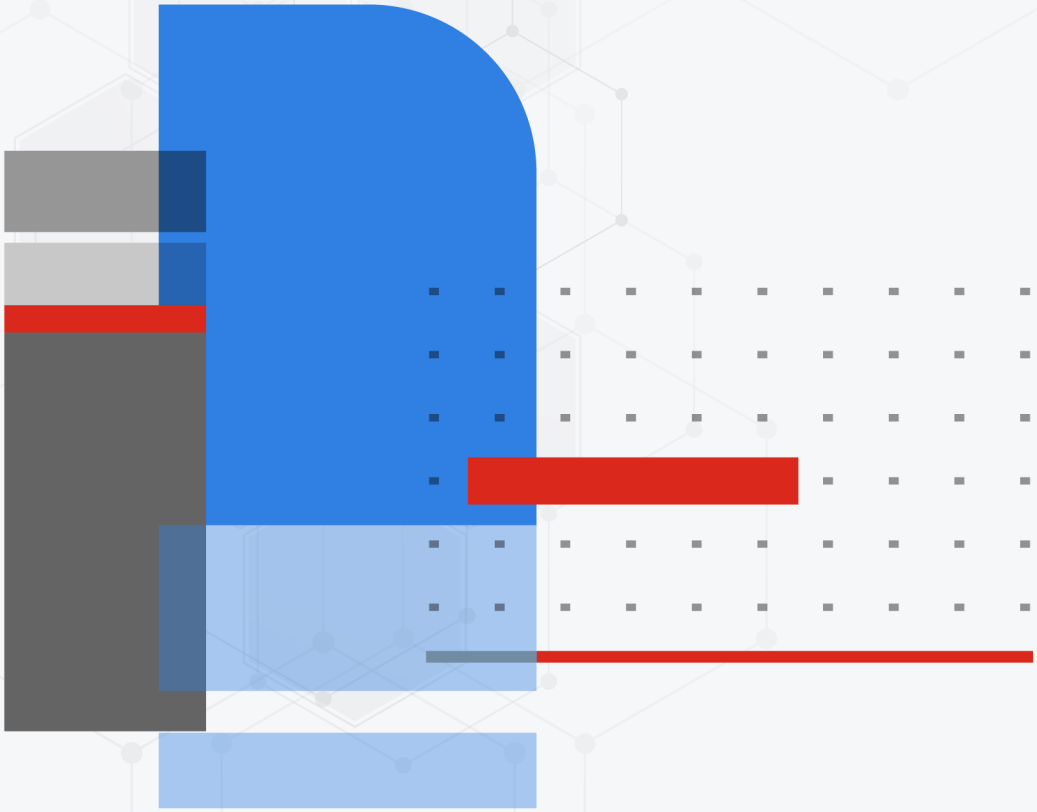
Release Notes

FortiEdge Cloud 25.3



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

Oct 21, 2025
FortiEdge Cloud 25.3 Release Notes
53-253-1200229-20251021

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-10	FortiEdge Cloud 25.3 release version.
2025-09-16	Added 1048G to Supported Devices (New Features).
2025-10-21	Added 3032G to Supported Devices (New Features).

