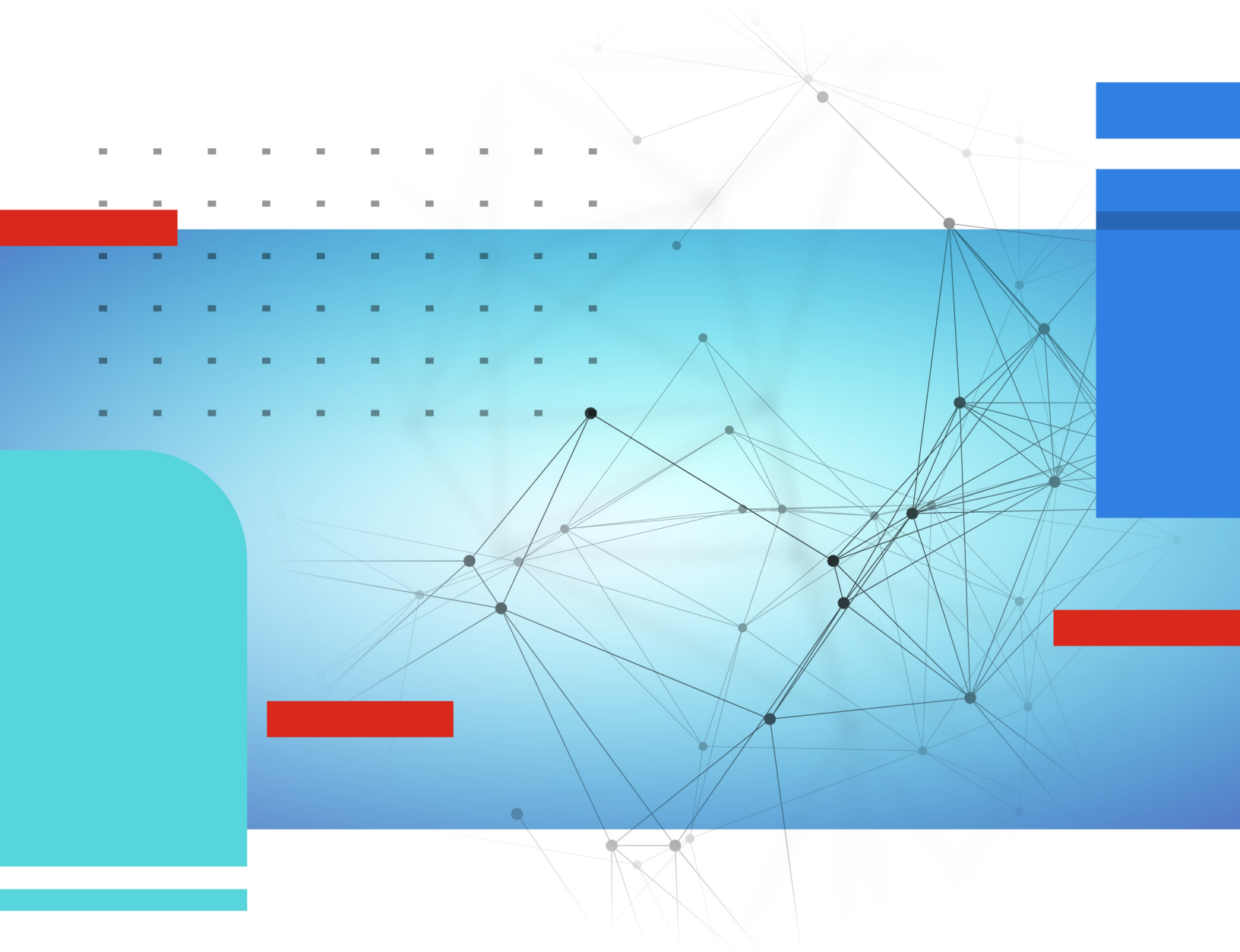
Release Notes

FortiAppSec Cloud 25.3.b



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

September 26, 2025
FortiAppSec Cloud 25.3.b Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
September 26, 2025	Initial release.

Introduction

This document provides a list of new features and changes, and product integration support information for FortiAppSec Cloud 25.3.b. Please review all sections of this document before using this service.

FortiAppSec Cloud is an advanced SaaS based, cloud-native Web Application and API Protection (WAAP) platform designed to defend web applications and APIs from modern cyber threats. It delivers a unified security framework that combines cutting-edge threat intelligence, AI-driven detection, and automated response capabilities, ensuring comprehensive protection against evolving attack vectors.

- **Web Application Firewall (WAF)**
  Protects web and API applications from OWASP Top 10 threats, zero-day vulnerabilities, and sophisticated Layer 7 attacks with adaptive security policies and real-time threat intelligence.
- **DDoS**
  Mitigates network and application layer attacks, featuring real-time customizations, automation, and a 24/7 SOC.
- **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.
- **Vulnerability Scan**
  Provides automated, continuous scanning of web applications protected by FortiAppSec to detect known security weaknesses (including OWASP Top 10), misconfigurations, and exposed components.

What's new

FortiAppSec Cloud 25.3.b offers the following new features:

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 Actions icon for the 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.

Product integration and supported web browsers

This section lists the product integrations and web browsers supported by FortiAppSec Cloud 25.3.b.

Supported products for ABP Integration:

Product	Tested Versions
FortiWeb	FortiWeb 7.4.9 and later versions
FortiADC	FortiADC 7.4.6 and later versions

Supported web browsers:

- Mozilla Firefox 59 and later versions
- Google Chrome 65 and later versions

We strongly recommend you set either of the web browsers as your default web browser when working with FortiAppSec Cloud. You may also use other (versions of the) browsers, but you may encounter certain issues with FortiAppSec Cloud's Web GUI.

Resolved issues

This release has no resolved issues. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Known issues

There are no known issues in FortiAppSec Cloud version 25.3.b. For inquiries on particular bugs, please contact Fortinet Customer Service & Support.

www.fortinet.com

Release Notes

FortiAppSec Cloud 25.3.b