Administration Guide

FortiGate-as-a-Service 26.2

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

May 07, 2026
FortiGate-as-a-Service 26.2 Administration Guide
88-262-1286326-20260507

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-05-07	Initial release.

Introduction

FortiGate-as-a-Service (FGaaS) is Fortinet's security platform delivered as a service, providing dedicated Fortinet hardware with OPEX-based consumption, while preserving customer control, architectural flexibility, and compliance requirements.

FGaaS includes:

- FortiGate-as-a-Service (FGaaS) for network and security enforcement
- FortiManager-as-a-Service (FMGaaS) for centralized management
- FortiAnalyzer-as-a-Service (FAZaaS) for logging, analytics, and reporting

These services deliver physically isolated Fortinet appliances hosted in Fortinet-managed datacenters, combining the performance of dedicated hardware with the operational simplicity of cloud delivery. Customers retain full control over configuration, policies, and architecture, enabling customized deployments aligned with enterprise and regulatory requirements.

FGaaS is supported by FortiGuard security services, routable IP addresses, and guaranteed bandwidth, and is available through monthly FortiPoint consumption or annual SKUs. See Marketplace in the FortiCloud Asset Management guide for more information on FortiPoints.

FortiPoint values included in screenshots throughout this guide are for demonstrative purposes only. Refer to the product for exact FortiPoint charges.

The Data Centers that are currently supported include:

- Ashburn, USA
- Burnaby, Canada
- Chicago, USA
- London, England
- Madrid, Spain
- Paris, France
- Plano, USA

Getting started

To begin using the FortiGate-as-a-Service portal, review the following topics:

For more information, see the Getting Started guide.

Requirements

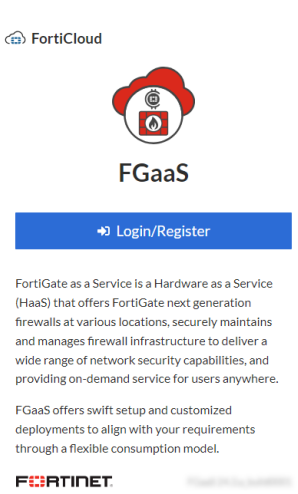
See the Getting Started guide for a list of requirements to use the FortiGate-as-a-Service portal.

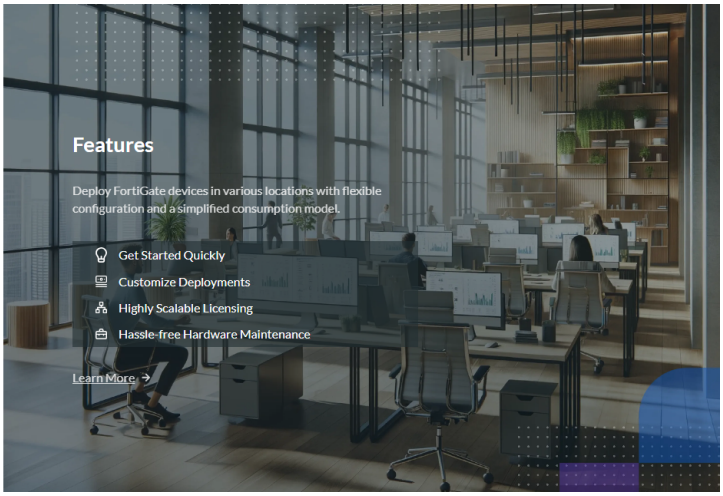
Logging into the FortiGate-as-a-Service portal

FortiGate-as-a-Service can be accessed through fgaas.forticloud.com. Portal permissions depend on the account being used to access the portal.

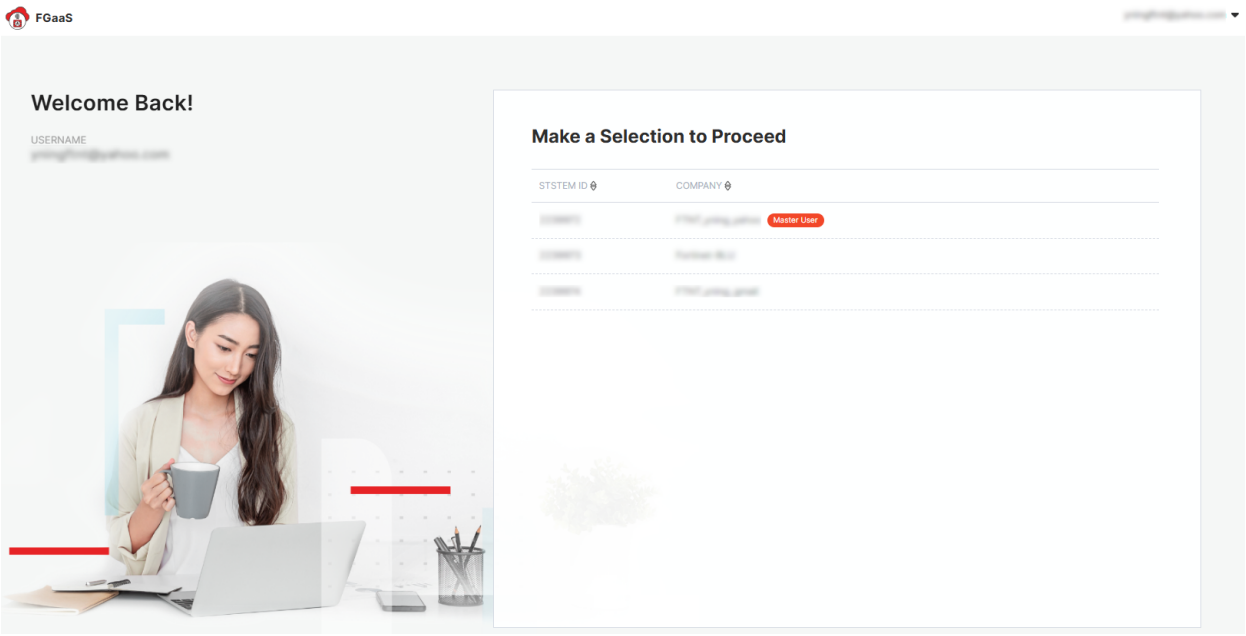
To log into FortiGate-as-a-Service:

1. Go to fgaas.forticloud.com.





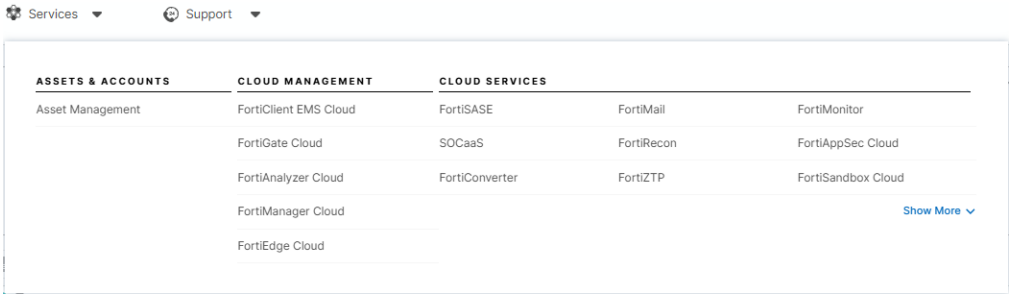
2. Click *Login/Register*.
3. Enter your account credentials and select *Log In*.
4. Select the account you want to use to access the portal.



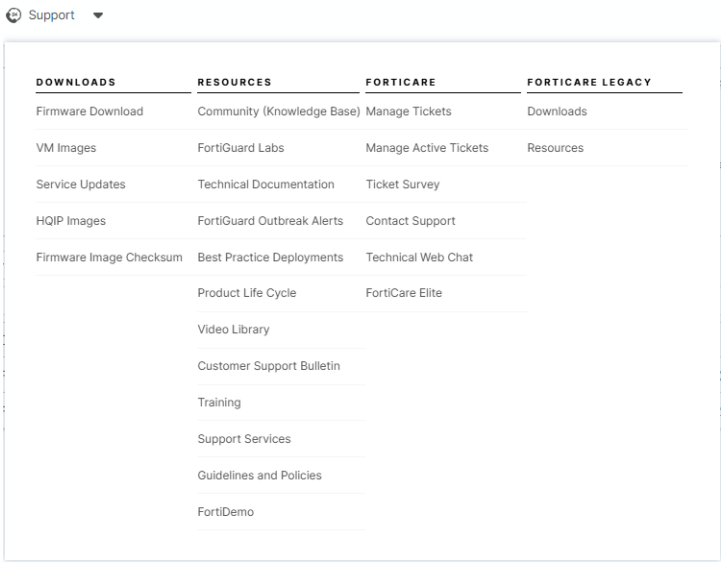
Banner

The top banner of the FortiGate-as-a-Service console provides access to account services, support, and functionality.

The *Services* menu allows you to access other portals included in your account permission scope. Select *See More* to view more available portals.



The *Support* menu allows you to access support features, such as the FortiCare ticketing portal.

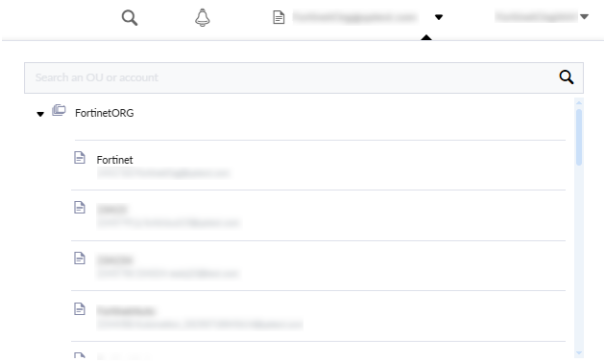


This section includes the following:

User menu

View the username and account information of the currently logged in user.

If this account is part of an Organization, use this menu to switch to another account. For more information on Organizations, see the FortiCloud Organization Portal guide.

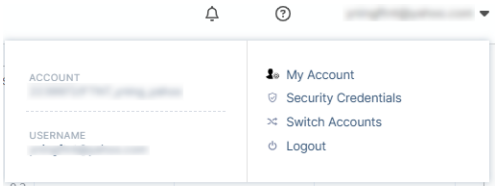


Account menu

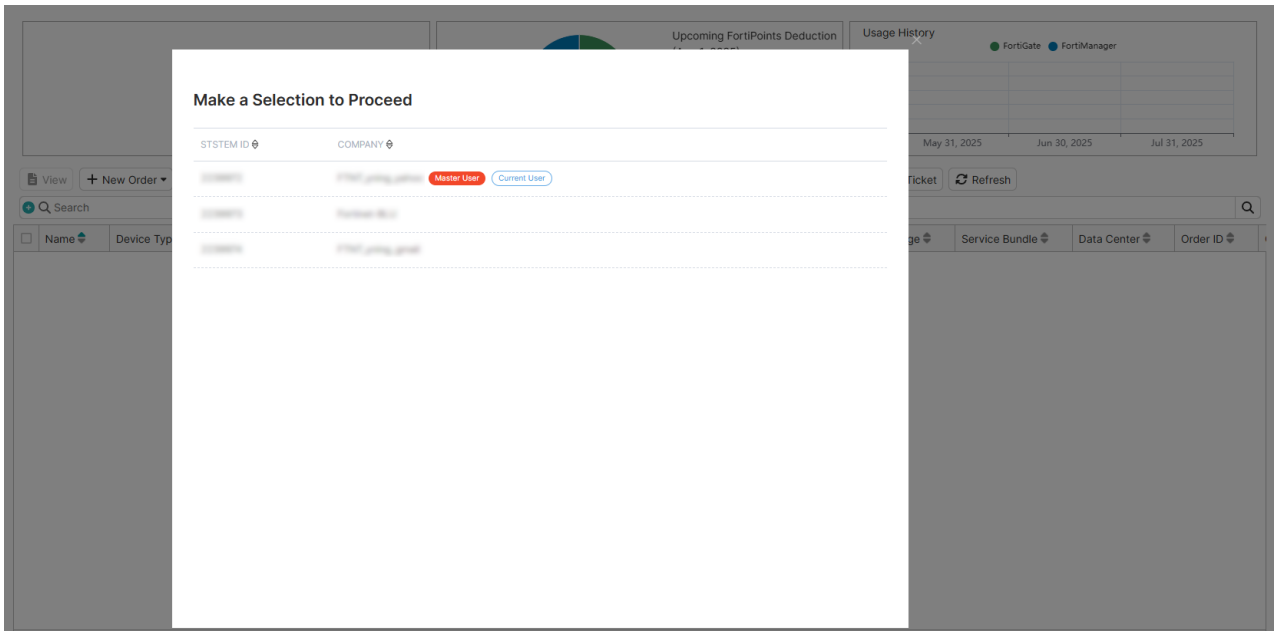
The account menu displays the account username and provides access to the following:

- *My Account*: Access your account details.
- *Security Credentials*: Access your security preferences.
- *Switch Accounts*: Switch to another connected account.

