

Administration Guide

Managed FortiGate Service Q4, 2025



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



December 17, 2025

Managed FortiGate Service Q4, 2025 Administration Guide

81-254-889123-20251217

TABLE OF CONTENTS

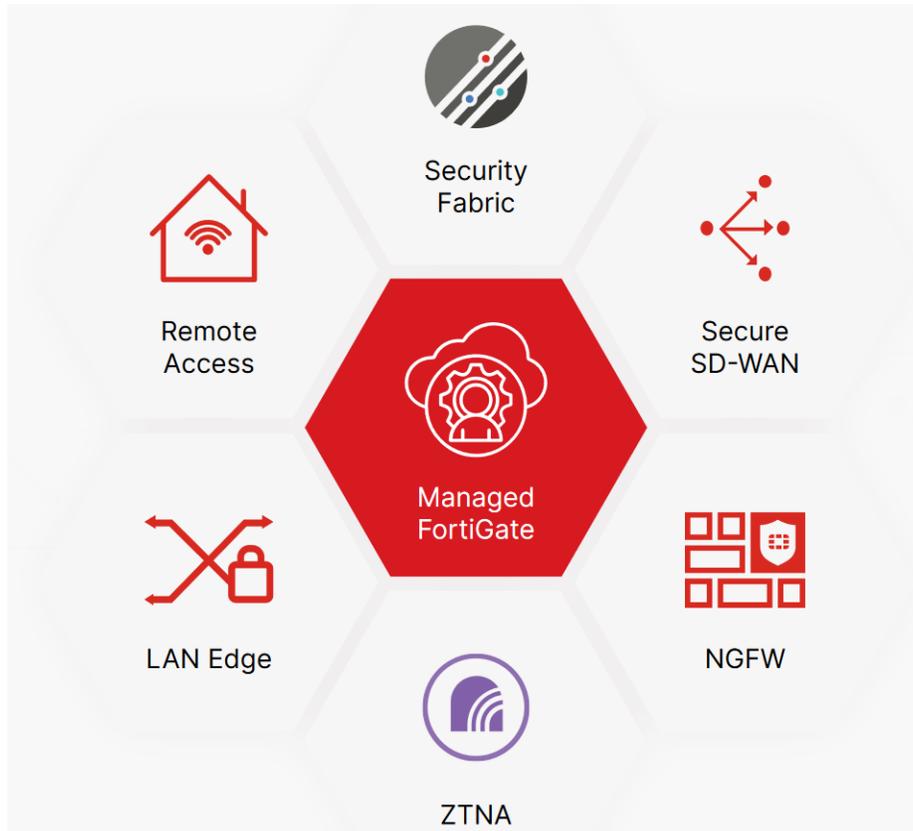
Change Log	4
Introduction	5
Onboarding to Managed FortiGate Service	6
Determine your onboarding type	7
MSSP onboarding	7
Regular customer onboarding	11
Post-onboarding request submission	14
Accessing the Managed FortiGate Service portal	15
Portal customization	15
Pending Service Request popup window	16
Dashboard	17
Service Requests	19
Service request type	19
Service request status	20
Creating service requests	22
Device Onboarding	23
My Assets	27
User Management	28
Login FortiManager	28
Client Management	29
Reports	30
Submitting feedback	32

Change Log

Date	Change Description
2025-12-17	Initial release of Managed FortiGate Service 25.4.

Introduction

Managed FortiGate Service (MFGS) is a cloud-based network security solution available 24x7. It accelerates deployments, simplifies daily operations and enhances your security posture. This service is designed to help partners and customers efficiently scale their operations according to Fortinet Security Best Practices and ITIL methodologies.



Onboarding to Managed FortiGate Service

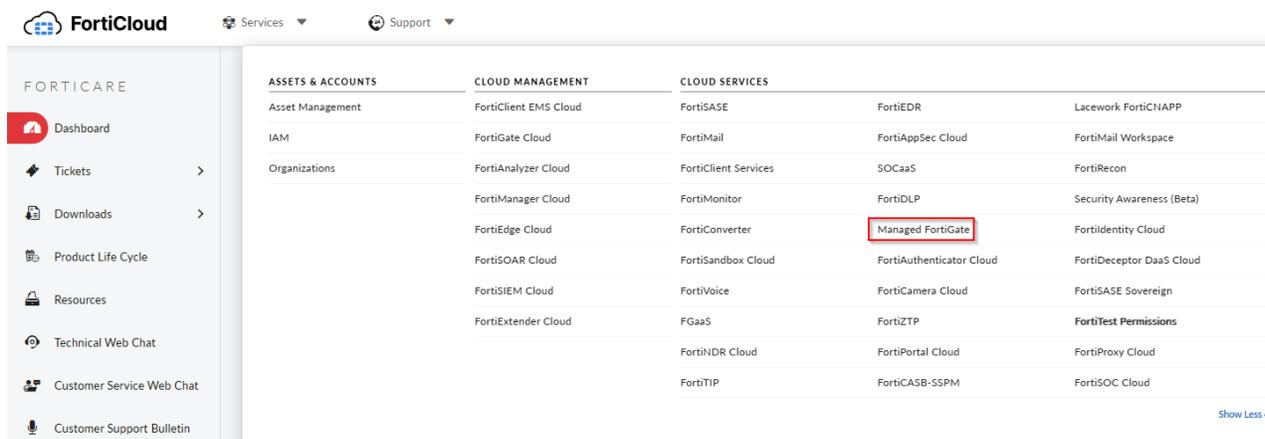


This service requires exclusive central management and cannot coexist with on-site or cloud-based management platforms. If needed, the following modifications will be implemented on devices to finalize onboarding:

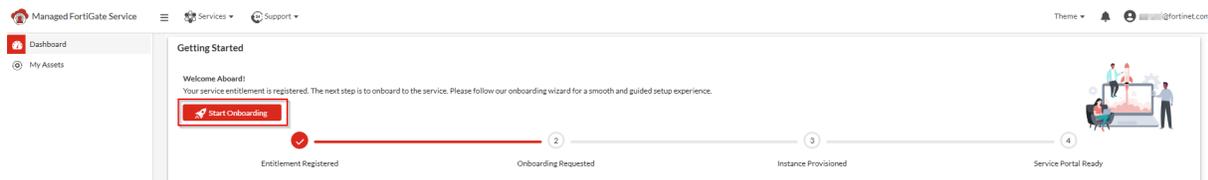
- Unused objects will be deleted.
- Conflicting objects will be renamed.

To submit an onboarding request:

1. Log in to [FortiCloud](#).
2. In the FortiCloud banner, click *Services > Cloud Services > Managed FortiGate*.



3. Click the *Start Onboarding* button to launch the Managed FortiGate Service Onboarding Wizard.



For more information on onboarding, please see: [Managed FortiGate new customer onboarding video](#).

If you have any questions or issues with onboarding, please contact mfgs_success@fortinet.com.

Determine your onboarding type

During the initial onboarding step, you will be asked to choose your onboarding type, either as an *MSSP* or a *Regular Customer*.

A managed security service provider (MSSP) offers network security services to an organization. For more information, see [What is a Managed Security Service Provider \(MSSP\)?](#)

You manage client FortiGates under your own FortiCare account	You manage your own FortiGates under your individual FortiCare account
Complete an <i>MSSP</i> onboarding request	Complete a <i>Regular Customer</i> onboarding request.