About This Release

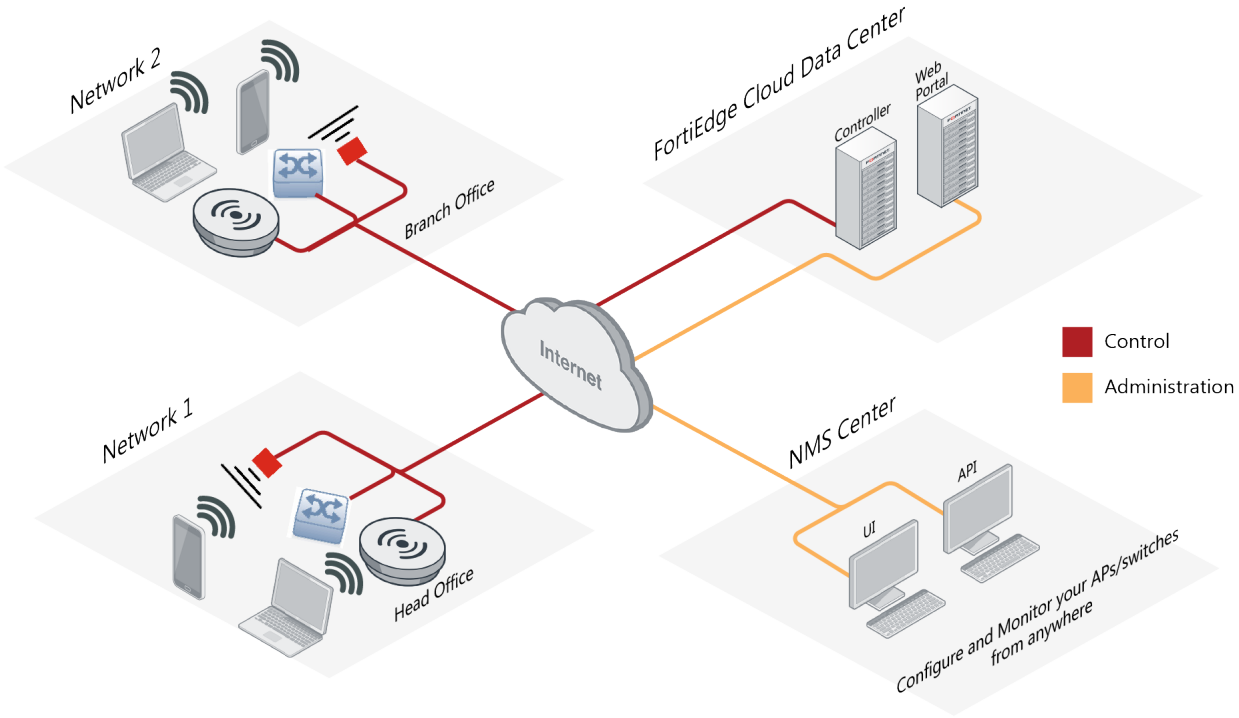
This release delivers key new features and resolves some outstanding product issues. For more information, see New Features and Resolved issues.

FortiEdge Cloud will no longer support multi-tenancy license extensions after December 31, 2026. Any multi-tenancy license extended will have its expiration date set to December 31, 2026, regardless of the start date.

If you currently use multi-tenancy feature, you must now transition to use the *FortiCloud Organization* feature for managing multiple entities within FortiEdge Cloud. See FortiCloud Organization.

What is FortiEdge Cloud

FortiEdge Cloud is a unified management platform for standalone FortiAP, FortiSwitch, and FortiExtender deployments. It provides configuration management and monitoring control for a handful of devices and can scale up to thousands of devices across multiple sites.



This document provides a list of new features, product integration information, resolved issues, and known issues for FortiEdge Cloud version 25.3. Review all sections of this document before you use this service.

Product integration and support

The following table lists supported web browsers for FortiEdge Cloud version 25.3. Other web browsers may work correctly but Fortinet does not support them.

Item	Supported version
Windows OS	• Microsoft Edge version - 128.0.2739.67 • Mozilla Firefox version - 130.0 • Google Chrome version - 128.0.6613.120
MacOS	• Apple Safari version - 17.6

The following table lists FortiEdge Cloud language support information. Language settings are determined by region.