- *Logout*: Log out of FortiGate-as-a-Service.



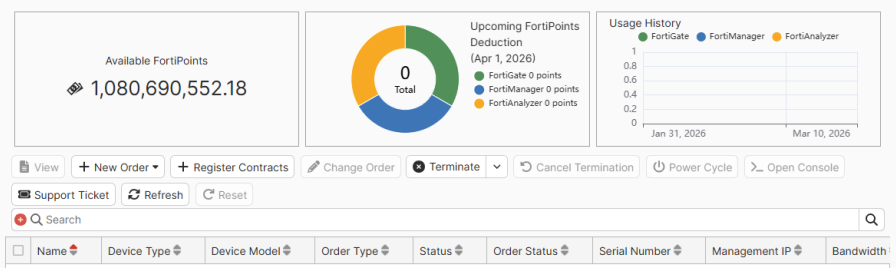
If you have multiple accounts, selecting *Switch Accounts* will display a dialog list of your available accounts. This list will align with the account list presented when logging in. See Logging into the FortiGate-as-a-Service portal on page 7.



For more information on the account menu, see Account management in the FortiCloud IAM guide.

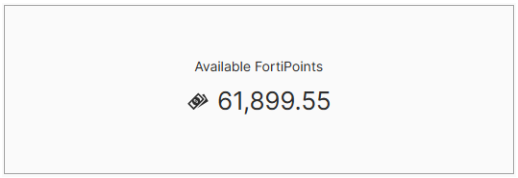
Devices

The *Devices* page displays the details of your devices and the status of your account's FortiPoints balance.

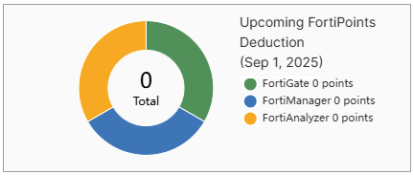


The status of your account's FortiPoints are displayed at the top of the page:

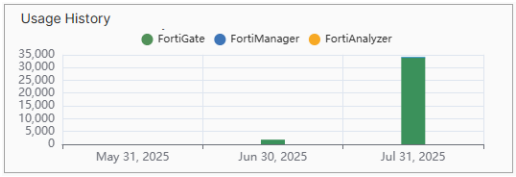
- The *Available FortiPoints* field denotes the current FortiPoints balance of your account.



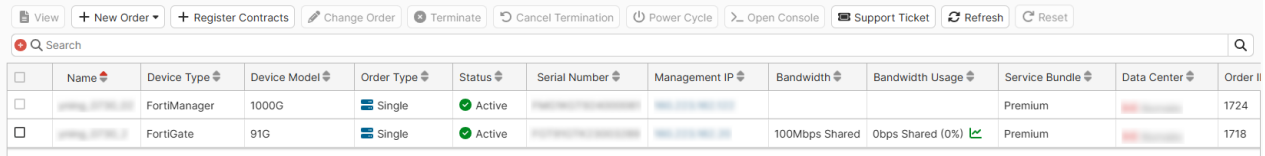
- The *Upcoming FortiPoints Deduction* graph presents upcoming usage of FortiPoints for pending orders. It displays the next billing date and amount, categorized by device type to show the proportion of costs.



- The *Usage History* graph displays the amount of FortiPoints previously spent each month, categorized by device type to show the proportion of costs.



Existing device orders and contracts are listed in the *Devices* table. You can control your orders, including updating and changing the order details, terminating the device, and power cycling the device.



Each row of the *Devices* page displays a single order. For HA-type devices, select the + to expand the rows to view the sub-devices.

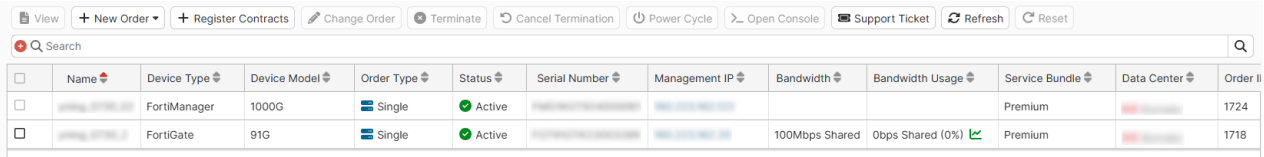
> You should not change HA-related settings. Any HA changes may impact the ability to reach your devices.
>
> Single devices may be marked as the primary HA device. This is by design and should not be changed.

> Devices added through registered contracts cannot be terminated. See Contract-based orders on page 37.

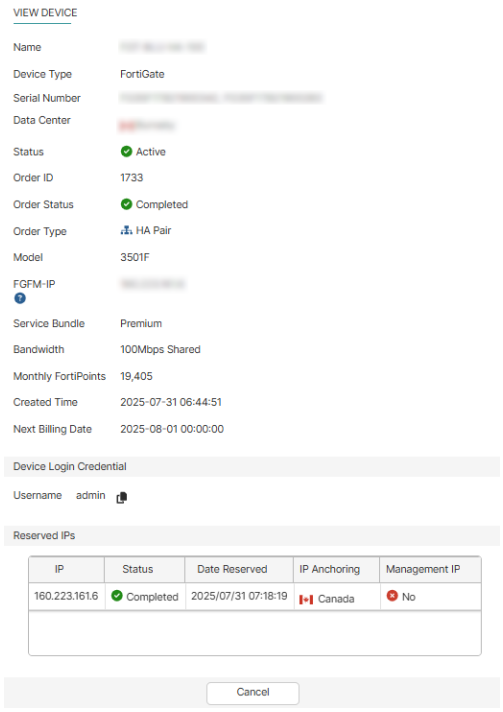
This section includes:

Viewing device details

Select a device and click *View* to review details of the order.

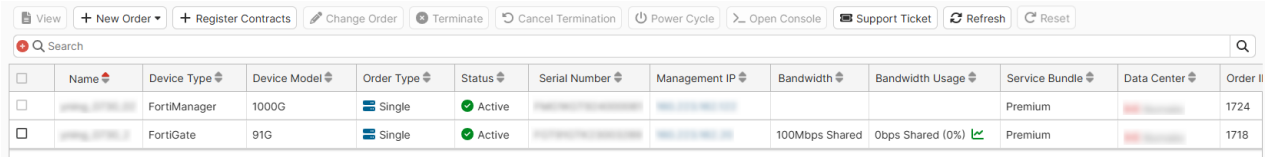


The *View Device* page includes details on the device from the *Devices* page, your login credentials, and the reserved IP addresses.

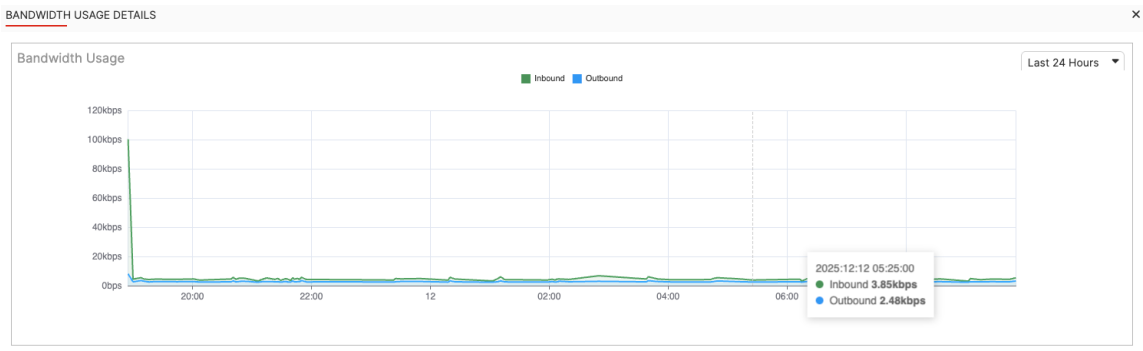


Bandwidth usage

The current bandwidth usage of a device is included in the *Realtime Bandwidth Usage* column.



Select an entry in the column to view a detailed report of the usage over time. If bandwidth exceeded the usage threshold, the event is noted in the table.



Select the dropdown menu to select the time frame displayed.

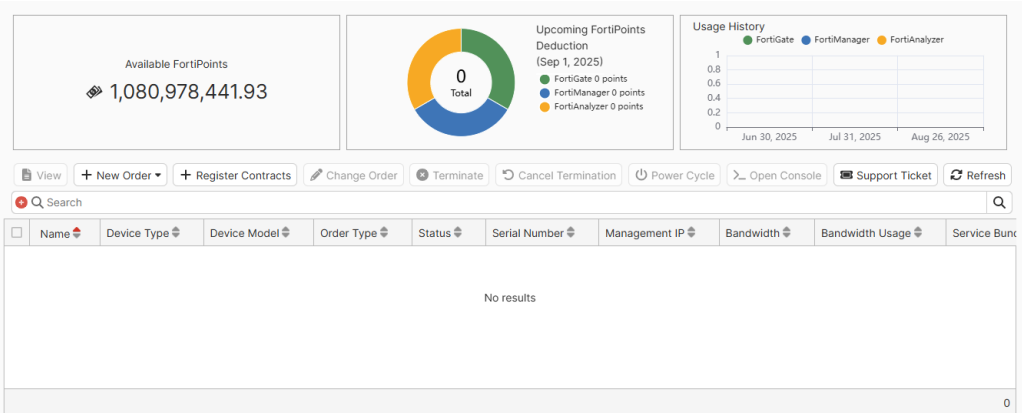
Creating a new order

You can create an order for a new device using the *New Order* button on the *Devices* page.

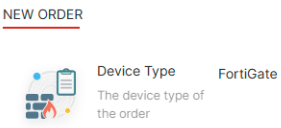
> Orders created in this method use FortiPoints. For information on ordering devices using registered SKUs, see Contract-based orders on page 37.

To create a new FortiGate order:

1. Go to *Devices*.



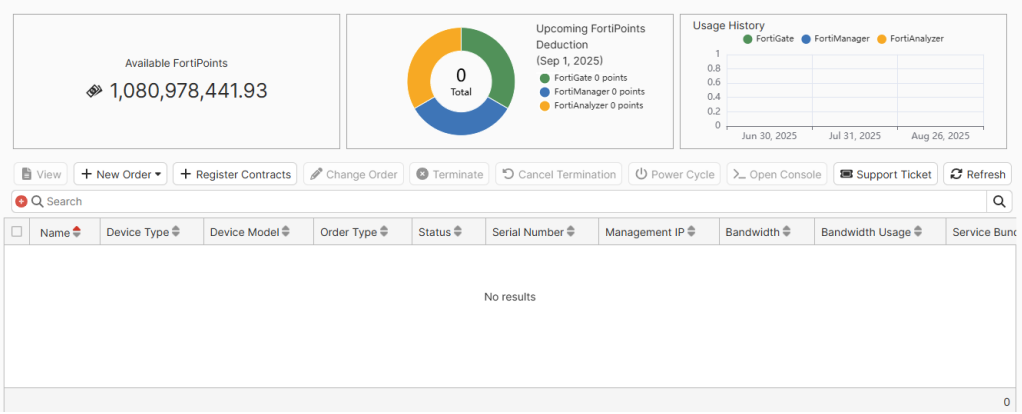
2. Select *New Order* > *FortiGate*. The *New Order* page will display.



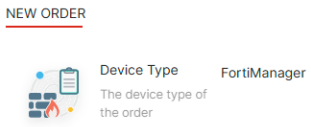
3. Configure the FortiGate. See Creating a FortiGate order on page 30 for more information.

