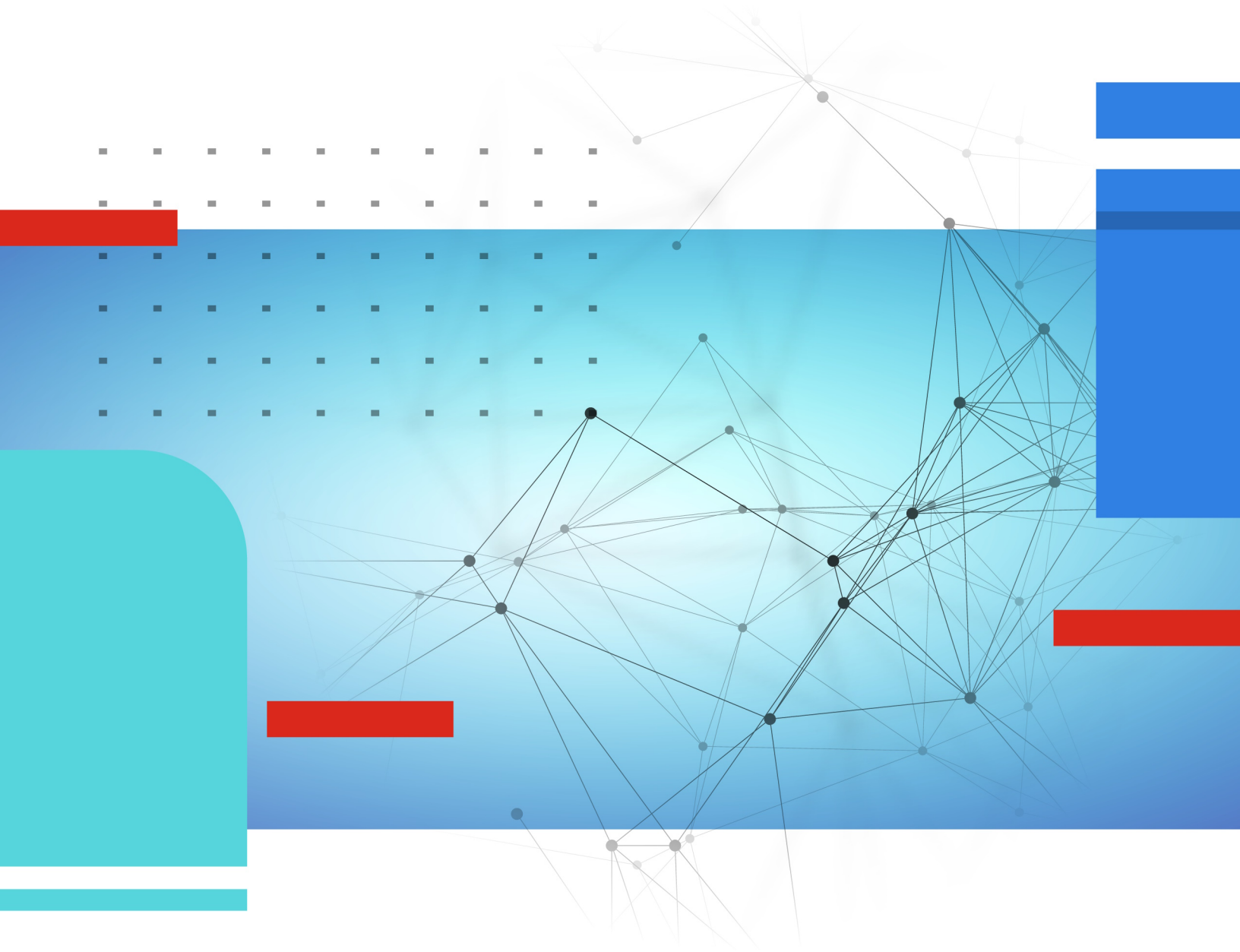
Administration Guide

Overlay-as-a-Service 24.4



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

January 05, 2025
Overlay-as-a-Service 24.4 Administration Guide
85-244-1111713-20250205

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-01-03	Initial release.
2025-02-05	Updated Accessing the OaaS portal on page 10.

Introduction

FortiCloud Overlay-as-a-Service (OaaS) is a service for FortiGate devices to easily provision new SD-WAN overlay networks from FortiCloud. OaaS is a subscription service providing an easy-to-use GUI wizard that simplifies the process of configuring an SD-WAN overlay within a single region.

The OaaS hub acts as a bridge to allow overlay shortcuts to be formed between your spokes.

OaaS and the spokes rely on Fortinet Inc.'s Auto-Discovery VPN (ADVPN), which allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. ADVPN shortcut tunnels, also known as shortcuts, are formed between spokes, such as between branches and the data center, or between branches themselves so that traffic does not need to pass through the hub.