Once you have determined your onboarding type, you can follow the relevant onboarding instructions below:

- [MSSP onboarding on page 7](#)
- [Regular customer onboarding on page 11](#)

You can review the following topic for information about the post-onboarding request submission process.

- [Post-onboarding request submission on page 14](#)

MSSP onboarding

To onboard as an MSSP:

1. Select the *MSSP* option.

Selection



Cancel

2. Choose the region to deploy your FortiManager Cloud instance.

The screenshot shows the 'MSSP Customer Onboarding Wizard' in the 'Managed FortiGate Service' portal. The wizard is at step 1, 'Select Region'. The progress bar shows steps: 1. Select Region (active), 2. Add Client, 3. Add Contacts, 4. Additional Info, and 5. Review Summary. The main content area contains the following text: 'The Managed FortiGate Service leverages FortiManager cloud as its platform for cloud-based management. Please choose a region for deploying your FortiManager Cloud instance.' Below this is a dropdown menu with 'Spain (Madrid)' selected. At the bottom, there are 'Cancel', 'Save Draft', and 'Next' buttons.

3. Add a client.

Add the first client organization you will be managing. Additional clients can be added after completing the onboarding.

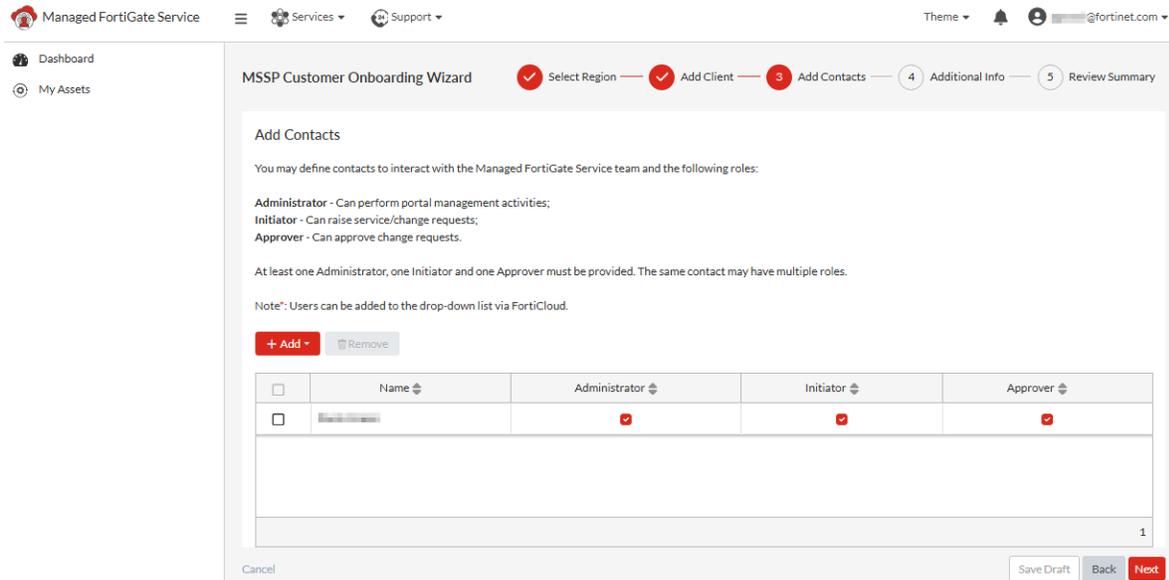
The screenshot shows the 'MSSP Customer Onboarding Wizard' in the 'Managed FortiGate Service' portal. The wizard is at step 2, 'Add Client'. The progress bar shows steps: 1. Select Region (completed), 2. Add Client (active), 3. Add Contacts, 4. Additional Info, and 5. Review Summary. The main content area contains the following text: 'Specify a name for the new client organization you'll be managing. After completing onboarding, you can add more clients through the Managed FortiGate Service portal.' Below this is a text input field with 'Client1' entered. At the bottom, there are 'Cancel', 'Save Draft', 'Back', and 'Next' buttons.

4. Define contacts to interact with the Managed FortiGate Service team and the corresponding roles. At least one *Administrator*, one *Initiator*, and one *Approver* must be provided. The same contact may have multiple roles.

- *Administrator*: can perform portal management activities.
- *Initiator*: can raise service/change requests.
- *Approver*: can approve change requests.

Click on the **+Add** button to select a user from the dropdown list. This list is populated based on the users available on your FortiCloud account.

Users can be added to the dropdown list via FortiCloud. Follow the [FortiCloud Identity & Access Management Module](#) for more information.



5. On the *Additional Info* page, add an email address where you want to receive email notifications related to the onboarding process.

- Special requests and/or instructions for the Managed FortiGate Service team can be provided in the *Notes* textbox.
- Useful files such as network diagrams can be shared with the team using the *Upload Attachments* button.

Select option *FortiGuard SOCaaS alert containment/remediation pre-authorization* if you have subscribed to both FortiGuard SOCaaS and Managed FortiGate services. By enabling this feature, you grant Fortinet pre-approval to implement configuration changes to contain escalated SOCaaS alerts, impact minor or significant, WITHOUT requiring individual approvals for each change request.

Select option *I wish to receive Service Request updates via email* to get the latest service request updates via email plus the three most recent comments instead of a generic update notification.



Both the *FortiGuard SOCaaS alert containment/remediation pre authorization* and *I wish to receive Service Request updates via email* options can be disabled or re-enabled after onboarding by submitting a *Service Request* of type *Service Inquiry*.

The screenshot shows the 'Additional Info' step of the MSSP Customer Onboarding Wizard. The progress bar at the top indicates that 'Select Region', 'Add Client', and 'Add Contacts' are completed, while 'Additional Info' is the current step. The form includes a text input for a contact email address (pre-filled with '@fortinet.com'), a text area for optional notes, and an 'Upload Attachments' section with a 'No file selected' message. There are two checkboxes for optional authorization and email preferences. At the bottom, there are 'Cancel', 'Save Draft', 'Back', and 'Next' buttons.

- Review the details on the *Review Summary* page. Once all fields are completed, you can review the summary before submitting the onboarding request. Click each tab to view the details you provided in previous steps. Click *Back* to return to a previous step in the wizard.

The screenshot shows the 'Review Summary' step of the MSSP Customer Onboarding Wizard. The progress bar at the top indicates that all steps are completed. The form displays a summary of the information provided, with tabs for 'Selected Region', 'Client', 'Contacts', and 'Additional Info'. The 'Selected Region' tab is active, showing 'Spain (Madrid)' as the selected region. At the bottom, there are 'Cancel', 'Save Draft', 'Back', and 'Submit' buttons.

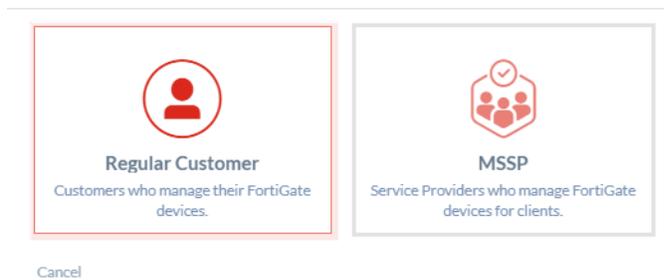
- Click *Submit* to send the onboarding request to the Managed FortiGate Service team. Any time before submitting the request, you can click *Save Draft* to save your progress and return to it later.