To create a new FortiManager order:

1. Go to *Devices*.



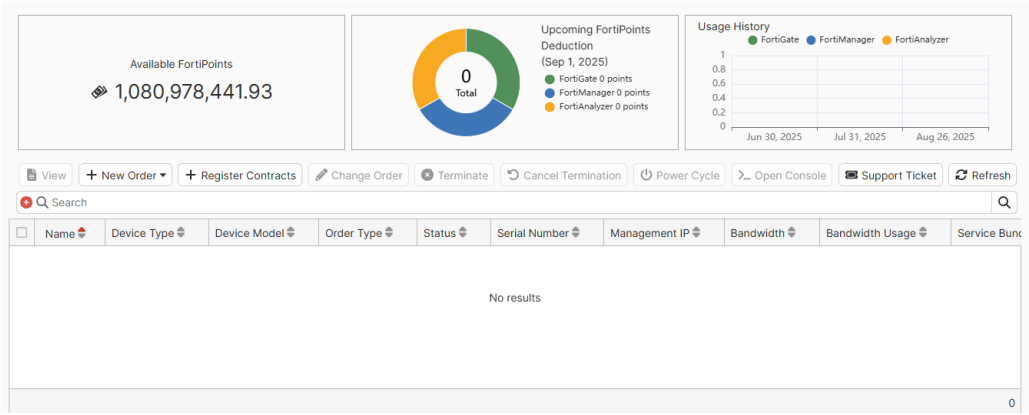
2. Select *New Order* > *FortiManager*. The *New Order* page will display.



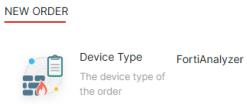
3. Configure the FortiManager. See Creating a FortiManager order on page 32 for more information.

To create a new FortiAnalyzer order:

1. Go to *Devices*.



2. Select *New Order* > *FortiAnalyzer*. The *New Order* page will display.



3. Configure the FortiAnalyzer. See Creating a FortiAnalyzer order on page 34 for more information.

Service quotas

The following is a list of the default service quotas for FortiGate-as-a-Service:

- Total rentable devices per customer: 2
- Total IP addresses per device: 5
- Maximum bandwidth per device: 10Gbps Shared

> If you reach the service quota limit, open a Service Request within the FortiGate-as-a-Service portal to request a quota increase. See the Service Requests on page 50.

Changing an existing order

You can change the order specifics of a device using the *Change Order* button. Once you select *Change Order*, the *Order* > *Change Order* page will display. See Changing an order on page 36 for more information.

Terminating a device

You can define the termination date of a device from the *Devices* page. Devices can be defined to terminate on either the billing date or immediately.

The *Terminate Immediately* option allows administrators to immediately terminate an active FGaaS instance when the service is no longer required. When this action is executed, the associated firewall instance is permanently removed and the service is stopped without waiting for the scheduled termination or billing cycle. This capability helps organizations quickly decommission unused resources, control costs, and free up allocated infrastructure when environments are being retired, replaced, or re-architected.

Once you terminate a device, you are canceling the order. The terminated device and all service entitlements, including the services IP addresses, and bandwidth, will be removed permanently from your account.

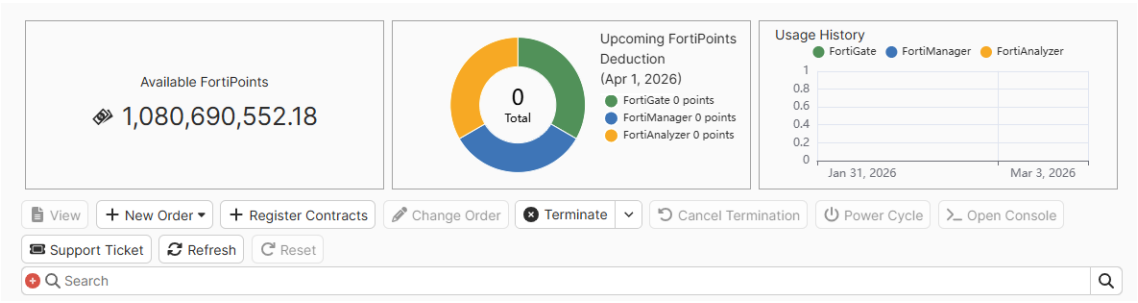
Terminating a FGaaS instance will immediately will stop the service and permanently remove the associated device. Any active traffic sessions will be interrupted, and the configuration will be deleted. This action cannot be undone. Be sure before you want to continue.

For HA-type FortiGates, you can only terminate the primary list. You cannot terminate a sub-FortiGate within the list.

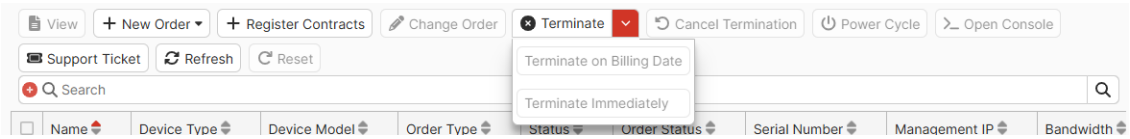
Devices added through registered contracts cannot be terminated. See Contract-based orders on page 37.

To terminate a device:

1. Go to *Devices*.



2. Select the device you want to cancel.
3. Click the *Terminate* dropdown menu to select the termination date:
   - *Terminate on Billing Date*
   - *Terminate Immediately*



The *Terminate Device* pane will display.

4. Enter the provided phrase in the *Security Check* field.
5. Click *OK*.

Canceling a scheduled device termination

If you no longer wish to terminate a device that was set to *Terminate on Billing Date* and the next billing date has not yet occurred, you can cancel the termination.

To cancel a scheduled termination:

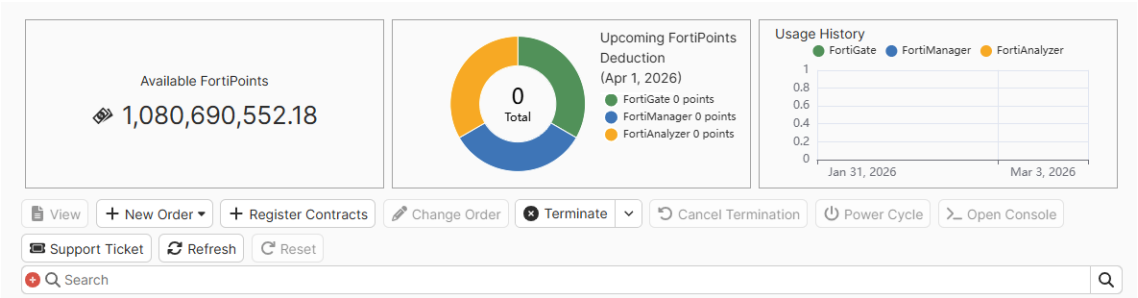
1. Go to *Devices*.
2. Select the device that has been scheduled for termination.
3. Click *Cancel Termination*. A confirmation dialog is displayed.
4. Click *OK*.

Power cycling a device

You can power cycle your device using the *Power Cycle* feature. Power cycling will impact the device's connections and lose any unsaved changes.

To power cycle your device:

1. Go to *Devices*.



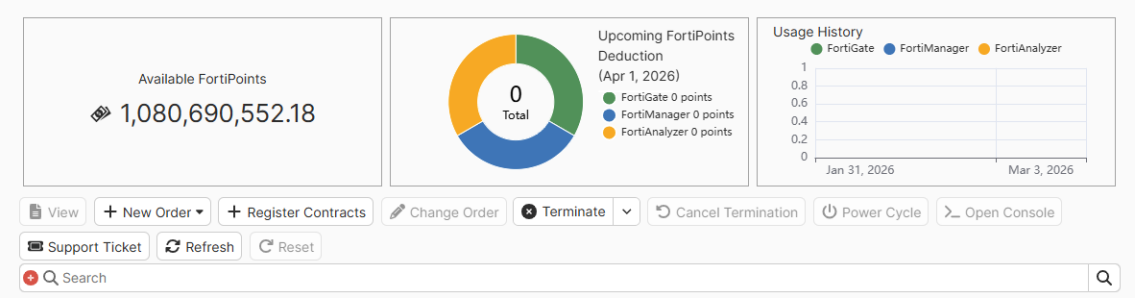
2. Select the device you want to reboot.
3. Click *Power Cycle*.
4. Click *OK* on the warning message to confirm.

Creating a support ticket

You can create a support ticket by selecting *Support Ticket*. See the FortiCare guide for more information on creating tickets.

Refreshing the list of devices

You use the *Refresh* button to update the *Devices* page details, such as *Status*.



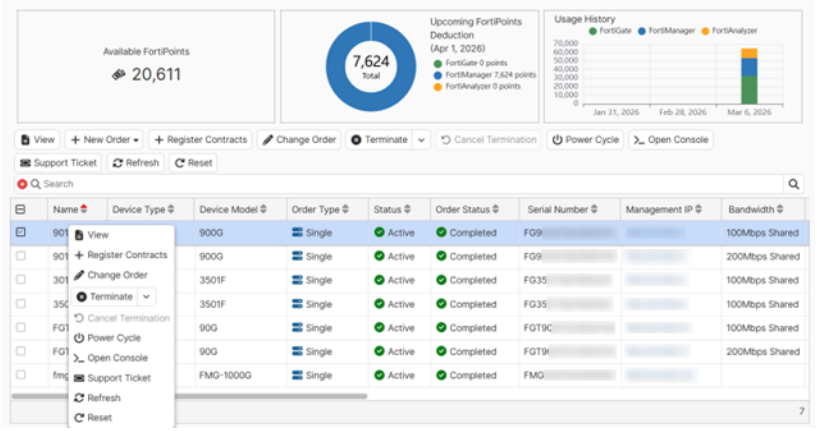
Restoring a device to provisioning

The *Reset* to provisioned state feature allows a FGaaS firewall instance to be quickly restored to its original provisioned configuration. This capability removes all runtime configuration changes and returns the device to the baseline state defined during initial deployment. It enables administrators and service providers to rapidly recover from configuration drift, testing changes, or operational issues without requiring manual reconfiguration or device replacement. By restoring a known good state in minutes, this feature simplifies troubleshooting, improves operational consistency, and ensures the firewall remains aligned with the intended service architecture

> ⚠ Resetting the device will restore it to its original provisioned state. All current configuration changes will be permanently removed and cannot be recovered. This action may interrupt active traffic and services. Be sure before you want to continue.

To restore a device to its provisioned state:

1. Go to *Devices*.
2. Select the device you would like to restore to its provisioned state.
3. Restore the device:
   - Right click the device and select *Reset*.
   - Select *Reset* in the banner options.



4. On the *Reset Device* pane, enter `Reset` in the Security Check field to confirm the intention to restore the device to its provisioned state.
5. Click *OK*. The process may take approximately 15 minutes to reset.

Accessing devices

Once orders have been completed, you can access your device instances from the FortiGate-as-a-Service portal. Once you have accessed the device and logged in, you can begin to use the device, such as create further policies, review traffic, and so on.

