Managed FortiGate Service ™

Expand Your Managed Security Offering with Managed FortiGate Service

Managed FortiGate Service (MFGS) is a cloud-delivered network security solution purpose-built to help partners scale their services, bridge resource gaps, and deliver consistent, enterprise-grade protection. Designed to augment your existing capabilities, MFGS allows to retain control over customer relationships while leveraging Fortinet-backed expertise for policy management, threat monitoring, and operational support. With MFGS, you can accelerate service delivery, reduce complexity, and confidently expand your security portfolio—without overextending internal teams.

Service Offerings

Managed FortiGate Service offers expert security management—including deployment, daily operation, and optimization—for all FortiGate models. It also covers LAN Edge devices (FortiSwitch, FortiAP, FortiExtender) ensuring tailored protection for your network. See the diagram below for details.

Seamless Onboarding
Effortless onboarding for Enterprise and MSSP environments

Firmware Upgrade
Rely on MFGS experts to manage your firmware upgrades

Fast Deployment
Rapidly deploy FortiGate and LAN Edge devices following best practices

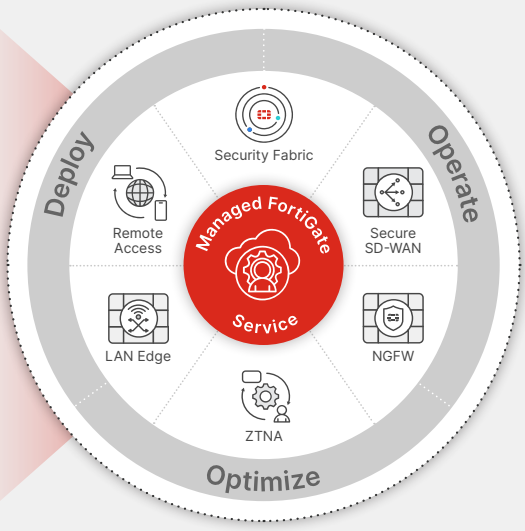
Security Posture Assessment
Uncover and fix FortiGate security gaps with expert recommendations

Active Threat Protection
Stop emerging threats with Fortinet-recommended best practices

Incident Management
Enable rapid containment of escalated SOCaaS alerts

Vulnerability Management
Identify FortiOS versions with PSIRT vulnerabilities and trigger automatic patching

Change Management Workflow
Ensure secure, transparent changes with ITIL-based processes and expert oversight



Discover all use cases and features in the Managed FortiGate Service Datasheet.

Ordering Information

Managed FortiGate Service is available for all FortiGate models, whether hardware-based or virtual, ensuring flexibility for diverse deployment environments.

You can choose from flexible subscription terms of 1, 3 or 5 years to best match your organization's needs.
Pricing is based on your specific FortiGate model and selected subscription length.

Our transparent pricing structure is composed of
- One-time setup fee: Charged in the first year only, covering initial onboarding and configuration.
- Annual service fee: Recurring each year of your subscription.

Choosing a long-term option provides savings and maximizes the value of our service.

PRODUCT	SKU	DESCRIPTION
Managed FortiGate Service	FC-10-[FortiGate Model Code]- 660-02-DD	Managed FortiGate service, available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management

If deploying FortiGate devices in a High Availability (HA) cluster, you must purchase a separate Managed FortiGate Service entitlement for each cluster member. For example, a two-unit HA cluster requires two entitlements.

Connected LAN Edge devices—such as FortiAP, FortiSwitch, and FortiExtender—are fully covered under the entitlement of their managing FortiGate. No separate service entitlement is required for these devices; they are included with your FortiGate's subscription.

For detailed service onboarding steps, please refer to the Getting started with Managed FortiGate Service.

Frequently Asked Questions

Who is this service designed for?

This service is ideal for:

Partners transitioning from Value-Added Reseller (VAR) to Managed Security Service Provider (MSSP) who need support with operational challenges.

Customers who manage their own operations but are understaffed and need assistance, especially those comfortable working directly with a vendor.

This service is not intended for customers seeking a fully managed solution with a single point of contact for all security needs (including licensing, provisioning ,and support). Such customers should be referred to a Fortinet certified partner.

Is on-site installation and cabling included in this service?

No, the service is delivered remotely only.

In which languages is the service delivered?

English only.

Does this service include network design and planning?

Network design, planning, and migration assistance are not included in this service. For these tasks, please engage Fortinet certified partners or Fortinet professional services.

What is the SLA?

