Release Notes

FortiAIGate 8.0.1

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

June 3, 2026
FortiAIGate 8.0.1 Release Notes
102-801-1295339-20260603

TABLE OF CONTENTS

Change log 4
What's new in FortiAIGate 8.0.1 5
Introduction 6
Web browser support 6
Prerequisites 6
Upgrade information 8
Resolved issues 9
Known issues 10

Change log

Date	Change Description
June 3, 2026	Initial release of FortiAIGate 8.0.1

What's new in FortiAIGate 8.0.1

Release 8.0.1 provides the following new features:

- MCP tool security scanning supports the bidirectional security scanning of MCP tool and other AI agent tools/list, tools/call, and tools/response methods for prompt injection, data leak prevention, and toxicity detection:
  - MCP tool security scanning in the Input Guard direction includes tools/list and tools/response.
  - MCP tool security scanning in the Output Guard direction includes tools/call.
- Programming languages detection enhancements support 53 programming languages for intelligent routing in AI Flows. Refer to the *FortiAIGate 8.0.1 Administration Guide* for details.
- Data leak prevention enhancements support additional data types across 6 categories and 35 PII/secret entities.

  You can now scan for personal identifiers, contact information, financial information, technical information, identification, and sensitive attributes in the DLP scanner.
- Log viewer enhancements. You can now review all traffic logs or specify a custom time range for viewing traffic logs.
- Security scanner caching. The prompt injection, data leak prevention, and toxicity detection scanners now cache previously scanned system prompts, assistant messages, and tool lists for a faster response time. These scanner caches are available with the Alert, Alert & Deny, and Redact action policies.
- Change of FortiAIGate management GUI URL. Use the `https://<IP_address>/ui` URL to access the FortiAIGate management GUI; previously, the management GUI URL was `https://<IP_address>`.

Introduction

FortiAIGate serves as the central gateway between your AI applications and major large language model (LLM) providers such as OpenAI, Anthropic, and AWS Bedrock. Positioned at the core of your AI infrastructure, it enables organizations to deliver AI services efficiently while maintaining strict security controls over all LLM interactions.

FortiAIGate provides two primary capabilities:

- AI Flow handles intelligent AI application delivery, routing requests based on content and ensuring that traffic is processed securely and efficiently.
- AI Guard delivers comprehensive security aligned with the Open Worldwide Application Security Project (OWASP) LLM Top 10, offering protections such as prompt injection detection, data leak prevention, toxicity detection, and support for customizable security rules tailored to specific needs.

FortiAIGate includes a fully featured graphical interface that simplifies configuration and management. Administrators can easily set up AI Flow routing policies, define AI Guard security rules, and monitor real-time system activity. Detailed traffic logs and a visual dashboard provide full visibility into all AI-related requests passing through the system.

Built for modern environments, FortiAIGate runs as a containerized solution on Kubernetes, allowing the seamless deployment across public clouds, private clouds, or on-premise clusters. Its cloud-native architecture ensures scalability, portability, and operational consistency across diverse infrastructures.

This document provides the following information for FortiAIGate 8.0.1 build 0031.

Web browser support

Web browser	• Google Chrome 111 and later • Microsoft Edge 111 and later • Mozilla Firefox 111 and later • Apple Safari 16.4 and later Other browser versions have not been tested but might fully function. Other web browsers might function correctly but are not supported by Fortinet.

Prerequisites

The following are the minimum and recommended Kubernetes worker node resources allocated for all FortiAIGate containers.

Component	Minimum configuration	Recommended configuration
vCPUs	4 cores	24 cores

Component	Minimum configuration	Recommended configuration
RAM	25 GB	70 GB
GPU	1 x GPU with 24 GB VRAM (for example, NVIDIA L4)	2 x GPUs with 24 GB VRAM each
Local storage	1x 250 GB NVMe SSD	
Kubernetes cluster RBAC requirements	The deployment requires only minimal namespace-scoped permissions within the `fortiaigate` namespace.	