Regular customer onboarding

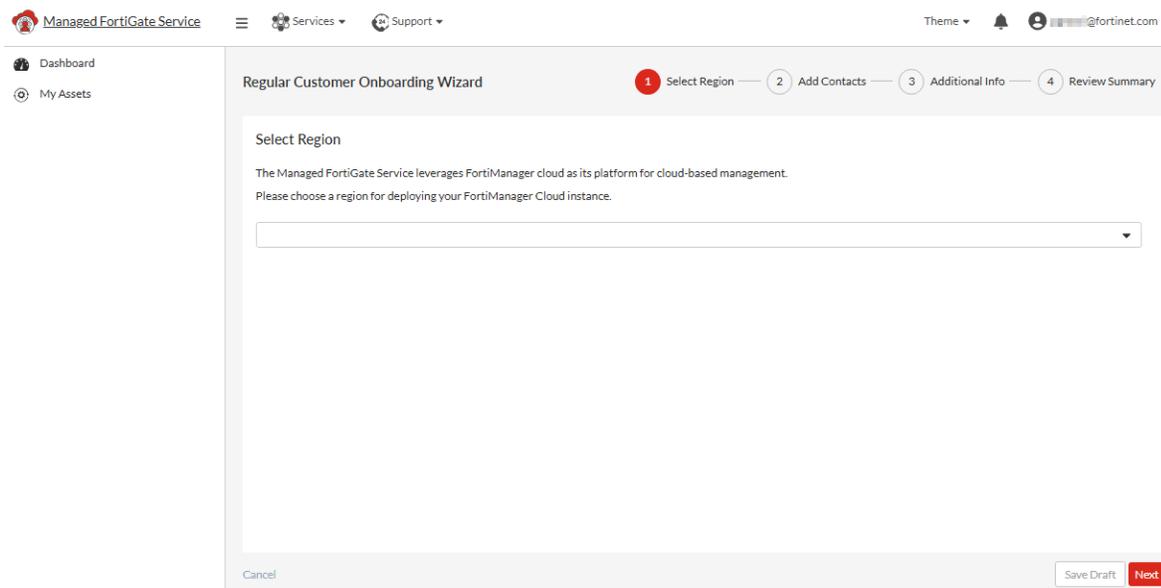
To onboard as a regular customer:

1. Select the *Regular Customer* option.

Selection



2. Choose the region to deploy your FortiManager Cloud instance.

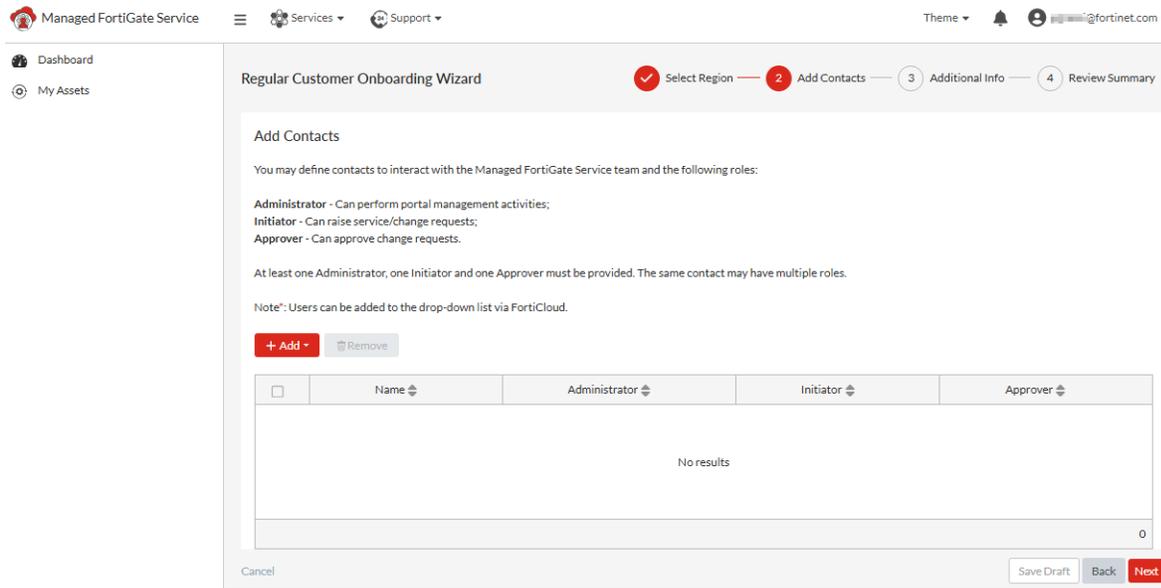


3. Define contacts to interact with the Managed FortiGate Service team and the corresponding roles. At least one *Administrator*, one *Initiator*, and one *Approver* must be provided. The same contact may have multiple roles.

- *Administrator*: can perform portal management activities.
- *Initiator*: can raise service/change requests.
- *Approver*: can approve change requests.

Click on the **+Add** button to select a user from the dropdown list. This list is populated based on the users available on your FortiCloud account.

Users can be added to the dropdown list via FortiCloud. Follow the [FortiCloud Identity & Access Management Module](#) for more information.



4. On the *Additional Info* page, add an email address where you want to receive email notifications related to the onboarding process.
 - Special requests and/or instructions for the Managed FortiGate Service team can be provided in the *Notes* textbox.
 - Useful files such as network diagrams can be shared with the team using the *Upload Attachments* button.

Select option *FortiGuard SOCaaS alert containment/remediation pre-authorization* if you have subscribed to both FortiGuard SOCaaS and Managed FortiGate services. By enabling this feature, you grant Fortinet pre-approval to implement configuration changes to contain escalated SOCaaS alerts, impact minor or significant, WITHOUT requiring individual approvals for each change request.

Select option *I wish to receive Service Request updates via email* to get the latest service request updates via email plus the three most recent comments instead of a generic update notification.



Both the *FortiGuard SOCaaS alert containment/remediation pre authorization* and *I wish to receive Service Request updates via email* options can be disabled or re-enabled after onboarding by submitting a *Service Request* of type *Service Inquiry*.

The screenshot shows the 'Regular Customer Onboarding Wizard' interface. The progress bar at the top indicates four steps: 'Select Region' (checked), 'Add Contacts' (checked), 'Additional Info' (active, highlighted in red), and 'Review Summary' (disabled). The 'Additional Info' section contains the following elements:

- A text input field for a contact email address with the placeholder text: "Please enter a contact email address to receive onboarding updates".
- A text area for "Notes (Optional)".
- An "Upload Attachments" button and a file selection field showing "No file selected".
- Two optional checkboxes:
 - FortiGuard SOCaaS alert containment/remediation pre-authorization (Optional). I expressly authorize Fortinet to apply configuration changes in order to contain and/or remediate FortiGuard SOCaaS escalated alerts with minor or significant impact.
 - I wish to receive Service Request updates via email (Optional). Please note: to update service requests you need to login to the portal.

At the bottom of the form, there are buttons for "Cancel", "Save Draft", "Back", and "Next".

5. Review the details on the *Review Summary* page. Once all fields are completed, you can review the summary before submitting the onboarding request. Click each tab to view the details you provided in previous steps. Click *Back* to return to a previous step in the wizard.
6. Click *Submit* to send the onboarding request to the Managed FortiGate Service team. Any time before submitting the request, you can click *Save Draft* to save your progress and return to it later.

