Administration Guide

Managed FortiGate Service Q1, 2026

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

March 25, 2026
Managed FortiGate Service Q1, 2026 Administration Guide
81-261-889123-20260325

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-26	Initial release of Managed FortiGate Service 26.1.

Introduction

Managed FortiGate Service (MFGS) is a cloud-based managed security service built around customer needs that delivers rapid deployment, expert change management and continuous optimization.

This service is designed to help partners and customers efficiently augment their operations according to Fortinet Security Best Practices and ITIL methodologies.

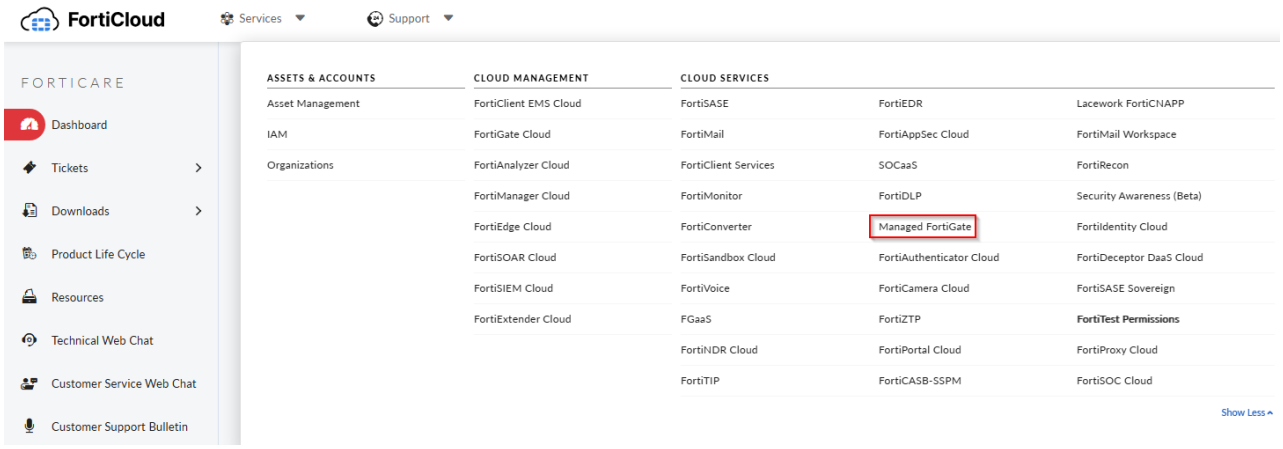
Onboarding to Managed FortiGate Service

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:

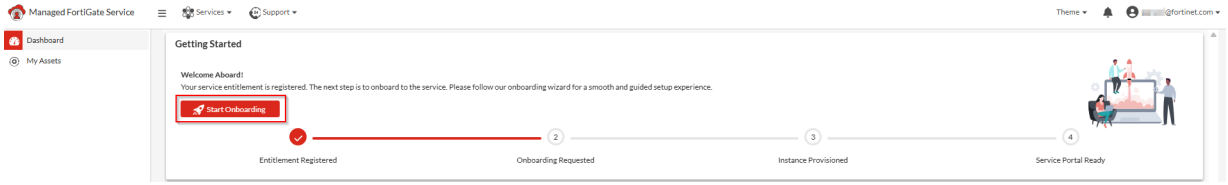
- Unused objects will be deleted.
- Conflicting objects will be renamed.

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) delivers network security services to multiple organizations, making multi-tenancy a core requirement.

You manage client FortiGates under your individual FortiCloud account	You manage your own FortiGates under your individual FortiCloud account
Complete an *MSSP* onboarding request	Complete a *Regular Customer* 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

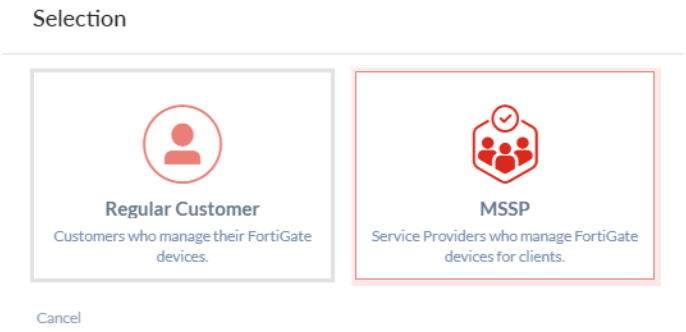
You can review the following topic for information about the post-onboarding request submission process.

- Post-onboarding request submission on page 14

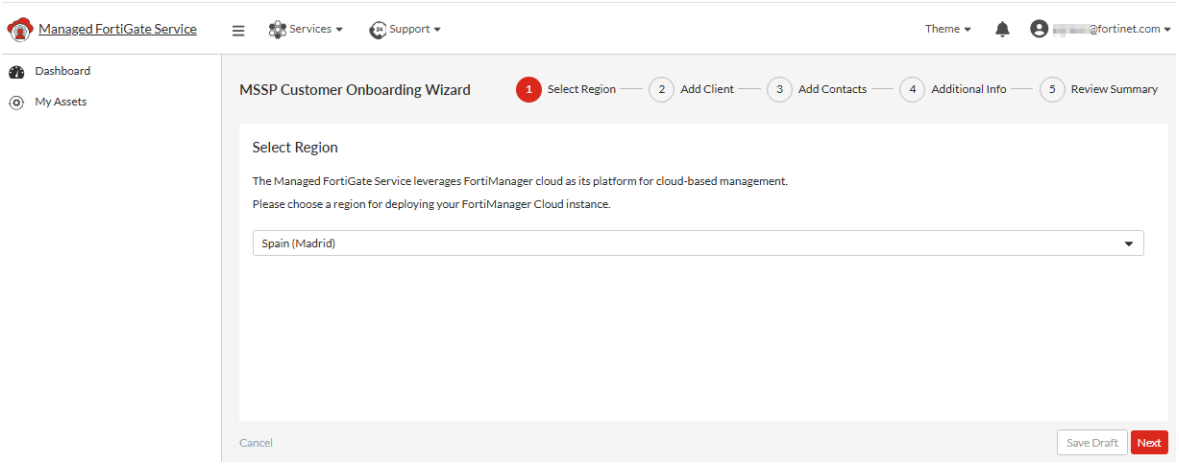
MSSP onboarding

To onboard as an MSSP and enable multi-tenancy:

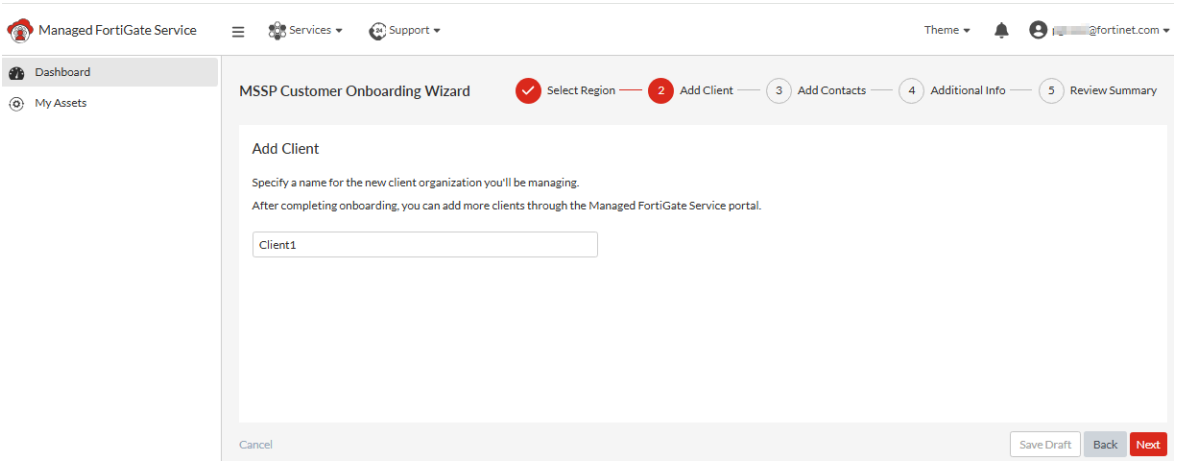
1. Select the *MSSP* option.



