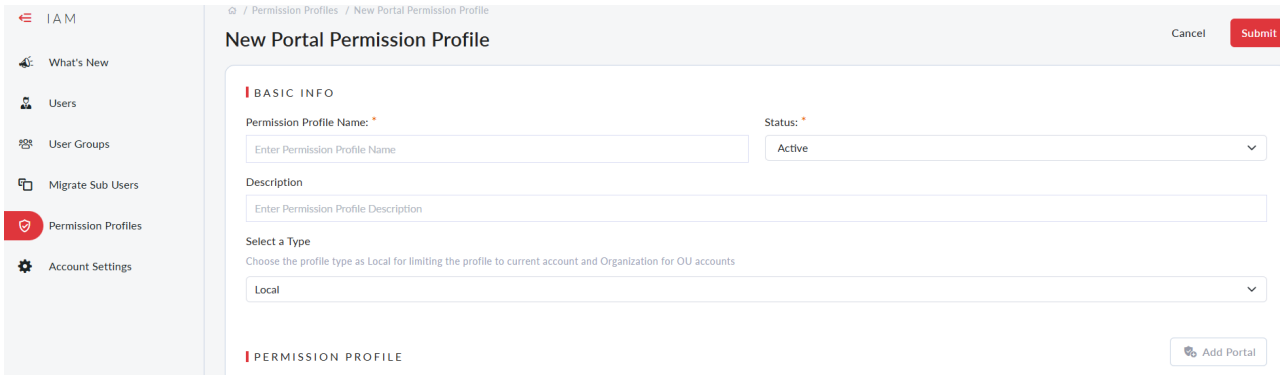


Create a new FortiAppSec Cloud portal permission profile

1. On the admin home page, go to **Services > Assets&Accounts > IAM** in the top navigation bar.

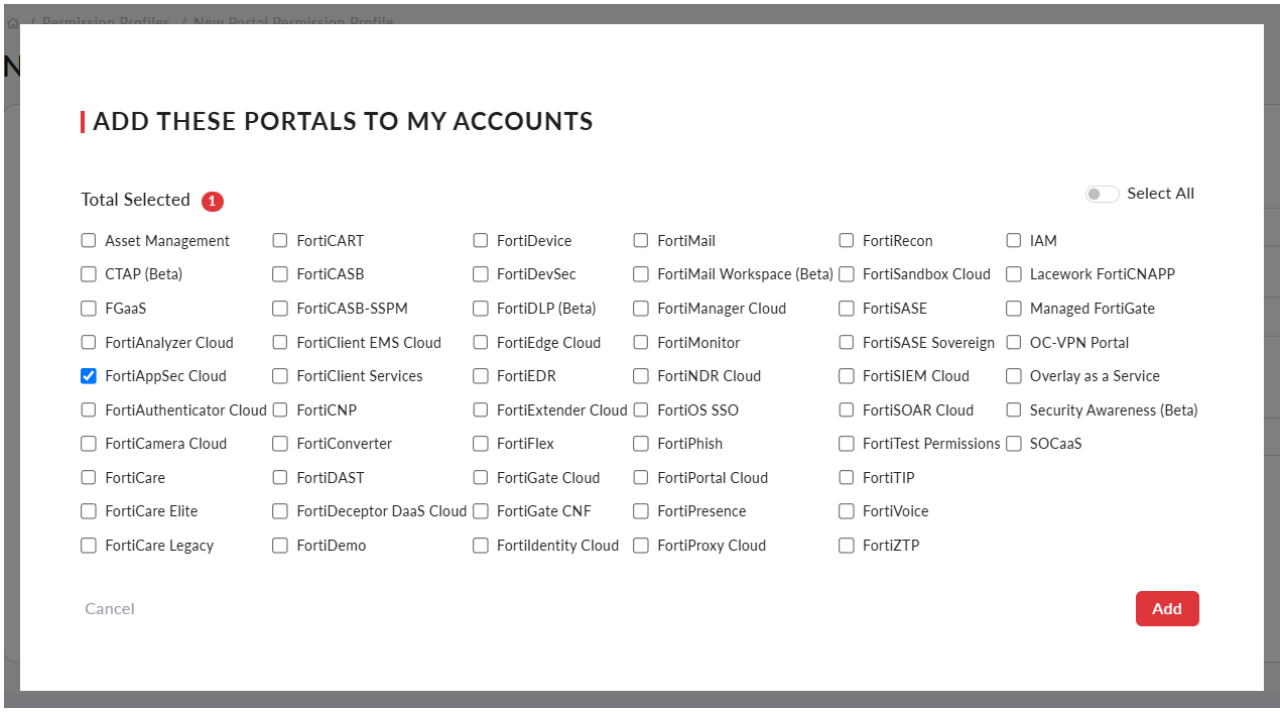


2. Click on **Permission Profiles** in the left-hand navigation bar.
3. Click **Add New** to create a new Permission profile.

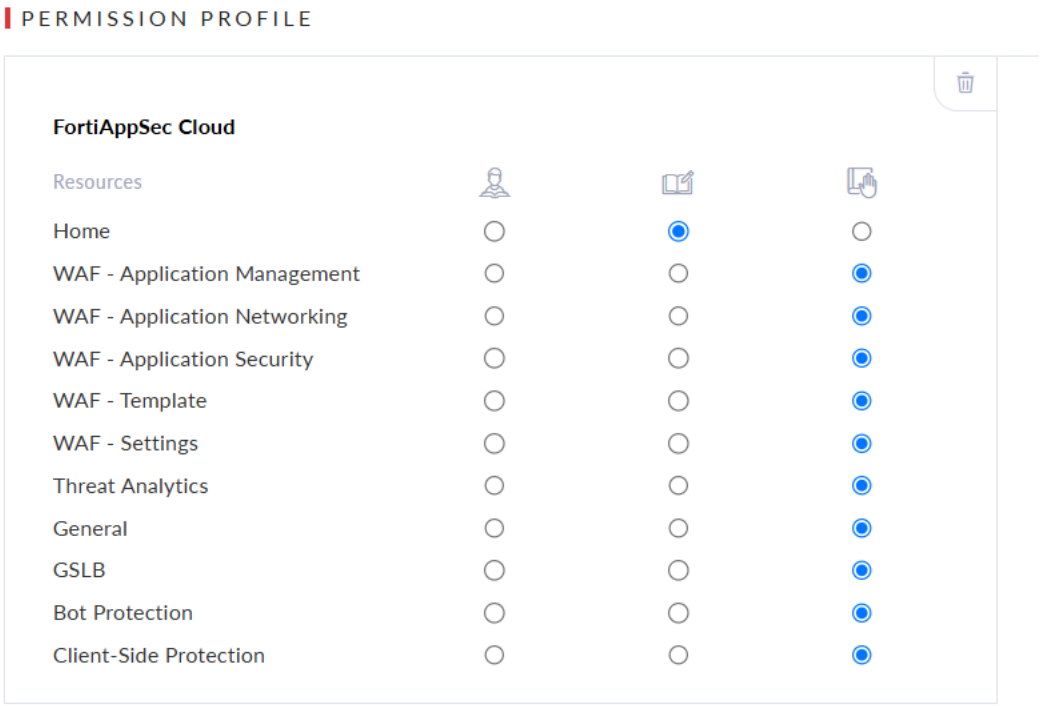


a. Enter a name for the profile in the Permission Profile Name field.
b. Set the **Status** to **Active**.
c. Enter a description of the portal permissions in the Description field.

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

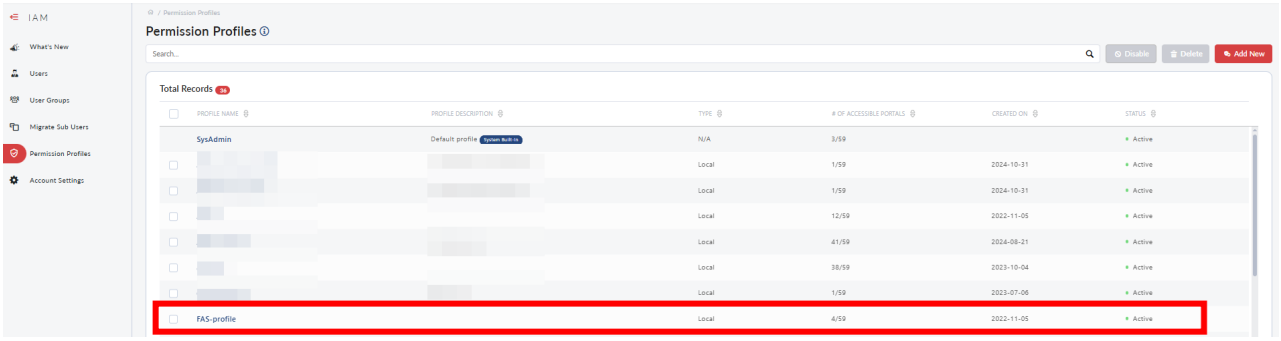


5. To use this Permission Profile with FortiAppSec Cloud, select the FortiAppSec Cloud portal.
6. Click **Add**. The new FortiAppSec Cloud portal displays as a card under **Permission Profile**
   - Click the switch under **Access** to enable the portal, then select your desired access settings for this profile. For details on the various WAF resources, please refer to



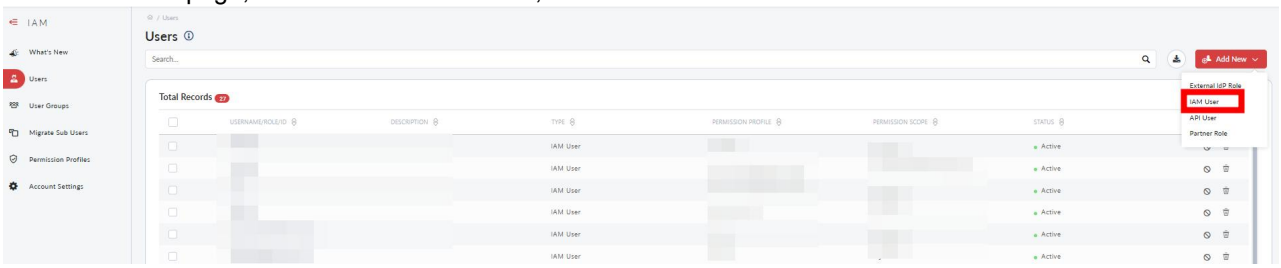
- For other portals with role-based permissions, enable access and specify the portal Access Type and any Additional Permissions.

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

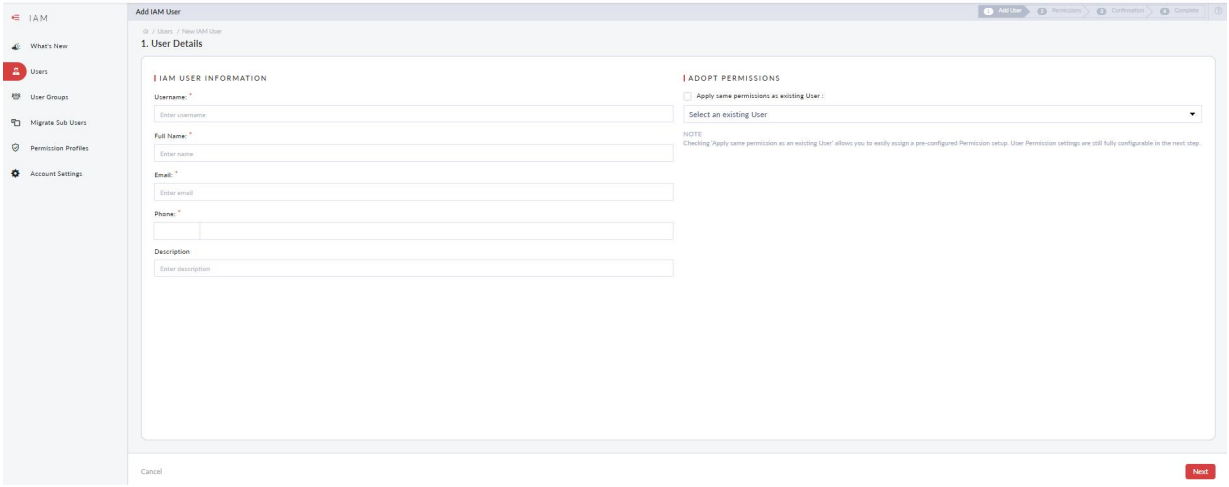


Add an IAM User to FortiAppSec Cloud

1. Go to the **Users** page, click the **Add New** button, and click ***IAM User***.



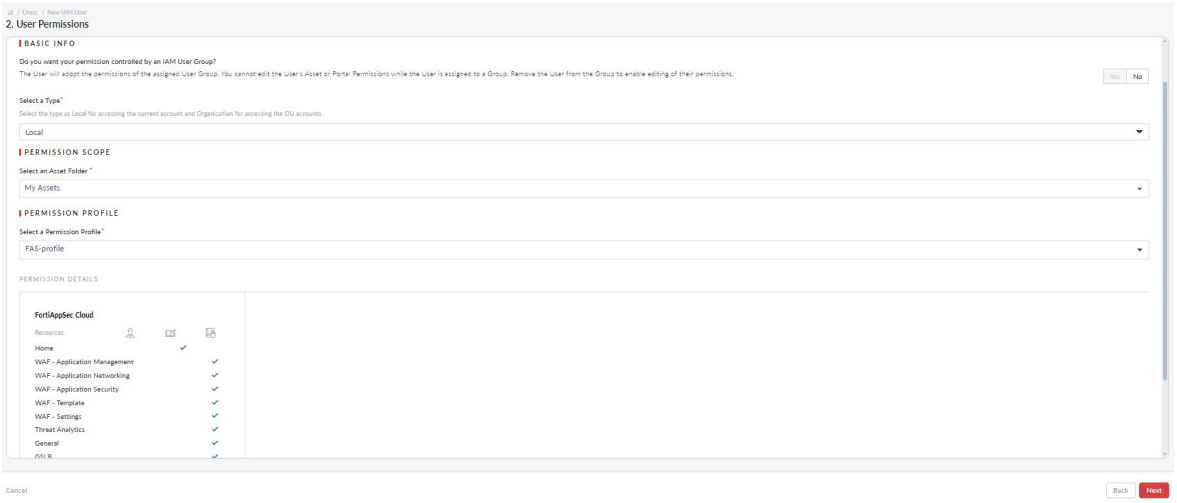
a. Step 1: User Details - Fill in the basic fields and click *Next*.



b. Step 2: User Permissions

i. Select any Asset Folder of your choice.