This section includes:

Prerequisites

The prerequisites of using the OaaS portal are as follows:

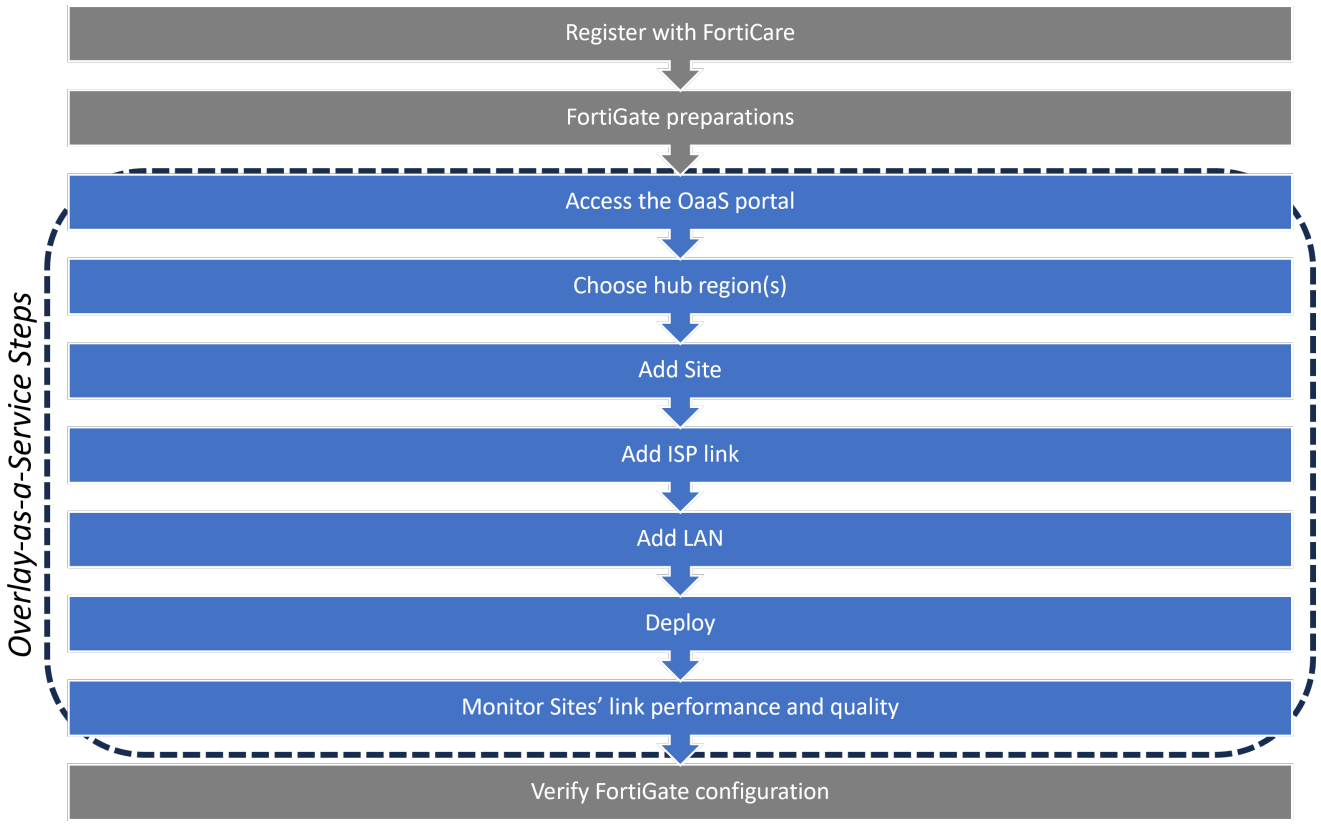
- FortiOS 7.4.4 and later on the FortiGates acting as spokes.
- FortiCloud Overlay-as-a-Service licenses for all spokes.
- FortiCloud SD-WAN Network Monitor licenses for the Bandwidth feature.
- Sites must be running FortiOS 7.6.0 or later to support security profiles.

For successful setup of ADVPN tunnels, the spokes' ISPs must allow traffic over UDP port 500 and UDP port 4500 for NAT traversal (NAT-T).

FOS 7.6.1 is not supported on Overlay-as-a-Service.

Configuration overview

The general process of configuring Overlay-as-a-Service is demonstrated as follows:



When you first go to the *Topology* page, a high level walk through demonstrates how you will configure the configuration. For more information, see Welcome tour on page 15 and Creating the initial topology on page 19.

For a demonstration on performing a complete OaaS configuration from beginning to end, see the Overlay-as-a-Service Deployment Guide.

To configure SD-WAN using FortiCloud Overlay-as-a-Service:

1. Prepare your devices and access for OaaS. See Getting started on page 8.
2. Define the hub region for the SD-WAN network. See Topology on page 15.
3. Define and deploy the site, ISP, and subnet for the hub in the SD-WAN network. See Topology on page 15.
4. Monitor link performance and quality across devices in the SD-WAN network. See Home on page 33.
5. Test and verify connectivity between sites deployed using OaaS. See Testing and verification on the FortiGate on page 101.