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



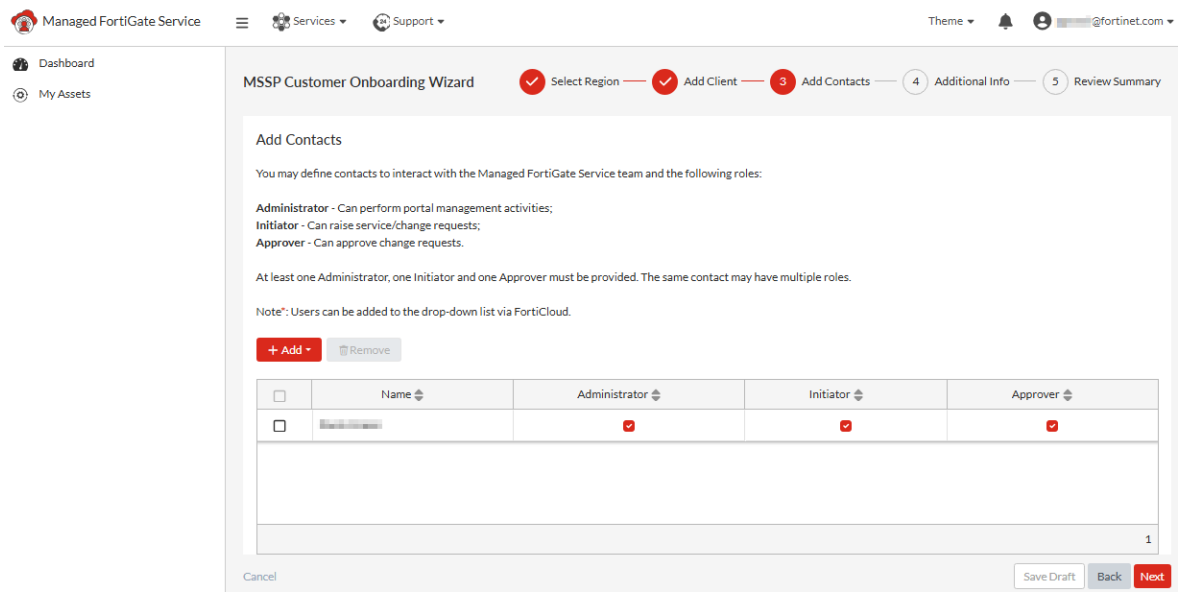
3. Add a client.
   Add the first client organization you will be managing. Additional clients can be added after completing the onboarding.



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.

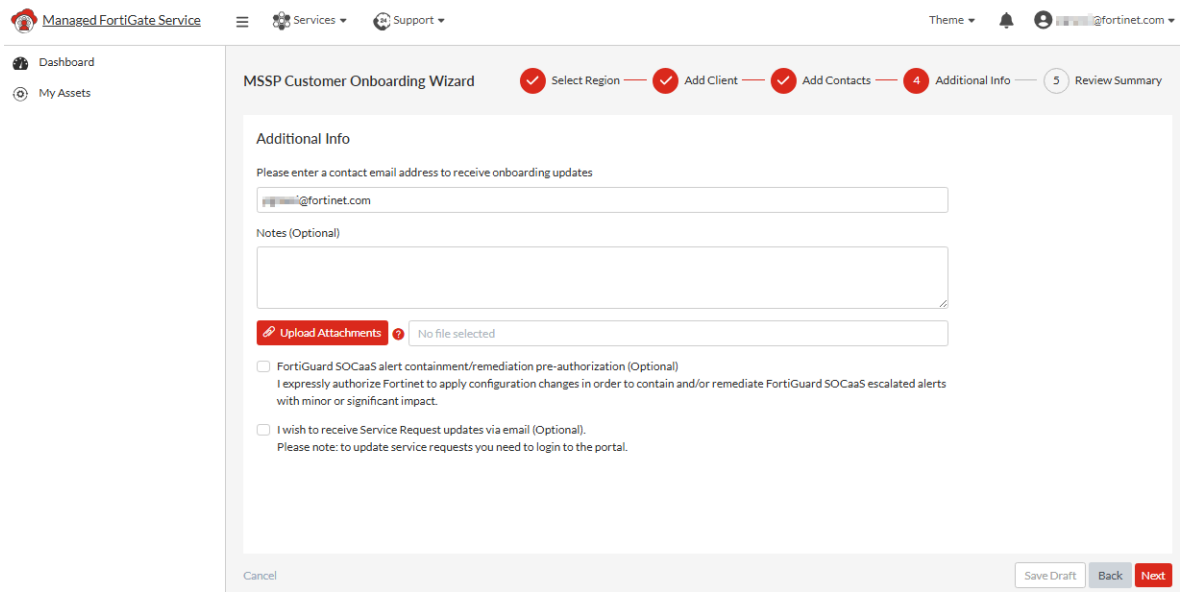


5. On the *Additional Info* page, add an email address where you want to receive email notifications related to the onboarding process.
   - Special requests and/or instructions for the Managed FortiGate Service team can be provided in the *Notes* textbox.
   - Useful files such as network diagrams can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

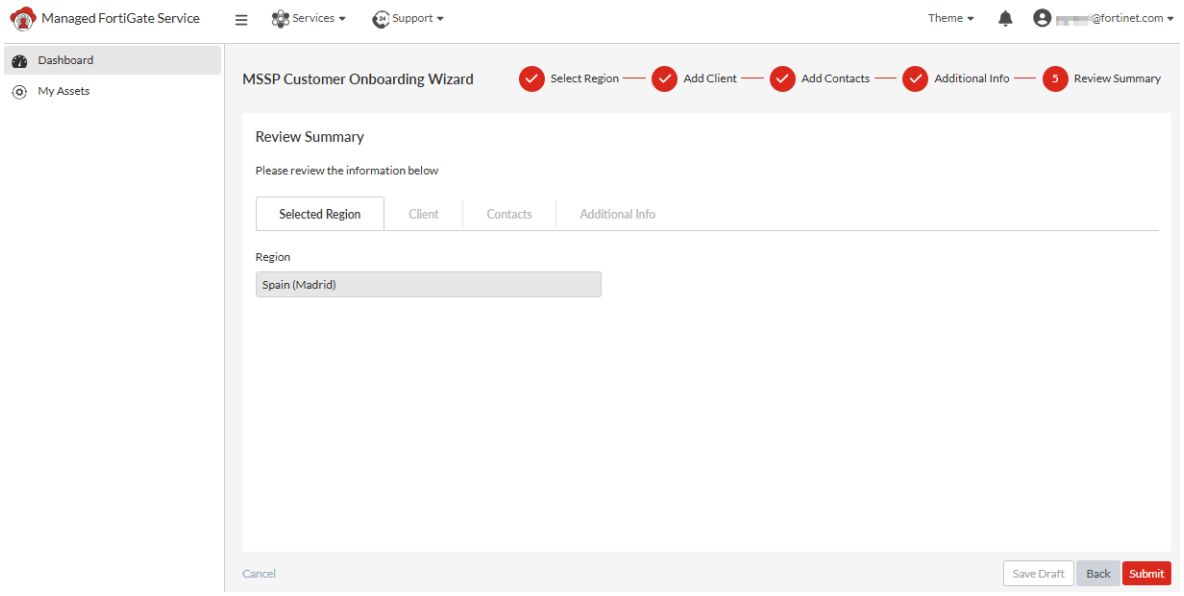
   Select option *FortiGuard SOCaaS alert containment/remediation pre-authorization* if you have subscribed to both FortiGuard SOCaaS and Managed FortiGate services. By enabling this feature, you grant Fortinet pre-approval to implement configuration changes to contain escalated SOCaaS alerts, impact minor 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 FortiGuard SOCaaS alert containment/remediation pre authorization and I wish to receive Service Request updates via email options can be disabled or enabled after onboarding via page *Administration > Additional Info*.



6. 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.

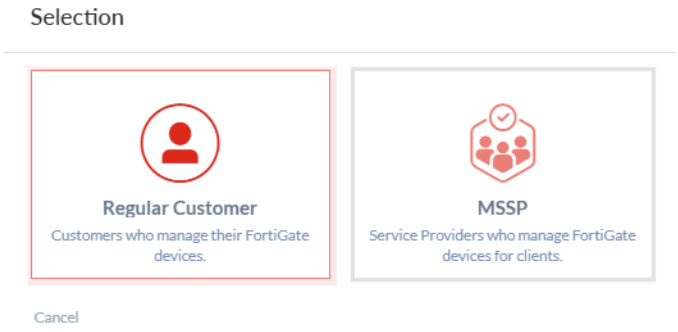


7. Click *Submit* to send the onboarding request to the Managed FortiGate Service team. Any time before submitting the request, you can click *Save Draft* to save your progress and return to it later.