Language	GUI	Documentation
English	x	x
Japanese	x	—
Spanish	x	—
Portuguese	x	—

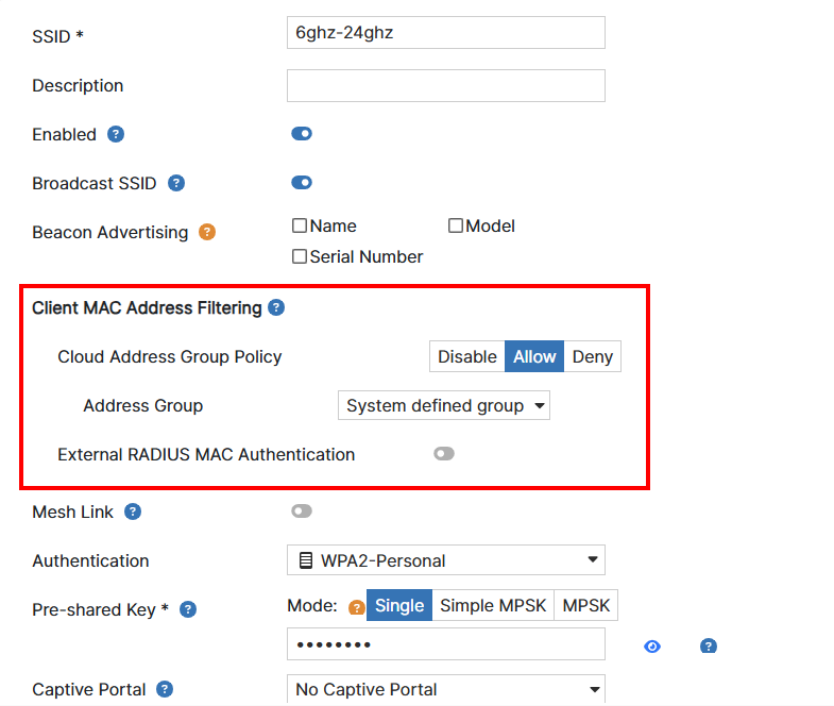
New Features

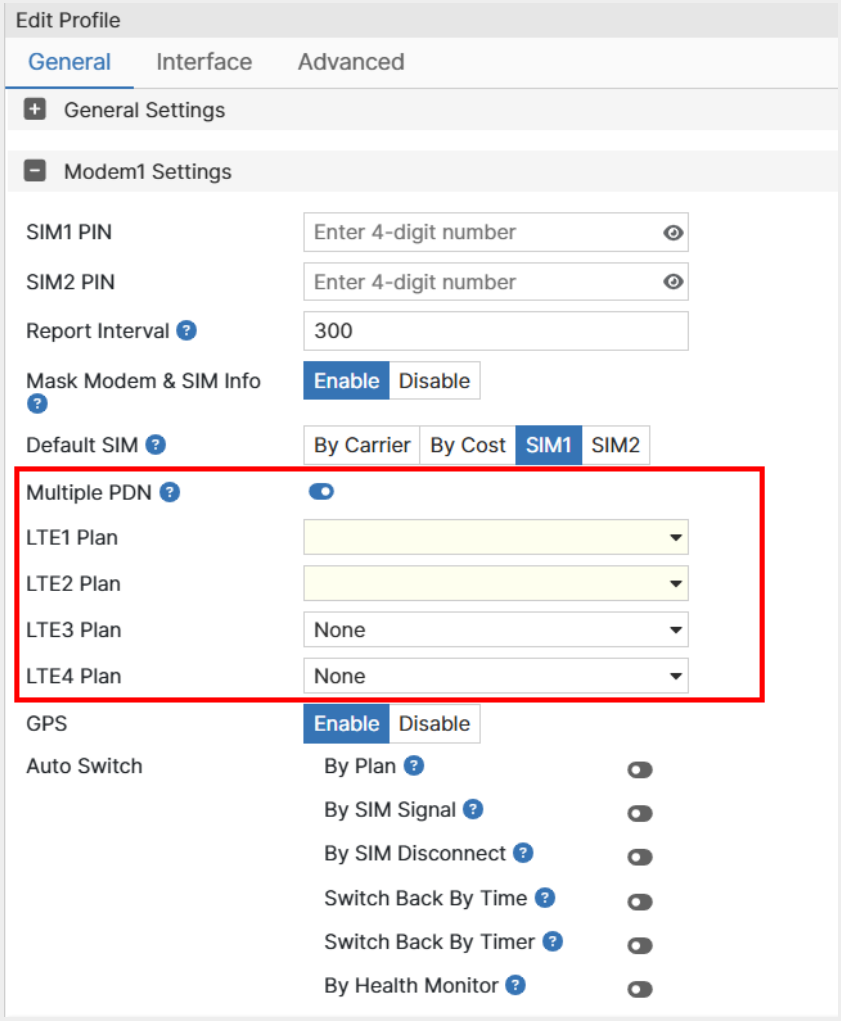
FortiEdge Cloud 25.3 delivers the following features/enhancements to FortiEdge Cloud. For more information, see FortiEdge Cloud 25.3 New Features document.