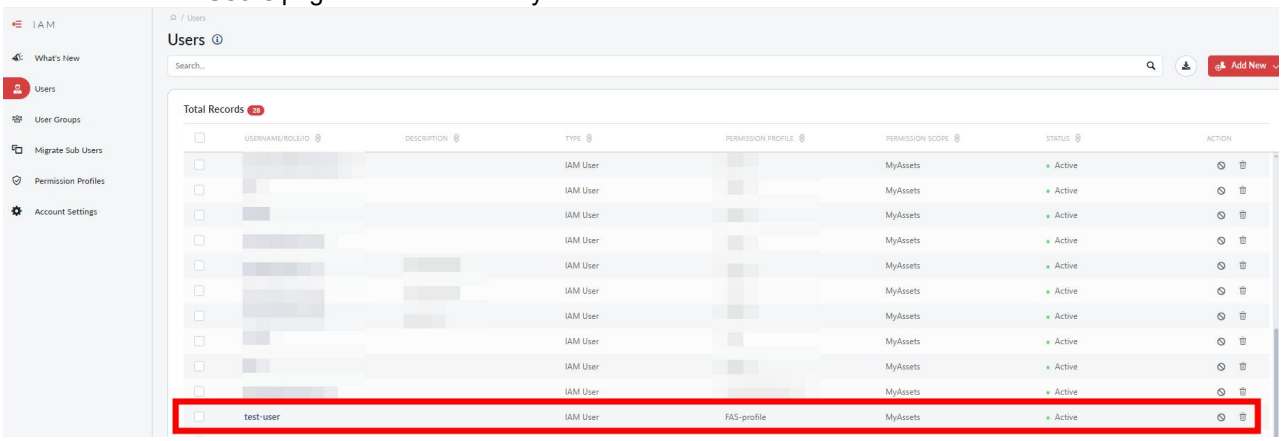
ii. Under the **Permission Profile** subsection, select a permission profile with a FortiAppSec Cloud portal. Click **Next**.



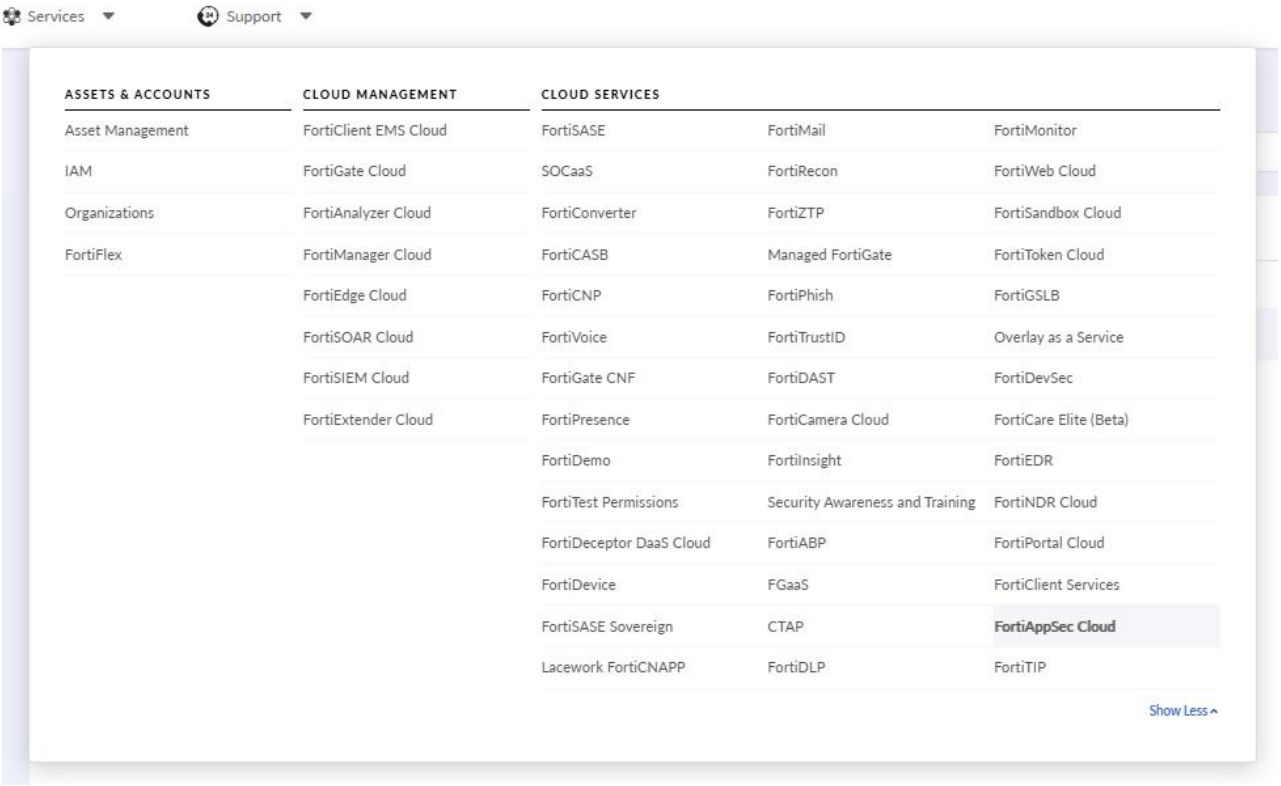
c. Review the user information, and click **Confirm**. The user's details are displayed.

i. Account credentials must be shared with the user. The account password can be configured using Generate Password. See Generating Password Reset Link for instructions on how to configure the account password and share user credentials.

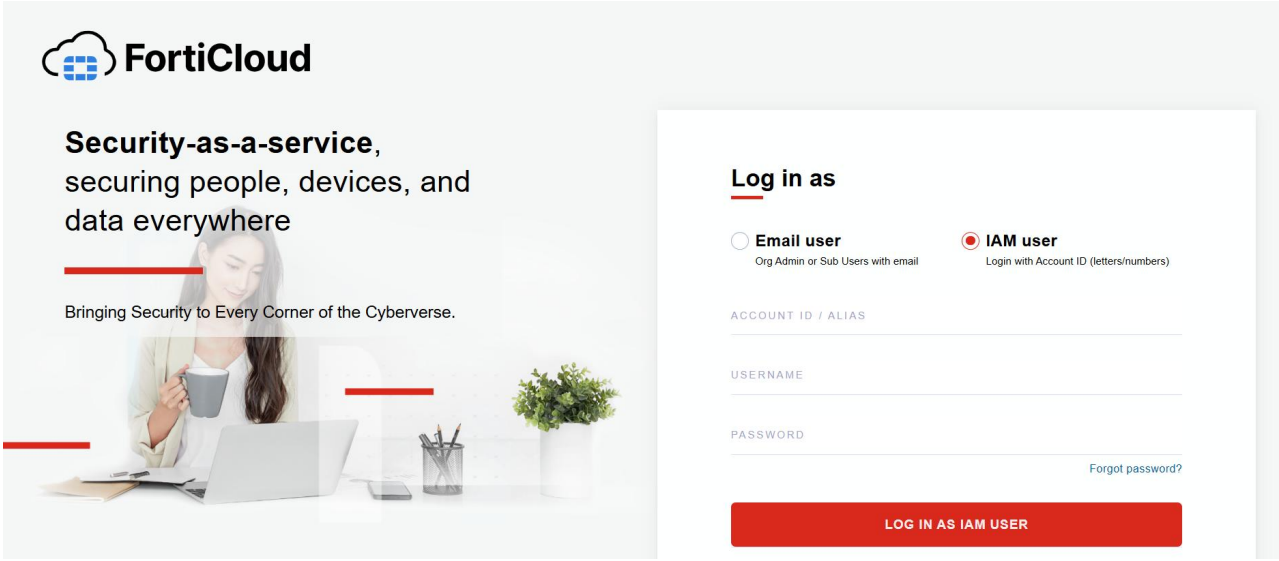
2. Return to the **IAM Users** page and find the newly added user listed.



3. Navigate to the top menu bar and click **Services > FortiAppSec Cloud**. You may need to click **Show More** to access this option.
Please note, you must access FortiAppSec Cloud from here in order to see the newly added user.



4. The IAM user can log in by clicking **Sign in as IAM user** on the login page.



Manage IAM users

For updated information on managing IAM users, please refer to the latest FortiCloud documentation.

FortiCloud Organizational Units

FortiAppSec Cloud supports FortiCloud Organization, enabling centralized management and control of all Fortinet SaaS solutions through FortiCloud. This centralized account management service consolidates multiple FortiCloud accounts into a structured system of Organization/Organizational Units (OUs).

FortiCloud Roles

FortiCloud supports the following roles:

- **Non-OU Account:** A FortiCloud account not part of an organization.
- **Root Account:** Can create or invite member accounts and appoint OU admins. There is no option to choose an OU or member account when logging in.
- **Member Account:**Join an organization and cannot have IAM users or permission profiles of the OU type, so they cannot manage OUs or other member accounts.
- **OU Admin:** An IAM user with the Organization type that manages specific OUs or member accounts within those OUs.