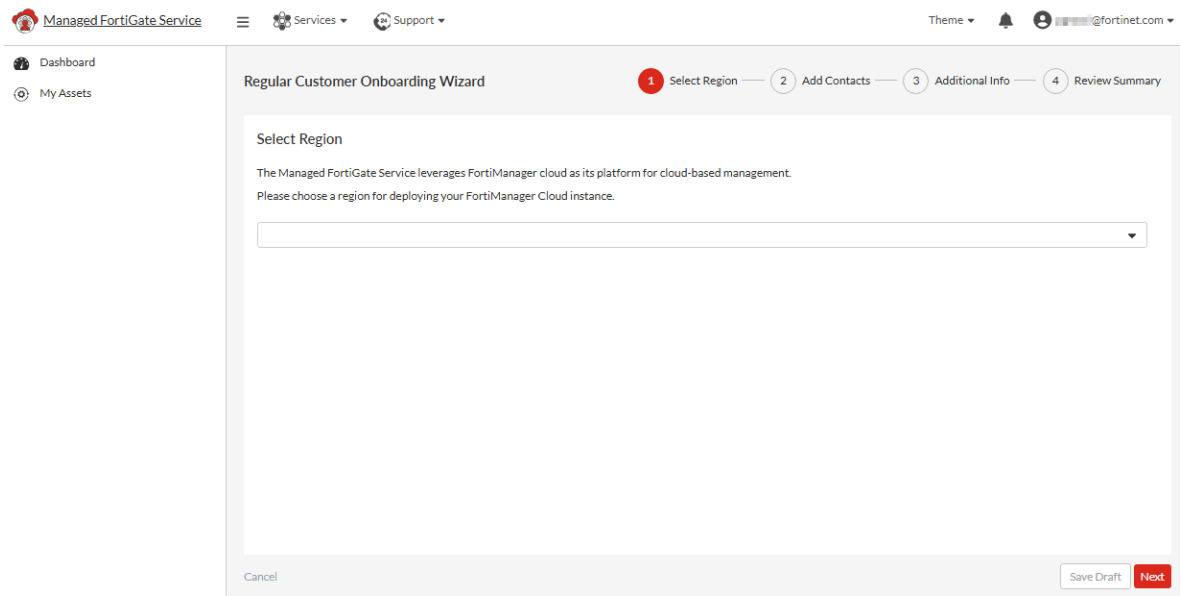
Regular customer onboarding

To onboard as a regular customer:

1. Select the *Regular Customer* option.



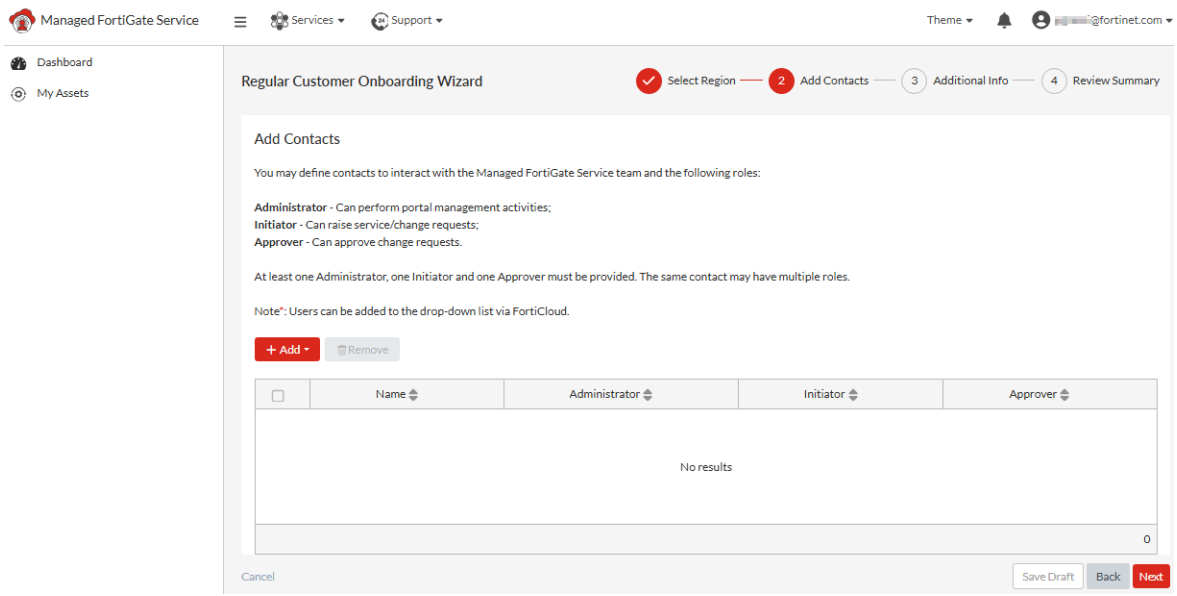
2. Choose the region to deploy your FortiManager Cloud instance.



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.

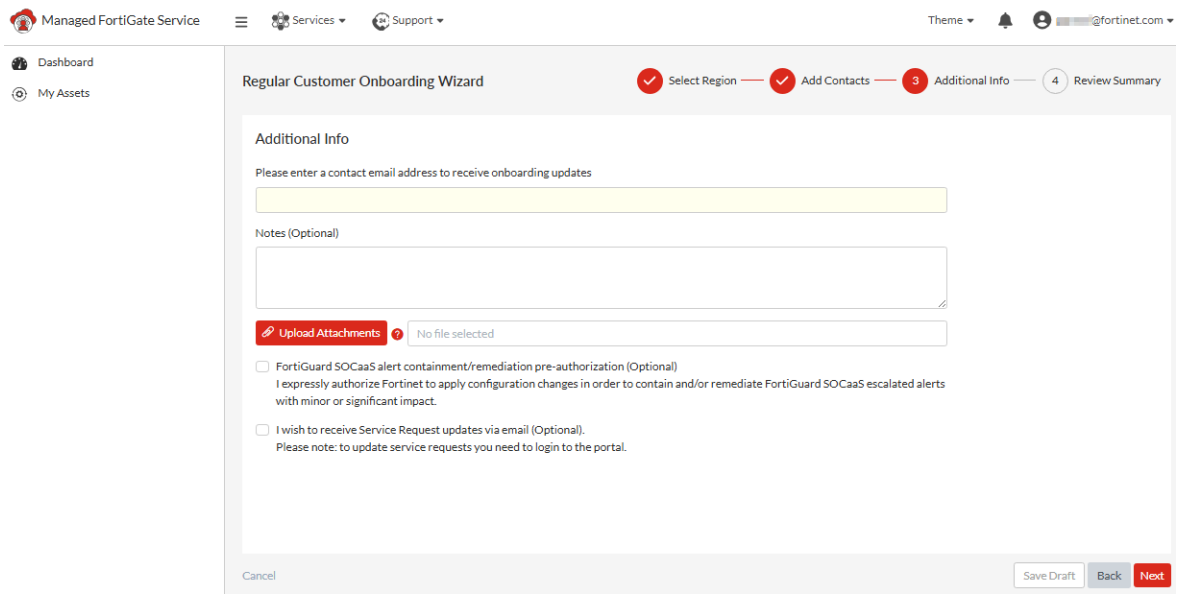


4. On the *Additional Info* page, add an email address where you want to receive email notifications related to the onboarding process.
   - Special requests and/or instructions for the Managed FortiGate Service team can be provided in the *Notes* textbox.
   - Useful files such as network diagrams can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

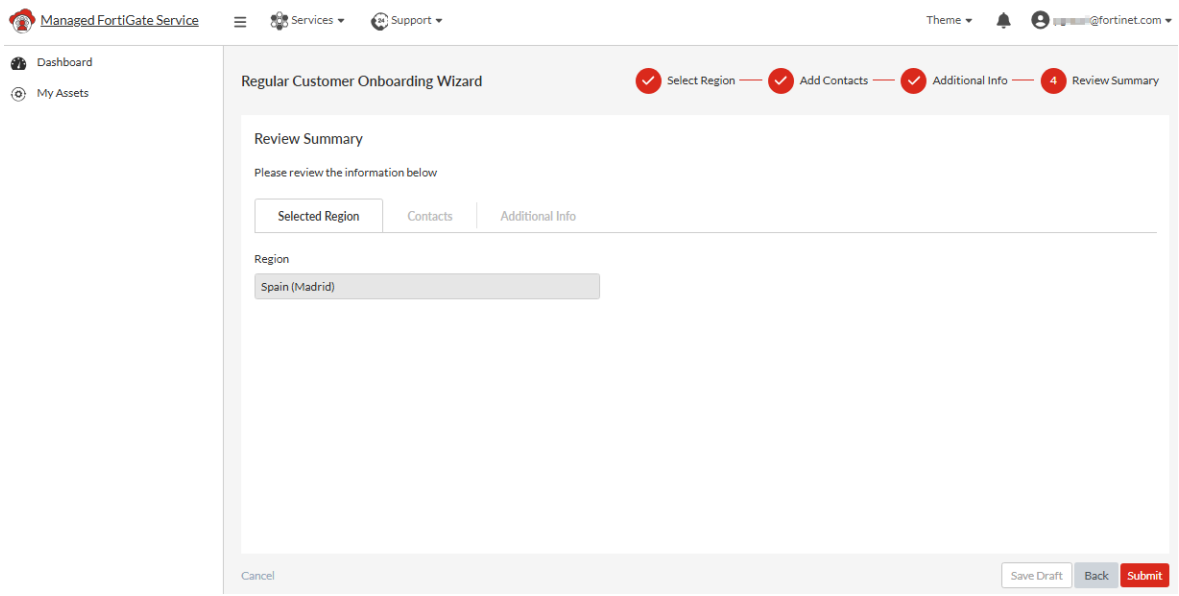
   Select option *FortiGuard SOCaaS alert containment/remediation pre-authorization* if you have subscribed to both FortiGuard SOCaaS and Managed FortiGate services. By enabling this feature, you grant Fortinet pre-approval to implement configuration changes to contain escalated SOCaaS alerts, impact minor 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 FortiGuard SOCaaS alert containment/remediation pre authorization and I wish to receive Service Request updates via email options can be disabled or enabled after onboarding via page *Administration > Additional Info*.