Getting started

Before you can begin configuring within the OaaS portal, you must:

- Register your OaaS license with FortiCloud. See Registering FortiCloud Overlay-as-a-Service licenses on page 8.
- Prepare the site FortiGate devices for OaaS. See Preparing site FortiGate devices for OaaS on page 8.
- Enable access to the OaaS portal. See Accessing the OaaS portal on page 10.

Registering FortiCloud Overlay-as-a-Service licenses

In FortiCloud, register the following licenses:

License	Description
Overlay-as-a-Service	The OaaS SKU is in the format FC-10-XXXXX-657-02-DD where XXXXX corresponds to the model code and DD corresponds to the validity period of the license in months. Please refer to the OaaS ordering guide for details.
SD-WAN Network Monitor	The OaaS SKU is in the format FC-10-XXXXX-288-02-DD where XXXXX corresponds to the model code and DD corresponds to the validity period of the license in months. Please refer to the OaaS ordering guide for details. This is a optional license for the Monitor SDWAN Bandwidth Service.
Hub FortiGate	You do not need to register an extra license for the Hub. As long as you have an OaaS FC-10-XXXXX-657-02-DD SKU registered (for a site or spoke FortiGate), you will be allowed to create a Hub.
Site or spoke FortiGates	Register an OaaS SKU to each FortiGate that will be used in a site or spoke. You must register each FortiGate device that will be used with OaaS to the same FortiCloud account that will be used to log in to OaaS. You must also obtain a FortiCloud OaaS license, and apply it to each FortiGate device to be used as a site or spoke in the overlay.

For details on registering products, see Registering assets.

Preparing site FortiGate devices for OaaS

Complete the following tasks to prepare your FortiGate devices to be used by OaaS as site or spoke devices in the SD-WAN network:

1. Register the FortiGate devices with FortiCloud, and activate the FortiGate devices with FortiGate Cloud. See Registering with FortiCloud and activating with FortiGate Cloud on page 9.

2. Configure each FortiGate with a WAN IP address and a default gateway IP address for accessing the Internet. See Configuring FortiGates for sites on page 10.

Registering with FortiCloud and activating with FortiGate Cloud

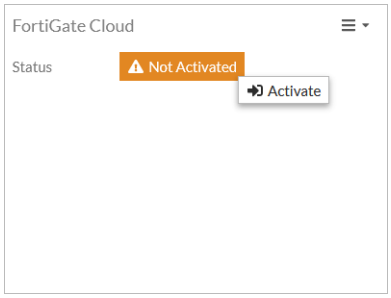
Your FortiGate devices must be registered with FortiCloud and activated with FortiGate Cloud.

This step is required because OaaS uses the FortiCloud management tunnel to FortiGates to retrieve interface information and to install configuration settings orchestrated from OaaS.

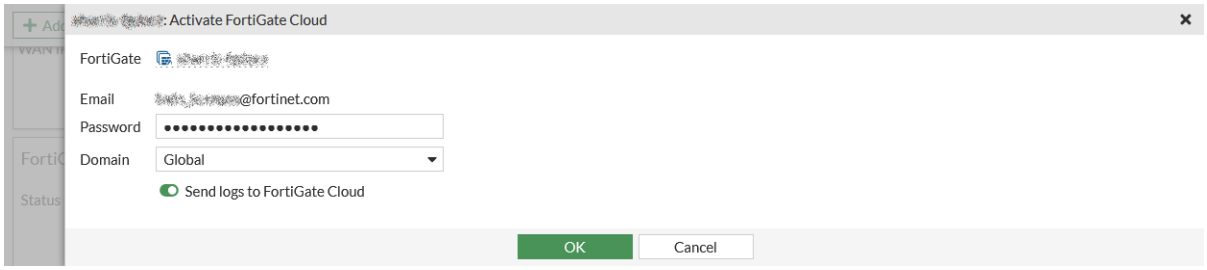
Typically, for FortiGate devices already registered with FortiCloud, you can activate them on the FortiGate GUI.

To configure an additional incoming interface on a spoke:

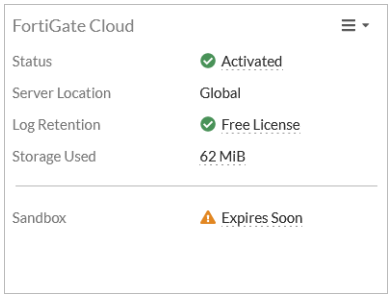
1. Go to *Dashboard* > *Status*.
2. In the *FortiGate Cloud* widget, click *Not Activated* > *Activate*.



3. Enter the password for the account that was used to register the FortiGate.



4. Click *OK*.
   The *FortiGate Cloud* widget now shows the activated FortiCloud account.



For details on registering products, see Registering assets in the FortiCloud Asset Management Guide.