The screenshot shows the 'Regular Customer Onboarding Wizard' interface at the 'Review Summary' step. The progress bar at the top indicates four steps: 'Select Region' (checked), 'Add Contacts' (checked), 'Additional Info' (checked), and 'Review Summary' (active, highlighted in red). The 'Review Summary' section contains the following elements:

- A heading "Review Summary" and a sub-heading "Please review the information below".
- Three tabs: "Selected Region" (active), "Contacts", and "Additional Info".
- A "Region" section with a dropdown menu showing "Spain (Madrid)".

At the bottom of the form, there are buttons for "Cancel", "Save Draft", "Back", and "Submit".

Post-onboarding request submission

- You will be able to follow your onboarding progress by looking at the *Dashboard > Getting Started* widget where timelines are reported.
- After submitting an onboarding request, the Managed FortiGate Service team may require up to three (3) business days to prepare your environment. Once the backend setup is complete, your onboarding timeline will be updated to reflect the current status.
- Once your customer onboarding is complete, you can onboard FortiGate devices by submitting device onboarding service requests. See [Device Onboarding on page 23](#).

Accessing the Managed FortiGate Service portal

The Managed FortiGate Service portal provides comprehensive visibility into service and usage details. It serves as the primary channel for interacting with the MFGS team.

Via the MFGS portal you can:

- View open change requests with their corresponding type and consult the change request calendar. See [Dashboard on page 17](#).
- Create service requests or comment on existing requests. See [Service Requests on page 19](#).
- View your asset list, including entitled devices, onboarded devices, expiring licenses, and devices not subscribed to the Managed FortiGate Service. See [My Assets on page 27](#).
- Manage users that have access to the portal and the assigned role. See [User Management on page 28](#).
- Manage MSSP clients. See [Client Management on page 29](#).
- View reports available. See [Reports on page 30](#).

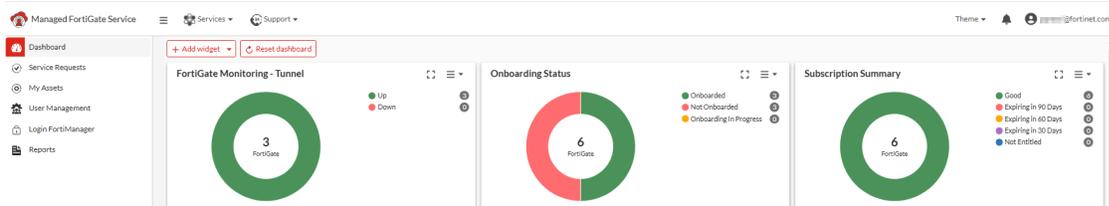


Customers onboarded as MSSP can filter the content of *Dashboard*, *Service Requests*, *Reports*, and *My Assets* for each managed client.

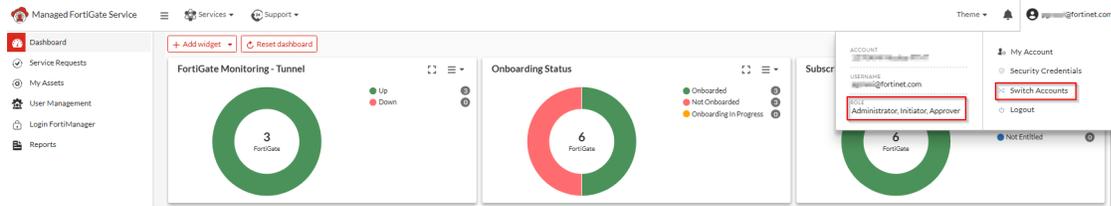
Portal customization

Several customization options are available on the portal:

- To change the portal theme, click the Theme menu and select Light or Dark.

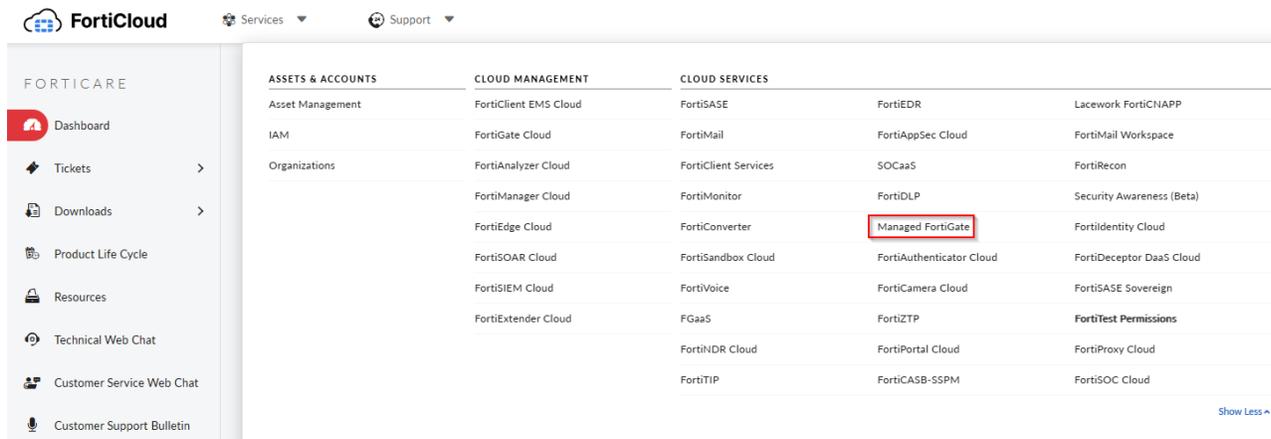


- To switch accounts, click the Account menu and select *Switch Accounts*.
- When you click on the account menu, the roles assigned to your user, such as *Administrator*, *Initiator*, or *Approver* are shown.



To access the Managed FortiGate Service portal:

1. Log in to [FortiCloud](#).
2. In the FortiCloud banner, click *Services > Cloud Services > Managed FortiGate*.



Pending Service Request popup window

When there are active service requests that need your input, a “Service Requests Needing Your Attention” popup window will appear. This notification lists service requests with any of the following statuses: *Awaiting Customer Feedback, Pending Connector, Pending Approval, Pending CloseConf, Activation on Hold, or Onboarding on Hold*.

To view more details, click on any service request in the popup. This action will redirect you to the service request page.

Once you close the Pending Service Request popup window, it will NOT appear again for the next 12 hours. For more information about service statuses, refer to [Dashboard on page 17](#).