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.



Post-onboarding request submission

- After submitting a request, allow up to 3 business days for environment setup — the timeline under Dashboard > Getting Started updates automatically once complete.
- Once your customer onboarding is complete, submit device onboarding service requests to add FortiGate devices. See Device Onboarding on page 23.

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

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:

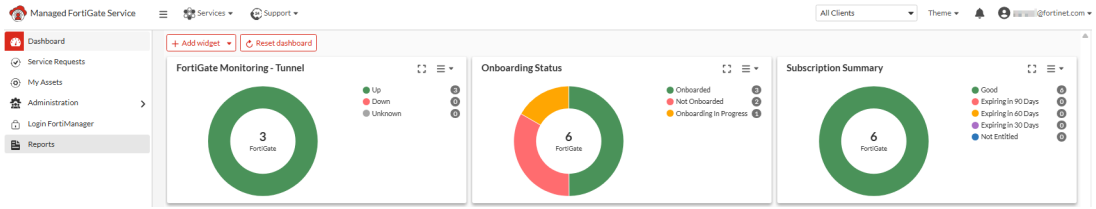
- View open change requests with their corresponding type and consult the change request calendar. See Dashboard on page 17.
- Create service requests or comment on existing requests. See Service Requests on page 19.
- View your asset list, including entitled devices, onboarded devices, expiring licenses, 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 Administration on page 28.
- Manage MSSP clients. See Administration on page 28.
- View reports available. See Reports on page 31.

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

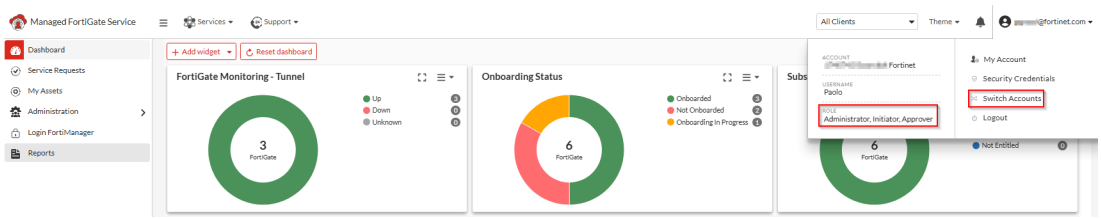
Portal customization

Several customization options are available on the portal:

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

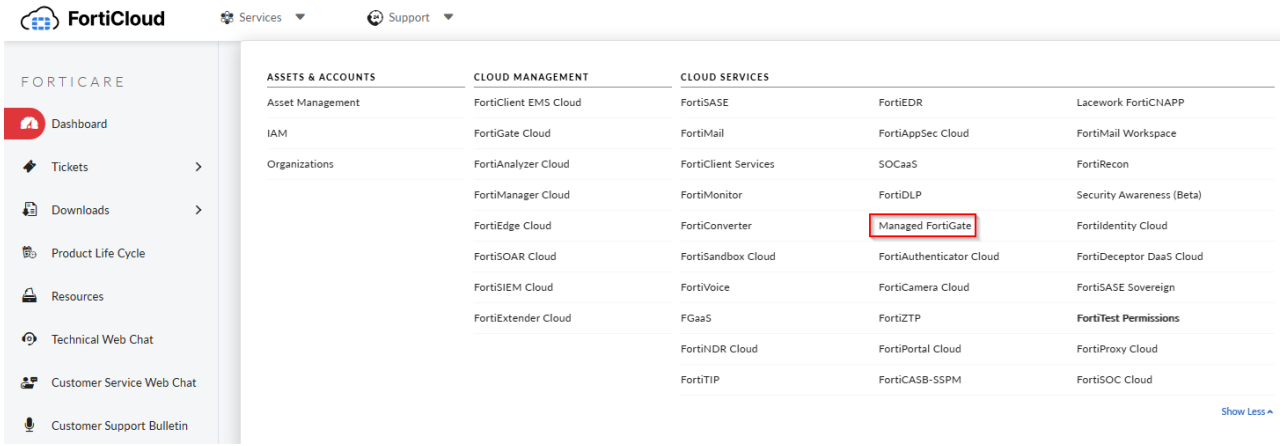


- To switch accounts, click the *Account* menu and select *Switch Accounts*.
- When you click on the account menu, the roles assigned to your user, such as *Administrator*, *Initiator*, or *Approver* are shown.



To access the Managed FortiGate Service portal:

1. Log in to FortiCloud.
2. In the FortiCloud banner, click *Services* > *Cloud Services* > *Managed FortiGate*.

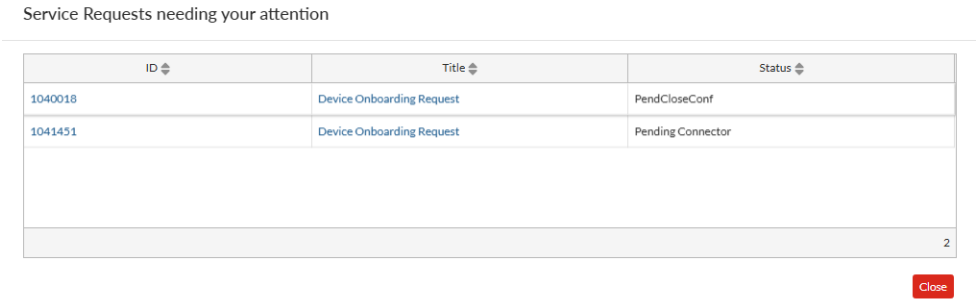


Pending Service Request popup window

When there are active service requests that need your input, a popup window will appear. This notification lists service requests with any of the following statuses: *Awaiting Customer Feedback*, *Pending Connector*, *Pending Approval*, *PendCloseConf*, *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.

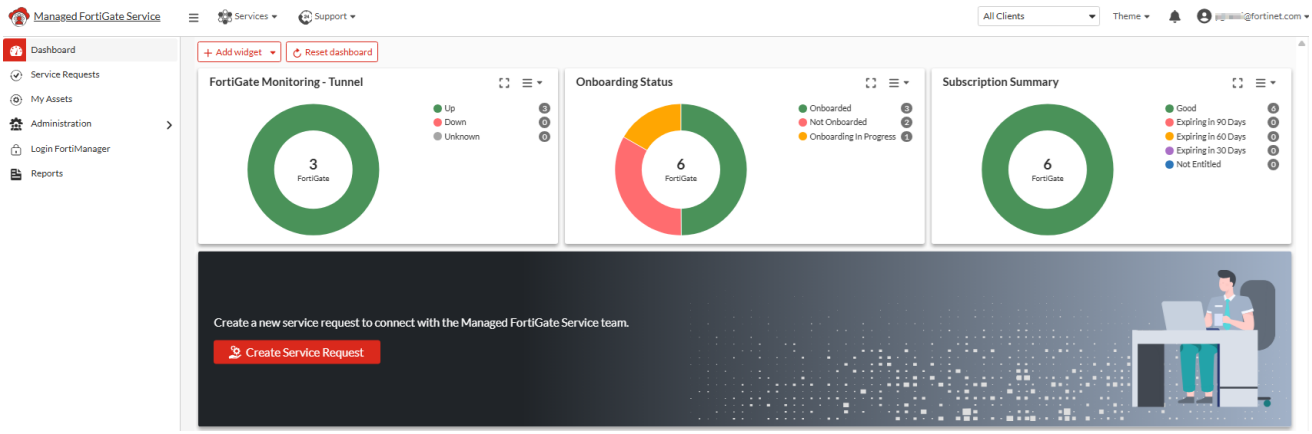
Once you close the Pending Service Request popup window, it will NOT appear again for the next 12 hours. For more information about service statuses, refer to Dashboard on page 17.



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.