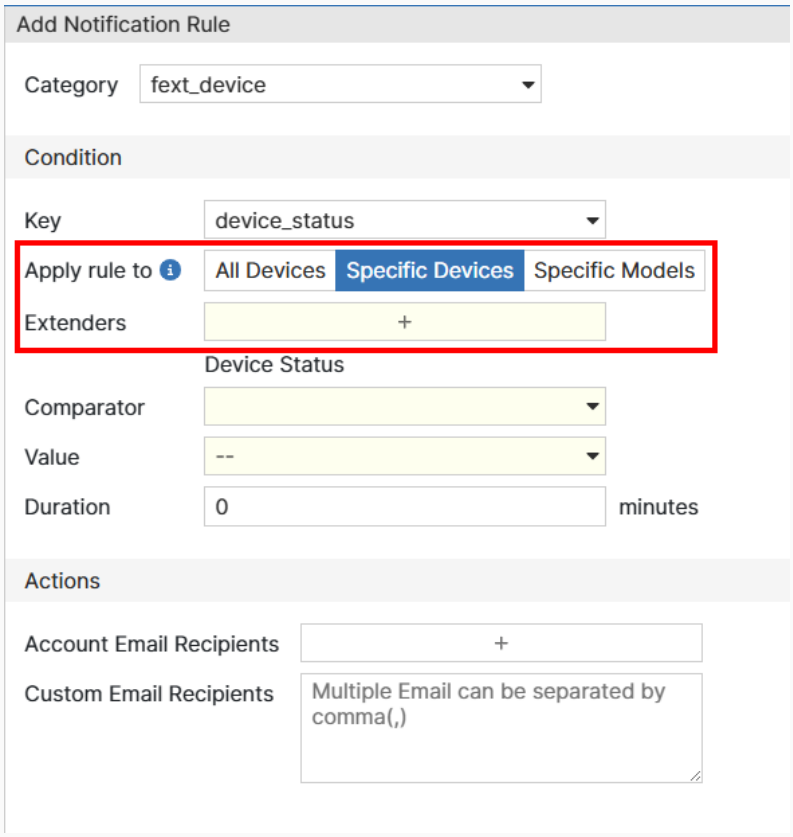
Feature	Description

Device Support	This release of FortiEdge Cloud now supports the following devices:
	• **FortiExtender**
	  • FER-511G
	  • FEV-511G
	• **FortiSwitch**
	  • 2048F-B2F
	  • 1048G
	  • 3032G

Wi-Fi Client MAC Filtering Improvements	In this release, MAC filtering is enhanced by adding a deny list option. The **Cloud Address Group Policy** field now has three settings to provide more control over network access: • **Disable**: Bypasses MAC address authentication for the listed addresses. • **Allow**: The **MAC Access Control** list works as a whitelist, only allowing the listed MAC addresses to connect. • **Deny**: The **MAC Access Control** list now works as a blacklist, blocking access for the listed addresses while allowing all others to connect. This new deny list option gives you more flexibility to manage network access, whether you need to restrict specific devices or allow only certain ones. Configure the allowed list of MAC addresses that can connect to an SSID in the **MAC Access Control** list (**Wireless** > **User Access Control** > **MAC Access Control**) and add or edit an SSID in the **Wireless** > **SSID** window. Navigate to the **Client MAC Address Filtering** section:

Feature	Description
	 **Note**: • When **Cloud Address Group Policy** is enabled, MAC address is validated in **MAC Access Control** list. • We can select either **External RADIUS MAC Authentication** or **Cloud Address Group Policy**, not both. When **External RADIUS MAC Authentication** is chosen, AP acts as authenticator and when **Cloud Address Group Policy** is chosen, cloud acts as authenticator.
Multiple PDN Support for FortiExtender (FEX- 511G and FEX-511G-WiFi)	FortiEdge Cloud is now enhanced to support multiple PDN (Packet Data Network) for your devices. **Note**: This feature only works when a single SIM card is in the FortiExtender. **Extender Profile Settings** FortiExtender 511G profiles now have a **Multiple PDN** option under **Modem Settings**, allowing you to select up to four LTE interface plans. The first two plans are mandatory, and you can add two more. You can reuse the same carrier plans across different interfaces, but only plans already configured under **Carrier Plan Settings** are available for selection. Once a carrier plan is used in a **Multiple PDN** configuration, it cannot be removed from the profile.