Service Requests needing your attention

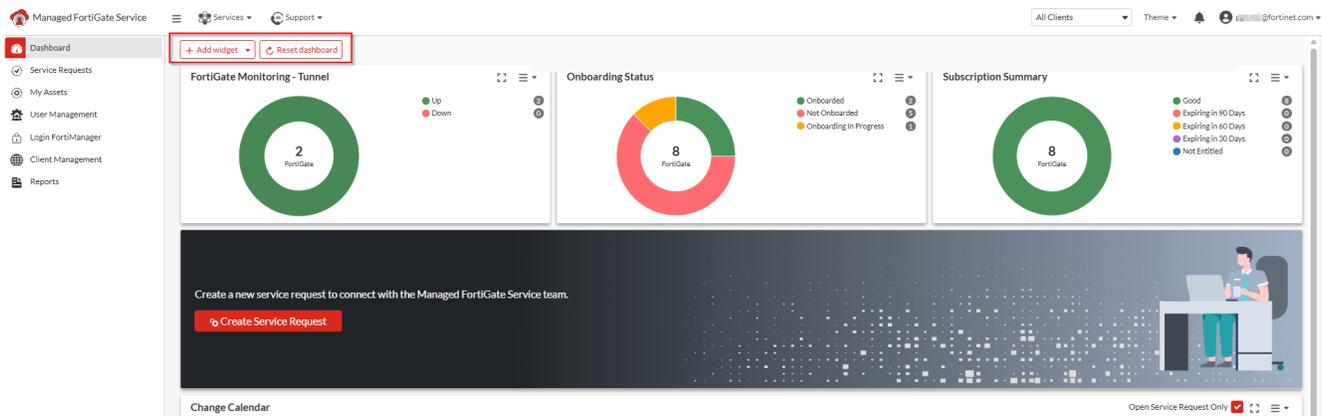
ID	Title	Status
1040018	Device Onboarding Request	PendCloseConf
1041451	Device Onboarding Request	Pending Connector

Close

Dashboard

The *Dashboard* serves as default landing page for the Managed FortiGate Service. It displays a variety of customizable widgets that you can add, remove or adjust to highlight the most important information about your environment.

The two header buttons “Add widget” and “Reset dashboard” let you add widgets not shown by default and reset to the original layout.



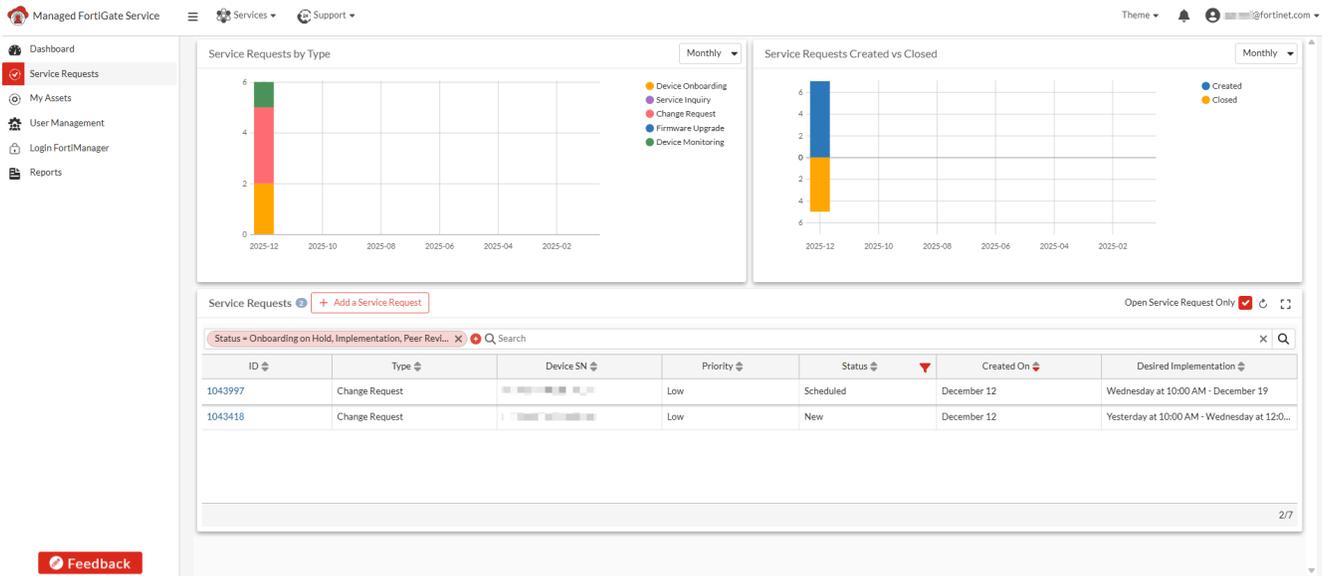
The following widgets are available on the dashboard:

Widget Name	Description
FortiGate Monitoring Tunnel	Management Tunnel status between FortiManager Cloud and onboarded FortiGates: <ul style="list-style-type: none"> • <i>Green</i>: Management tunnel is UP. • <i>Red</i>: Management tunnel is DOWN.
Onboarding Status	Onboarding status for FortiGate devices registered under the FortiCloud account: <ul style="list-style-type: none"> • <i>Not Onboarded</i>: FortiGate devices with a valid Managed FortiGate Service entitlement that have not yet been onboarded.

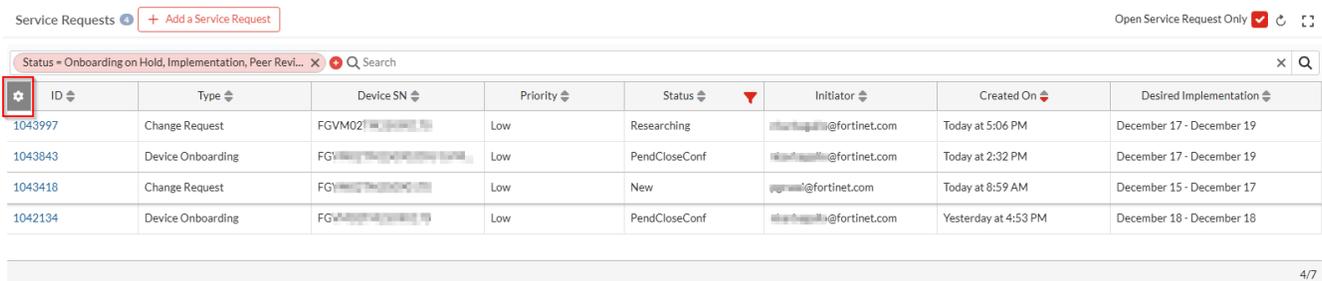
Widget Name	Description
	<ul style="list-style-type: none"> • <i>Onboarded</i>: FortiGate devices onboarded to the service. • <i>Onboarding in Progress</i>: FortiGate devices currently undergoing the onboarding process.
Subscription Summary	<p>Managed FortiGate Service entitlement status for FortiGate devices registered under the FortiCloud account.</p> <ul style="list-style-type: none"> • <i>Good</i>: Entitlement expires in more than 90 days. • <i>Expiring in 90 days</i>: Entitlement expires in 90 days or less. • <i>Expiring in 60 days</i>: Entitlement expires in 60 days or less. • <i>Expiring in 30 days</i>: Entitlement expires in 30 days or less. • <i>Not Entitled</i>: Entitlement not applied.
Create Service Request	Static widget for creating Service Requests.
Change Calendar	<p>Displays past and upcoming Service Requests of type <i>Firmware Upgrade</i> or <i>Change Request</i>, along with key details such as <i>ID</i>, <i>Title</i>, <i>Schedule</i>, and <i>Status</i>.</p> <p>By default, the "Open Service Requests Only" checkbox is selected, which excludes any Service Requests marked as <i>Canceled</i> or <i>Completed</i>.</p>
News	Latest updates on Managed FortiGate Service releases and new features.
Resources	Recommended service resources, including curated documentation and professional collateral materials.
Video Guides	Recommended service video guides, featuring curated tutorials and instructional content.
Open Changes	<p>Count of open change requests grouped by priority, including all request types:</p> <ul style="list-style-type: none"> • <i>Low</i>: Changes that are not time-sensitive and can be scheduled for implementation at a later date. • <i>Medium</i>: Changes that are moderately urgent but do not require immediate action. • <i>High</i>: Business critical changes that must be implemented as soon as possible to avoid significant disruption or risks.
FortiGate Monitoring – Config Status	<p>Config status between FortiManager Cloud and onboarded FortiGates:</p> <ul style="list-style-type: none"> • <i>Synchronized</i>: The FortiManager Cloud configuration (revision history) aligns with the managed device configuration. • <i>Out of sync</i>: The FortiManager Cloud configuration (revision history) differs from the managed device configuration. • <i>Unknown</i>: The status cannot be determined because FortiManager Cloud is unable to connect to the managed device.
Outbreak Alerts	Latest Outbreak alert updates

Service Requests

On the Managed FortiGate Service portal under Service Requests, you can consult existing Service Requests or raise new ones.