This section includes the following:

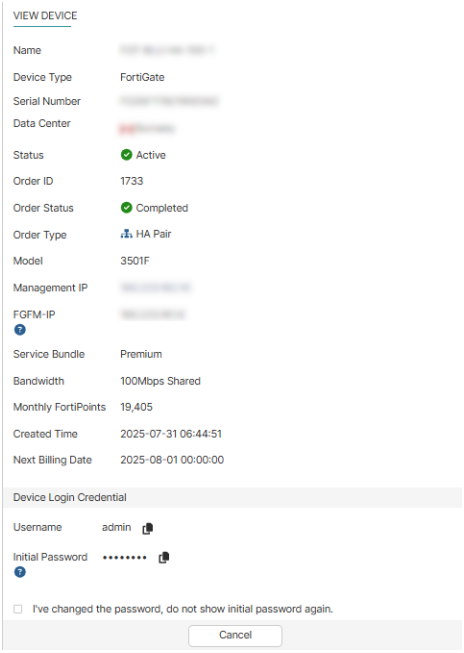
- Accessing the FortiGate from FortiGate-as-a-Service on page 19
- FortiCare registration requirements for FortiManager on page 21
- Accessing FortiManager from FortiGate-as-a-Service on page 22
- Accessing FortiAnalyzer from FortiGate-as-a-Service on page 26

Accessing the FortiGate from FortiGate-as-a-Service

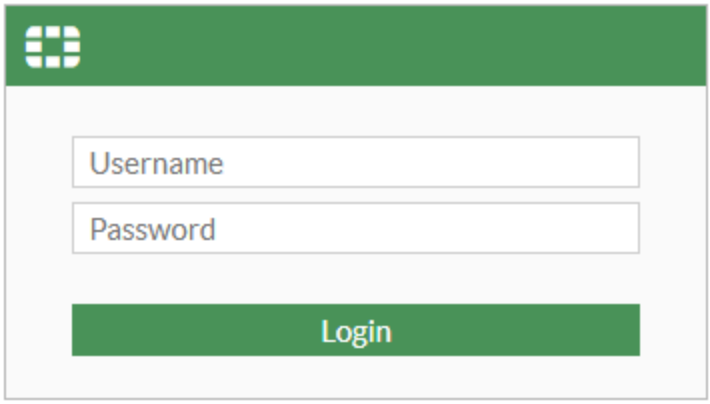
The FortiGate can be accessed from the *Devices* page.

To access the FortiGate:

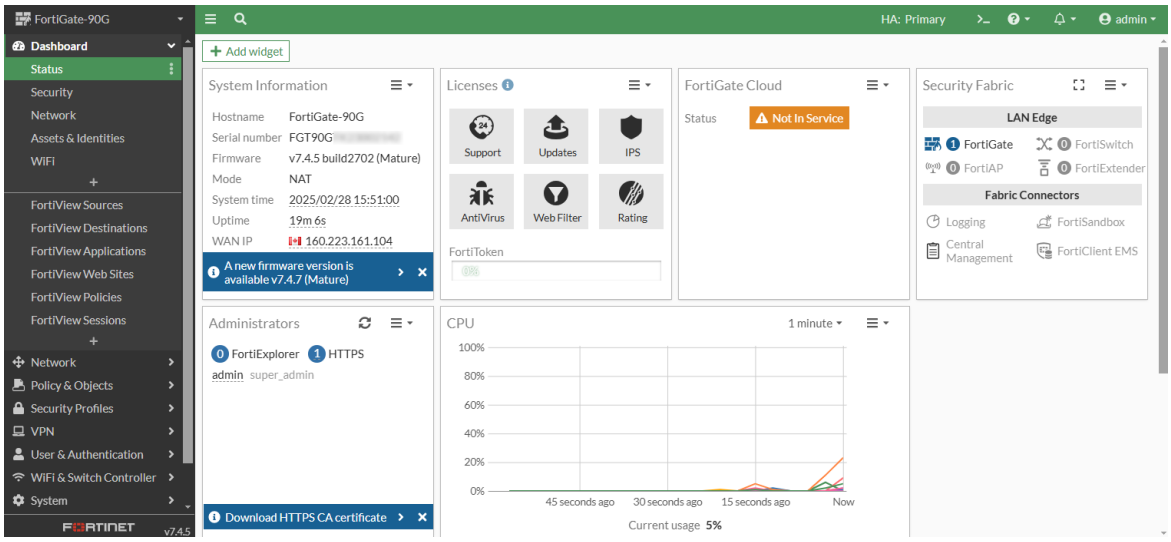
1. Order a FortiGate. See Creating a new order on page 14.
2. Once the order status is *Complete*, go to *Devices* and select the FortiGate order to view more details.



3. Copy the *Username* and *Initial Password* to your device.
4. Select the *Management IP*. The FortiGate credentials page is displayed.



5. Enter the *Username* and *Initial Password* into the provided fields.
6. Click *Login*. The FortiGate instance will open.



FortiCare registration requirements for FortiManager

When you access FortiManager for the first time, a setup wizard is displayed that includes a FortiCare registration step. The FortiCare registration step cannot be skipped.

To ensure successful registration to FortiCare, configure the outbound rules in the security group associated with FortiManager to allow the following traffic:

- HTTPS (TCP/443)
- DNS (UDP/53)

This configuration enables the device to connect to and register with FortiCare automatically.

See Security Group on page 43 for more information.

Post-registration

Once the FortiManager device has been successfully registered with FortiCare and has downloaded the associated entitlements, the outbound rules are no longer required and can be removed from the security group if desired.

Troubleshooting

If the device is not registered to FortiCare:

1. Verify that the security group allows TCP/443 and UDP/53 outbound.
2. After updating the security group, wait for a short period.
   The device will automatically attempt to connect and complete the registration process.

Accessing FortiManager from FortiGate-as-a-Service

FortiManager can be accessed from FortiGate-as-a-Service after an order has been completed. Once the device has been configured, FortiGate devices ordered through FortiGate-as-a-Service can be added to the FortiManager.

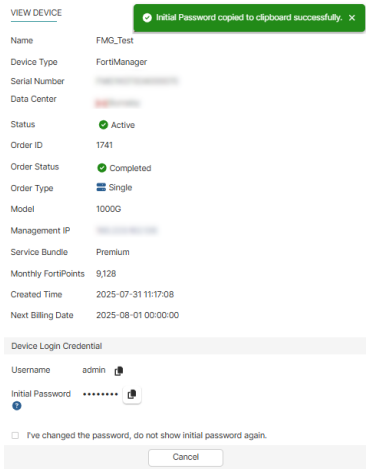
FortiManager and FortiAnalyzer devices require FortiCare registration. Temporary outbound rules in the associated security group can aid automatic FortiCare registration when you access the device for the first time. See FortiCare registration requirements for FortiManager on page 21 for more information.

Accessing a FortiManager instance

After a FortiManager order has completed, the FortiManager instance can be accessed through FortiGate-as-a-Service.

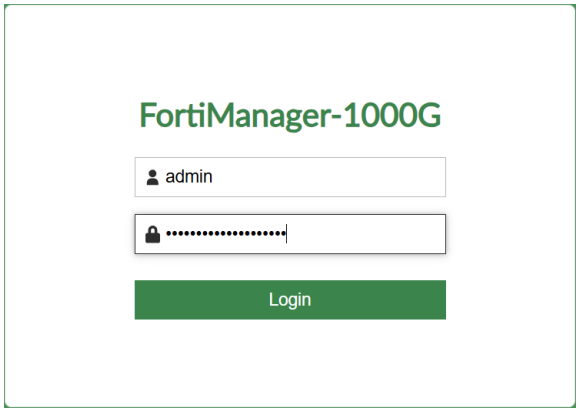
To access FortiManager:

1. Go to *Devices*.
2. Select *New Order* > *FortiManager*.
3. Define the *Management Security Group*:
   - To allow access to every network, select the default *allow_all* security group.
   - To allow access to only a specific network or client:
     i. Create a custom security group with inbound and outbound rules defined to only allow a specific client IP address to access the FortiManager instance. See Creating a security group on page 43.
     ii. Select the custom security group.
4. Configure the other FortiManager order fields, as needed.
5. Click *Place Order*.
6. Once the order status is *Complete*, go to *Devices* and select the FortiManager order to view more details.
7. Copy the *Username* and *Initial Password* to your device.

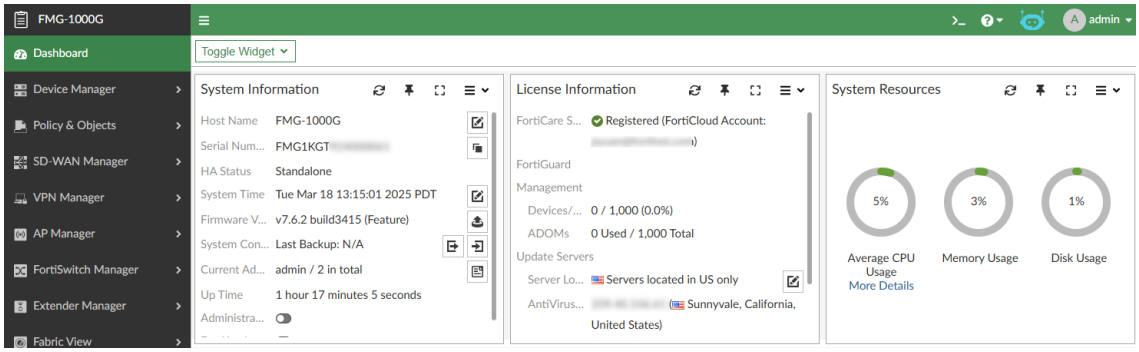


8. Select the *Management IP*. The FortiManager credentials page is displayed.

9. Enter the *Username* and *Initial Password* into the provided fields.



10. Click *Login*. The FortiManager instance will open.



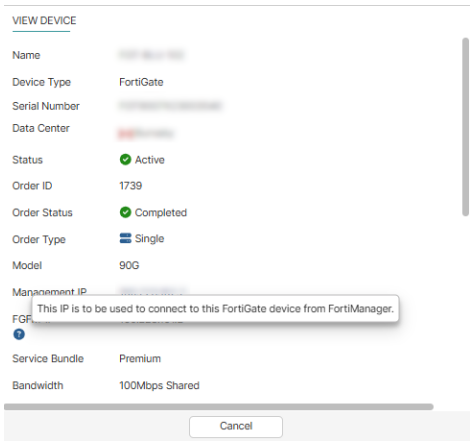
Adding a FortiGate device to FortiManager

Once you have configured the FortiManager instance, you can add your FortiGate device to the *Device Manager*.

> The FortiGate and FortiManager orders must be listed as *Active* and *Complete* in the *Devices* page. The FortiGate may be a part of a FortiPoints order or a registered contract.

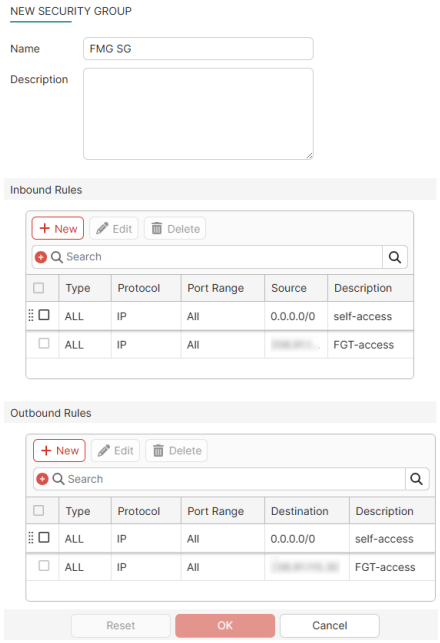
Adding FortiGate devices to the FortiManager instance:

1. Go to *Devices*.
2. Access and log into the FortiGate instance. See Accessing the FortiGate from FortiGate-as-a-Service on page 19.
3. In the FortiGate device details in FortiGate-as-a-Service, identify the *FGFM-IP* address.



This address will be used to add the FortiGate device to the FortiManager and allow traffic to pass.

4. Go to *Security Group*.
5. Create a security group for your FortiManager instance that allows access to the FortiGate:
   - Create inbound and outbound traffics to allow you to access the FortiManager. For example, select *Anywhere* or *Custom > My IP* for the *Source* and *Destination* fields.
   - Create an inbound and outbound rule that allows traffic from the FortiGate's *FGFM-IP* address.

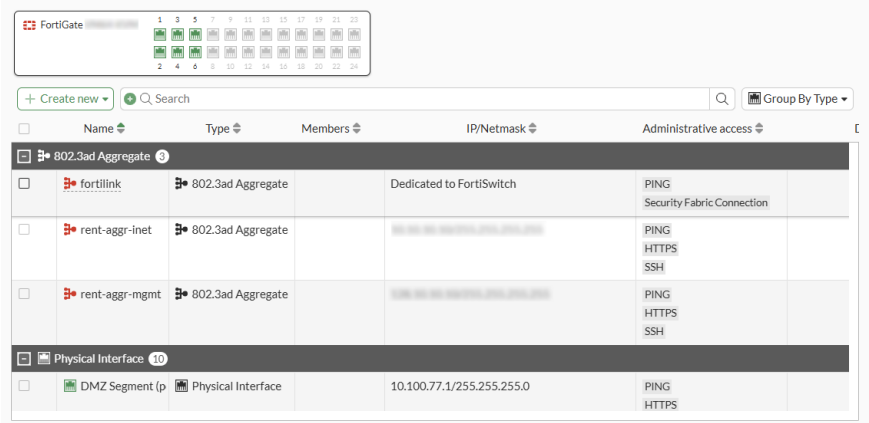


See Creating a security group on page 43.