For details on activating the FortiGate with FortiGate Cloud, see FortiCare and FortiGate Cloud login in the FortiOS Administration Guide.

Configuring FortiGates for sites

FortiGate devices that will be used in the Overlay-as-a-Service portal in a SD-WAN network must be properly configured in order to successfully connect as a site. These steps are required because OaaS obtains the interface configuration from the FortiGate and displays it for overlay configuration in the OaaS portal. See Site on page 42 for more information.

The requirements necessary for a FortiGate to be used as a site include:

- Any FortiGate that will be used as a site in the SD-WAN network must be configured with a WAN IP address and default gateway IP address for accessing the internet. See Basic configuration in the FortiOS Administration Guide.
- The local interface IP address for the local subnet must be configured as well. See Interface settings in the FortiOS Administration Guide.
- WAN and LAN ports must not be in any predefined zone or must not be a member of any other SD-WAN zone. See Zone in the FortiOS Administration Guide.
- WAN and LAN ports must not be bound to any existing firewall policies. See Firewall policy in the FortiOS Administration Guide.
- For the direct or indirect local subnet port configured in OaaS, do not use a switch or aggregate interface member port. See Software switch, Hardware switch, and Aggregation and redundancy in the FortiOS Administration Guide.

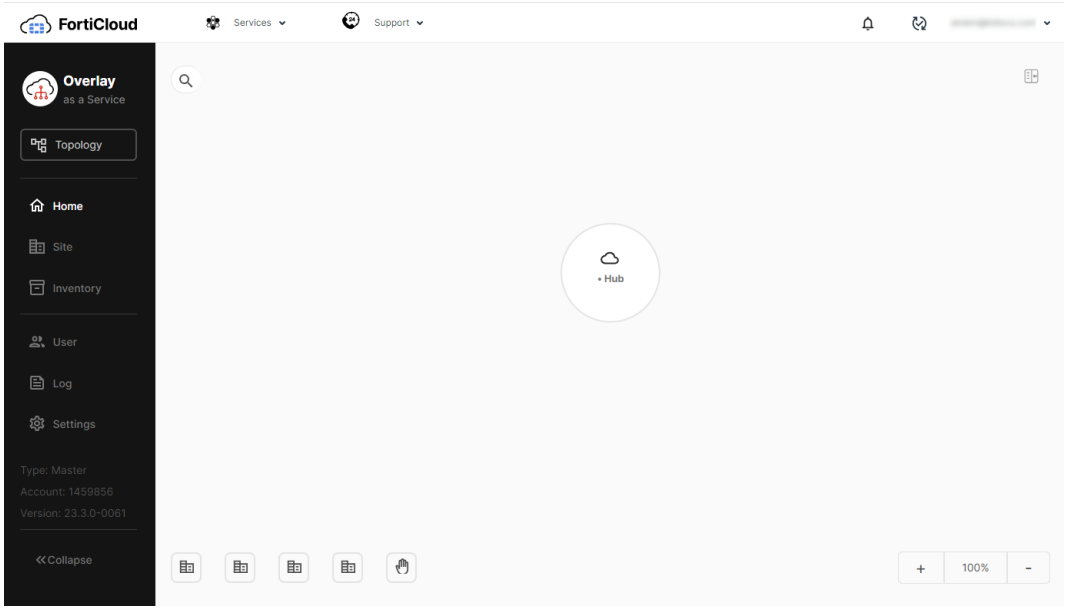
Accessing the OaaS portal

You can access the Overlay-as-a-Service portal from https://overlay-as-a-service.forticloud.com. Once you have access to the OaaS portal, you can set up your OaaS topology using the step-by-step walk through. See Creating the initial topology on page 19.

To access the OaaS portal:

1. Go to https://overlay-as-a-service.forticloud.com.
2. Log in using your FortiCloud account.

After logging in, the *Home* page is displayed.