The Service Requests table can be customized by clicking the "Configure Table" icon, which appears when hovering over the ID column.



When the *Open Service Requests Only* checkbox is selected, the service request list excludes *Canceled* or *Completed* Service Requests. See [Service request status on page 20](#).

Service request type

Service Requests can be classified under one of the following types to specify the nature or purpose of the request.

Change Request

A request to add, modify, or remove configuration items on a managed FortiGate device.

	You can choose an implementation date starting from the next business day or later.
Customer / MSSP Onboarding	A request to activate the Managed FortiGate Service for a new Regular or MSSP customer. This request is generated by the system upon completion of the onboarding wizard .
Device Monitoring	A request automatically generated by the system when the management tunnel between FortiManager Cloud and a FortiGate device is down for 10 minutes or longer. It closes automatically upon restoration of connectivity.
Device Onboarding	A request to add a new FortiGate device to the Managed FortiGate Service. You can choose an implementation date starting 3 working days from today or later.
Firmware Upgrade	A request to upgrade the firmware on a FortiGate device. You can select a desired implementation date starting 7 working days from today or later. For the list of firmware versions supported by the service, refer to the Requirements section of the Getting Started Guide .
Service Inquiry	A general request for information about the service.

Service request status

Service Requests can have one of the following statuses, offering clear visibility into the current stage of each request in the process.

Status	Description	Action Pending On
Activation in Progress	The MFGS team is onboarding a new customer to the service.	MFGS team
Activation on Hold	The MFGS team is unable to onboard a new customer to the service due to service requirements not met. See Service Requirements .	Customer
Awaiting Customer Feedback	The MFGS team has requested additional information to continue their analysis and is awaiting feedback. If no response is received within 7 calendar days, the status will be updated to <i>PendCloseConf</i> .	Customer
Completed	The service request has been fulfilled, and it's now closed	n/a
Canceled	The activity has been canceled, the service request is now closed.	n/a
Config Validation in Progress	The MFGS team is validating the FortiGate configuration file. The action is with the MFGS team.	MFGS team

Status	Description	Action Pending On
Config Validation Completed	The MFGS team completed validating the FortiGate configuration file and they will soon reach out to share their findings.	MFGS team
Implementation	Implementation of the activity is currently underway by the MFGS team.	MFGS team
New	A new Service Request has been opened and is pending assignment. The action is with the MFGS team.	MFGS team
Onboarding in Progress	The MFGS team is onboarding one or more FortiGate devices to the service. The action is with the MFGS team.	MFGS team
Onboarding on Hold	The MFGS team is unable to onboard one or more FortiGate devices due to service requirements not met. See Service Requirements .	Customer
On Hold/Blocked	Standard processing is currently On Hold.	MFGS team
Peer Review Completed	The MFGS team completed reviewing the configuration changes and they will soon reach out to share their findings.	MFGS team
Peer Review in Progress	The MFGS team is reviewing the configuration changes. The action is with the MFGS team.	MFGS team
Peer Review Pending	The MFGS team is about to start reviewing the configuration changes. The action is with the MFGS team.	MFGS team
PendCloseConf	The MFGS team fulfilled the request, acknowledgement pending from customer to close the request. If no response is received within 7 calendar days, the status will be updated to Completed.	Customer
Pending Approval	The MFGS team requires the customer approval to schedule the activity. If no response is received within 7 calendar days, the status will be updated to PendCloseConf.	Customer
Pending Connector	The MFGS team has provisioned the FortiManager Cloud instance. Customer action is required to enable the FortiManager Cloud connector on the FortiGates to onboard.	Customer
RcvdCustFB	Status set automatically for any new customer comment posted. The action is with the MFGS team.	MFGS team

3. Enter the service request details:

Type	Select the service request type. For more information, see Service request type on page 19 .
Client (MSSP customers only)	Identify the client associated with this Service Request.
Title	Enter the Service Request title.
Device	Select the FortiGate device(s) to which the request applies.
Upgrade to Version (Firmware Upgrade only)	Enter the FortiGate firmware version to upgrade to.
Desired Implementation	Select the desired implementation date/time interval. (optional field)
Notification Email Address	The email address to which updates will be sent. By default, this field is pre-filled with the requester's email address.
Description	Description of the service request.
Upload Attachments	Click to upload network diagrams, files, or other supporting information related to the request. The following upload limits apply: <ul style="list-style-type: none"> • Maximum file size: 20 MB • Maximum number of files: 3 • Supported file types: csv, docx, jpg, log, pdf, png, txt, xlsx, xml.

Device Onboarding

Service Requests type Device Onboarding are created to add FortiGate devices to the service and configure them as needed.

Add a Service Request

Type

Site

Deployment Type
 Greenfield - New Deployment
 Brownfield - Existing Deployment

Device
 Select the FortiGates to onboard:

- Only FortiGates entitled to the Managed FortiGate Service are listed.
- Exclusive central remote management by Fortinet is required.
- Ensure your FortiGates meet our service requirements before proceeding.

 For more information about service requirements, click [here](#).