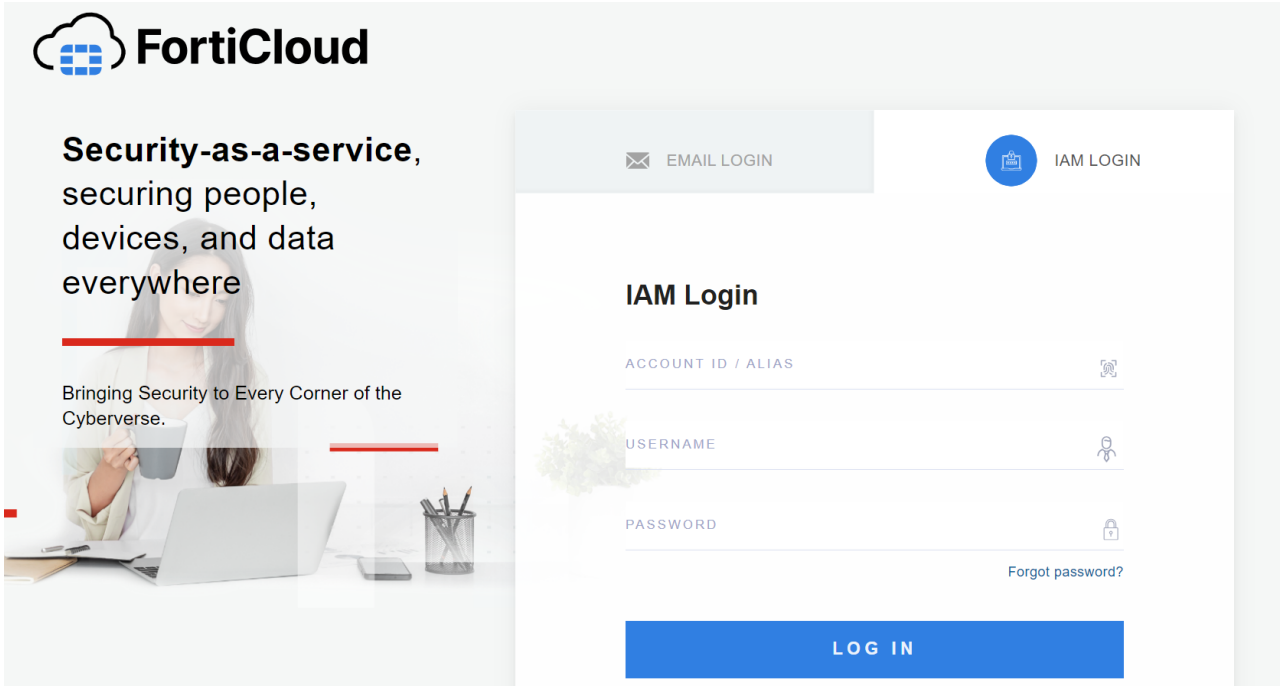
How to use FortiCloud Organization

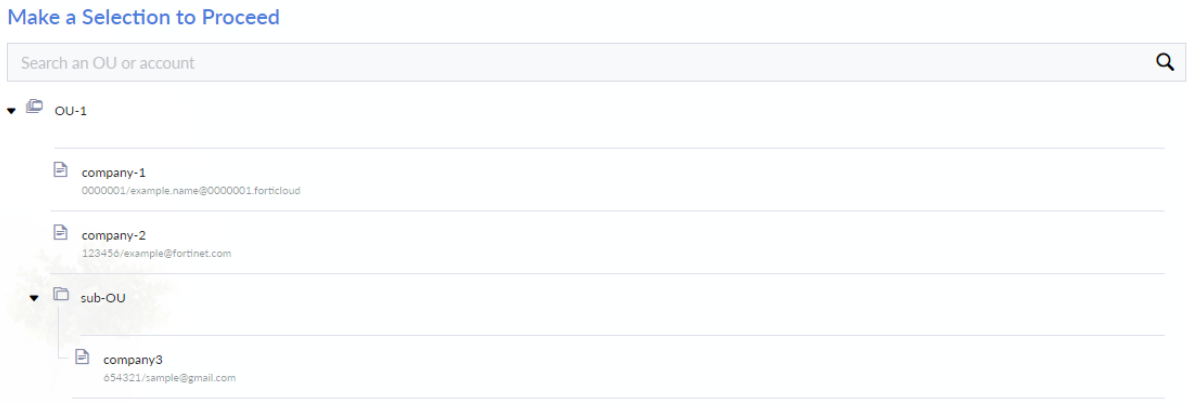
1. Turn on the Organization feature.
   a. Access the Organizational portal. Go to *My Account* > *My Account (IAM version)* > *Account Preferences* and click *Enable Organization Feature*.
2. Create Organizations.

   a. Go to https://support.fortinet.com/organization.
   b. Please refer to Creating an organization for detailed steps on creating organizations.
3. Create member accounts under Organizations.
   a. Member accounts are independent FortiCloud accounts linked to a primary account, each with its own billing, configuration, and resources. They allow different departments or business units to operate separately but remain associated with a central account.
   b. AM users and permission profiles created by a member account cannot have the OU (Organizational Unit) type. This means they cannot select OUs or manage other member accounts, even if those accounts belong to the same OU.
   c. Refer to Creating new member accounts for detailed steps on creating member accounts.
4. Enable and create permission profiles.
   a. Permission profiles determine the level of access granted to users. These profiles must be created before you can assign them to users and user groups.
   b. For details on the distinction between users with Local and Organization access types, see Permission scope with Organizatio
   c. Please refer to Creating a permission profile for detailed steps on creating permissions.
5. Create IAM users.
   a. IAM Users are identities created within a single FortiCloud account. The primary account manages their permissions and access to resources, providing fine-grained control over user access within the account.
   b. When creating an IAM user, you must assign them to permission profiles created in the previous step.
   c. Please refer to Creating a new IAM user for detailed steps on creating IAM users.
6. Manage users.
   - To manage IAM users' access to FortiAppSec Cloud resources under different member accounts, you can either edit an existing IAM user and set their *Type* to *Organization*, or create a new *Organization* type IAM user.
   - An IAM user with Organization type can transfer products between different OUs and register assets to member accounts. For guidance on navigating the Asset Management portal, refer to the Viewing assets in the Organization.
   - Assigning IAM users with a local type to an organization on the FortiAppSec Cloud organization page will no longer be effective if the organization is associated with a member or root account. IAM users from the member or root account will always have the ability to manage resources under the account, as long as their permission profile allows it.

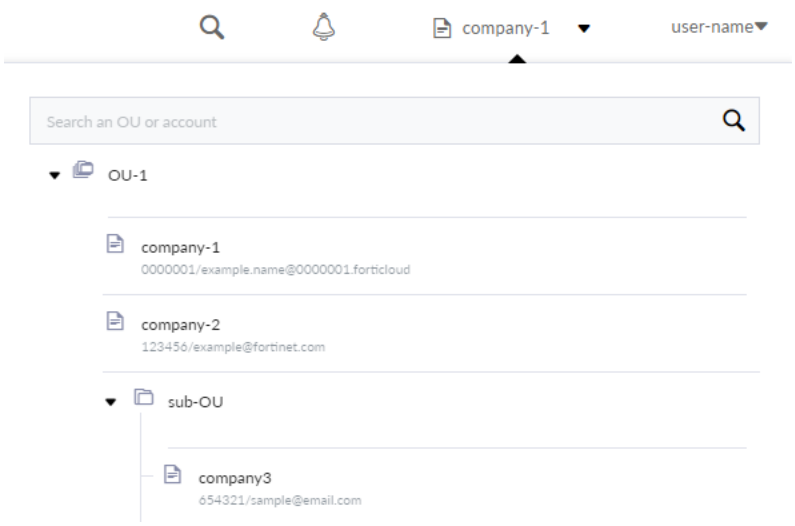
Switching between organizations in FortiCloud

1. Logging into the FortiAppSec Cloud portal as an IAM user with the Organization type will lead to a selection page where you must choose an account to proceed with resource operations.





2. After selecting an account, you can switch accounts using the dropdown menu in the top right corner.



Best Practices

This section provides guidelines on how to configure your FortiAppSec Cloud to best fit your operational needs.

While many features are optional and flexible, best practice recommendations offer helpful guidance for effective protection and provide insights to consider across different use cases.



This section includes recommendations that apply to combinations of multiple features, to the entire appliance, or to your overall network environment.

Please see feature-specific recommendations in the relevant feature's instructions.

Compliance

FortiAppSec Cloud helps ensure compliance with data protection regulations by offering features like secure data handling, access control, and audit logging, supporting your operational needs.

- General on page 457
- WAF on page 457
- Advanced Bot Protection on page 458
- GSLB on page 459

Notable Data Protection Regulations

The following list highlights widely recognized regulations but is not exhaustive of all data protection and privacy laws that may apply.

- **General Data Protection Regulation (GDPR)** is an EU regulation that governs the processing of personal data of individuals in the European Economic Area (EEA) to protect data privacy.

While there is no single, universally recognized GDPR certificate, organizations that handle personal data of EU residents can undergo third-party audits to verify compliance. FortiAppSec Cloud supports GDPR compliance by enabling secure data transfer and ensuring that data belonging to EU residents remains within EU-based data centers.

- **Health Insurance Portability and Accountability Act (HIPAA)** is a U.S. regulation that protects personal health information (PHI) by enforcing strict security and privacy standards.

  While there is no official HIPAA certification, companies handling PHI can undergo third-party audits to verify compliance.



Different countries may have specific regulations that apply. It is important to stay informed and up to date on the regulations relevant to your regions of operation, and configure your settings accordingly.

For assistance, please contact our support team.

General

Logging and Auditing

Maintaining traffic logs and server access logs is crucial for audit trails and compliance with data access and processing requirements. By monitoring and logging security events, including incidents and anomalies, you can track potential security breaches and unauthorized access attempts.

Geo-location tagging and traffic monitoring can help identify whether any breaches or violations, such as those required by HIPAA or GDPR, have occurred by providing detailed logs of access requests to specific data centers.

Sample Regulations to Note

- General Data Protection Regulation (GDPR):
  - Article 30 requires audit logs to ensure proper handling of Personally Identifiable Information (PII).
  - Article 33 requires breach logs to identify when and how breaches occurred.

How to meet regulations with FortiAppSec Cloud

FortiAppSec supports regulatory compliance providing robust audit and logging capabilities. It logs every administrative action and configuration change, and securely retains all audit logs for future review and accountability. These logs help demonstrate operational transparency and support forensic analysis if needed.

- Go to General > Audit Logs to view logs.
- Go to General > Reports to configure scheduled email reports.

WAF

Secure data processing

The Web Application Firewall's features help ensure compliance with regulatory frameworks concerning technical measures for securing data processing by preventing attacks, securing access, logging events, and ensuring real-time monitoring.

The WAF and Threat Analytics services are also SOC 2 compliant.

Sample Regulations to Note

- **General Data Protection Regulation (GDPR):** The following articles outline key aspects of the GDPR that FortiAppSec Cloud WAF can help support through secure configuration. For complete details, please refer to the full text of each article.
  - Article 25 – Data protection by design and by default: Requires the integration of data protection measures from the outset.
  - Article 32 – Security of processing: Mandates the implementation of technical and organizational measures to ensure a level of security appropriate to the risks.

How to meet regulations with WAF

FortiAppSec Cloud's WAF service is SOC 2 compliant, indicating that it has met rigorous standards for security, availability, and confidentiality. To further strengthen your application's data protection posture, enable WAF modules such as Data Loss Prevention, Machine Learning-based Threat Detection, Security Rules, File Protection, and Information Leakage Prevention.

For instructions on enabling WAF modules, please refer to Add and Remove Modules on page 128.

Advanced Bot Protection

Data Protection

Advanced Bot Protection supports regulatory compliance by helping you demonstrate appropriate technical measures for securing personal data.

Sample Regulations to Note

- **General Data Protection Regulation (GDPR):** The following articles outline key aspects of the GDPR that FortiAppSec Cloud can help support through secure configuration. For complete details, please refer to the full text of each article.
  - Article 5 - Personal Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
  - Article 32 - Security measures used to protect personal data must be regularly tested, assessed, and evaluated to ensure they remain effective.

How to meet regulations with Advanced Bot Protection

Enable Advanced Bot Protection to demonstrate "appropriate technical measures" under GDPR by reducing the risk of unauthorized processing and enabling timely detection, reporting, and response to security incidents.

Our professional engagement team will analyze your application and apply tailored protections for you, so you do not need to configure specific settings yourself to meet regulatory requirements.

GSLB

Data Region

Data Region regulations dictate restrictions on where data must be stored and processed, or the requirements associated with moving data between regions.

Sample Regulations to Note

- **General Data Protection Regulation (GDPR):** The following articles outline key aspects of the GDPR that FortiAppSec Cloud can help support through secure configuration. For complete details, please refer to the full text of each article.
  - Articles 44-50 - Restricts the transfer of personal data outside the EU to countries with an adequacy decision or to those with appropriate safeguards in place, such as Standard Contractual Clause (SCCs), Binding Corporate Rules (BCRs), or other measures like approved codes of conduct or certifications.

How to meet regulations with GSLB

To ensure compliance with legal data boundaries, limit the geographic areas to which sensitive data is routed. For example, traffic from the EU should only be routed to servers in countries that have received GDPR Adequacy decisions.

You can achieve this by using regional data centers and geolocation-based routing. To deploy regional data centers,

1. Go to **Virtual Server > Data Center**.
2. Click **Add Data Center**.
3. Set the **Region** to a location that complies with your applicable data protection regulations.
4. Repeat steps **1** through **3** until you have covered all desired regions of operation.

To use geolocation-based routing, please refer to How to load-balance by geolocation on page 346.

WAF Best practices

The following topics introduce the best practices when using FortiAppSec Cloud WAF.