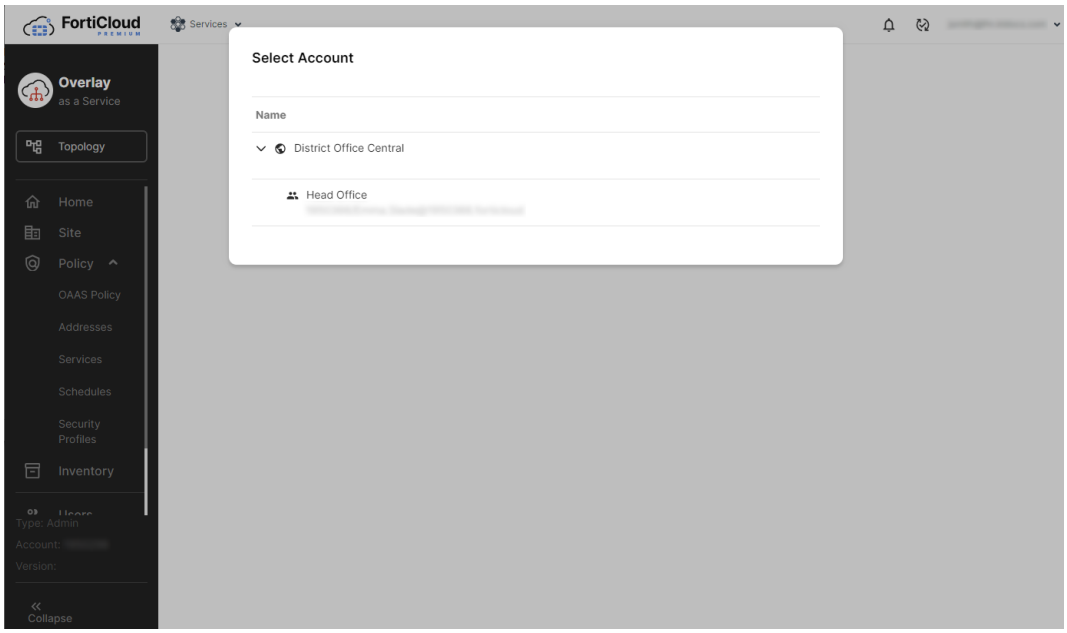


Organization support for Overlay-as-a-Service

Overlay-as-a-Service supports accessing your account through Organizational Unit (OU) accounts. OU access allows users to navigate the Overlay-as-a-Service portal depending on the assets and access assigned to the OU account. Assets and Overlay-as-a-Service topologies are dependent on the available and selected scope of the user. For more information on Organizations and OUs, see the FortiCloud Organization Portal guide and Organization user management in the Identity & Access Management (IAM) guide.

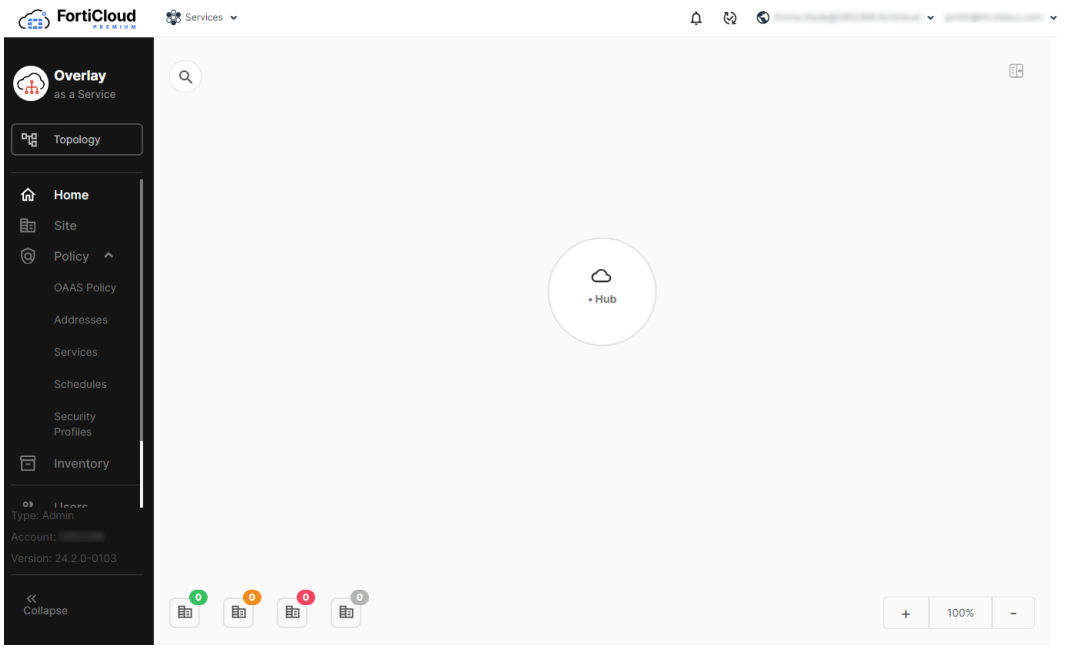
To log into the Overlay-as-a-Service portal with OU access:

1. Go to https://overlay-as-a-service.forticloud.com.
2. Click *Log In*.
3. Click *IAM Login*.
4. Enter your IAM user credentials.
5. Click *Log In*. The *Select Account* dialog is displayed.