Desired Implementation

Notification Email Address

Description

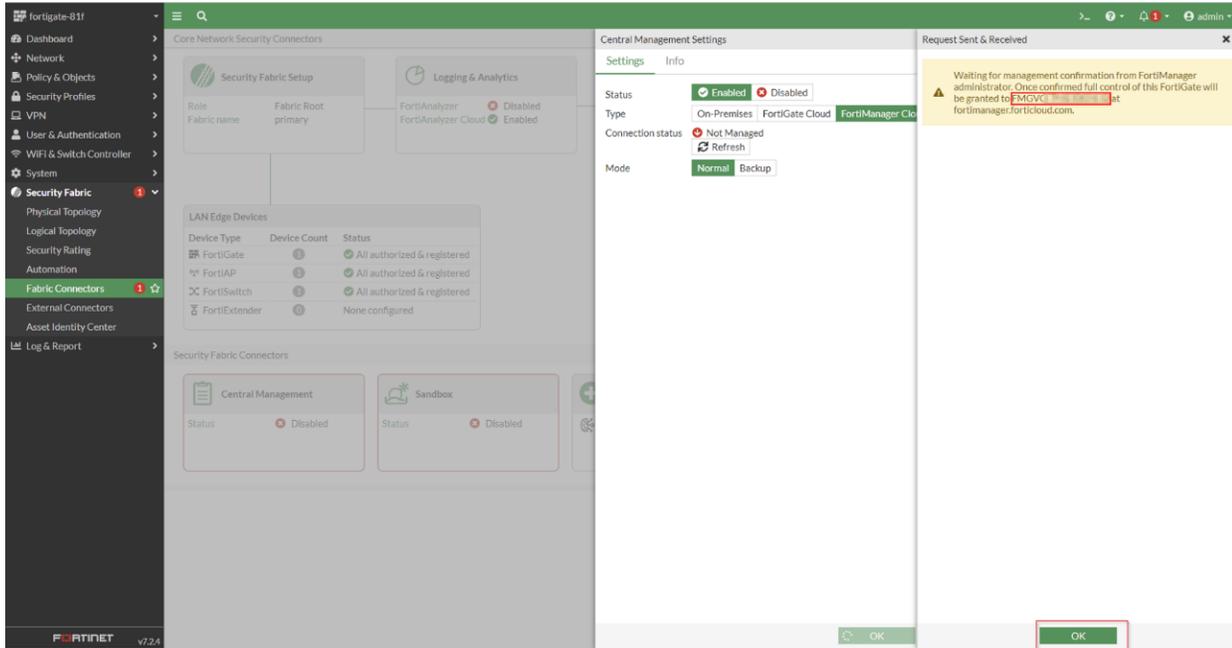
No file selected

Enter the following details when submitting a Device Onboarding Service Request:

Type	Select Device Onboarding.
Client (MSSP customers only)	Identify the client associated with this Service Request.
Site	Enter the site name
Deployment Type	Select one of the following options: <ul style="list-style-type: none"> <i>Greenfield</i>: New deployment that requires configuration by the Managed FortiGate Service team. <i>Brownfield</i>: Existing deployment that does not require configuration by the Managed FortiGate Service team.
Device	Select the FortiGate device(s) to onboard. Multiple FortiGate devices can be included in the same onboarding request only if they belong to the same HA cluster and are located on the same site.
Desired Implementation	Select the desired implementation date/time interval. (Optional field - if selected, a three-business-day timeframe from today will apply.)
Notification Email Address	The email address to which updates will be sent. By default, this field is pre-filled with the requester's email address.
Description	Description of the onboarding request.
Upload Attachments	Click to upload network diagrams, files, or other supporting information related to the request. The following upload limits apply:

- Maximum file size: 20 MB
- Maximum number of files: 3
- Supported file types: csv, docx, jpg, log, pdf, png, txt, xlsx, xml

Once the MFGS team processes the request, they will notify you through the service request for additional info and to enable the FortiManager Cloud connector in your FortiGate GUI under *Security Fabric > Fabric Connectors > Central Management*.



To enable FortiManager Cloud, you are required to login with an admin user associated to a *super_admin* profile or with *Access Permissions* for the categories *Configuration* and *Maintenance* set to *Read/Write* (see below example):

The screenshot displays the 'Edit Admin Profile' configuration page in the FortiGate Managed Service portal. The left sidebar shows the navigation menu with 'System' expanded to 'Admin Profiles'. The main content area shows the profile name 'fmg_admin-fos7013' and a comments field. Below is the 'Access Permissions' table, which lists various system components and their associated permissions (None, Read, Read/Write, Custom).

Name: fmg_admin-fos7013
Comments: 0/255

Access Permissions

Access Control	Permissions
Security Fabric	None Read Read/Write
FortiView	None Read Read/Write
User & Device	None Read Read/Write
Firewall	None Read Read/Write Custom
Log & Report	None Read Read/Write Custom
Network	None Read Read/Write Custom
System	None Read Read/Write Custom
Administrator Users	None Read Read/Write
FortiGuard Updates	None Read Read/Write
Configuration	None Read Read/Write
Maintenance	None Read Read/Write
Security Profile	None Read Read/Write Custom
VPN	None Read Read/Write
WAN Opt & Cache	None Read Read/Write
WiFi & Switch	None Read Read/Write

Permit usage of CLI diagnostic commands



GUI options to enable FortiManager Cloud or to customize admin profiles may differ based on the FortiGate firmware version.

In a FortiGate cluster, both members must have a valid Managed FortiGate Service entitlement; otherwise, the FortiManager Cloud option will be grayed out.

Once you click on the OK button, an authorization request will be triggered from your FortiGate that will be processed by the Managed FortiGate Service team.

Once authorized, your FortiGate(s) will be added to the Managed FortiGate Service and an exclusive management tunnel will be established to the provisioned FortiManager Cloud instance.

My Assets

The My Assets page displays all FortiGates registered under the FortiCloud account, along with their corresponding tunnel status, onboarding details, and subscription summary.

The My Assets table can be customized by clicking the *Configure Table* icon, which appears when hovering over the *Device SN* column.

Device SN	Location	Registration Date	License Expiry	Tunnel Status	Config Status	HA Primary	Deployment Method	Site
FGVM02TM25090210	905 rue Albert Einstein, V...	September 17	September 17, 2026	Up	Synchronized	HA Not Configured	Brownfield - Existing Deploy...	Site_1
FGVM02TM25090210	52 Lime Street, London, 7...	September 17	September 17, 2026	Up	Synchronized	HA Not Configured	Brownfield - Existing Deploy...	Site_1
FGVM02TM25090210	4190 Still Creek Drive, su...	September 19	September 19, 2026	Up	Synchronized	HA Not Configured	Brownfield - Existing Deploy...	Site_1
FGVM02TM25090210		October 9	October 9, 2026	Up	Synchronized	FGVM02TM25090210	Greenfield - New Deployment	Cluster site
FGVM02TM25090210		Yesterday at 8:13 AM	December 11, 2026	Up	Synchronized	FGVM02TM25090210	Greenfield - New Deployment	Cluster site
FGVM02TM25090210		Yesterday at 8:14 AM	December 11, 2026	Up	Synchronized	FGVM02TM25090210	Greenfield - New Deployment	Cluster site

FortiGate devices are grouped into different tabs based on the following criteria:

- **All:** All FortiGates registered under the FortiCloud account.
- **Onboarded:** FortiGates onboarded to the Managed FortiGate Service.
- **Onboarding:** FortiGates in the process of onboarding.
- **Not Onboarded:** FortiGates with an active Managed FortiGate Service entitlement but not onboarded to the service yet.
- **About to Expire:** FortiGates with an active Managed FortiGate Service entitlement expiring in 90 days or less.
- **Not Entitled:** FortiGates without a managed FortiGate service entitlement.

User Management

The User Management page provides the option to carry out the following user administrative tasks:

- **Adding Users:** This allows granting Managed FortiGate portal access to new users who already exist under the corresponding FortiCloud account as either Primary/Sub User or IAM. Please refer to the FortiCloud Identity & Access Management Module for more information on how to add users to FortiCloud.
- **Modifying Roles:** Customers can change the Initiator/Approver roles for existing users.
- **Deleting Users:** This action removes MFGS portal access for specific users.



Only users with the Administrator role can access the *User Management* section.

Name	Email	Administrator	Initiator	Approver	Action
Administrator	admin@fortinet.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Initiator	initiator@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Approver	approver@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Primary User	primary@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Sub User	subuser@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Guest	guest@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
FortiCloud IAM	iam@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Administrator	admin@fortinet.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

The *User Management* table can be customized by clicking the *Configure Table* icon, which appears when hovering over the *Name* column.

Login FortiManager

The *Login FortiManager* page redirects you to the FortiManager Cloud instance provisioned by the Managed FortiGate Service. Your access to this instance is limited to read-only mode.