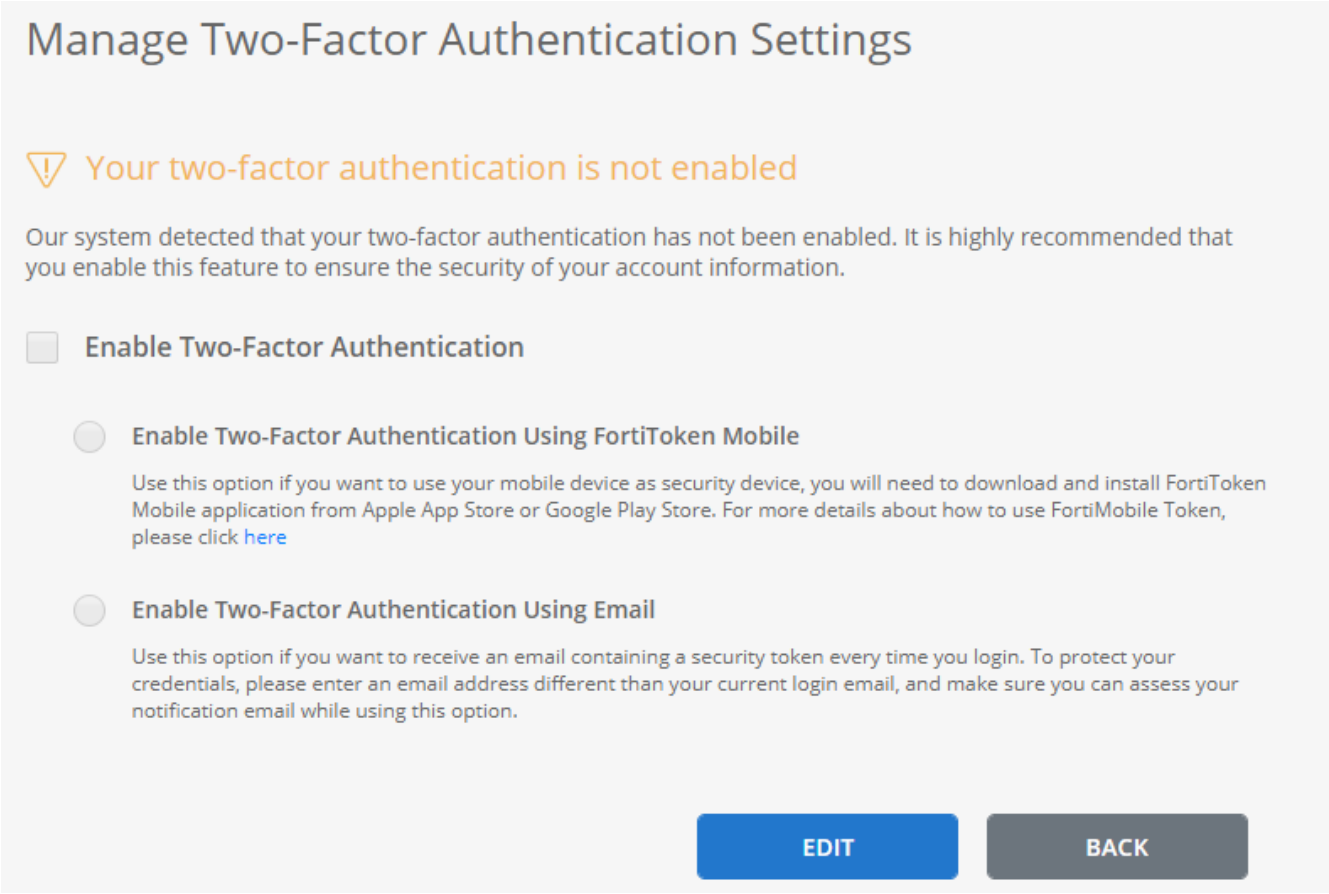
- Using Dashboard to monitor important notices
- Using FortiView to reduce false positives
- Setting up a secure environment

Two-Factor Authentication

You can enable **Two-Factor Authentication** via FortiCloud. 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



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. FortiAppSec 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 Log Settings.

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.

Statistics on requests

The following widgets display the number of requests to the application, and how many requests are blocked by FortiAppSec 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.

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 ().

If you have multiple origin servers, it's recommended to enable Health Check, so that when a server becomes unavailable FortiAppSec Cloud can distribute its traffic to other servers.

Using FortiView to reduce false positives

Legitimate traffic may occasionally be detected as attacks if security rules are configured with inappropriate thresholds.

Certain web pages, such as stock list pages, can trigger rule violations even for regular users; frequent page refreshes can cause normal users to be identified as bots.

Monitoring and Analysis

To minimize the risk of blocking legitimate traffic, regularly review attack statistics in FortiView. This interface provides detailed insights into attack patterns and facilitates identification of false positives.

Identifying False Positives

1. Pattern Analysis:
   - If attacks originate from multiple source IPs but target the same URL, they may represent false positives.
   - Investigate by navigating to Threat by Source IPs and selecting Source IPs.
   - If the URLs tab for multiple source IPs displays the same URL, consider this potential false-positive behavior.
2. Mitigation Steps:
   - Known Attacks: Click Add Exception next to the signature ID. This prevents traffic to the affected URL from being treated as an attack, even if it matches the signature.
   - Other Attack Types: Edit the corresponding security rules to add the affected URL as an exception.

Recommendations

The method described above serves as one example. Administrators are encouraged to explore additional functionality within FortiView Threat View to identify and manage false positives effectively.

How to block an 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 FortiAppSec 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

- **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.

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 174.

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.

- **Bot Mitigation > ML Based Bot Detection**

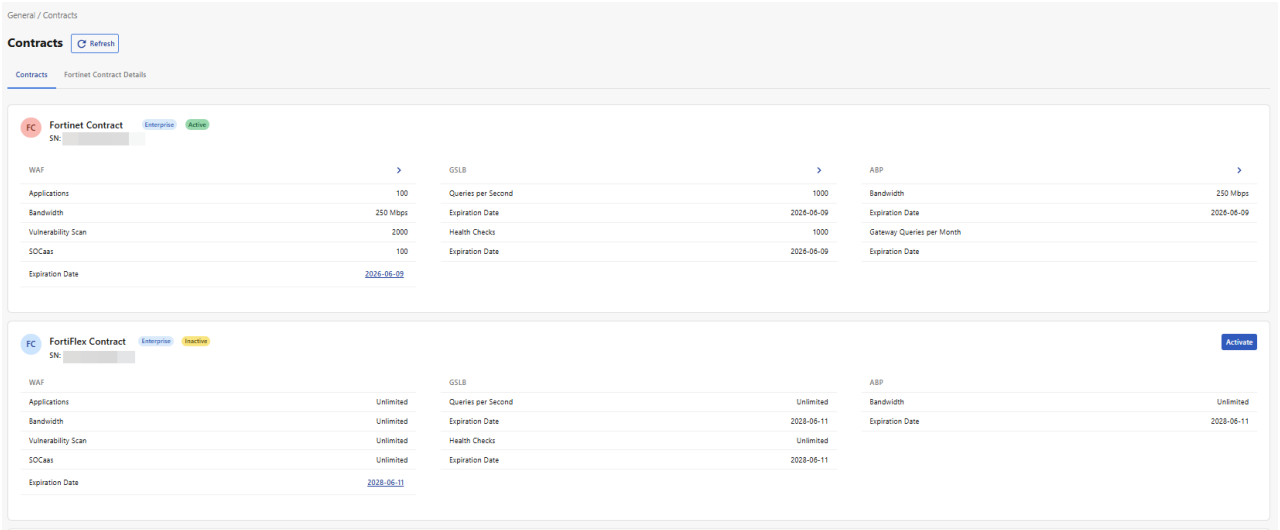
Enable **Machine Learning Based Bot Detection**. This complements existing signature and threshold-based rules to detect sophisticated bots that can sometimes go undetected.For more information, see ML Based Bot Detection on page 164.

Support

If you need assistance or have any questions about the upcoming changes, please contact your local reseller or reach out to Fortinet Support.

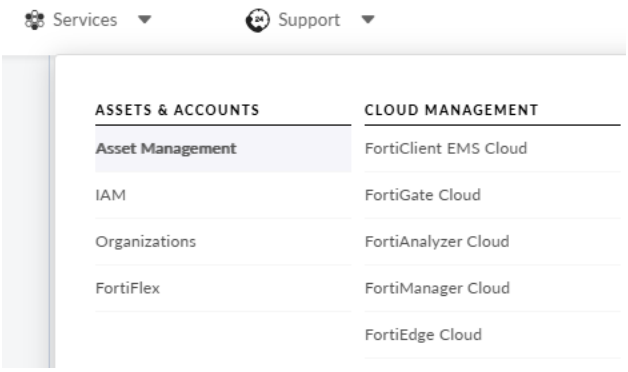
Registering serial number

1. Navigate to **General > Contracts**. The serial number (SN) for your service is located under the title of your active contract.



2. Go to https://support.fortinet.com, follow the guidelines provided in the FortiCloud documentation Registering Assets to register serial numbers (assets).

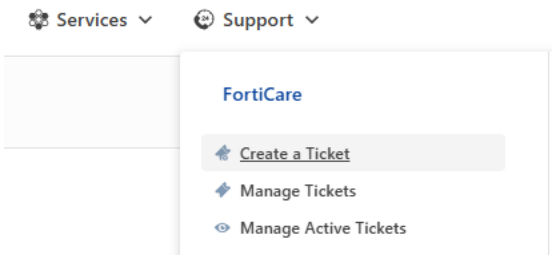
Once all of your serial numbers are registered, you can view them in FortiCloud through **Services > Asset Management > Products**.



Submitting support tickets

To submit a technical support tickets, you will be required to enter the serial number of an active license.

1. In the top navigation bar, go to **Support > Create a Ticket**.



2. Select **Technical Support Ticket**, enter the serial number of a valid license, then click **Submit Ticket**.

FAQs

This section answers frequently asked questions about FortiAppSec Cloud.

You can jump to the relevant topic areas:

- General on page 465
- WAF FAQ on page 472
- ABP FAQ on page 479
- GSLB FAQ on page 481
- Threat Analytics FAQ on page 488
- Migrating from preceding Fortinet services on page 493

General

- Overview on page 465
- FortiAppSec contracts on page 467
- Notifications and Communication on page 470
- Miscellaneous on page 471

Overview

Why migrate from FortiWeb Cloud/ FortiGSLB/ FortiGuard ABP to FortiAppSec Cloud?

FortiAppSec Cloud is Fortinet's integrated platform for application security services. It unifies four previously standalone solutions — FortiWeb Cloud (Web Application Firewall and Threat Analytics), FortiGSLB (Global Server Load Balancing), and FortiGuard Advanced Bot Protection — into a single, cohesive platform. This integration streamlines management and operations while delivering a comprehensive application security solution. FortiAppSec Cloud addresses a broad spectrum of needs, from traffic optimization and load balancing to advanced threat protection, ensuring robust and efficient security for modern applications.

How is the FortiAppSec Cloud Platform delivered?

The FortiAppSec Cloud Platform is a SaaS service accessible via https://appsec.fortinet.com.

What are the advantages of the FortiAppSec Cloud Platform?

The advantages of the new solution include:

- Unified management for web application security, advanced bot protection, threat analytics, and server load balancing.
- End-to-end protection for web applications and APIs.
- Centralized security management for hybrid cloud environments.
- Advanced delivery capabilities, including GSLB and content routing.

- Faster content delivery with a global CDN.
- Improved visibility and reduced complexity for easier application security management.

Is the FortiAppSec Cloud Platform SOC2 compliant?

The WAF and Threat Analytics services are SOC2 compliant. The GSLB and Advanced Bot Protection services are under review and are expected to pass SOC2 compliance shortly. SOC2 compliance ensures services meet rigorous security, availability, and confidentiality standards.

Are there any changes in functionality/features for existing services?

Most functionality and features remain the same between the previous standalone products and FortiAppSec Cloud. However, with FortiAppSec Cloud, we aim to highlight the evolution of the Cloud WAF industry towards a unified, all-inclusive offering that encompasses all cloud-based web application protection features.

Where can I check the status of FortiAppSec Cloud and access incident history?

Visit https://status.appsec.fortinet.com/ to check the real-time service status, review incident history, and subscribe for updates. Subscribing ensures you stay informed about any outages or changes affecting the system.

Can I access the FortiAppSec Cloud portal via API?

Yes, you can access the FortiAppSec Cloud portal through its API. This API enables you to manage configurations, automate workflows, and access application data. For more details, please refer to the FortiAppSec Cloud RESTful API Reference.

What is FortiAppSec Cloud's bandwidth capacity?

FortiAppSec Cloud is deployed on cloud service providers (CSPs) that support traffic in the tens to hundreds of Gbps, depending on the region and availability zone. With its auto-scaling capability, FortiAppSec can easily expand to growing customer traffic needs.

What export options are supported for FortiAppSec Cloud insights?

FortiAppSec Cloud supports the following export options for logs:

- Audit logs: Can be exported to FortiAnalyzer, FortiSIEM, Syslog, or Elasticsearch.
- Attack logs: Can be exported to FortiAnalyzer, FortiSIEM, Syslog, or Elasticsearch.
- Traffic logs: Can be exported to AWS S3 buckets or Azure Blob storage containers.
- Splunk integration: Supports exporting Attack and Audit logs to Splunk (requires the FortiAppSec Cloud Add-on for Splunk).

FortiAppSec Cloud also supports the following export options for reports:

- WAF Network Diagnostics reports: Can be exported as PDF files.
- Scheduled system-wide reports: Automatically sent via email.

There are currently no direct export options for dashboard widgets.

FortiAppSec contracts

What features are included in a FortiAppSec Cloud Contract, and can services be purchased separately?

The FortiAppSec Fortinet Contract is a comprehensive solution designed to enhance application security and optimize performance. The contract includes the following features:

- **Web Application Firewall (WAF)**: Requires both **website** and **bandwidth** contracts to ensure proper protection and performance. The available features vary based on Standard and Advanced plans.
- **Dynamic Application Security Testing (DAST)**: Supports a defined number of **assets** for security testing.
- **Global Server Load Balancing (GSLB)**: Includes features such as **Queries Per Second (QPS)** and **health checks** to maintain server efficiency.
- **Advanced Bot Protection (ABP)**: Provides robust defenses against malicious bot activity.
- **Threat Analytics**: Delivers real-time visibility, actionable insights, and advanced reporting on application-layer security events for proactive threat detection and response.
- **Security Operations Center (SOC)**: Offers managed security monitoring and incident response services for comprehensive threat management.

What are the different WAF plans in FortiAppSec Cloud Contracts?