The table below shows our service SLAs for Change Requests:

PRIORITY	DESCRIPTION	TARGET EVALUATION TIME	TARGET IMPLEMENTATION TIME
High	Business critical changes that must be implemented as soon as possible to avoid ificant disruption or risks.	1 hour	2 hours
Medium	Changes that are moderately urgent but do not require immediate action	4 hours	1 business day
Low	Changes that are not time sensitive and can be scheduled for implementation at a later date.	1 business day	2 business days

How long does it take to set up the service?

The team is targeting to fulfill new customer and device onboarding requests within three business days.

Which Fortinet Devices Are Supported by Managed FortiGate Service?

The service is available for FortiGates and any FortiSwitch, FortiExtender, or FortiAP devices that are connected to those.

How can I try this service before the purchase?

A trial is currently not available due to the exclusive remote management nature of this service and potential configuration changes needed to onboard FortiGates.

For more information, we recommend discussing your specific needs with your Fortinet sales representative.

If I'm already onboarded to the service as customer, how can I add additional FortiGates?

Customers already onboarded to the service can add new FortiGates by submitting a Device Onboarding service request from the Managed FortiGate Service portal.

Can customers make configuration changes to the FortiGates?

Yes, customers can make changes locally to the FortiGate as they keep local FortiGate read/write access.

This is useful for the following scenarios:

- Troubleshooting sessions with Fortinet TAC when changes must be applied instantaneously without going through the ITIL change management process.
- To implement locally use cases not yet covered by the service.

Can customers make configuration changes to the FortiManager Cloud instance used by the MFGS team to manage my FortiGates?

No, customers have read only access to the FortiManager Cloud instance, configuration changes on the FortiManager cloud instance are not allowed.

If I already have a FortiManager on-premises or a FortiManager Cloud instance, can I migrate it to MFGS?

Migrations from existing FortiManager instances, either on-premises or FortiManager Cloud are not supported. During onboarding your existing FortiManager Cloud instance will be deleted and a new Managed FortiGate Service instance will be provisioned under your FortiCloud account.

When can we expect to see support for the latest FortiGate firmware versions?

This service leverages FortiManager Cloud as a management platform, therefore only firmware images supported by FortiManager Cloud are covered. For more information on service requirements, please see the Managed FortiGate Service Getting Started Guide

Is it my responsibility to upgrade the FortiManager Cloud instance if it is impacted by a PSIRT vulnerability?

No. The Managed FortiGate Service team oversees your cloud instance, consistently implementing suitable patches and mitigation strategies to maintain your system's security and protection.

What happens to the provisioned FortiManager Cloud instance if I choose not to renew the service?

If there are no FortiGates with active entitlements, the FortiManager Cloud instance will be reset to its factory default. Data will be erased according to Fortinet Data Privacy Practices Data Sheet

How does this service integrate with FortiGuard SOCaaS?

The combination of FortiGuard SOCaaS and Managed FortiGate service provides a holistic incident management solution, according to the below workflow:

1. **Log Generation:** The customer's FortiGate device generates a log message.
2. **SOCaaS Analysis:** The SOCaaS platform receives and analyzes the log message. During this process, the log may evolve into an event or an alert, which is then escalated to customers.
3. **MFGS Added Value:** The Managed FortiGate Service (MFGS) team becomes involved at this stage. The incident is simultaneously escalated to the MFGS team, who proactively develop and propose appropriate configuration changes to contain or remediate the alert.
4. **Customer Authorization:** The customer reviews and authorizes the FortiGate configuration changes proposed by the MFGS team.
5. **Implementation**: Once approved, the MFGS team initiates the change management process to apply the authorized configuration changes to the customer's production FortiGate device.

This integrated approach ensures a seamless flow from initial log generation to containment and remediation, combining automated analysis with expert human intervention and customer oversight. To learn more about the specific SOCaaS scenarios that can be addressed using the Managed FortiGate Service, please see the SOCaaS Alert Containment/Remediation with MFGS document.

Does this service cover RMA and technical support?

Technical support (break/fix) and RMA are not covered by the Managed FortiGate Service. Customers can reach out to Fortinet TAC that will assist based on the purchased support level.

If your FortiGate device has been replaced via RMA, please submit a device onboarding request to enroll the new device into the Managed FortiGate Service.

Is this service reachable by telephone?

No, via Managed FortiGate Service portal only.

August 1, 2025 11:59 AM

MFGS-OG-R1-20250518