Ensure that you have the following components before deployment:

- **Kubernetes 1.25.0 or later**–linux/amd64 or linux/arm64
- **CNI Plugin**–The Container Network Interface plugin must be installed and configured.
  - Common options: Calico, Flannel, Weave Net, and Cilium
  - Must support pod-to-pod communication
- **kubectl**–Ensure that your client can access the Kubernetes API server.
  - kubectl documentation
- **Helm 3.10.0 or later**
  - Helm installation guide
- Container registry ready and accessible
- Ingress controller deployed
- Optional: GPU nodes (if the GPU mode is required)
  - The supported GPU models include NVIDIA L4, NVIDIA A10, and NVIDIA A100.

Upgrade information

FortiAIGate 8.0.1 supports upgrading from FortiAIGate 8.0.0.

In FortiAIGate 8.0.1, the data types of personally identifiable information (PII) that the data leak prevention (DLP) scanner examines have changed. AI Guards created in FortiAIGate 8.0.0 that use the DLP scanner will have their PII data types converted to the new data types. If no corresponding new data type exists, the PII type will be dropped. See the following table for how the PII data types are converted.

8.0.0 PII categories	8.0.0 PII types	8.0.1 PII data types
General	'DATE_TIME'	none
	'IP_ADDRESS'	‘ipv4’
	'LOCATION'	‘city’, ‘state’, ‘postcode’, ‘country’, ‘county’, street_address’
Global Finance	'URL'	none
	'IBAN_CODE'	‘account_number’
National IDs	'US_PASSPORT'	‘national_id’
	'US_ITIN'	‘tax_id’
	'US_SSN'	‘ssn’
	'US_BANK_NUMBER'	‘account_number’
Personal Information	'EMAIL_ADDRESS'	‘email’
	'MEDICAL_LICENSE'	'medical_record_number', 'health_plan_beneficiary_number'
	'CREDIT_CARD'	'credit_debit_card'

Resolved issues

The following issues have been fixed in FortiAIGate 8.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1213070	The AI Flow *Path* configuration currently only supports paths starting with `/v1/`; otherwise, the system returns 404.
1245419	FortiAIGate does not support streaming traffic when connecting to an HTTPS backend using a self-signed certificate.
1250163	When you upgrade FortiAIGate with a new license, the license status does not update immediately because the license managers checks the FortiGuard Distribution Network at a fixed interval of 15 minutes.
1261680	The license manager fails to start, then restarts several times, and stops working.
1263044	The value for the *Custom Rule Header* in the Input Guard should be case insensitive.
1265290	With an active session, users are not automatically redirected from the login page to the dashboard, even though it remains accessible using the direct URL
1270303	When the backend LLM provider is set to OpenAI with the gpt-5.3-codex model, using the Codex Agent returns an error message.

Known issues

The following known issues have been identified with FortiAIGate 8.0.1. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
1242983	When using Open WebUI as the AI client, FortiGateAI blocks Open WebUI's OPTIONS requests to the LLM server.
1254357	The event log does not include license-related information.
1289168	AWS Bedrock fails when using the Response API with the nvidia.nemotron-nano-12b-v2 model.
1293783	When sending prompts to FortiAIGate through Codex, <timezone> is automatically attached to the user input inside of the <environment_context>. This will trigger the data leak prevention scanner if the country/city category is enabled.
1293870	The FortiAIGate log drops the OpenAI built-in tool identity (web_search).
1297921	If you create a custom rule that has multiple selectors (such as A AND B OR C) and you try to delete the first selector (A), you will get an error when trying to save. **Workaround:** Delete the entire rule and make a new one again.
1298170	• The Cline AI agent bypasses the input guard scanner blocks. • The output guard custom rule scanner cannot scan Azure/Anthropic responses because the Cline AI agent wraps the responses inside of attempt_completion tool calls.
1298581	When the FortiAIGate AI Guard blocks a Codex request or response, Codex correctly stops processing and does not retry. However the FortiAIGate block message is not displayed to the user.
1298605	When Codex sends requests through FortiAIGate to an Anthropic provider, the request fails with 400 Bad Request.
1299004	Opening the *Logs* page in the Web UI becomes progressively slower and degrades sharply as the selected time window widens.

www.fortinet.com