There are three tiers of FortiAppSec Cloud contracts:

- **Standard**: Focuses on core protections, including negative security model policies, default configurations such as signatures, request limits, and more.
  This plan requires separate licenses for the number of applications and bandwidth.
- **Advanced**: Includes all features of the **Standard** plan and adds advanced capabilities, such as machine learning for web/API/bot protection, Threat Analytics, and additional security enhancements.
  This plan requires separate licenses for the number of applications and bandwidth.
- **Enterprise:** Includes all features of the **Advanced** plan, and also bundles services that are billed separately in the **Standard** and **Advanced** plans, such as Advanced Bot Protection, GSLB, and SOCaaS.
  - Each GSLB application includes a lifetime allocation of 10 GSLB health checks (HC).
  - For every 5 Mbps of licensed bandwidth, the system allows a monthly average of up to 20 queries per second (QPS).

  This plan is charged as an annual subscription, with pricing based on bandwidth limit.

For a detailed comparison of the Standard, Advanced, and Enterprise plans, please visit the FortiAppSec Cloud Plan Comparison.

Please note that the features and usage limits of these plans are fixed and cannot be customized. For example, you cannot "mix and match" the bandwidth limit of the standard plan with the application limit of the Advanced plan.

Can I have multiple license types active in my account at the same time?

No, only one primary license type can be active at a time within a single account. Inactive licenses cannot be used while another license type is active.

Exception: Gateway licenses remain active regardless of which other license type is in use. This is because they provide essential services, such as traffic routing, load balancing, and secure application delivery, which are critical for maintaining uninterrupted operations. By staying active, gateway licenses ensure that core functionality continues seamlessly, even when other licenses are inactive or switched.

How do I check my current active license type?

You can check your current active license by navigating to **General > Contracts** in the FortiAppSec Cloud web portal. On this page, you will see all your contracts along with their statuses, including an indication of which license type is currently active.

If you do not see your license or encounter any issues, please contact Fortinet Support.

How do I switch my current license to a newly purchased license?

Log into the FortiAppSec Cloud web management console, navigate to **General > Contracts**, select the desired license type you wish to activate, and follow the on-screen prompts to confirm the switch.

How can I increase the number of applications supported by my FortiAppSec Cloud contract?

FortiAppSec Cloud contracts are seat-based and, unlike legacy FortiWeb Cloud contracts, do not support stacking or overlapping multiple contracts. When a new contract is registered, it is automatically scheduled to begin after the current contract expires.

If you need to increase the number of applications (seats) before the current contract ends, contact your Fortinet sales representative and request a contract adjustment via co-term to reflect the increased seat count.

What happens when my current license expires?

When your current license expires, FortiAppSec Cloud will continue protecting your applications for 21 days.

During this 21-day grace period:

- Your applications remain protected.
- However, you cannot edit the configurations for your applications unless the contract is renewed.

After the 21-day extension:

- Your applications will be deleted from your FortiAppSec Cloud account.

To avoid service interruptions and potential data loss, ensure your contract is renewed before the grace period ends. For assistance, please contact Fortinet Sales.

How is the number of WAF sites and bandwidth calculated in FortiAppSec Cloud Contracts?

The number of WAF sites and the allocated bandwidth are determined by the specific SKU purchased. Each SKU defines the allowed number of application sites and the corresponding bandwidth allocation per seat.

For detailed contract information, refer to the FortiAppSec Cloud Ordering Guide.

How do I extend a FortiAppSec Cloud Fortinet Contract?

To extend your FortiAppSec Cloud Fortinet Contract, contact your sales representative (SE) to adjust the quantity or expiration date of your existing contract instead of purchasing a new one.

If you would like to change contract types, (eg. from Standard to Advanced) you may also purchase a new FortiAppSec Cloud Fortinet Contract with an effective date at the end of your current contract, rather than extending the current contract's duration.

You will receive an email notification as your license approaches its expiration date.

How does GSLB QPS and health check work?

GSLB QPS (Queries Per Second) and health checks in FortiAppSec Cloud Contracts are managed based on the license's specifications. The GSLB QPS determines the number of queries your Global Server Load Balancing can handle per second, while health checks monitor the availability and performance of your services. These parameters are defined in your contract and are enforced to ensure optimal load balancing and service reliability.

For detailed contract information, refer to the FortiAppSec Cloud Ordering Guide.

How does the Advanced Bot Protection (ABP) quota work?

The Advanced Bot Protection (ABP) quota in FortiAppSec Cloud Contracts defines the number of bot queries your system can handle per month. This quota ensures that the ABP features are used within the licensed limits. If the quota is exceeded, additional bot traffic may be restricted unless the license allows for overuse or an upgrade is performed.

For detailed contract information, refer to the FortiAppSec Cloud Ordering Guide.

What are the SOCaaS features available?

SOCaaS (Security Operations Center as a Service) features include real-time security monitoring, event response, and threat analysis. SOCaaS helps in identifying, analyzing, and mitigating security threats to protect your applications and data, providing an added layer of security management.

For detailed contract information, refer to the FortiAppSec Cloud Ordering Guide.

How does the DAST scanning quota work?

The DAST (Dynamic Application Security Testing) scanning quota specifies the number of assets that can be scanned for vulnerabilities. This quota ensures that security testing is conducted within the licensed limits. The exact number of assets that can be scanned depends on the specific FortiAppSec Cloud Contract SKU you have purchased.

For detailed contract information, refer to the FortiAppSec Cloud Ordering Guide.

Can I buy WAF features A-La-Carte?

No, you can only choose between the **Standard**, **Advanced** and **Enterprise** plans.

What should I do if my account is in read-only mode?

Your account may enter read-only mode due to one of the following reasons. The next steps depend on the cause:

- **Bandwidth Overage**
  If your bandwidth usage exceeds your quota limits for two consecutive months, your account will enter **read-only** mode.
  To regain full access:
  - *Increase your bandwidth limit*
    Contact your sales representative to adjust the quantity on your existing contract.
  - *Wait for the next billing cycle*
    The 95th percentile bandwidth usage resets at the start of each billing cycle. If your usage remains within the quota throughout the next billing cycle, access will be automatically restored at the start of the following cycle.
- **Application Overage**
  If you have more applications than is supported by your contract, your account will enter **read-only** mode.

To regain full access:

- *Increase your application limit*
  Contact your sales representative to adjust the quantity on your existing contract.
- *Decrease number of applications*
  Delete applications until the number of applications falls under your contract quota.

- **Expired Contract**
  When your contract expires, your account enters a 21-day grace period during which it remains in **read-only** mode.
  To regain full access:
  - *Purchase additional contracts*
    You can purchase additional FortiAppSec Cloud contracts through any supported platform.
  - *Extend expiration date*
    Contact your sales representative to extend your current contract.

Does the FortiAppSec Cloud serial number change when the license is replaced?

It depends on the type of license change.

- If you upgrade within the same license type (for example, from Standard to Advanced or Enterprise), the serial number remains the same.
- If you switch from a FortiAppSec Cloud license to a FortiFlex or Public Cloud Marketplace subscription, the serial number will change.

How will I know if my service has entered the grace period?

When a change occurs that affects your level of access to applications, the FortiAppSec Cloud web portal displays an alert banner upon login. You also receive a corresponding email notification.

Notifications and Communication

Will I be notified before my license or contract expires?

Yes, the FortiAppSec Cloud system will send notifications to inform you before your license or contract expires. These notifications serve as reminders to renew or switch to a different contract to avoid service interruptions.

How will I be notified about service impacts when switching licenses?

Service impacts due to license switches will be communicated through confirmation dialogs in the management console. These dialogs will display specific warnings related to the potential effects on your services, ensuring you are aware of any disruptions before confirming the change.

What notifications will I receive about quota usage and limitations?

You will receive notifications when you approach or exceed your quota limits for various services such as bandwidth, GSLB QPS or ABP queries. These alerts help you manage your resource usage effectively and consider upgrading your license if necessary.

Once your bandwidth usage exceeds your contract quota limits for two consecutive months, your application will enter read-only mode, restricting you from making any changes to your application configurations.

How can I track my resource usage and receive alerts?

Resource usage can be tracked through the **Usage** page in the management console, where usage reports are available. Additionally, you can set up alerts to notify you when your usage approaches predefined thresholds, enabling proactive management of your resources.

Why am I not receiving notification emails from FortiAppSec Cloud even after subscribing to email notifications?

Please ensure that emails from FortiAppSec Cloud are white-listed and not filtered as spam. You will not be able to receive any emails from FortiAppSec Cloud if the address is blocked by the firewall. If FortiAppSec Cloud emails are filtered as spam, then the email notifications would not arrive in the email inbox and may be in the "Spam" folder.

Miscellaneous

What is Two-Factor Authentication used for?

FortiAppSec Cloud offers Two-Factor Authentication to secure your FortiAppSec Cloud account by an additional security token generated by Virtual MFA Devices. See Two-Factor Authentication.sent through email or the FortiToken Mobile application. See Two-Factor Authentication on page 459.

What are the supported web browsers?

FortiAppSec Cloud supports the following web browsers:

- Mozilla Firefox version 59 or higher
- Google Chrome version 65 or higher

Who should I contact for assistance?

- **Technical Support:** For configuration issues, troubleshooting, or technical queries, reach out to Fortinet Support through the Fortinet Support Portal.
- **Sales Team:** For inquiries about upgrades, licensing, or contract modifications, contact Fortinet Sales.

How do I view the serial number of my license?

You can find the serial number of your FortiAppSec Cloud license by logging into the web portal and navigating to **General > Contracts**.

If the serial number (SN) has already been registered, you can also find it in FortiCloud under **Asset > Manage/ View Products**.

For instructions on registering serial numbers, please see Registering Assets.

How long can I stay logged in to the FortiAppSec Cloud portal, and how long can the browser remain idle?

The FortiAppSec Cloud portal logs you out after 15 minutes of browser inactivity.

If you remain active, the session ends after 1 hour of login time.

Is it possible to restrict access to the FortiAppSec Cloud management portal to specific source client IPs within my organization?

IP-based access restrictions are not currently supported. However, you may be able to control access using IAM profiles or organizational units (OUs).

Why are my WAF applications no longer visible after logging in?

The cause of this issue may depend on your FortiCloud OU permissions and account type.

1. If you are a Master user:
   - **Contract expiration**: If your contract has expired beyond the grace period, all applications may have been automatically deleted.
   - **Account ID change or migration**: If you changed or migrated your FortiCloud account ID without notifying the FortiAppSec team, your applications may not appear. Submit a support ticket including:
     - Old FortiCloud account ID
     - New FortiCloud account ID
     - A brief note stating that the ticket is for account migration or rebinding
2. If you are an IAM user:
   - **Asset Group restrictions**: Your managing primary account may have enabled Asset Groups but not configured them correctly. You may not have access to any applications.
   - **Permission changes**: Your managing primary account may have recently modified your FortiAppSec permissions, removing your access to view applications.

WAF FAQ

- Application Onboarding on page 472
- Network on page 474
- Usage on page 478
- Miscellaneous on page 478

Application Onboarding

What is a FortiAppSec Cloud application, and how many domains does a WAF application support?

In FortiAppSec Cloud, an application can include:

- A primary declared domain name.
- Up to 9 additional domain names that belong to the same root domain and point to the same origin server(s).

For example,

- Domains such as "example.com" and "test.example.com" can be part of the same application "example.com."
- However, "test.com" would be considered a different application because it does not share the same root domain.

This structure ensures that all domains within an application share consistent security and origin configurations.

How do I onboard WAF applications?

For instructions on onboarding WAF applications, please see Onboard WAF applications on page 65.

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 IP address provided by FortiAppSec Cloud.
- Configure your origin servers to only accept traffic from FortiAppSec Cloud IP addresses. See this article for a list of FortiAppSec Cloud IP addresses.
- Configure security rules and observe the attack logs in FortiView Threat View 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 Attack logs on page 412 for how to add exceptions.
- Enable **Block Mode** in **WAF > 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 FortiAppSec Cloud IP addresses to make sure access from FortiAppSec Cloud to your web application is uninterrupted. See this article for a list of FortiAppSec Cloud IP addresses.

What is an application in FortiAppSec Cloud?

In FortiAppSec 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, FortiAppSec 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 FortiAppSec Cloud scrubbing center which is deployed in the same region with your origin server. See this article for a list of FortiAppSec 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 FortiAppSec Cloud scrubbing centers?

FortiAppSec 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 FortiAppSec 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 FortiAppSec Cloud IP addresses.

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

Network

What public cloud regions are currently supported?

For a complete list of supported regions, please see Restricting direct traffic & allowing FortiAppSec Cloud IP addresses on page 76.

How do I request support for additional Public Cloud regions?

Please contact your local sales representative for the latest roadmap on adding additional regions.

Can one account protect applications in multiple regions?

Yes, the WAF module allows each application to be assigned a region during onboarding, so customers are not restricted to a single region. Additionally, the GSLB module enables load balancing across multiple locations and regions.

Can FortiAppSec Cloud WAF protect applications that are not hosted on a public cloud?

Yes, FortiAppSec Cloud WAF is not limited to applications hosted on a specific public cloud.

Can FortiAppSec Cloud WAF protect applications that are hosted on non-standard ports?

Yes, predefined non-standard ports are available for selection during the onboarding process. If you need support for a different port, please contact support.