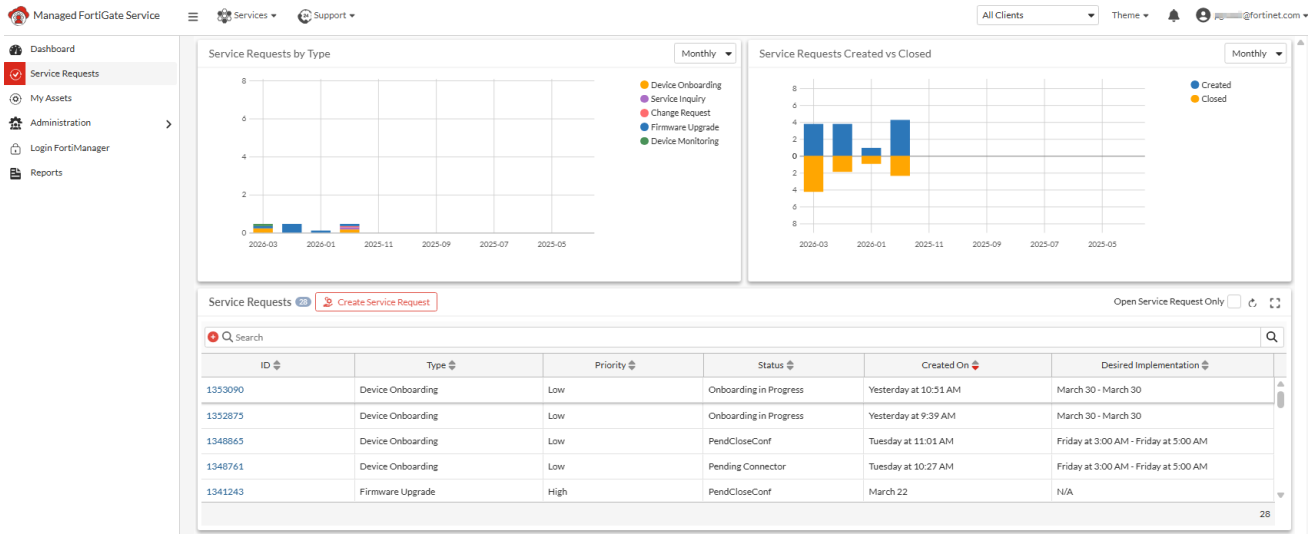
The following widgets are available on the dashboard:

Widget Name	Description
FortiGate Monitoring Tunnel	Management Tunnel status between FortiManager Cloud and onboarded FortiGates: • *Green*: Management tunnel is UP. • *Red*: Management tunnel is DOWN.
Onboarding Status	Onboarding status for FortiGate devices registered under the FortiCloud account: • *Not Onboarded*: FortiGate devices with a valid Managed FortiGate

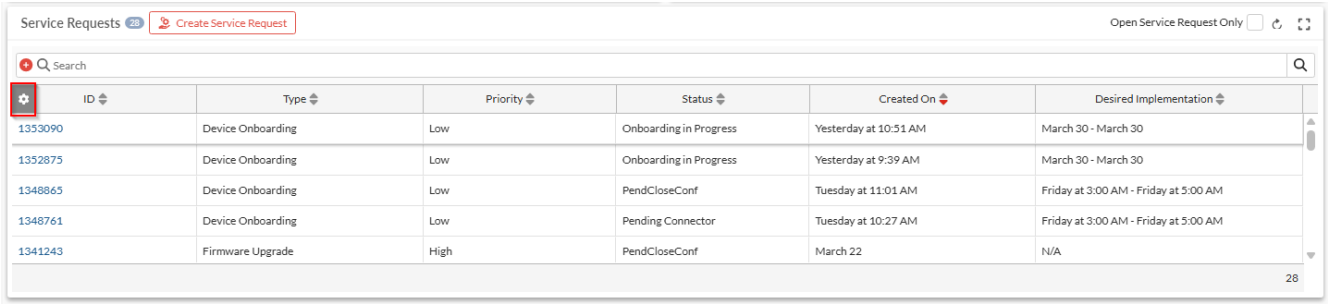
Widget Name	Description
	Service entitlement that have not yet been onboarded. • *Onboarded*: FortiGate devices onboarded to the service. • *Onboarding in Progress*: FortiGate devices currently undergoing the onboarding process.
Subscription Summary	Managed FortiGate Service entitlement status for FortiGate devices registered under the FortiCloud account. • *Good*: Entitlement expires in more than 90 days. • *Expiring in 90 days*: Entitlement expires in 90 days or less. • *Expiring in 60 days*: Entitlement expires in 60 days or less. • *Expiring in 30 days*: Entitlement expires in 30 days or less. • *Not Entitled*: Entitlement not applied.
Create Service Request	Static widget for creating Service Requests.
Change Calendar	Displays past and upcoming Service Requests of type *Firmware Upgrade* or *Change Request*, along with key details such as *ID*, *Title*, *Schedule*, and *Status*. By default, the "Open Service Requests Only" checkbox is selected, which excludes any Service Requests marked as *Canceled* or *Completed*.
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	Count of open change requests grouped by priority, including all request types: • *Low*: Changes that are not time-sensitive and can be scheduled for implementation at a later date. • *Medium*: Changes that are moderately urgent but do not require immediate action. • *High*: Business critical changes that must be implemented as soon as possible to avoid significant disruption or risks.
FortiGate Monitoring – Config Status	Config status between FortiManager Cloud and onboarded FortiGates: • *Synchronized*: The FortiManager Cloud configuration (revision history) aligns with the managed device configuration. • *Out of sync*: The FortiManager Cloud configuration (revision history) differs from the managed device configuration. • *Unknown*: The status cannot be determined becauseFortiManager 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 any of the following conditions persist for 10 minutes or more: • Managed FortiGate CPU usage ≥ 70% • Managed FortiGate Memory usage ≥ 80% • Managed FortiGate HA status = Out of Sync • FortiSwitch or FortiAP status ≠ Online Once the triggering condition is resolved, the request closes automatically.
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 may schedule the implementation for any date at least 5 working days from today. 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 *PendCloseConf*.	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

Status	Description	Action Pending On
Config Validation in Progress	The MFGS team is validating the FortiGate configuration file. The action is with the MFGS team.	MFGS team
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

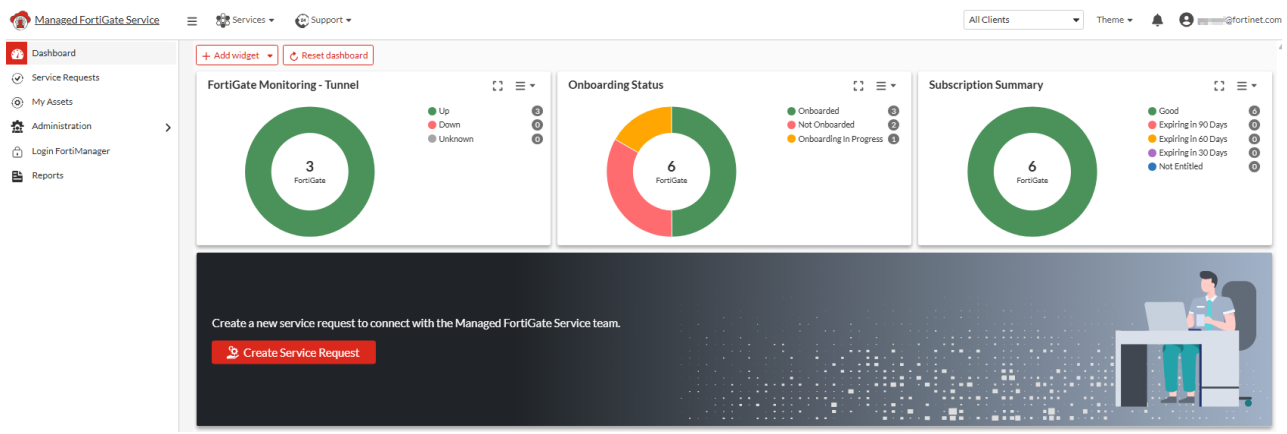
Status	Description	Action Pending On
RcvdCustFB	Status set automatically for any new customer comment posted. The action is with the MFGS team.	MFGS team
Researching	The MFGS team is looking into your inquiry and will contact you to review and discuss their findings. The action is with the MFGS team.	MFGS team
Sanity Check Completed	The MFGS team completed a sanity check on the target FortiGate. The action is with the customer.	MFGS team
Sanity Check in Progress	The MFGS team is performing a sanity check on the target FortiGate. The action is with the MFGS team.	MFGS team
Scheduled	The Service Request is scheduled to take place at the specified date and time. The action is with the MFGS team.	MFGS team

Creating service requests

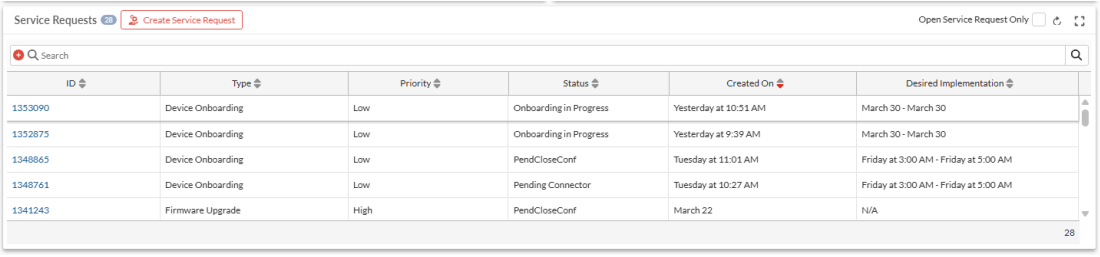
Only users with the *Initiator* role can raise service requests.