ID	Title	Schedule	Status
1039652	AV Security Profile		Researching
1047321	Weekly Vulnerability Report - Recommended Action		PendCloseConf



Only users with the Administrator role can access page *Login FortiManager*.

Client Management

The *Client Management* pane offers a range of administrative tasks for managing clients effectively. These tasks include:

- **Client Overview:** Provides a concise view of the number of clients created and the onboarded FortiGates associated with each client versus the total onboarded in the FortiCloud account.
- **Client Editing:** Allows modification of existing client details, including client name and comments, as well as the selection of FortiGates to associate with the client.
- **Client Deletion:** Enables the deletion of clients, but only if they do not contain any associated FortiGates.
- **Client Addition:** Supports the creation of new clients directly from the GUI. To add new devices to specific clients, users must submit a device onboarding service request

Accessing the Managed FortiGate Service portal



Only users with the *Administrator* role for accounts onboarded as MSSP have access to the *Client Management* section.

The *Administrator* role requires access to *All Clients*, it cannot be limited to specific clients

The client management table can be customized by clicking the *Configure Table* icon, which appears when hovering over the *Name* column.

Reports

The Managed FortiGate Service portal offers automated weekly reports detailing scope and generation date.

The following reports are available:

Category	Description
Vulnerability Report	This report identifies security vulnerabilities across your FortiGate estate that can be remediated by upgrading to the Managed FortiGate Service recommended firmware.

Category	Description
	<p>The recommended firmware may differ from the latest FortiOS patch. See the Managed FortiGate Service FAQ for rationale and details.</p> <p>The <i>Upgrade To</i> column indicates the FortiOS version to install on each individual FortiGate to resolve all vulnerabilities rated medium or higher.</p> <p>The <i>Recommended Upgrade</i> field indicates the firmware version that will remediate all medium or higher vulnerabilities across the entire estate.</p> <p>For the most up-to-date information on FortiOS vulnerabilities, visit https://fortiguard.fortinet.com/psirt.</p>
Security Posture Assessment	<p>Managed FortiGates undergo weekly security posture assessments to continuously identify and address configuration weaknesses ensuring optimal security and a stronger security posture.</p>

To filter the list, click the filter icon () in the column heading or enter a term in the *Search a Report* field. To view more pages in the list, click the arrow keys (| < > > |) at the bottom of the page.

The Reports table can be customized by clicking the *Configure Table* icon, which appears when hovering over the *Created On* column.

Reports can be downloaded as PDFs by clicking on the report name.



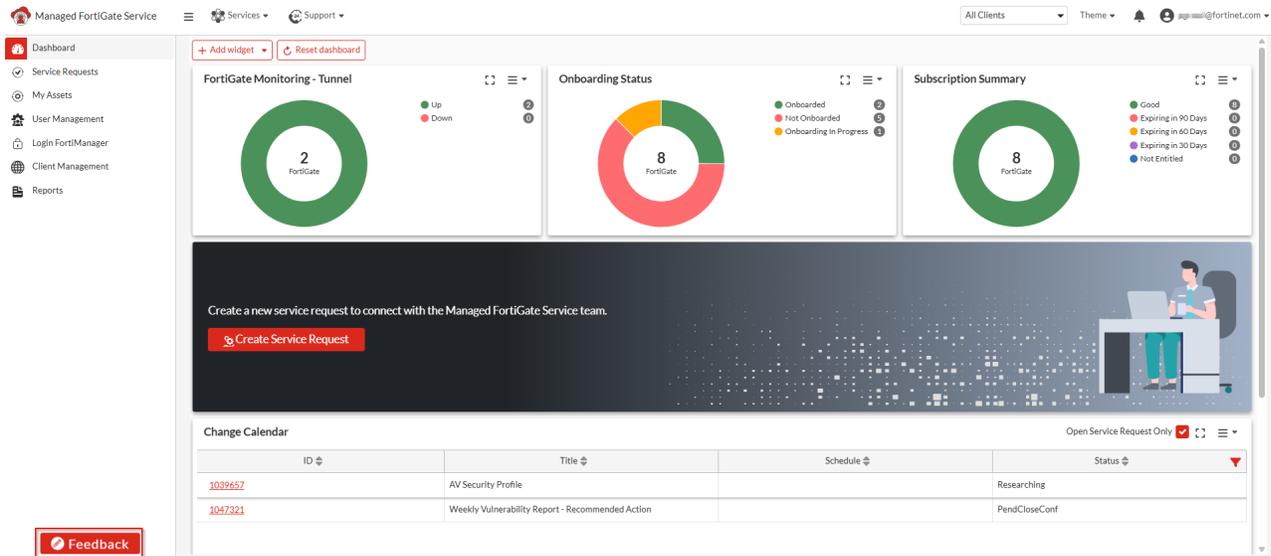
Security Posture Assessment reports are only available for FortiGate devices with a valid Attack Surface Security Rating subscription.

Submitting feedback

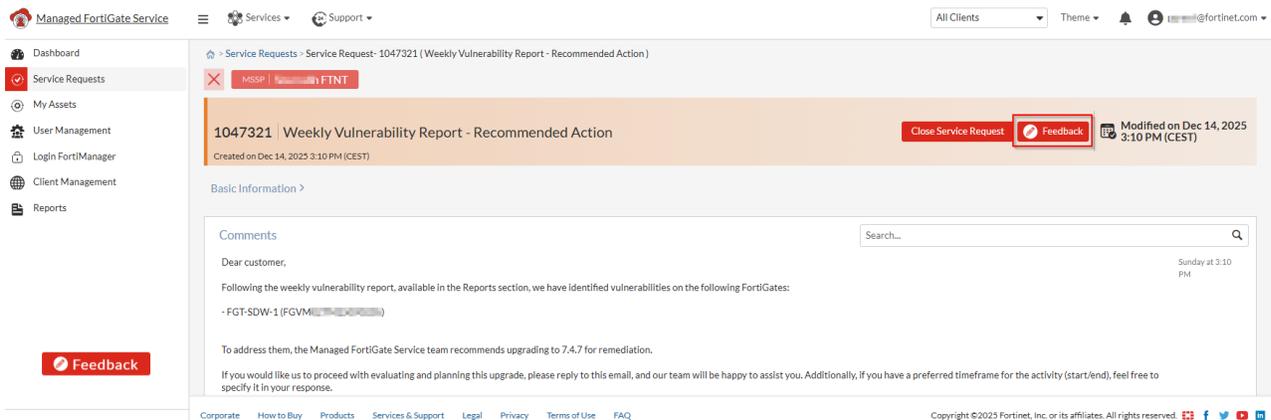
You can provide feedback on the quality of service by participating in surveys, which are accessible for active or recently closed service requests (within one month).

Several options are available to submit your feedback:

- On the portal blue menu area.



- On the service request banner.



- Alternatively, you can access the survey by clicking the direct link sent to you via email when your service request is completed

The survey is simple to complete and consists of one rating question along with an optional free-text field for additional comments.

Customer Satisfaction Survey
#1038499 Device Onboarding Request

How satisfied are you with your recent Managed FortiGate Service experience?

Please rate on a scale of 1 (Very Dissatisfied) to 5 (Very Satisfied)



What could we do to improve your Managed FortiGate Service experience?

BACK

SUBMIT

Your input is highly valued, please take a moment to complete the survey and help us enhance the quality of our service.



www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.