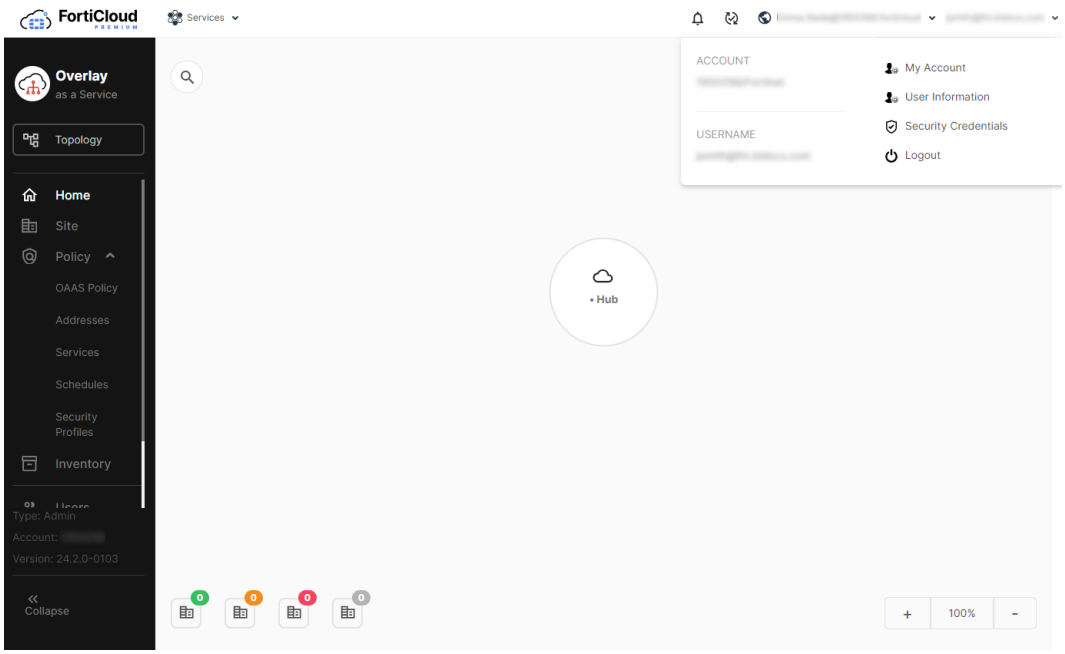


The OUs and member accounts visible are dependent on the permission scope of the IAM user in the Organization. See Permission scope with Organizations in the FortiCloud Identity & Access Management (IAM) guide.

6. Select the OU member account you want to access. The *Home* page is displayed.



The user and OU information displayed in the top banner.



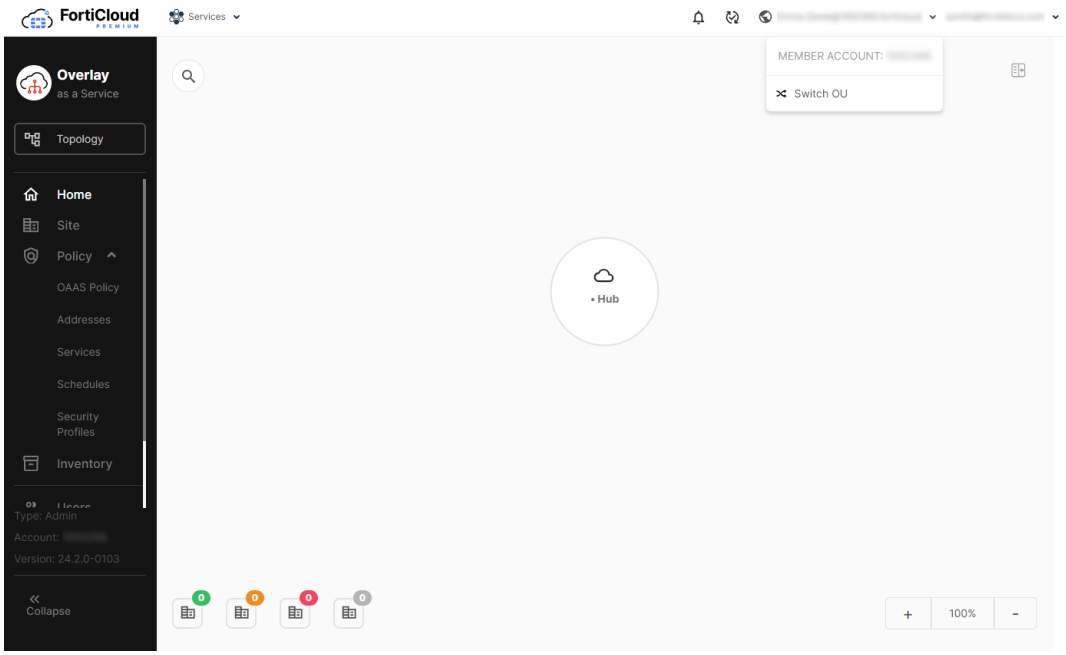
You can also log into your Organization IAM user account through www.forticloud.com. After logging into the IAM user account and selecting the OU member account you want to access, navigate to the Overlay-as-a-Service portal by selecting *Services* > *Overlay as a Service*. See Logging into an OU account in the FortiCloud Identity & Access Management (IAM) guide.