To create a service request:

1. On the Dashboard, click *Create Service Request*.



2. Alternatively, go to *Service Requests* and click *Create Service Request*.

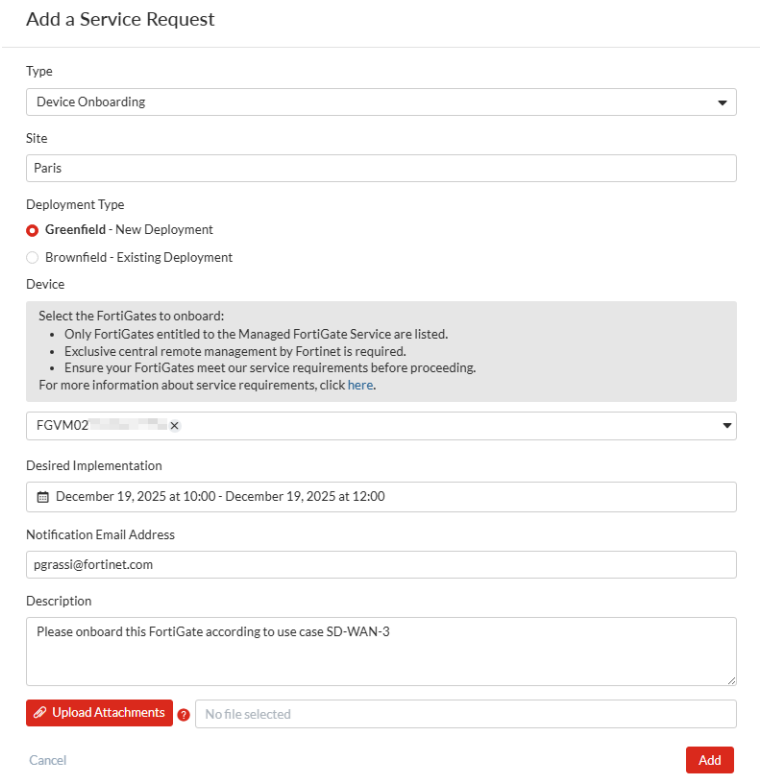


3. Enter the service request details:

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: • 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.

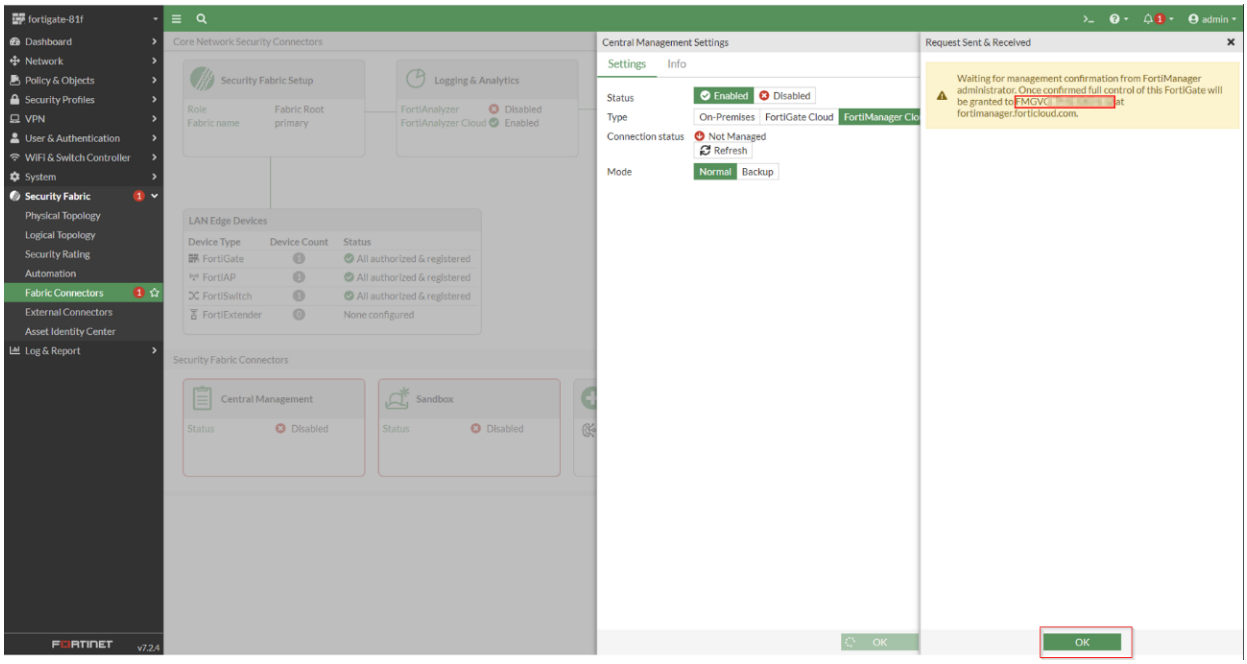


Enter the following details when submitting a Device Onboarding Service Request:

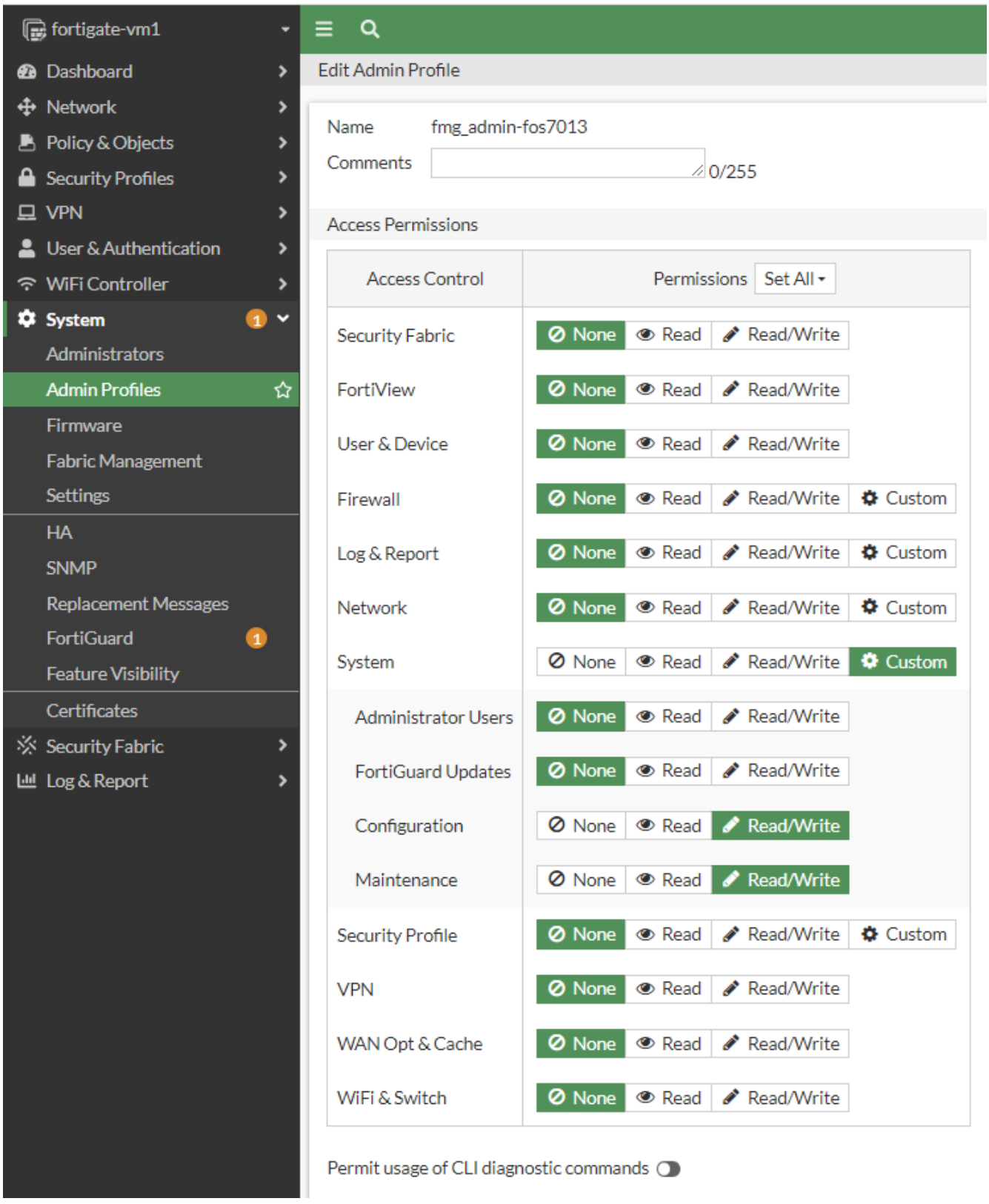
Type	Select Device Onboarding.
Client (MSSP customers only)	Identify the client associated with this Service Request.
Site	Enter the site name
Deployment Type	Select one of the following options: • *Greenfield*: New deployment that requires configuration by the Managed FortiGate Service team. • *Brownfield*: 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):


fortigate-vm1
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Administrators
Admin Profiles
Firmware
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
Edit Admin Profile
Name fmg_admin-fos7013
Comments 0/255
Access Permissions
Access Control
Permissions Set All
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.