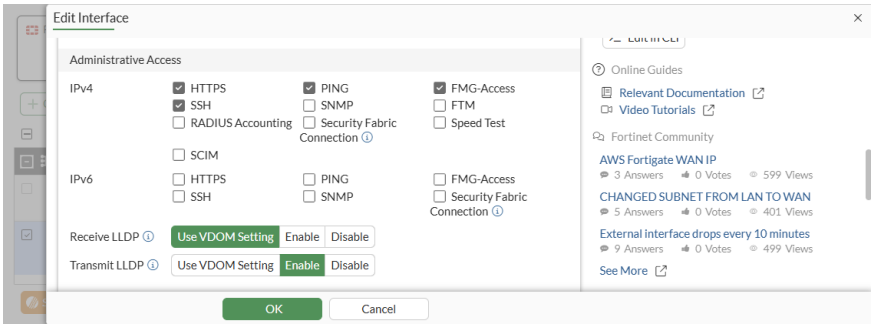
> The security group of the FortiGate may be customized, as needed, but should include access for the FortiManager instance as well.

6. Go to *Orders*.
7. For the FortiManager order, select *Change Order*.
8. Replace the *Management Security Group* with the new security group to allow access to the FortiGate. See Changing an order on page 36.
9. Allow FortiManager access from the FortiGate:

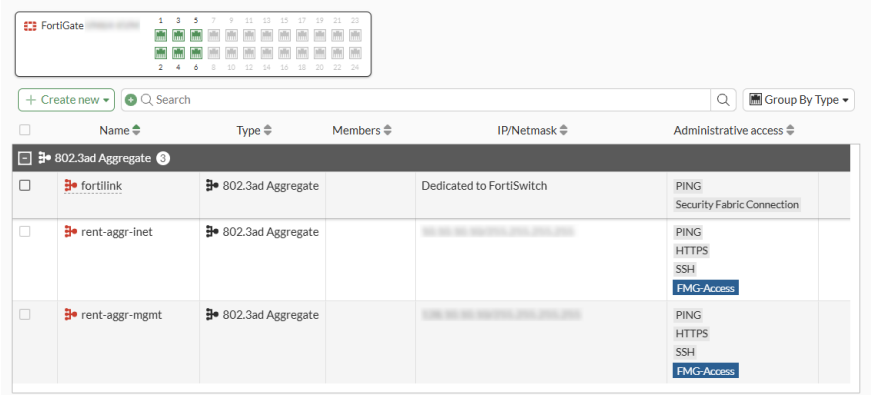
a. Go to *Devices* and access the FortiGate instance again.
b. Go to *Network* > *Interfaces*.



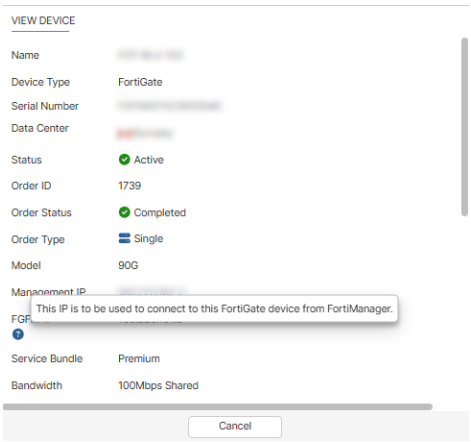
c. Edit the *rent-aggr-inet* interface.
d. In *Administrative Access*, enable *FMG-Access* for *IPv4*.



e. Click *OK*.
f. Perform the same steps to enable *FMG-Access* in the *rent-aggr-mgmt* interface.



10. Add the FortiGate device to the FortiManager instance:
    a. Go to *Devices* and access the FortiManager instance.
    b. Log in to FortiManager.
    c. Go to *Device Manager* > *Device & Groups*.
    d. Use the FortiGate *FGFM-IP* address from the FortiGate order details and the login credentials to add the device.



The FortiGate must be added using the legacy login method by providing the username and password. See Adding online devices using Discover mode and legacy login in the FortiManager Administration Guide.

Once the device has successfully been added and the configuration has been imported, you can begin to create policies, as needed.

Accessing FortiAnalyzer from FortiGate-as-a-Service

FortiAnalyzer can be accessed from FortiGate-as-a-Service after an order has been completed. Once the device has been configured, FortiAnalyzer can be added to FortiGate devices ordered through FortiGate-as-a-Service.

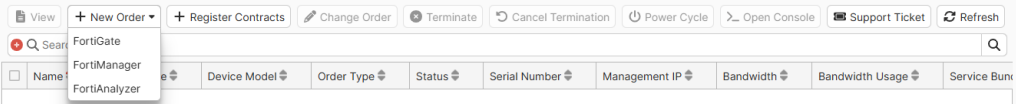
FortiManager and FortiAnalyzer devices require FortiCare registration. Temporary outbound rules in the associated security group can aid automatic FortiCare registration when you access the device for the first time. See FortiCare registration requirements for FortiManager on page 21 for more information.

Accessing a FortiAnalyzer instance

After a FortiAnalyzer order has completed, the FortiAnalyzer instance can be accessed through FortiGate-as-a-Service.

To access FortiAnalyzer:

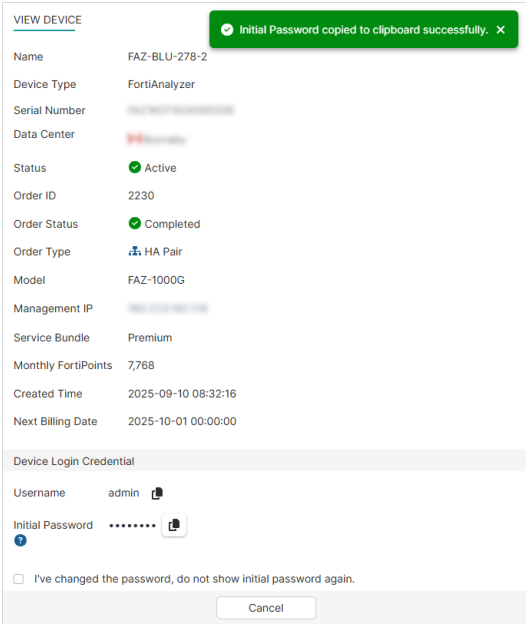
1. Go to *Devices*.
2. Select *New Order* > *FortiAnalyzer*.



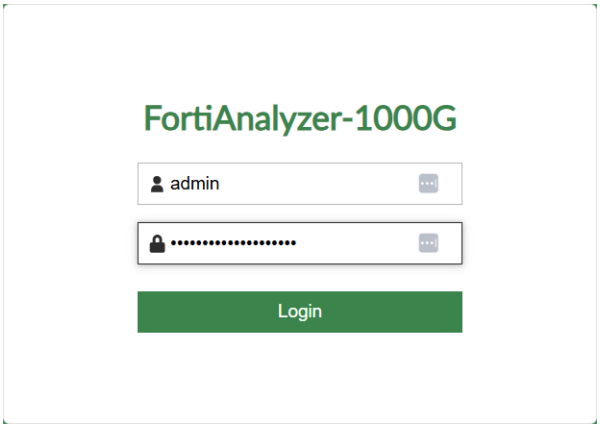
3. Define the *Management Security Group*:

- To allow access to every network, select the default *allow_all* security group.
- To allow access to only a specific network or client:
  i. Create a custom security group with inbound and outbound rules defined to only allow a specific client IP address to access the FortiAnalyzer instance. See Creating a security group on page 43.
  ii. Select the custom security group.

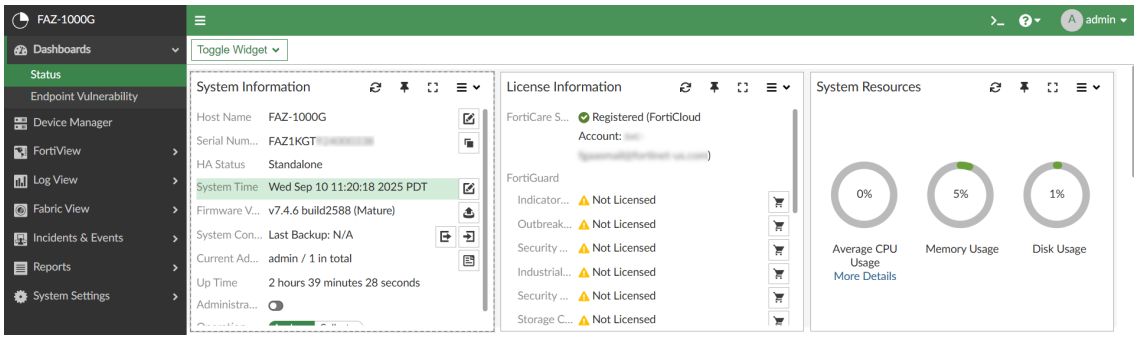
4. Configure the other FortiAnalyzer order fields, as needed.
5. Click *Place Order*.
6. Once the order status is *Complete*, go to *Devices* and select the FortiAnalyzer order to view more details.
7. Copy the *Username* and *Initial Password* to your device.



8. Select the *Management IP*. The FortiAnalyzer credentials page is displayed.
9. Enter the *Username* and *Initial Password* into the provided fields.



10. Click *Login*. The FortiAnalyzer instance will open.


FAZ-1000G
admin
Dashboards
Status
Endpoint Vulnerability
Device Manager
FortiView
Log View
Fabric View
Incidents & Events
Reports
System Settings
Toggle Widget
System Information
Host Name FAZ-1000G
Serial Num... FAZ1KGT
HA Status Standalone
System Time Wed Sep 10 11:20:18 2025 PDT
Firmware V... v7.4.6 build2588 (Mature)
System Con... Last Backup: N/A
Current Ad... admin / 1 in total
Up Time 2 hours 39 minutes 28 seconds
Administra...
License Information
FortiCare S... Registered (FortiCloud
Account:
FortiGuard
Indicator... Not Licensed
Outbreak... Not Licensed
Security ... Not Licensed
Industrial... Not Licensed
Security ... Not Licensed
Storage C... Not Licensed
System Resources
0%
5%
1%
Average CPU Usage
More Details
Memory Usage
Disk Usage

Orders

The *Orders* page allows you to order devices using FortiPoints and through registered contracts.

This section includes:

FortiPoints-based orders

New orders purchased using FortiPoints can be ordered and configured in the *Orders* page.

For FortiPoints-based orders, the following default service quotas apply:

- A maximum of 2 devices per user
- A maximum of 5 IP addresses per order

If higher limits are required, customers can request a quota increase by opening a Service Request under the appropriate *Service Quota Increase* category. See Service Requests on page 50.

This section includes following:

Creating an order

You can create an order for a new device from the *Order* page. The number of FortiPoints required to complete the purchase will vary depending on the order particulars, including the model of device, service bundle, IP addresses, and bandwidth. The estimated number of FortiPoints needed are displayed as you fill in the order details.

Orders are dependent on the availability of devices. If the type or number of devices you need are not currently available in the inventory, you will not be able to complete the order.

Once the order has been completed, you can access and log into the device. See Accessing devices on page 19.

This section includes the following:

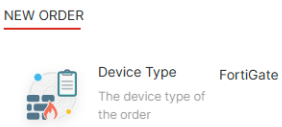
- Creating a FortiAnalyzer order on page 34

Creating a FortiGate order

FortiGate-as-a-Service (FGaaS) delivers dedicated FortiGate hardware as a service, providing enterprise-grade network security and connectivity with OPEX-based consumption while retaining full customer control.