Can FortiAppSec Cloud WAF protect multiple web applications on the same account?

Yes, please review License & Contract on page 21 for information on usage limits for different license options.

Does FortiAppSec Cloud WAF offer a Content Delivery Network (CDN) service?

Yes, you can enable Global CDN at no additional cost. For more details, please refer to the CDN on page 79 section.

When using the WAF service for my application, what do I need to implement outside of the FortiAppSec Cloud web portal?

To implement the WAF service's WAF service, please make the following changes outside of the FortiAppSec Cloud platform:

- **DNS Update:** Modify the DNS entry of your web application to point to FortiAppSec Cloud WAF.
- **Traffic Forwarding Configuration:** Configure FortiAppSec Cloud with the original web application IP to forward traffic accordingly.
- **Client Traffic Flow:** With this setup, traffic from clients will first reach FortiAppSec Cloud and then be forwarded to your web application.

FortiAppSec Cloud WAF's onboarding wizard will guide you through these steps for seamless implementation.

How can I add applications running on non-standard port?

FortiAppSec 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 FortiAppSec Cloud Support or your sales representative for further help. Notice not all non-standard ports can be used, and HTTP and HTTPS services must use different ports.

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?

WAF automatically obtains an SSL certificate on your behalf from Let’s Encrypt within two minutes of the DNS CNAMEA record change. It will be used in HTTPS connections to encrypt or decrypt the traffic. If FortiAppSec Cloud fails to obtain the certificate, it will try again 12 minutes later.

Thirty days before your certificate expires, WAF verifies again that your DNS CNAMEA record is still correct. If it is, FortiAppSec Cloud renews your certificate for another 90 days, so it never expires. For more information, see Automatic Certificate on page 98.

What do I need to pay attention to if I use automatic certificates?

FortiAppSec Cloud WAF 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 FortiAppSec Cloud, make sure to add "letsencrypt.org" in the CAA value. This allows Let's Encrypt to issue certificates for your domain name.

What TLS versions are supported?

FortiAppSec Cloud supports 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 FortiAppSec Cloud WAF, 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 475
    - What’s a Certification Authority Authorization (CAA) record and do I need to use it? How does it affect automatic certificate? on page 475

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. FortiAppSec Cloud WAF 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 FortiAppSec Cloud WAF is bypassed.
   b. If there are more than one origin servers, FortiAppSec Cloud WAF 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 FortiAppSec 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 FortiAppSec Cloud causing the error.
   If the origin server is not accessible, it suggests that the connectivity issue is unrelated to FortiAppSec Cloud WAF 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 FortiAppSec Cloud WAF 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?

FortiAppSec Cloud WAF supports 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 for instructions on exporting logs to your syslog server.

How can I use FortiAppSec Cloud WAF with AWS ALB/ELB?

When using FortiAppSec Cloud WAF, the client's requests from the Internet are forwarded to WAF 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 the WAF service 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. The WAF service updates the IP address according to this TTL value. If the TTL indicates the IP address expires, WAF will resolve the domain name to obtain the latest IP address.

The IP addresses of my origin servers keep changing. How can I configure FortiAppSec 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 FortiAppSec Cloud WAF to access the resources in your public cloud account. See Cloud Connectors on page 205.
2. In **Network > Origin Servers**, select **Dynamic** for **Server Type**, then configure **Cloud Connector** and **Filter** as instructed in Origin Servers on page 103.

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 241 for more information.

How can I get notified of newly added WAF IP addresses?

- Check the inbox of your account email. Search for keywords "new WAF cluster" from "noreply@appsec.fortinet.com".
- Check out the What's New on page 8.
- Use the following APIs to retrieve the IP lists:
  - IPv4: https://appsec.fortinet.com/ips-v4
  - IPv6: https://appsec.fortinet.com/ips-v6

You can find the full list of WAF IP addresses at Restricting direct traffic & allowing FortiAppSec Cloud IP addresses on page 76.

How do I configure SSLVPN?

FortiAppSec Cloud does not provide SSL VPN functionality.

To secure web traffic to your applications, configure SSL/TLS certificates in the portal under **Network > Endpoints**. These certificates enable encrypted HTTPS access but are not used for VPN connections.

To forward traffic to your FortiGate SSLVPN portal, configure FortiAppSec Cloud as the front-end:

1. **Update DNS**: Point your DNS record (for example, vpn.yourcompany.com) to the FortiAppSec Cloud Anycast IP address(es).
2. **Configure SSL/TLS**: In FortiAppSec Cloud, upload or select the SSL/TLS certificate for vpn.yourcompany.com.
   a. Navigate to **WAF > Network > Endpoints**.
   b. Scroll down to **SSL/TLS certificate Management**.
   c. Click **Add New Certificate**. For more details on the configuration options on this page, refer to SSL/TLS Certificate Management on page 97.
3. **Set Origin Server**: Specify the public IP address or FQDN of your FortiGate SSLVPN interface as the origin server.
   a. Navigate to **WAF > Network > Origin Servers**.
   b. Click **Create Server Pool** or edit an existing Server Pool. For more information on the configuration options on this page, refer to Create Server Pool on page 104.
   c. Click the **Edit** icon on one of the server pools to add servers to the server pool. For the server type, select **IP** or **Domain** and enter the public IP address or FQDN of your FortiGate SSLVPN. For more information on the configuration options on this page, refer to Create Server on page 106.

This configuration creates a traffic flow where:

User's Browser → FortiAppSec Cloud (inspects and filters traffic) → FortiGate SSLVPN Portal → User authenticates and connects to the corporate network.

Usage

How does WAF calculate bandwidth?

FortiAppSec 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 FortiAppSec 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.

Miscellaneous

This section answers frequently asked questions about WAF that are not covered in other FAQ topics.

How do I troubleshoot Traffic Log Setting errors?

If your traffic log export is failing, check the notification message for details on the issue. Below are common errors and their possible causes:

Server Type	Error Message	Description
AWS S3	S3 bucket connection failure from our traffic log server	The AWS IAM user corresponding to the S3 bucket lacks the necessary permissions. Please check and update the IAM user permissions in AWS to ensure the required access is granted.
AWS S3	The specified bucket does not exist	The specified S3 bucket does not exist. Please recreate the bucket or update the configuration to the correct bucket name.
AWS S3	The AWS Access Key Id you provided does not exist in our records	The IAM credentials you provided are either non-existent, invalid, or expired. Please update the credentials in **WAF > Log Settings**, under **Traffic Log Export** to ensure proper authentication.
Azure Blob	ContainerNotFound (404)	The specified Azure blob container does not exist. Please update the container name to a valid and existing container.
Azure Blob	AuthenticationFailed (403)	The Azure Blob credential is invalid, which may be caused by an incorrect access key or an improperly configured Azure Blob network firewall. Please update your access key in **WAF > Log Settings**, under **Traffic Log Export**, and check the network configuration in Azure Blob to ensure proper access.

ABP FAQ

This section answers frequently asked questions about ABP.

You can jump to the relevant topic areas:

- Onboarding on page 480
- Integration (deployment mode) on page 480
- Security and Resilience
- Miscellaneous on page 481

Onboarding

This section answers frequently asked questions about the ABP onboarding.

How do I onboard an application onto Advanced Bot Protection?

Onboarding an application onto Advanced Bot Protection is a straightforward process.

Here are the basic steps you should follow:

1. **Install the License**: Install the license (standalone) and verify the connector of FortiADC or FortiWeb is enabled.
2. **Access FortiAppSec Cloud**: login to appsec.fortinet.com and navigate to **Advanced Bot Protection**.
3. **Create an application**: Locate your dashboard's **Add New Application** option.
4. **Integration**: ABP is currently only deployed through integration with FortiADC and FortiWeb. For integrated deployment, follow the integration instructions with FortiADC and FortiWeb.
5. **Monitoring**: Once the application is onboarded and protected, use the FortiAppSec Cloud dashboard to monitor traffic and security incidents. You can set up alerts and notifications for suspicious activities.

The onboarding process is also detailed in this user guide, ABP Setup on page 264.

Integration (deployment mode)

This section answers frequently asked questions about the ABP integration (deployment mode).

What are the deployment options for Advanced Bot Protection?

FortiAppSec Cloud requires injecting JavaScript into the client's session to collect data. Two options are available:

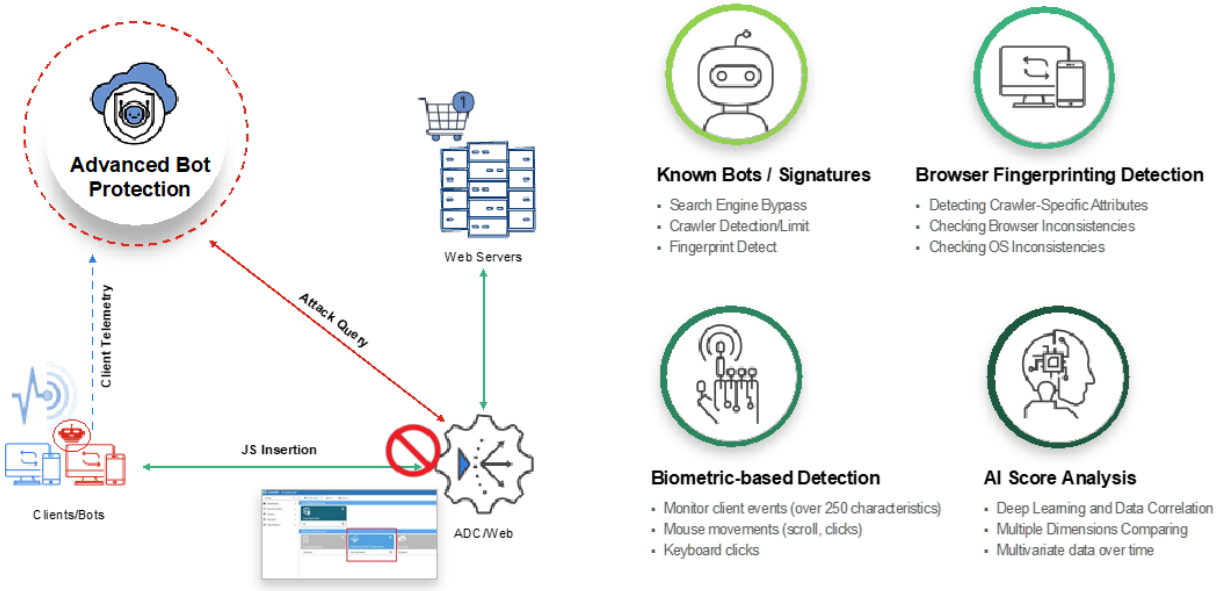
A. Standalone Deployment (coming soon): You can deploy Advanced Bot Protection as a standalone solution. In this mode, you will need to install a snipped code on the web application for browser JS insertion. This mode operates only in monitoring (visibility) mode and cannot enforce or block bots.

B. Integrated Deployment with FortiADC and FortiWeb: Alternatively, you can integrate Advanced Bot Protection with FortiADC and FortiWeb, two leading products in the Fortinet ecosystem. This integrated solution enhances your overall security posture by combining the advanced bot protection capabilities of Advanced Bot Protection with the robust application delivery and web application firewall capabilities of FortiADC and FortiWeb.

How does the integration work?

1. The client reaches the web application via the FortiADC/FortiWeb (acting as a Reverse Proxy).
2. FortiADC/FortiWeb returns an HTTP/S response to the client with JavaScript insertion (via) for telemetric information.
3. The client and the FortiADC/FortiWeb (via fabric connector) communicate with the Advanced Bot Protection Cloud for data telemetry info (headers, device fingerprinting, and more).
4. Advanced Bot Protection inspects the request to determine if the client – is human or a bot.

5. Based on the result of the analysis, Advanced Bot Protection analyzes the request and sends an instruction back to FortiADC/FortiWeb (block, CAPTCHA, allow).



Does Advanced Bot Protection charge for blocked attacks?

No. The FortiAppSec Cloud provides attack information to the FortiADC and FortiWeb, which blocks access to the application and stops the threats.

Miscellaneous

This section answers frequently asked questions about ABP that are not covered in other FAQ topics.

Does Advanced Bot Protection offer real-time reporting and analytics?

Yes, FortiAppSec Cloud's ABP provides real-time reporting and analytics dashboards, allowing you to monitor traffic, bot activity, and security incidents, helping you make informed decisions to enhance your bot protection strategy.

GSLB FAQ

Refer to the following Frequently Asked Questions for any questions or issues you may have. If they do not address your concern, please contact our support team for assistance and we will respond to your request as soon as possible.

- GSLB and DNS Services on page 482
- Health check on page 484
- One-click GSLB on page 485
- Fabric connectors FAQ
- Synthetic testing on page 486

- DevOps on page 486
- Miscellaneous on page 488

GSLB and DNS Services

How long does it take to get the expected DNS response after creating a new FQDN or Zone?

Normally it takes between 30 seconds to several minutes to get the correct DNS response after a new FQDN or Zone is created.

How do you link GSLB to a DNS service?

Create a Zone with the same domain as the GSLB service. The A/AAAA records of the GSLB service should appear in the DNS service resource records list automatically.

