



Release Notes

FortiAppSec Cloud 26.1



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

February 1, 2026

FortiAppSec Cloud 26.1 Release Notes

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new	6
WAF	6
Advanced Bot Protection	6
Product integration and supported web browsers	7
Resolved issues	8
	9
Known issues	10

Change Log

Date	Change Description
February 1, 2026	Initial release.

Introduction

This document provides a list of new features and changes, and product integration support information for FortiAppSec Cloud 26.1. 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 26.1 offers the following new features:

WAF

Custom file type support for File Protection

You can now define and manage custom file types for File Protection under **WAF > Security Rules > File Protection**.

For more information, refer to [File Protection](#).

Header exception support for Known Attacks

Known Attacks now supports configuring HTTP header name and value settings within **Exception Rules**.

For more information, refer to [Known Attacks](#).

CSV upload support for Geo IP Exceptions

The Geo IP Exception feature now supports uploading a CSV file, in addition to manually entering IP addresses and IP ranges.

For more information, refer to [IP Protection](#).

HTTP Request Constraints Update

Additional request limits have been added to bolster HTTP conformance and protocol security.

For more information, refer to [Request Limits](#).

Advanced Bot Protection

AutoDiscovery Email Notifications

You will now receive email notifications when AutoDiscovery returns no results or encounters a connection issue.

Subresource Integrity

Advanced Bot Protection scripts now include integrity JS hash values to detect and prevent unauthorized changes.

Cross-Domain Cookie Support

Different root domains in your application are now recognized as a single client, enabling you to track the same user identity across multiple domains (for example, example.com, example.de, shop.example.com).

Product integration and supported web browsers

This section lists the product integrations and web browsers supported by FortiAppSec Cloud 26.1.

Supported products for ABP Integration:

Product	Tested Versions
FortiWeb	FortiWeb 7.6.5 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 26.1. For inquiries on particular bugs, please contact [Fortinet Customer Service & Support](#).



Release Notes

FortiAppSec Cloud 26.1