To create a FortiGate order:

1. Go to *Orders*.
2. Click *Order* > *FortiGate*. The *New Order* page is displayed.



3. Enter the FortiGate details:

Field	Description
Name	Enter a *Name* for the FortiGate.
Tenure	Select the subscription period from the dropdown list.
Location	Select the *Location* of the Data Center from the dropdown list. The Data Centers that are currently supported include: • Ashburn, USA • Chicago, USA • London, England • Madrid, Spain

Field	Description
	• Paris, France • Plano, USA
Device Model	Select the *Device Model* you want: • FGT91G • FGT901G • FGT3501F
Order Type	Select the *Order Type*. The *Order Type* can either be a single device or an HA pair. See High Availability in the FortiOS Administration guide for more information on HA pairs.
Service Bundle	Select the product SKU. Details for the SKU, such as the associated service bundle, are listed. The *Sovereign SASE* bundle is only available if the 91G or 901G *Device Model* was selected and the *Sovereign SASE Cloud Orchestrator and Portal* or the *Sovereign SASE User License* SKUs are already be registered in the FortiCloud Asset Management portal. Sovereign SASE is available for 2, 12, 24, 36, 48, and 60-month terms. See Registering assets in the Asset Management guide. After completing the order, register the FortiGate 91G or 901G model SKU in the Asset Management portal. The *Sovereign SASE FortiGate License* support type will be listed in the *Product List*. See Product list in the Asset Management guide.
Add-ons	Select any add-ons.
IPs	Enter the number of IP addresses required in the *IPs* field. The *IPs* value must be at least two. The default value is two IP addresses for a single FortiGate and three IP addresses for an HA pair. Neither type can have more than five IP addresses.
Bandwidth	Select the *Bandwidth* you need from the dropdown list.
Firmware Version	Select the *Firmware Version* you need from the dropdown list.
Internet Security Group	Select the *Internet Security Group*. Internet security groups are designated for internet traffic while management security groups are designated for management traffic. New security groups can be created in the *Security Group* page. See Security Group on page 43. If *allow_all* is selected, a notification is displayed to denote that your devices can be accessed by any IPv4 address.
Management Security Group	Select the *Management Security Group*.

Field	Description
	Management security groups are designated for management traffic. New security groups can be created in the *Security Group* page. See Security Group on page 43. If *allow_all* is selected, a notification is displayed to denote that your devices can be accessed by any IPv4 address.
End User Type	Select the *End User Type*. To be defined as a government user, you must be affiliated with any central, regional, or local government department, agency, or other entity performing governmental functions. Orders and contracts may be blocked if the government user is from a sanctioned country.

4. Click *Review Your Order*.

   Click *Edit Order* if you would like to change configuration details before proceeding.

5. Click *Place Order*. The order is displayed as *Provisioning* in the *Orders* page.

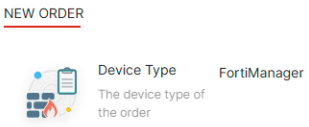
Creating a FortiManager order

FortiManager-as-a-Service (FMGaaS) provides FortiManager hardware as a service for centralized configuration, policy management, and life cycle operations across Fortinet security platforms.

FortiManager and FortiAnalyzer devices require FortiCare registration. Temporary outbound rules in the associated security group can aid automatic FortiCare registration when you access the device for the first time. See FortiCare registration requirements for FortiManager on page 21 for more information.

To create a FortiManager order:

1. Go to *Orders*.
2. Click *Order* > *FortiManager*. The *New Order* page is displayed.



3. Enter the FortiManager details:

Field	Description
Name	Enter a *Name* for the FortiManager device.
Tenure	Select the subscription period from the dropdown list.
Location	Select the *Location* of the Data Center from the dropdown list. The Data Centers that are currently supported include: • Ashburn, USA • Burnaby, Canada • Chicago, USA
Device Model	Select the *Device Model* you want: • FMG1000G • FMG3100G • FMG3700G
Order Type	Select the *Order Type*. The *Order Type* can either be a single device or an HA pair. If the FortiManager devices are ordered as an HA pair, they will still initially operate in standalone mode. You will need to setup and configure the HA pair after activation. See High Availability and Configuring model HA cluster members in the FortiManager Administration guide for more information on HA pairs.
Service Bundle	Select the product SKU. Details for the SKU, such as the associated service bundle, are listed.
Add-ons	Select any add-ons.
Firmware Version	Select the *Firmware Version* you need from the dropdown list.
Management Security Group	Select the *Management Security Group*. Management security groups are designated for management traffic. New security groups can be created in the *Security Group* page. See Security Group on page 43. If *allow_all* is selected, a notification is displayed to denote that your devices can be accessed by any IPv4 address. For information on accessing the FortiManager instance, see Accessing FortiManager from FortiGate-as-a-Service on page 22.

Field	Description
End User Type	Select the *End User Type*. To be defined as a government user, you must be affiliated with any central, regional, or local government department, agency, or other entity performing governmental functions. Orders and contracts may be blocked if the government user is from a sanctioned country.

4. Click *Review Your Order*.

   Click *Edit Order* if you would like to change configuration details before proceeding.

5. Click *Place Order*. The order is displayed as *Provisioning* in the *Orders* page.

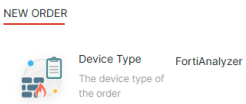
Creating a FortiAnalyzer order

FortiAnalyzer-as-a-Service (FAZaaS) offers FortiAnalyzer hardware as a service to enable centralized logging, analytics, reporting, and visibility across Fortinet security deployments.

FortiManager and FortiAnalyzer devices require FortiCare registration. Temporary outbound rules in the associated security group can aid automatic FortiCare registration when you access the device for the first time. See FortiCare registration requirements for FortiManager on page 21 for more information.

To create a FortiAnalyzer order:

1. Go to *Orders*.
2. Click *Order* > *FortiAnalyzer*. The *New Order* page is displayed.



3. Enter the FortiAnalyzer details:

Field	Description
Name	Enter a *Name* for the FortiAnalyzer device.
Tenure	Select the subscription period from the dropdown list.
Location	Select the *Location* of the Data Center from the dropdown list. The Data Center that is currently supported is as follows: • Burnaby, Canada
Device Model	Select the *Device Model* you want: • FAZ1000G • FAZ3700G
Order Type	Select the *Order Type*. The *Order Type* can either be a single device or an HA pair. If the FortiAnalyzer devices are ordered as an HA pair, they will still initially operate in standalone mode. You will need to setup and configure the HA pair after activation. See High Availability in the FortiAnalyzer Administration guide for more information on HA pairs.
Service Bundle	Select the product SKU. Details for the SKU, such as the associated service bundle, are listed.
Add-ons	Select any add-ons.
Firmware Version	Select the *Firmware Version* you need from the dropdown list.
IPs	The default value is one IP address for a standalone FortiAnalyzer and two IP addresses for an HA pair.
Management Security Group	Select the *Management Security Group*. Management security groups are designated for management traffic. New security groups can be created in the *Security Group* page. See Security Group on page 43. If *allow_all* is selected, a notification is displayed to denote that your devices can be accessed by any IPv4 address. For information on accessing the FortiAnalyzer instance, see Accessing FortiAnalyzer from FortiGate-as-a-Service on page 26.
End User Type	Select the *End User Type*. To be defined as a government user, you must be affiliated with any central, regional, or local government department, agency, or other entity performing governmental functions. Orders and contracts may be blocked if the government user is from a sanctioned country.

4. Click *Review Your Order*.

Click *Edit Order* if you would like to change configuration details before proceeding.

5. Click *Place Order*. The order is displayed as *Provisioning* in the *Orders* page.

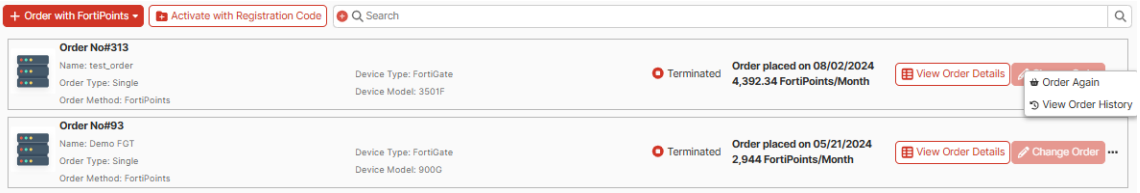
Creating an order based on an existing order

You can create a new FortiPoints-based order using the same configuration as an existing order using the *OrderAgain* feature.

> Devices added through registered contracts will not have the *Order Again* option. View details of the registered contract device to order a device with the same configuration. See Contract-based orders on page 37 and Viewing device details on page 12.

To repeat an order:

1. Go to *Orders*.
2. Find the order you want to use as a base for the new order and select *Order Again* from the ... menu.



   The *New Order* page is displayed with the settings preconfigured to use the same options as the selected order.
3. Enter a *Name* for the new order.
4. Click *Review Your Order*.
5. Click *Place Order*.

Changing an order

You can change your order from the *Orders* page.

For orders using FortiPoints, you can only change the device's name, service bundle, IP addresses, bandwidth, Internet security group, management group, and the IP anchoring for a non-management IP address. Other configuration particulars cannot be edited for an active order. You cannot change an order if you do not have enough FortiPoints.

If the device being updated was registered as a contract, only certain fields can be edited. See Managing contracts on page 40.

> For order upgrades, such as adding IP addresses, increasing bandwidth, and additional services, the change and FortiPoint charges will take effect immediately.
>
> For order downgrades, such as deleting IP addresses, decreasing bandwidth, or reducing services, the change will be scheduled for the next billing cycle.

The *IP Anchoring* field can only be updated when changing an order. FortiGate-as-a-Service publishes IP geolocation information for its service IP addresses. The published information reflects the current service configuration and may be used by external services according to their own geolocation policies.

The geolocation feed is available for download as a CSV file from https://fgaas.forticloud.com/portal/geofeed.csv. The file is available directly from the link. You do not need to be logged into the FortiGate-as-a-Service portal to access the feed.

To change an order:

1. Go to *Orders*.
2. Select *Change Order* for the order you would like to edit.
3. Edit the fields, as required.

   If you would like to delete IP addresses, click *View IPs List* and select the IP addresses you would like to delete. You cannot delete the *Management IP* address.

4. Click *Review Your Change*.
5. Click *Submit Your Change*.

Contract-based orders

Devices can be added to FortiGate-as-a-Service through registered contracts. Device contracts can be registered in the *Orders* page. Once a device is registered, additional configuration information, such as version number and DC location, can be defined.

Contracted devices will appear in the *Devices* and *Orders* pages once configured. See Devices on page 11 and Orders on page 29.

This section includes:

Registering a contract

Contracts can be registered and configured in the *Orders* page.

Orders are dependent on the availability of devices. If the type or number of devices you need are not currently available in the inventory, you will not be able to complete the order.

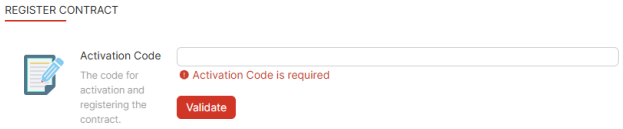
This section includes following:

Registering a device contract

New device contracts can be registered in the *Orders* page.

To register and configure a FortiGate device:

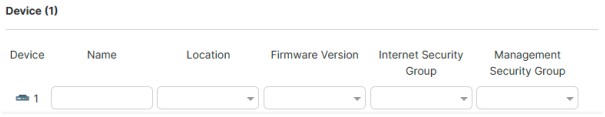
1. After you have received the activation code for the device, go to *Orders*.
2. Click *Activate with Registration Code*.
3. Enter the *Activation Code*.



4. Click *Validate*.
5. Review the preconfigured device details.
6. Select any *Add-ons*. If the contract includes any add-ons, they will be pre-selected.
7. Specify the device-dependent values, such as the number of IP addresses required, bandwidth, and so on.
8. Select the *End User Type*.

> To be defined as a government user, you must be affiliated with any central, regional, or local government department, agency, or other entity performing governmental functions. Orders and contracts may be blocked if the government user is from a sanctioned country.

9. Enter the device configuration details, including *Name*, *Location*, *Firmware Version*, *Internet Security Group*, and *Management Security Group*.