How long does it take for a modification in DNS configuration (like zone A record Rdata) to take effect?

The DNS configuration should be active within a few minutes.

How long does it take for the IP to update after the status of one of GSLB service's pool members changes?

It depends on the pool member health check parameters, including down/up retry, interval and timeout. The smaller the value is, the less time it takes for the IP to update. The approximate time it takes is: retry * interval + timeout + system_run_time (in a few seconds).

Why isn't the GSLB service or DNS service working? How do I troubleshoot?

For the GSLB service, first check the status on the GSLB services page and make sure the virtual server in the pool is up. If the status is up or if there is a DNS service resource record, check the Contact & License page and confirm that there are valid query licenses and that the number of used queries is smaller than total queries.

Alternatively, you can check the DNS response status directly. If it is REFUSED, most likely the user does not have valid personal licenses or the maximum capacity has been reached or the domain does not exist. If there is a NOERROR status with NS server information in the authority section, this means it can find that domain and record, but the virtual servers in pool are not available. If the status is NXDOMAIN with SOA record in authority section, it means the domain name exists but the record's hostname doesn't exist.

What's the difference between FQDN configure DNS-Query-Origin and Virtual Server Pool GEO?

Both methods match DNS queries based on client's DNS Server IP location.

DNS-Query-Origin method in FQDN uses location list to do the matching and can select multiple locations into the list. It only matches the region that is selected in location list.

GEO method in virtual server pool uses the virtual server's data center region to respond to the DNS query geographically. This method matches the DNS query location with the data center's region if they are in same region, country or continent.

What are the meanings of the special Regions?

Reserved: IP addresses that are not assigned (e.g. 10.0.0.0/24)

Anonymous Proxy: IP addresses that are defined as anonymous proxy in GeoIP-DB (e.g. 46.19.137.0/24)

Satellite Provider: IP addresses that are defined as satellite provider in GeoIP-DB (e.g. 57.72.6.0/24)

Other Country: Reserved for further use, and no IP address are assigned to this region

Asia/Pacific Region: IP addresses that are defined as Asia/Pacific Region in GeoIP-DB, but not belonging to any specified Asian countries

Europe Region: IP addresses that are defined as Europe in GeoIP-DB, but not belonging to any specified European countries

What are the meanings of the special Locations?

Any: Any client IP GEO location

How does GSLB GEO work?

Assume that the user uses DNS-Query-Origin method in GSLB services and wants to perform load balancing according to DNS query source IP. The work flow is as follows:

1. Client sends DNS query to the local DNS server
2. The local DNS server functions as a resolver to ask who knows the IP for this DNS query.
3. After doing recursion from root server, the query is sent to GSLB with the local DNS server's source IP address. GSLB will respond with a best matched IP according to the DNS query source IP (local DNS server's IP) location and send a DNS response to the client's local DNS server.
4. Then, the local DNS server will send a DNS response to the client.

What is the expected result if the source IP matches both the address group and location or one of the address groups or location when the DNS-Query-Origin virtual server pool selection method is selected in GSLB Services?

GSLB will respond to the DNS query based on its source IP according to the address group and location parameter configured in the VSP.

If the source IP matches both the address group and location of one VSP, GSLB will respond to the DNS query with the VS IP from this VSP.

If the source IP matches multiple VSP's address group or location, GSLB will respond to the DNS query with the VS IP from the address group that matches the VSP first, and then the location (as the address group matched VSP has priority over the location matched VSP).

If the source IP matches one VSP's address group or location, GSLB will respond to the DNS query with the VS IP from that VSP.

If the source IP matches no VSP's address group or location, GSLB will respond to the DNS query by weight for all VSP.

What if the DNS query source IP matches multiple Virtual Server Pool's address group?

GSLB will respond to the DNS query with the first matched VSP when multiple Virtual Server Pool's address groups are matched. You can reorder the VSP if you want the second matched VSP to be used to respond.

Health check

How does the health check function of Global Server Load Balance (GSLB) work?

GSLB checks the virtual server availability of backend servers by performing health checks. It sends out various probes according to the configuration and checks the response to determine the status of the virtual server. Virtual servers that respond successfully for the configured number of times are considered healthy and its IP address will be included in the DNS response. Virtual servers that fail to respond successfully for a certain number of times are determined to be unhealthy and its IP address will be not in the DNS query results.

How long does it take to get the virtual server status after initiating a health check on a virtual server?

Normally it takes no more than 1 minute for a newly configured health check to activate. After that, the time needed to get the result of the virtual server status is dependant on the health check configuration details including “Interval”, “Timeout”, “Up Retry” and “Down Retry”. For example, if the “Down Retry” value is 2 and the “Interval” value is 5 and the virtual server fails to respond, it will take about 10 seconds for the virtual server status to update to the down status. It will take about 0 to 5 seconds for the system to process the status so after the configuration is active, it will take about 15 seconds to get the virtual server status back.

Why are there default health checks?

The default health checks are configured for general usage and best practice. In the majority of cases, the default health checks can satisfy the user's need and additional health check are not needed.

Why is the health check result healthy even though the server is down?

There are several possibilities for this. If the health check is newly applied to the virtual server, it needs some time to activate and wait for the probe response before it can change the virtual server's status to down. If the number of active health checks exceeds the license limit, some of the health checks will stop probing.

Why is the health check result unhealthy even though the server is running normally?

The best way to find out why the health check is down is by capturing packages. In most of cases, the health check is down because there is no response to the probe packages. If there are return packages for DNS, HTTP and HTTPS health checks, you will need to check whether the content of the response is consistent with the configuration. For example, for the DNS health check, you will need to check whether the returned host IP address is same with the configuration.

How can I shorten the health check time and show the latest status more quickly?

There are four default health checks with parameter: interval 30, timeout 10, 1 time up retry, and 3 times down retry. These defaults cannot be changed. However, users can self-define health checks with shorter interval/timeout and retry times to decrease the health check time and see the status change quickly.

Does GSLB support IPv6 for health check?

No. GSLB does not currently support IPv6 type health check.

One-click GSLB

Some of my FortiADC virtual servers are not synced to GSLB. Why is this happening?

This may be due to a network issue. Disable/enable GSLB on FortiADC to make FortiADC attempt to do a full sync again. The full sync can be only performed once every 10 minutes. That means if the full sync fails, you will not be able to try again for 10 minutes. If you disable/enable the GSLB on FortiADC multiple times within 10 minutes, only one full sync will be performed.

Why is my FortiADC showing "Connecting URL Error"?

First, make sure your URL is typed correctly. Second, try to ping the URL from your FortiADC and check your FortiADC DNS server setting. Third, check the FortiADC license connected to the FortiCare account. Lastly, log into your GSLB with that account and verify that you have the correct license. Then disable/enable the GSLB on FortiADC.

How long does it take for FortiADC to do a full configure sync with GSLB?

It depends on the number of virtual servers you have enabled GSLB on your FortiADC device and the number of GSLB The more there is to configure, the longer it will take. Generally the process will take less than 10 minutes.

What should I set for the interval?

The interval value is used by FortiADC to update virtual servers' status and statistics to GSLB. The default setting is 15, which should fit in most cases. The general idea is that the more virtual servers you have, the bigger interval you should set. For more than 500 virtual servers, 30 is an adequate number.

How long does it take for my DNS to reflect the changes in virtual server status and statistics?

It depends on the interval you set. It usually does not take longer than the time interval + 10 seconds.

How long does it take for my DNS to reflect the changes in my virtual server configurations?

It depends on the FQDN and Zone configuration you have for the account on GSLB. Usually it should take no more than 1 minute.

What should I do if the status of GSLB on FortiADC displays 'Connected' but I can't get the DNS to respond?

First, check if your virtual servers are fully synced with GSLB. Search for the virtual server in the GSLB related server. If it is not there, then try to do the full sync again on FortiADC, and check your system event log on FortiADC. Second, check if the related GSLB service was automatically created. Search for the virtual server-related GSLB service by the virtual server's host name and domain name. If it is not there, then try to do the full sync again on FortiADC, and check your system event log on FortiADC.

DevOps

What are the source IP addresses from FortiAppSec Cloud GSLB?

Please allow access to your application from the host “sourceaddress.fortigslb.com” if you have health checks or Fortigate connectors configured.

Note: The IP Addresses under this host are subject to change. You can get the latest IP addresses using the dig/nslookup tool. For example:

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @8.8.8.8 sourceaddress.fortigslb.com.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48970
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;sourceaddress.fortigslb.com. IN A

;; ANSWER SECTION:
sourceaddress.fortigslb.com. 300 IN A 44.241.230.143
sourceaddress.fortigslb.com. 300 IN A 35.87.69.12
sourceaddress.fortigslb.com. 300 IN A 35.163.2.213
sourceaddress.fortigslb.com. 300 IN A 44.231.37.61
sourceaddress.fortigslb.com. 300 IN A 35.86.186.71
sourceaddress.fortigslb.com. 300 IN A 18.236.97.38
sourceaddress.fortigslb.com. 300 IN A 18.195.172.168
sourceaddress.fortigslb.com. 300 IN A 52.77.144.83