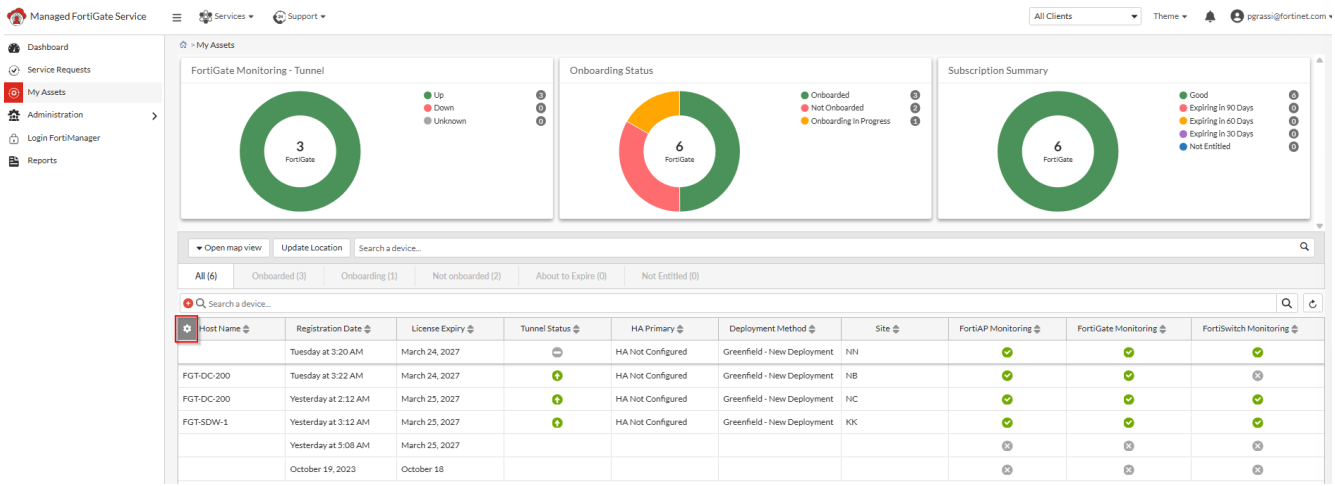
Once authorized, your FortiGate(s) will be added to the Managed FortiGate Service and an exclusive management tunnel will be established to the provisioned FortiManager Cloud instance.

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

My Assets

The My Assets page displays all FortiGates registered under the FortiCloud account and not decommissioned, 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 first column.



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

- *All*: All FortiGates registered under the FortiCloud account and not decommissioned.
- *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.

Administration

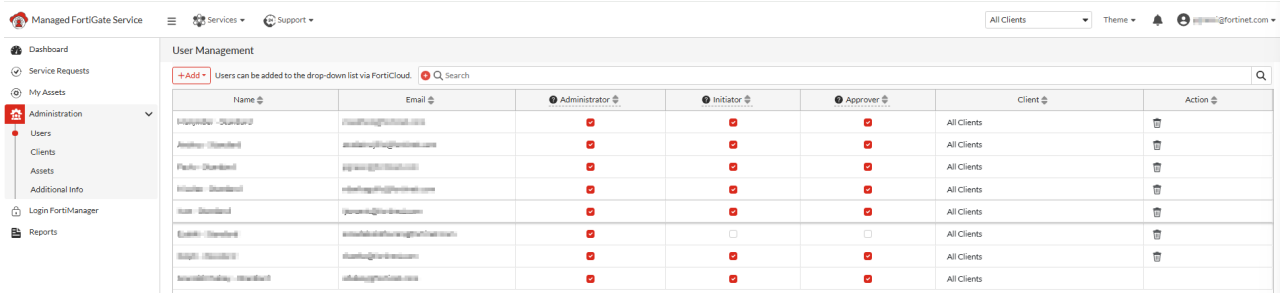
Only users with the Administrator role can access the Administration page.

The Administration page is where you manage administrative tasks on the MFGS portal. It's organized into the following sub-pages:

Users

The Users page lets you manage user access to the MFGS portal

- **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.



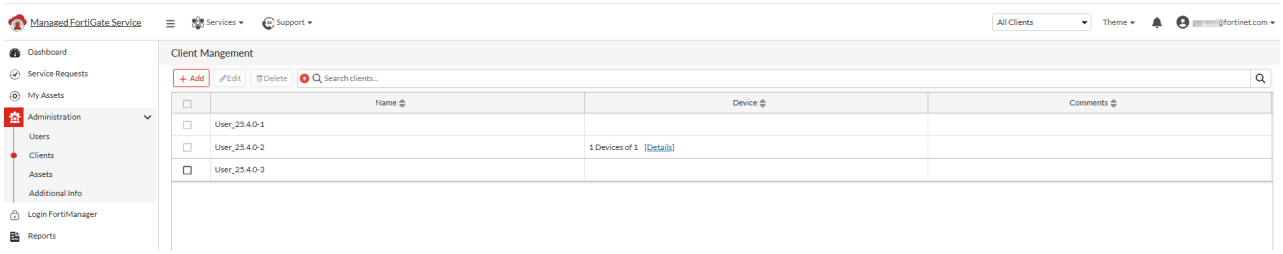
The *User Management* table can be customized by clicking the *Configure Table* icon, which appears when hovering over the first column.

Clients

The Clients page let you manage your clients on the MFGS portal:

- **Client Overview**: Displays the number of clients created and the FortiGates associated with each client, compared to the total onboarded in the FortiCloud account.
- **Edit Client**: Modify an existing client's name, comments, and associated FortiGates.
- **Delete Client**: Remove a client, provided it has no FortiGates currently associated with it.

- **Add Client**: Create a new client.

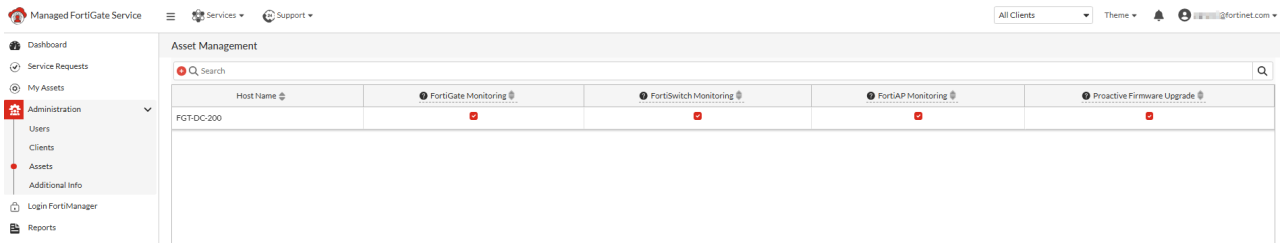


The Clients section is only accessible to users with the Administrator role on accounts onboarded as MSSP. The Administrator role requires access to All Clients, it cannot be limited to specific clients To add new devices to a specific client, submit a device onboarding service request.

Assets

The Assets page lets you enable monitoring for managed devices and configure proactive firmware upgrade requests.

- **FortiGate Monitoring**: A service request is automatically created if any of the following conditions persist for 10 minutes or more:
  - The management tunnel between FortiManager Cloud and the FortiGate is down.
  - CPU or memory usage exceeds the recommended threshold.
  - The HA status becomes Out of Sync
- **FortiSwitch Monitoring**: A service request is automatically created if the management tunnel between the FortiGate and any connected FortiSwitch remains down for 10 minutes or more.
- **FortiAP Monitoring**: A service request is automatically created if the management tunnel between the FortiGate and any connected FortiAP remains down for 10 minutes or more.
- **Proactive Firmware Upgrade**: A service request is automatically created if the FortiGate is affected by a PSIRT vulnerability, rated medium or higher, that can be resolved by upgrading to the recommended firmware version.



Additional Info

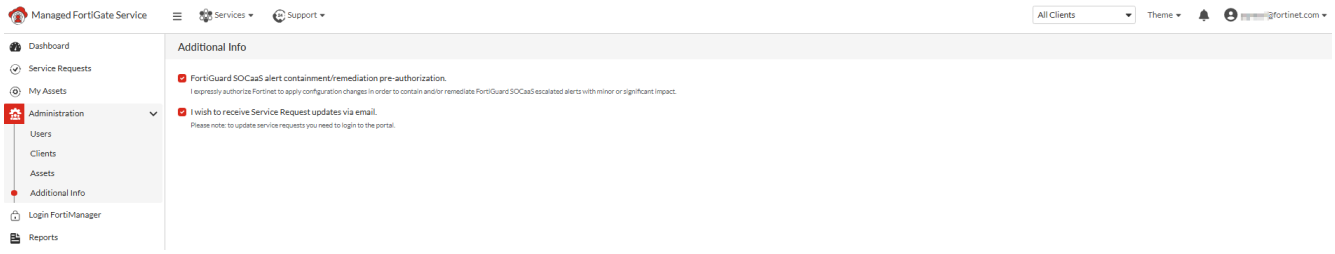
The Additional Info page lets you enable or disable the following options:

FortiGuard SOCaaS alert containment/remediation pre-authorization:

Enable this option if you have subscribed to both FortiGuard SOCaaS and Managed FortiGate services. This grants Fortinet pre-approval to apply configuration changes in response to escalated SOCaaS alerts — impact minor or significant — without requiring individual approval for each change request.