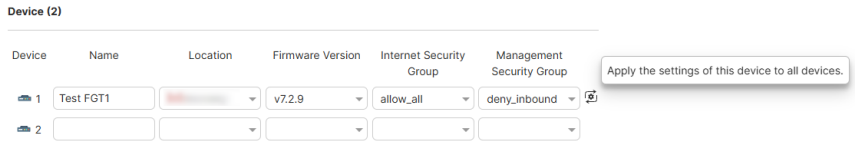


> For more information on security groups, see Security Group on page 43.

10. If there is more than one device in the contract:
    - Enter the configuration details of each device.

    - Duplicate the configuration onto each device:

i. Click *Apply the settings of this device to all devices* to use the same configuration as the first device.



A confirmation dialog is displayed.

ii. Click *Apply*. The names of each of the devices will be sequential from the name of the original device.

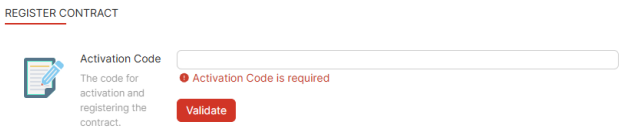
11. Click *Review Your Contract*.
12. Click *Register Your Contract*.

Registering an add-on contract

Additional capabilities, including increased bandwidth, additional IP addresses and FortiCare Elite, can also be registered to a device. Once you have completed registering and configuring a device, you can register an add-on and apply it to the device.

To register an add-on:

1. Go to *Orders*.
2. Click *Activate with Registration Code*.
3. Enter the *Activation Code*.



4. Click *Validate*. The add-on details and available devices are displayed.
5. Select the *End User Type*.

> To be defined as a government user, you must be affiliated with any central, regional, or local government department, agency, or other entity performing governmental functions. Orders and contracts may be blocked if the government user is from a sanctioned country.

6. Select the device you want to apply the add-on to.
7. Click *Review Your Add-Ons*.
8. Review the details and click *Register Your Add-Ons*.

Viewing contract details

Contract details can be viewed in the *Orders* page.

To view a contract:

1. Go to *Orders*.
2. Locate the contract you would like to review and select *View Order History* from the ... menu.

   Registered contracts can be identified in the *Orders* list by setting the filters to ensure that *Order Method* matches *SKU Contract*.

3. Click *View Order Details* for the activity entry you want. The *Order History* is displayed.
4. Select the *Contract Code* or *Add-On Contract List* for contract details.

Managing contracts

Contracts can be edited on the *Devices* and *Orders* pages. Due to the nature of contracts, only certain fields can be edited, such as the device name and security groups.

To edit a contract:

1. Locate the device in the *Orders* page.
2. Select the contracted device you want to edit.

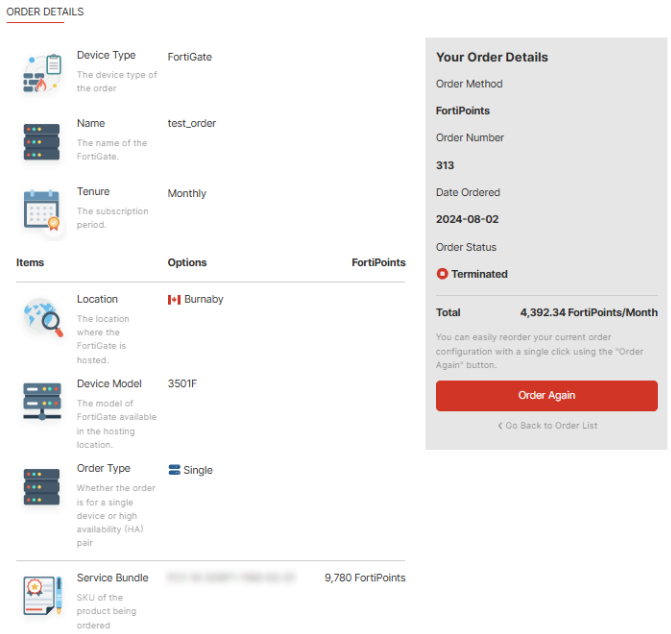
   Registered contracts can be identified in the *Orders* list by setting the filters to ensure that *Order Method* matches *SKU Contract*.

3. Click *Change Order*.
4. Edits the available fields as necessary.
5. Click *Review Your Changes*.
6. Click *Submit Your Change*.

Viewing order details

You can view the details of previously created orders from the *Orders* page. The *Orders* page displays the model information, order status, and FortiPoints used in the order.

If you select *View Order Details*, you can view the full details of an order, including configuration information, or to review the reason why an order has failed.



You can perform certain actions from the *Order Details* page:

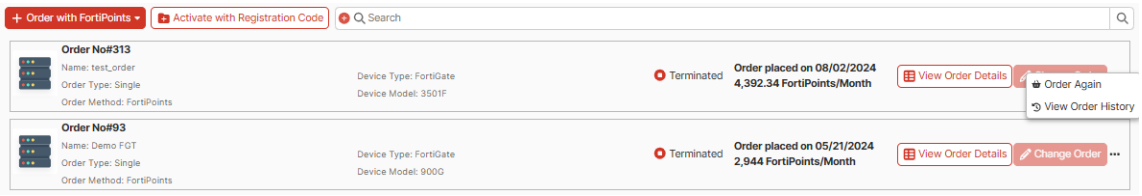
- Select *View IP List* list to expand the list of IP addresses.
- Select *Order Again* to order another device with the same configuration particulars as the current order you are viewing.
- Select *Change Order* to change order details. See Changing an order on page 36.

Reviewing order history

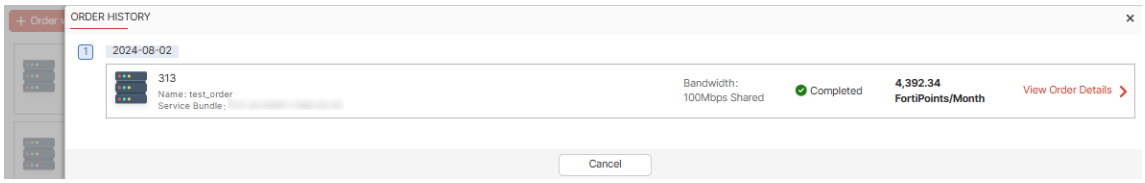
You can review the history of an order using the *Order History* feature. The *Order History* lists when an order was changed and allows you to review the configuration details of the change.

To review the order history:

1. Go to *Orders*.
2. Find the order you want to review and select *View Order History* from the ... menu.



The *Order History* pane is displayed.



3. Select *View Order Details* to view configuration details for that order activity.

Security Group

The *Security Group* page allows you to create new security groups for inbound and outbound traffic rule management. This is especially useful for the management of new devices to avoid exposure of the device after provisioning and before custom configuration.

Security groups can be used to specify a list of trusted hosts and subnets which are then translated into policies that manage traffic.

Security groups can be implemented for a device when the order is being configured. See Creating a new order on page 14.

This section includes:

FortiManager and FortiAnalyzer devices require FortiCare registration. Temporary outbound rules in the associated security group can aid automatic FortiCare registration when you access the device for the first time. See FortiCare registration requirements for FortiManager on page 21 for more information.

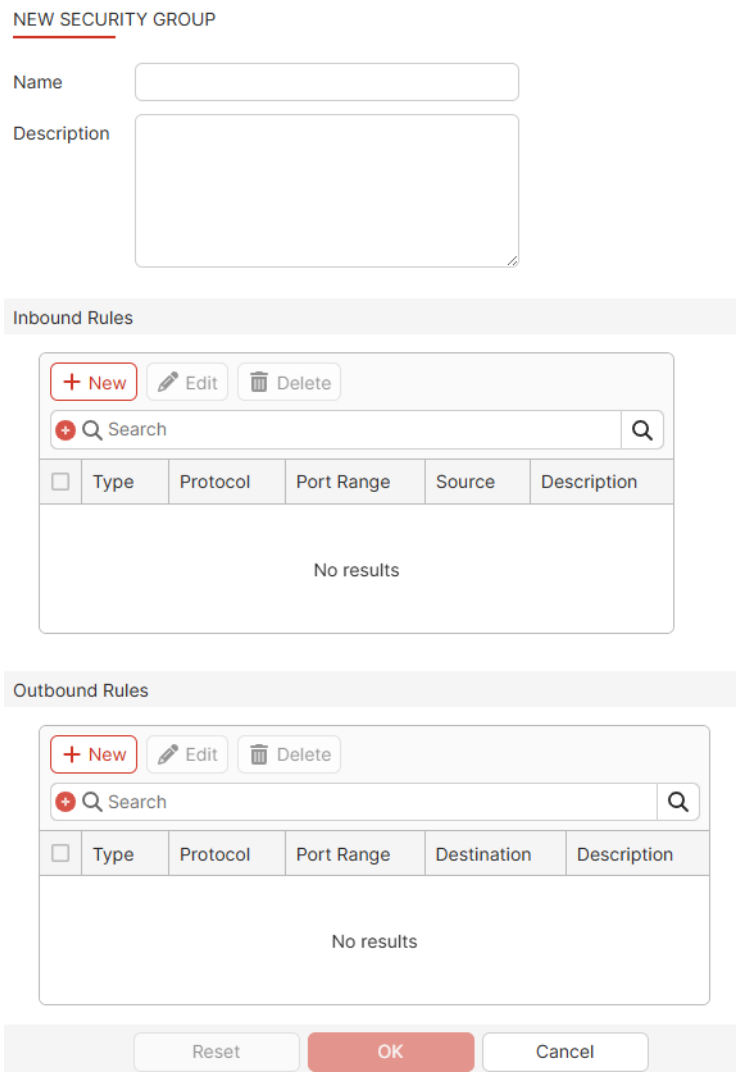
Creating a security group

You can create new security groups in the *Security Group* page.

Security groups can be implemented in a device by selecting it in the order. See Creating an order on page 29.
See also

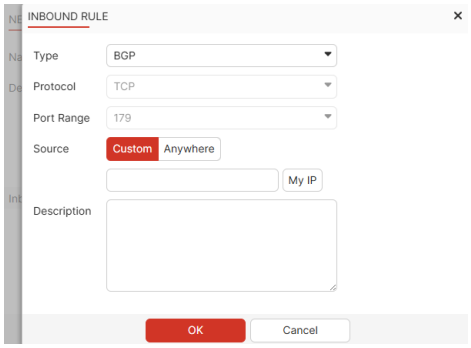
To create a new security group:

1. Go to *Security Group*.
2. Click *New*.



3. Enter a *Name*.
4. Under *Inbound Rules*, click *New*. The *Inbound Rule* pane is displayed.

a. Select a *Type*. The *Protocol* and *Port Range* fields are displayed.



b. Select a *Protocol* and *Port Range*, if applicable.

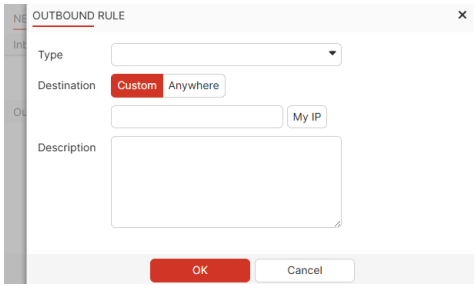
c. Select the *Source*.

> If *Anywhere* is selected, a notification is displayed to denote that your devices can be accessed by any IPv4 address.

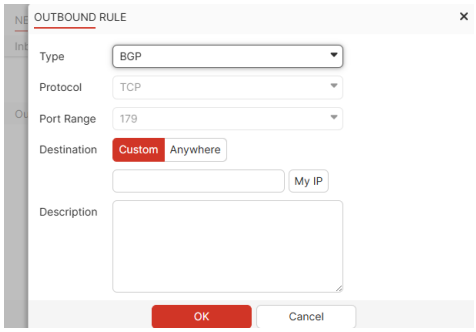
d. Click *OK*.

e. Repeat these steps to create another rule.

5. Under *Outbound Rules*, click *New*. The *Outbound Rule* pane is displayed.



a. Select a *Type*. The *Protocol* and *Port Range* fields are displayed.



b. Select a *Protocol* and *Port Range*, if applicable.

c. Select the *Source*.

d. Click *OK*.

e. Repeat these steps to create another rule.