;; Query time: 324 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Apr 30 00:11:06 UTC 2025
;; MSG SIZE rcvd: 152
```

Synthetic testing

Why is the HTTP health check result unhealthy even though I can get HTTP responses from the application?

There are many possible reasons why the HTTP health check result is unhealthy. In most cases, the health check is unhealthy because the HTTP health check configuration is not consistent with the HTTP request or response. The HTTP health check by default uses HTTP GET method (i.e. No Connection). For this kind of HTTP health check, you will need to check whether below configurations are consistent with the HTTP request and response:

1. The “Sending String” field contains the correct url that matches the request url
2. If you use the “HTTP HEAD” method, the health check is successful if the status code returned in response matches the code in “Status Code” field. Therefore, you will need to check whether the code in “Status Code” is expected. Typically, you use status code 200 (OK). Other status codes indicate errors.
3. If you use the “HTTP Get” method, the health check result is determined by the “Match Type” option and its associated fields “Receive String” and/or “Status Code”.

a. In the case of “Match String” option, the health check is successful if the string specified “Receive String” can be found in the HTTP response. So you will need to check whether the string specified in “Receive String” exists in the response returned by application.
b. In the case of “Match Status” option, the health check is successful if the status code returned in response matches the code in “Status Code” field. Therefore, you will need to check whether the code in “Status Code” is correct.
c. If “Match all” option is chosen, the health check is successful when the status code matches the “Status Code” field, while the string specified “Receive String” can be found in the HTTP response. Thus you will need to check both of the fields are consistent with response.

Why is the DNS health check result unhealthy even though I can get DNS responses from the application?

If the DNS reply is as expected while the health check is unhealthy, in many cases, it is due to the misconfiguration on DNS health check. You will need to check whether the “Domain Name” in DNS health check is correct, and the IP address in “Host address” field matches the host IP address returned in DNS response.

Miscellaneous

This section answers frequently asked questions about GSLB that are not covered in other FAQ topics.

How do you switch accounts for One-Click devices?

1. Disable the **GSLB** function on the One-Click device.
2. Log into FortiAppSec Cloud and navigate to **GSLB > Service > FQDN**.
3. Delete the GSLB FQDNs that were generated by this One-Click device.
4. Upload the license for the One-Click device that belongs to the new account. Check the One-Click device's license to confirm that the account information has changed.
5. Enable the one-click device GSLB function, and wait for the information to sync to the new account.

How do you move one domain from one account to another?

To move the domain example.com from account A to account B, do the following:

1. Delete the example.com domain in account A
2. Log out of account A and log into account B
3. Create the example.com domain in account B

Note: To prevent duplicate domains, you will not be able to create the domain directly in account B without deleting it from account A.

How does FortiADC HA cluster work with GSLB?

Only the config source role in your HA cluster will sync the virtual server configuration and status to GSLB. You will see the connectivity status on the GSLB page for your config source device and the message "Please Check HA Configure Primary Server" on your other device. When your config source device is turned down and your other device takes the config source role, then the new config source device will sync the virtual server configuration and status to GSLB. You will see the cloud status changed to "connected" and the assigned DNS server IP in this device. Your old config source device will show the status as "OFFLINE" on GSLB portal server page. As long as your cluster config source device is connected with GSLB, the DNS request should be answered correctly.

Threat Analytics FAQ

This section answers frequently asked questions about Threat Analytics.

- Onboarding on page 488
- Log Management on page 489

Onboarding

This section answers frequently asked questions about the Threat Analytics onboarding process.

Where is the onboarding process for Threat Analytics?

The WAF and Threat Analytics services share an onboarding process. For details on WAF onboarding, please refer to Onboard WAF applications on page 65

Log Management

How long are the logs kept in FortiAppSec Cloud?

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

Please refer to the table under Retention and Periodic clean on page 125for full retention information on each type of log.

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".

For more information, please refer to Sequence of scans on page 247.

Why is there no attack log while the request is blocked?

If the action of a corresponding security feature is configured as "Deny (no log)", FortiAppSec Cloud will actively deny the request and prevent it from proceeding further, but it will not generate a log entry specifically for that blocked request.

If you need to have detailed logs for auditing or analysis purposes, you may consider using a different action, such as "Deny" or "Block Period", which will not only block the request but also generate a log entry.

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 FortiAppSec 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 FortiAppSec Cloud's IP rather than the client real IP even if X-Forwarded-For related options are enabled?

Logs are sent from FortiAppSec Cloud to the origin server, so the `IP:` header (layer 3) of the logs is supposed to be FortiAppSec 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 FortiAppSec 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 Threat View ; 3) Blocked Requests widget on Dashboard. The ways they count the blocked requests are slightly different.

- To prevent Information Leakage, FortiAppSec 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 Threat View 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 FortiAppSec 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 Threat View , 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 do some signatures have actions that differ from the default action of their associated attack module?

The signature database is updated twice a month—on the 15th and 31st. You can refer to the FortiGuard Web Security Services page for the latest updates.

By default, new signatures are set to Alert mode and cannot be modified. Any customizations related to known attack handling will not apply to newly released signatures until the following database update.

For example, if signature 8888888 is released on March 15, it will remain in Alert mode from March 15 to March 31. Any changes for known attack detection will only take effect after April 1, during the next update cycle.

Migration

This section covers the most frequently asked questions regarding migration from legacy services FortiWeb Cloud, FortiGSLB, and FortiGuard ABP. For information on key updates and contract change information, please see Migrating from preceding Fortinet services on page 493.

- General Information on page 491
- API transition on page 491
- Legacy Contract Management on page 491

General Information

What happens to the existing portal? Where do new/existing customers login?

At launch, all pre-existing and new customers will use FortiAppSec Cloud. The old FortiWeb Cloud/ FortiGSLB/ FortiGuard ABP portals will be deactivated, and their domains will redirect to FortiAppSec Cloud

API transition

Can I access the FortiAppSec Cloud portal via API?

Yes, API access is available. For configuration details, please see the API documentation.

Is the API for FortiAppSec Cloud different from the legacy service API?

Yes, the API for FortiAppSec Cloud introduces some changes compared to the legacy APIs for WAF (previously FortiWeb Cloud) and GSLB (previously FortiGSLB). However, the primary update is in the **API paths**, while other changes are minimal.

Key differences:

- **New Endpoint**: The API endpoint has been updated to api.appsec.fortinet.com.
- **Path Updates**: The structure of API paths has been revised, making it necessary to adjust API calls accordingly.
- **Minor Adjustments**: Other changes, such as parameters and properties, are minimal and should not require significant rework.

For a detailed list of path changes and migration steps, refer to the FortiAppSec Cloud RESTful API Reference - Changes Section.

Legacy Contract Management

How do I transfer a legacy FortiWeb Cloud license to a FortiAppSec Cloud license?

Purchase your new FortiAppSec Cloud contract, ensuring it is registered under the same FortiCloud/FortiCare account as your existing FortiWeb Cloud account.

To switch between license types:

1. Log in to the FortiAppSec Cloud web management console.
2. Navigate to **General > Contracts**.
3. Select the desired license type you wish to activate, and follow the on-screen prompts to confirm the switch.

Please note, only one contract can be active at one time.

Once you switch from a legacy contract, reverting back is only possible by submitting a support ticket.

What features are included in my Legacy Contract?

Legacy Contracts continue to provide the features included before the launch of FortiAppSec Cloud. However, while these existing functionalities remain available, access to new features and enhancements introduced in the FortiAppSec Cloud system is not guaranteed under Legacy Contracts.

To ensure access to the latest features, consider transitioning to a FortiAppSec Cloud contract. For more information, please contact Fortinet Sales.

Why is my contract status displayed as Legacy?

Your contract displays as **Legacy** if it uses an older license type that predates FortiAppSec Cloud, such as one inherited from the previous FortiWeb Cloud, FortiGSLB, or FortiGuard ABP. This indicates that the contract is based on the older system and may not support all the features available in FortiAppSec Cloud Contracts.

Can a contract with Legacy status be converted to a FortiAppSec Cloud Contract?

No, Legacy contracts cannot be directly converted to FortiAppSec Cloud Contracts. If you wish to transition to a FortiAppSec Cloud Contract, please contact Fortinet Sales.

Can Legacy contracts be modified to add websites or increase bandwidth?

Yes, you can modify existing legacy contracts by adding more websites or increasing bandwidth. However, extending the contract duration is not supported.

Upon the expiration of a legacy contract, customers are required to transition to FortiAppSec Cloud contracts. To ensure a seamless transition, we recommend reviewing the available FortiAppSec Cloud contract options in advance. For more details or assistance, please contact Fortinet Sales.

Will legacy FortiFlex entitlements work after the FortiAppSec Cloud launch?

Yes, existing entitlements will work. However, once FortiFlex support is launched, new entitlements will only be FortiAppSec Cloud entitlements.

What should I do if my Legacy Contract is about to expire?

If your Legacy Contract is approaching its expiry date, we recommend purchasing a new FortiAppSec Cloud Contract to ensure uninterrupted service.

Please contact Fortinet Sales to initiate the purchase of a FortiAppSec Cloud Contract.

What happens to my existing services when switching from a Legacy Contract?

- **If you purchase a FortiAppSec Cloud Advanced Contract:** Your existing services will not be affected.
- **If you purchase a FortiAppSec Cloud Standard Contract:** Only the features supported by the Standard plan will remain available. Features that were supported exclusively under the Advanced plan will no longer be available.

Ensure that the contract you choose aligns with your service requirements to avoid any unintended service disruptions.

How do I migrate a FortiAppSec subscription from a public cloud marketplace (eg. AWS Marketplace, Azure Marketplace, Google Cloud Marketplace) to a Fortinet contract?

To migrate your FortiAppSec subscription from a public cloud marketplace to a Fortinet contract, please follow these steps:

1. Purchase and register a Fortinet contract.
   a. Purchase a new FortiAppSec Fortinet contract by contacting Fortinet Sales.
   b. For service continuity and correct licensing, ensure to register the new Fortinet contract under the same Fortinet (FortiCloud/FortiCare) account that you are currently using for your public cloud marketplace FortiAppSec subscription.
2. Activate the new contract in the FortiAppSec Portal.
   a. Log in to your FortiAppSec Cloud web portal.
   b. Navigate to **General > Contracts**.
   c. Find your newly registered Fortinet contract in the contract list.
   d. Click the **Activate** button next to this contract. Ensure the activation is successful.
3. Cancel the public cloud marketplace subscription.
   a. After confirming activation in the FortiAppSec Portal, log in to the cloud marketplace where you purchased the original subscription.
   b. Locate the **FortiAppSec** listing and follow the cancellation steps to prevent duplicate billing.

Migrating from preceding Fortinet services

FortiAppSec Cloud combines services from the former FortiWeb Cloud, Advanced Bot Protection, and FortiGSLB.

- FortiAppSec Cloud key updates on page 493
- Migration Changes on page 494
- Contract Migration on page 495

FortiAppSec Cloud key updates

The following features are new to FortiAppSec Cloud and were not available in previous services:

- **New Homepage:** A redesigned homepage allowing users to view the status and health of all services in one place.
- **New Domain:** The new domain for your web application protection services is now appsec.fortinet.com. Please use this new domain to access your services, as the previous domains will be retired.

WAF and Threat Analytics (previously FortiWeb Cloud)

- **Permissions Management:** The user permissions system has been upgraded, providing more flexible configuration options.

GSLB (previously FortiGSLB)

- **Topology Page:** A new page that displays the relationships between your configured objects, giving you a clearer view of your configuration flow.
- **Permissions Management:** The user permissions system has been upgraded, providing more flexible configuration options.
- **Contract Sharing Mode:** Enable Contract Sharing mode to allow all accounts within an organization to utilize the root account's contracts.

ABP (previously FortiGuard ABP)

- **FortiCloud Organization:** Integrate your ABP service with FortiCloud Organization, enabling centralized management and control of all Fortinet SaaS solutions.
- **Contract Sharing Mode:** Enable Contract Sharing mode to allow all accounts within an organization to utilize the root account's contracts.

Migration Changes

Your applications and logs will be automatically transferred to the new FortiAppSec Cloud backend; however, please make the following adjustments:

FortiWeb Cloud

- **API Change:** The API endpoint will change to api.appsec.fortinet.com, and the URL structure will be updated accordingly. If you have not already, please update your applications or API calls to use the new endpoint.
- **Terraform Changes:** Please update your Terraform modules to ensure compatibility with the new version.
- **FAZ Requirements:** Please verify that the new version meets FortiAnalyzer compatibility requirements.

FortiGSLB

- **API Change:** The API endpoint will change to api.appsec.fortinet.com, and the URL structure will be updated accordingly. If you have not already, please update your applications or API calls to use the new endpoint.
- **Complete Organization Migration:** Please complete migrating Organizations to FortiCloud before the launch date to ensure a smooth transition into the upgraded service.

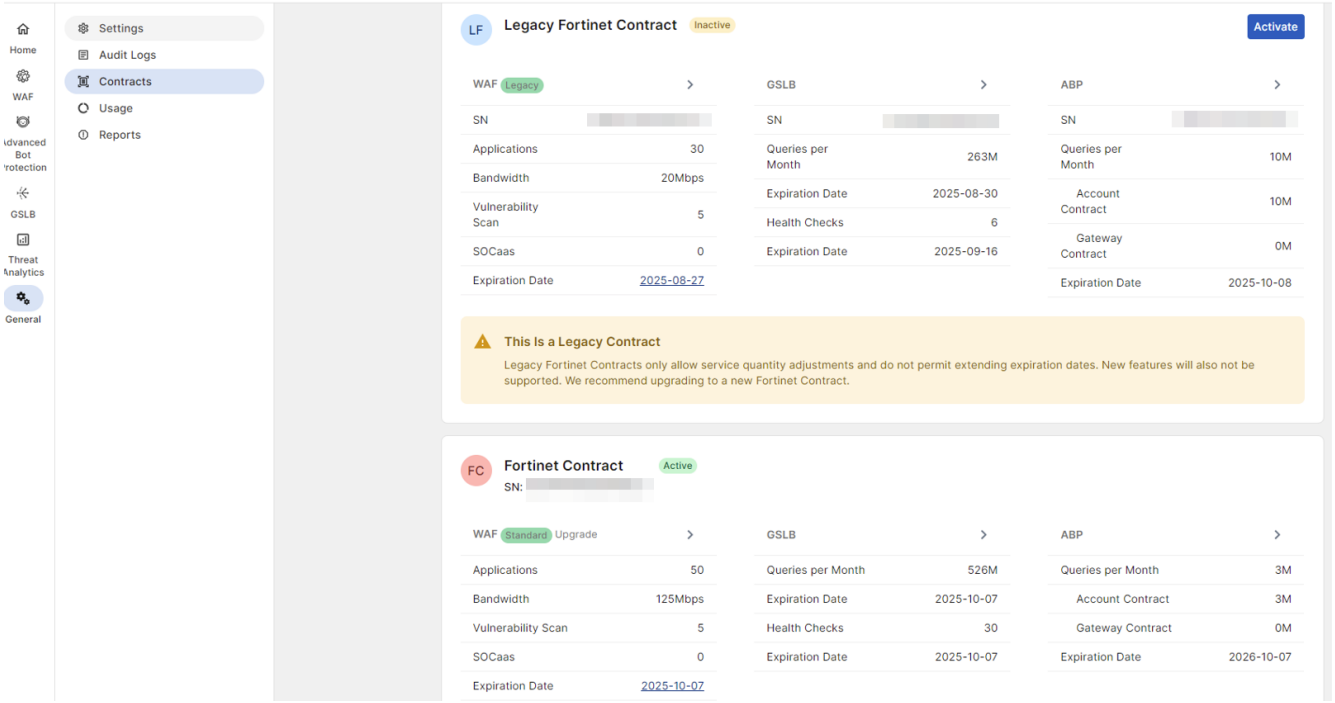
FortiGuard ABP

- **Review Permission Profiles:** After the launch, please go to the IAM portal and review the newly created permission profiles for FortiAppSec Cloud Application Security to ensure all permissions are correct and aligned with your operational needs.

Contract Migration

When FortiAppSec Cloud launched on December 1, your existing contract(s) for FortiWeb Cloud, FortiGuard Advanced Bot Protection, and FortiGSLB were transferred to FortiAppSec Cloud in the backend as **Legacy Contracts**. You can upgrade legacy contracts through co-term to add more applications or bandwidth. However, you

cannot extend their expiration date.



Upgrading to a FortiAppSec Cloud contract

1. Purchase a FortiAppSec Cloud contract. Depending on your license requirements and billing preferences, you could do this through via FortiFlex, Public Cloud Marketplace, or Fortinet Sales.

   For service continuity and correct licensing, ensure to register the new FortiAppSec Cloud contract under the same Fortinet (FortiCloud/FortiCare) account as your existing legacy service.
2. After purchasing the new contract, please log into your FortiAppSec Cloud portal and navigate to **General > Contracts**.

   Only one contract can be active at a time. Before activating your new contract, your legacy contract will remain active.
3. Click **Activate** in the new contract to activate it.

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.