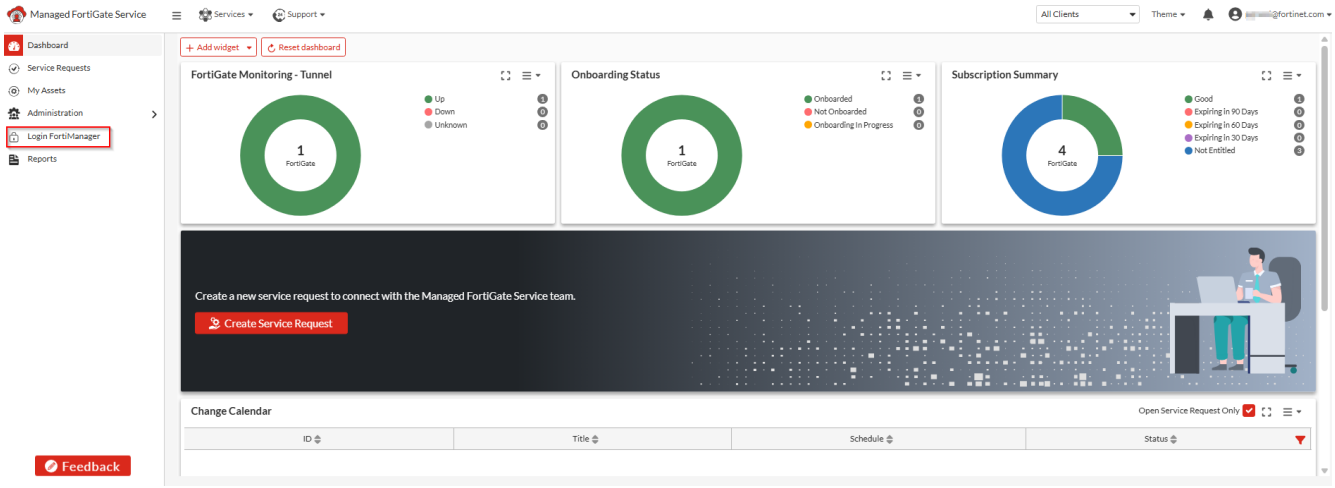
I wish to receive Service Request updates via email:

Enable this option to receive email notifications with the latest service request updates, including the three most recent comments, instead of a generic notification.



Login FortiManager

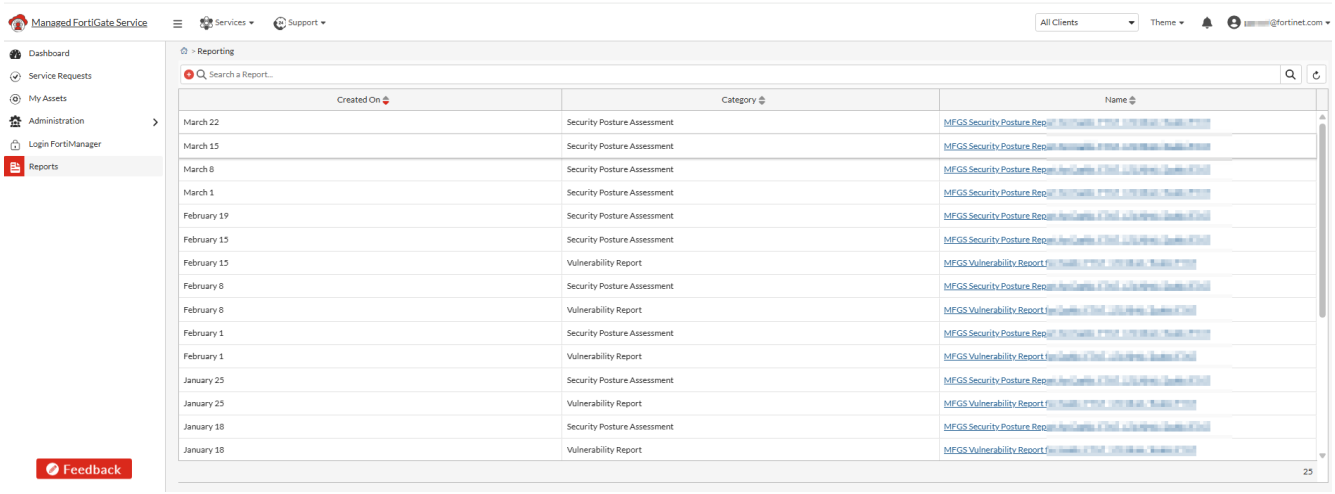
The *Login FortiManager* page redirects you to the FortiManager Cloud instance provisioned by the Managed FortiGate Service. Your access to this instance is limited to read-only mode.



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

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

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.

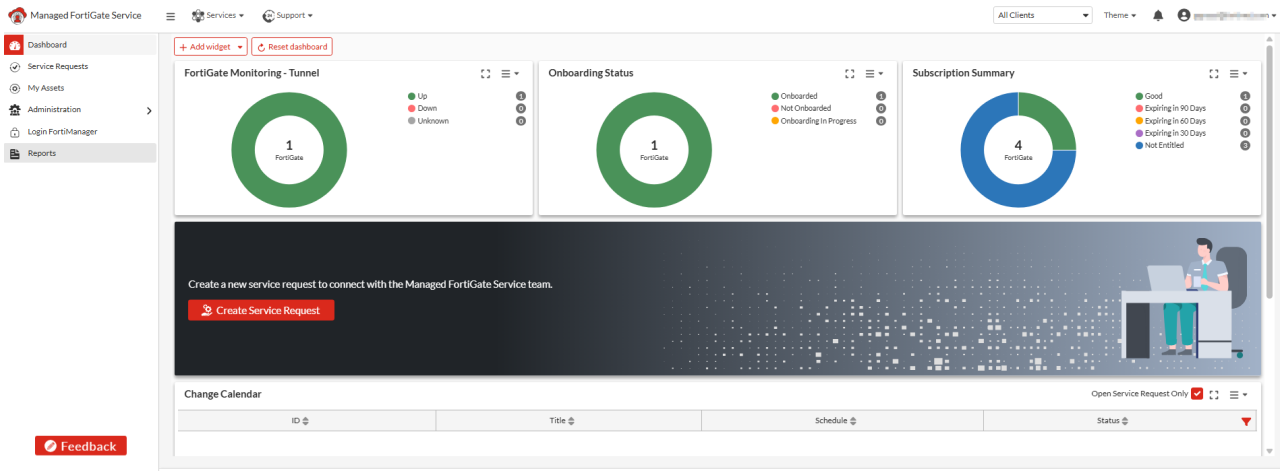
FortiGate devices with 2 GB of RAM running FortiOS v7.6.3 or later are excluded from this report due to an optimization introduced in v7.6.3

Submitting feedback

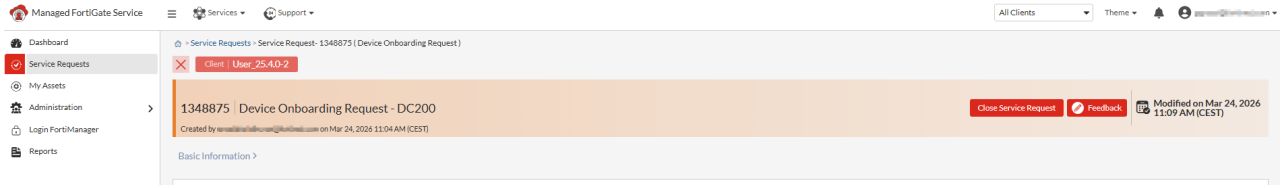
You can provide feedback on the quality of service by participating in surveys, which are accessible for active or recently closed service requests (within one month).

Several options are available to submit your feedback:

- On the portal page.

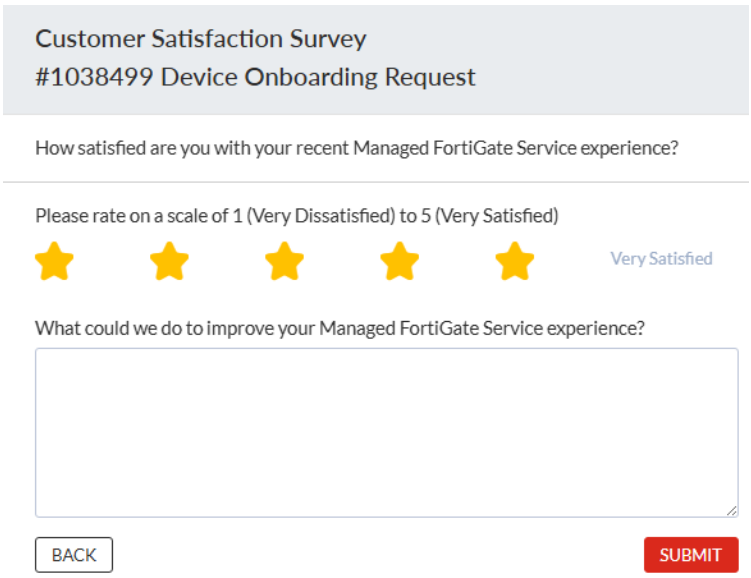


- On the service request banner.



- 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.



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