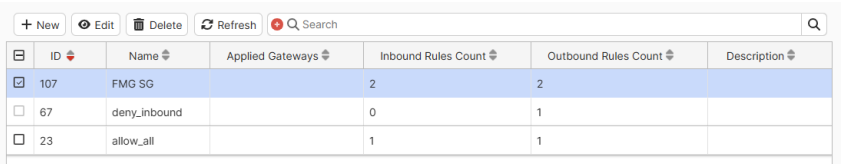
6. Click *OK*.

Managing security groups

You can manage security groups from the Security Group page.

To edit a security group:

1. Go to *Security Group*.
2. Select the security group.



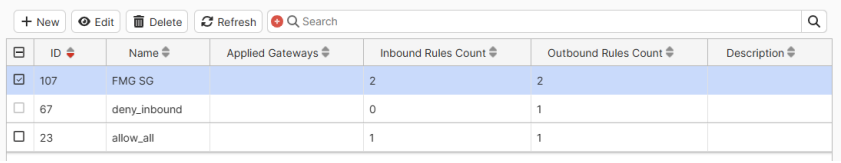
3. Click *Edit*.
4. Edit the security group as needed.

> To manage a rule, select the rule and click *Edit* or *Delete*. New rules can also be added as needed.

5. Click *OK*.

To delete a security group:

1. Go to *Security Group*.
2. Select the security group.



3. Click *Delete*.
4. Click *OK*.

Audit Logs

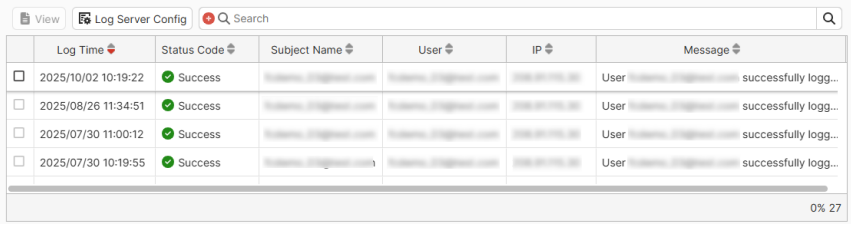
The *Audit Logs* page displays event information pertaining to FGaaS services and orders.

> The audit logs do not display information about events occurring on the device, such as HA events. These audit logs can be viewed on the device. See Viewing event logs in the FortiOS Administration Guide.

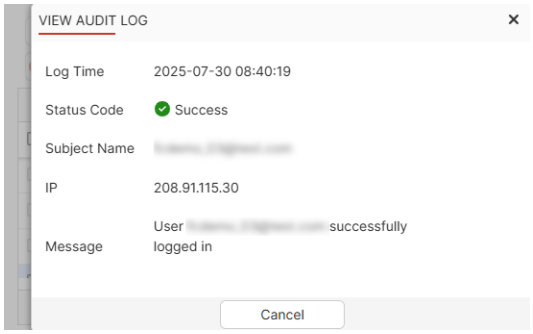
This section includes:

Viewing audit logs

High level audit information is displayed on the *Audit Logs* page.



Select the audit you want to review in more detail and click *View* to open the *View Audit Log* pane.



Forwarding audit logs to an external syslog server

Audits logs can be forwarded to an external syslog server from the *Audit Logs* page.

Protocol supported by FortiGate-as-a-Service includes syslog over TLS on port TCP 6514. When the syslog server is reachable, audit logs are forwarded immediately as they are generated. When the syslog server is unreachable, the system will retry every five minutes. When the server is reachable again, the system will forward any missing audit logs from the past 24 hours.

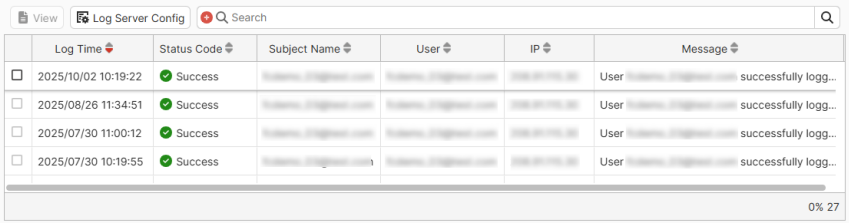
Each audit log is only forwarded once, with no duplication.

Syslog messages follow the RFC 5424 format where:

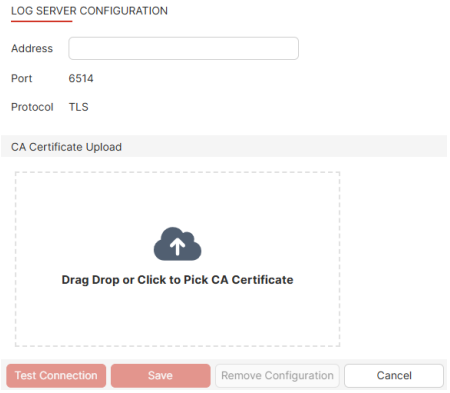
- Facility: 13 (log audit)
- Severity: 6 (informational)

To configure audit log forwarding:

1. Go to *Audit Logs*.



2. Click *Log Server Config*.



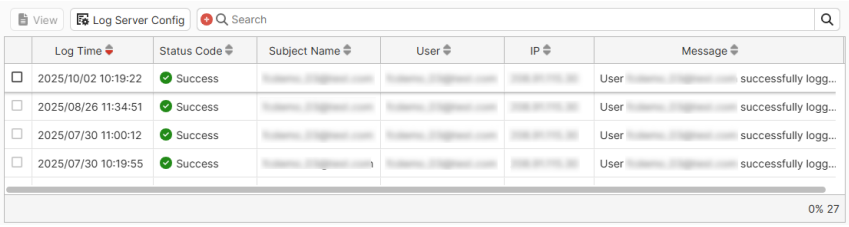
3. Enter the log server *Address* as either an IP or FQDN address.
4. (Optional) Upload a CA certificate if you want to verify the log server certificate.
   If a CA certificate is not provided, the connection will still be established but certificate verification will be skipped.
5. Click *Test Connection* to verify connectivity.
   If a CA certificate was uploaded, the system will also validate the log server certificate.
6. Click *Save* to enable log forwarding.

To allow FortiGate-as-a-Service to send audit logs to your log server, you may need to allowlist certain IP addresses. Create a FortiCare support ticket to determine the allowlist IP addresses relevant to your region. See Creating a support ticket on page 17.

These addresses may change as we continue to improve our security.

To disable audit log forwarding:

1. Go to *Audit Logs*.



2. Click *Log Server Config*.
3. Click *Remove Configuration*.

Service Requests

The *Service Requests* page allows you to request changes of the allowed inventory or quota of certain parameters. For example, if a higher service quota is required, a new service request can be submitted and discussed within the FortiGate-as-a-Service portal.

Email notifications will be sent to your account's email address each time when you create a new request, add a message in the request, or close the request.

This section includes:

Creating a new service request

You can submit a new service request in the *Service Requests* page. Available service request categories include:

Category	Description
Increase IP Service Quota	This request is used to increase the number of public IP addresses allocated to your FortiGate, FortiAnalyzer, or FortiManager. This is typically required when additional IP addresses are needed to support new services or to expand the network infrastructure.
Increase Device Service Quota	This request is used to increase the maximum number of devices (FortiGate, FortiAnalyzer, and FortiManager) that can be deployed or managed within the FGaaS portal.
EMAC VLAN Support	This request is used to configure EMAC VLAN support on a FortiGate device by mapping IP and MAC address pairs. This allows the FortiGate to respond to multiple IP/MAC combinations on the same interface and is commonly used in MSSP network environments to support multiple customers with unique IP address. EMAC VLAN supports up to 10 VDOMs per FortiGate.
Increase Bandwidth Quota	This request is used to increase the assigned bandwidth quota of a device. This allows for a streamlined process when additional bandwidth is required and reduce ambiguity on how to scale beyond limits.

Category	Description
Custom Architecture	This request is used to customize interface requirements, IP addressing needs, and topology details beyond the default configuration.

To submit a new service request:

1. Go to *Service Requests*.
2. Click *New*.
3. Select the service request *Category*.
4. Enter the *Title* of the request.
5. Enter the request requirements and details:

Selected *Category*	Request requirements
Increase Service Quota	• Number of additional IPs • Justification
Increase Device Service Quota	• Number of additional Devices • Justification
EMAC VLAN Support	• FortiGate Serial Number • IP MAC Pair Select the + to add new pairs of IP addresses. • Justification
Increase Bandwidth Quota	• Additional Bandwidth • Datacenter • Justification

Custom Architecture	• Justification
	  • Interface requirements
	  • IP addressing needs
	  • HA/topology details
	  • Additional notes

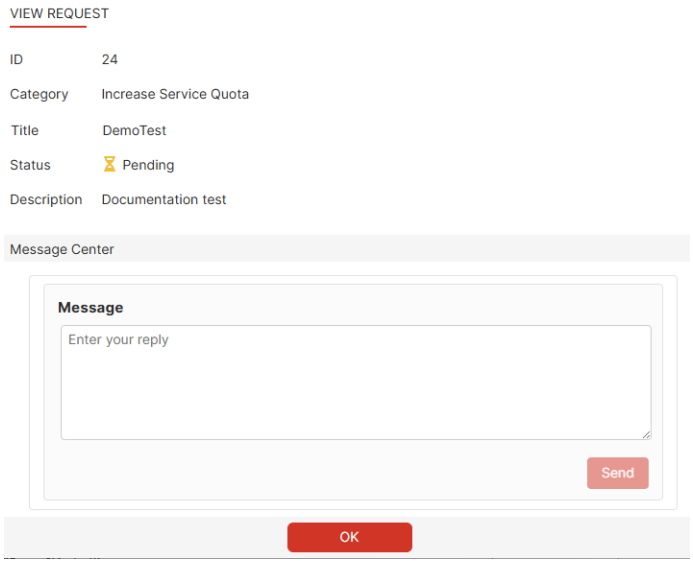
6. Click *OK*. The service request will be added to the *Service Requests* list.

Viewing service requests

You can view service requests and send messages to the FortiGate-as-a-Service team from the *Service Requests* page. The service request *Message Center* allows you to discuss the needs and status of a service request with the FortiGate-as-a-Service team.

To add a message within a service request:

1. Go to *Service Requests*.
2. Select the request you want to investigate.
3. Click *View*. Any previously posted messages by you or the FortiGate-as-a-Service team will appear in the *Message Center*.



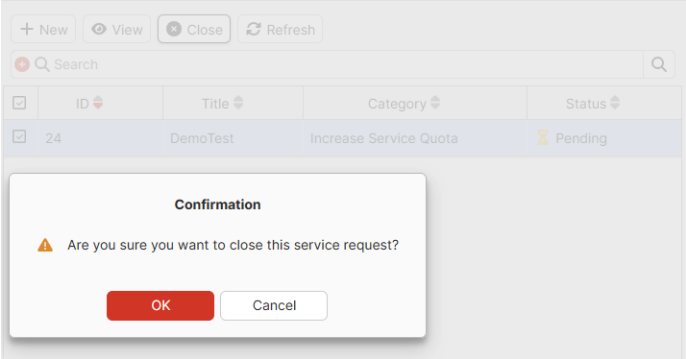
4. Enter your message in the *Message Center*.
5. Click *Send*.

Closing a service request

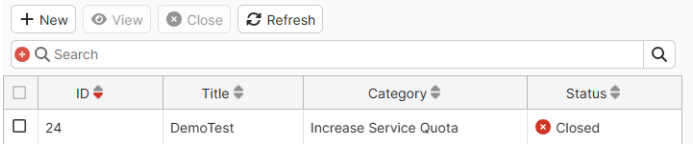
You can close a service request if it is no longer required. Service Requests with the status of *Completed* cannot be closed.

To close a request:

1. Go to *Service Requests*.
2. Select the request you want to close.
3. Click *Close*. A confirmation dialog is displayed.


New
View
Close
Refresh
Search
ID
Title
Category
Status
24
DemoTest
Increase Service Quota
Pending
Confirmation
Are you sure you want to close this service request?
OK
Cancel

4. Click *OK*.


New
View
Close
Refresh
Search
ID
Title
Category
Status
24
DemoTest
Increase Service Quota
Closed

www.fortinet.com