Feature	Description
	 **Extender Device Configurations Settings** The **LTE Settings Modem** for FortiExtender 511G profiles has also been updated with a **Multiple PDN** option. When you override carrier plans during device configuration, only those specific plans will be available for selection when **Multiple PDN** is enabled. Once a plan is selected for use, it cannot be deleted until its association is removed. **Note**: • A carrier plan that is being used cannot be deleted. • Add unique carrier plan/APN for Multiple PDN else Multiple PDN virtual interfaces will go down. • When configuring the carrier plans, first determine how many APNs your ISP supports. Then, attach the carrier plans according to the APN order provided by your ISP. • The **Affected Devices and Profiles** section for a carrier plan lists the

Feature	Description
	plan when used in **Multiple PDN** configuration as well.
Enhanced Device Notification Rules	With this release, you can now define notification rules with more precision. You can set up alerts for a single device, multiple devices, an entire device group, or all active devices. This gives you more granular control over when and how notifications are triggered, ensuring that alerts are highly relevant to your specific operational needs. To add notification rules to specific devices, navigate to **Extender** > **Notifications** and click **Add**.  Under **Condition** section, in the **Apply rule to** field, select one of the following options. • **All Devices**: Select to apply the notification rule to all the devices. • **Specific Devices**: Select to apply the notification rule for specific devices. Click **+** in the **Extenders** field to select the devices. • **Specific Models**: Select to apply the notification rule for specific models. Click **+** in the **Extender Models** field to select the models.

Feature	Description
API Enhancements for FortiCloud Multi-Tenancy	This release introduces new API support for FortiEdge Cloud's Multi-Tenancy feature, which is now part of FortiCloud Organization. Three new APIs are added to streamline management for API users. These APIs allow retrieval of ORG/OU structure and selecting member account. Once a member account is selected, all the subsequent REST APIs will work on the selected account. **Note**: The new APIs are available for only API Users and ORG Accounts. • `GET /api/v1/orgou/tree`: Retrieves the ORG/OU structure to get a clear view of your organization's hierarchy. • `POST /api/v1/orgou/select`: Selects a member account to choose a specific account to work with. Once an account is selected, all subsequent REST API calls will apply to that chosen account. • `GET /api/v1/orgou/selected`: Retrieves currently selected account. **Note**: Fortinet API documentation is available on FNDN at https://fndn.fortinet.net.

Resolved issues

The following issues have been resolved in FortiEdge Cloud version 25.3. For inquiries about a particular issue, visit the Fortinet Support website.

Issue ID	Description
1174695	For FortiExtender firmware versions older than 7.6.2, an incorrect cable ID is detected during OBM Scan.
1174702	When updating parameters via the API, the SSID values are populated with dummy values.
1185716	Account creation fails if the email address has more than 50 characters.
1180100	During an OBM or OBM Scan on a FortiExtender device with firmware older than 7.6.2 and only a single backend device connected, `OBM failed to start, no response from device` error message is displayed.
1188516	In the FortiExtender Cloud portal, the Carrier and Active SIM columns for a FortiExtender shows `no carrier` and `no active sim` because of a data update delay.
1172786	When trying to create a profile for a new locations the following error message is displayed: `error 400 number of network plans cannot exceed 1024 per network`.
1163720	A grace period for a license is always available for expired and active APs.
1192035	AP CLI always shows Dynamic VLAN as disabled though it is enabled with External Radius MAC.
1197661	An error occurs while provisioning the FortiExtender 511G on FortiZTP for FortiEdge Cloud, displaying the message: `Failed to provision. Error name: This field may not be null. :FXN51GS225003018`.

Known issues

The following issues have been identified in FortiEdge Cloud version 25.3. For inquiries about a particular issue, or to report an issue, visit the Fortinet Support website.

Issue ID	Description
1200714	Running the `execute debug` command on a device with a mapped wireless interface causes the debugging to fail.
1200282	After performing Swap Profile operation on a deployed FX212F device, its deployment status on the in-service page remains in `Syncing` state.
1200705	By default, a loopback IP is set as a trusted host in credential plans. If this IP is not removed, logins to the device fail.
1200704	The minimize option for the Console is not available in the Inservice and OBM Access Console views.
1200696	The FEX200F platform profile does not include port5, even though the device physically has ports 1 through 5.
1174115	Though the scheduled upgrade template was set to update the FortiAP to the latest firmware, the device does not upgrade.
1087878	After FortiSwitch deployment, some fields on the **Diagnostics** page are not updated for up to 15 minutes.
1201180	The **Scheduled Upgrade Status** page under **Monitor** menu is not presented in a graph format.

Additional Notes

Note the following while using FortiEdge Cloud.

- For swifter GUI and API responses, Fortinet recommends deploying a total of less than 2000 switches and FortiAPs in a network. Also, the number of switch ports should be less than 15000.
- The upgrade process completion takes approximately 30 minutes if you try to upgrade multiple FortiAPs (count in 3 digits or more) simultaneously.

www.fortinet.com