Switching accounts within an Organization

After you have logged into the Overlay-as-a-Service portal, you can switch between the member accounts and OUs included in the IAM user's permission scope.

To switch accounts:

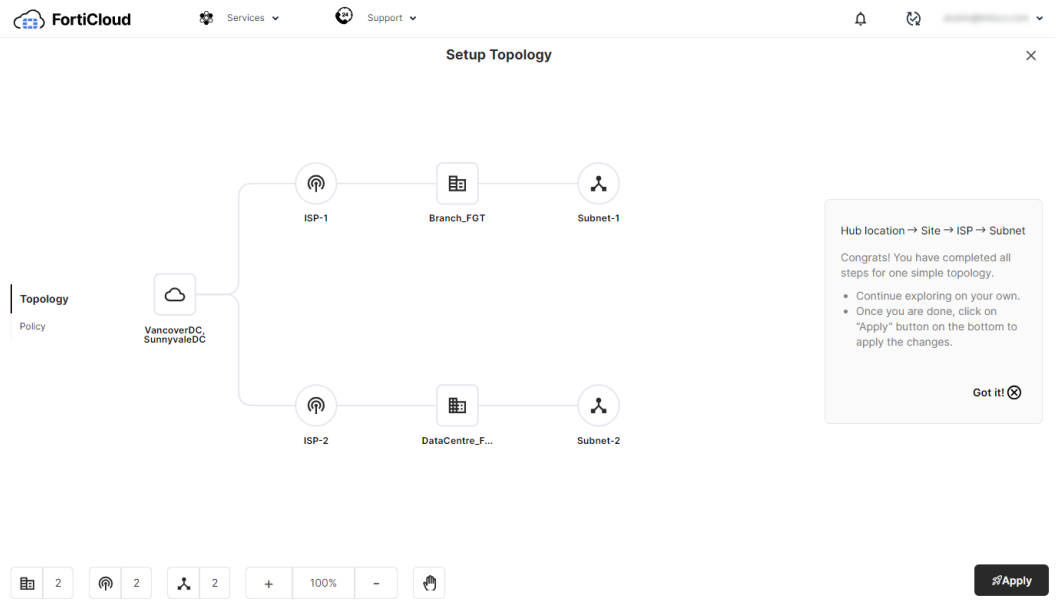
1. Select the OU dropdown menu in the top banner.



2. Click *Switch OU*. The *Select Account* dialog opens.
3. Select new OU or member account.

Topology

The *Topology* page displays the current configuration of the OaaS hub and site FortiGates. Hub and site devices can be configured and linked on the *Topology* page.



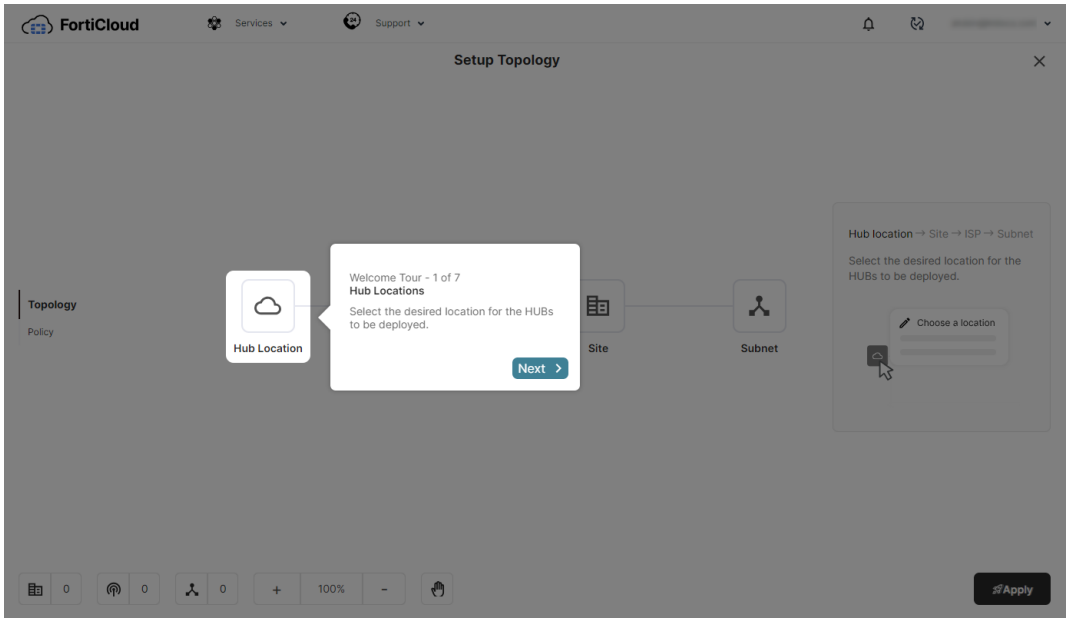
This section includes:

Welcome tour

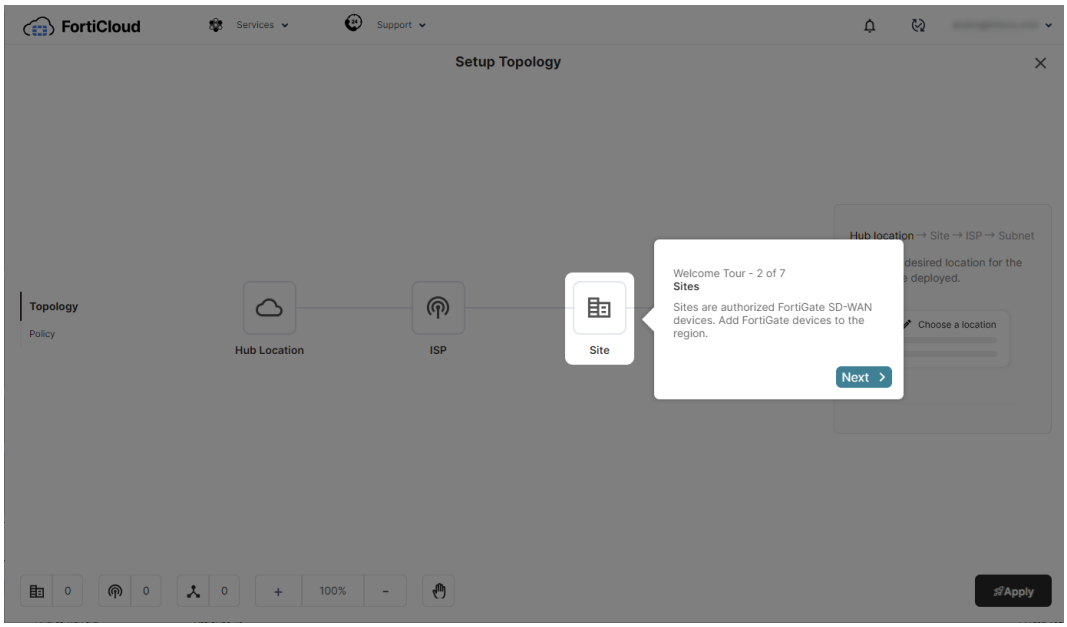
The *Topology* page provides a step-by-step walk through of configuring the topology for the first time. The walk through is split into several steps to provide an overview of the upcoming process. Once you complete the walk through, you can begin configuring your OaaS deployment. See Creating the initial topology on page 19.

The *Welcome Tour* talk through includes the following steps:

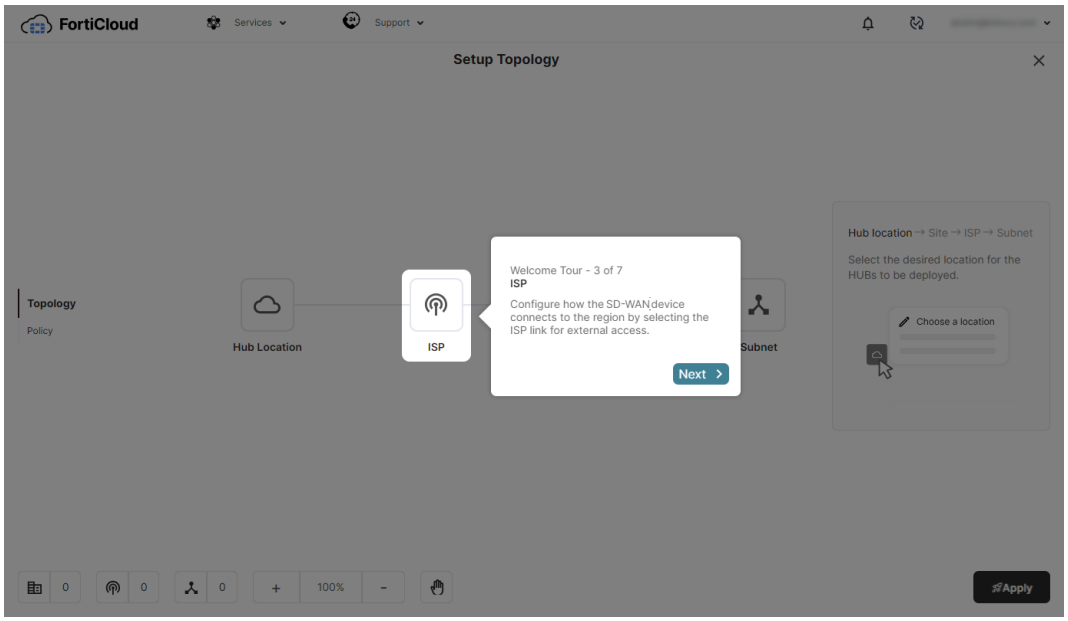
1. *Hub Locations*: You will first need to select two locations for the hub FortiGate.



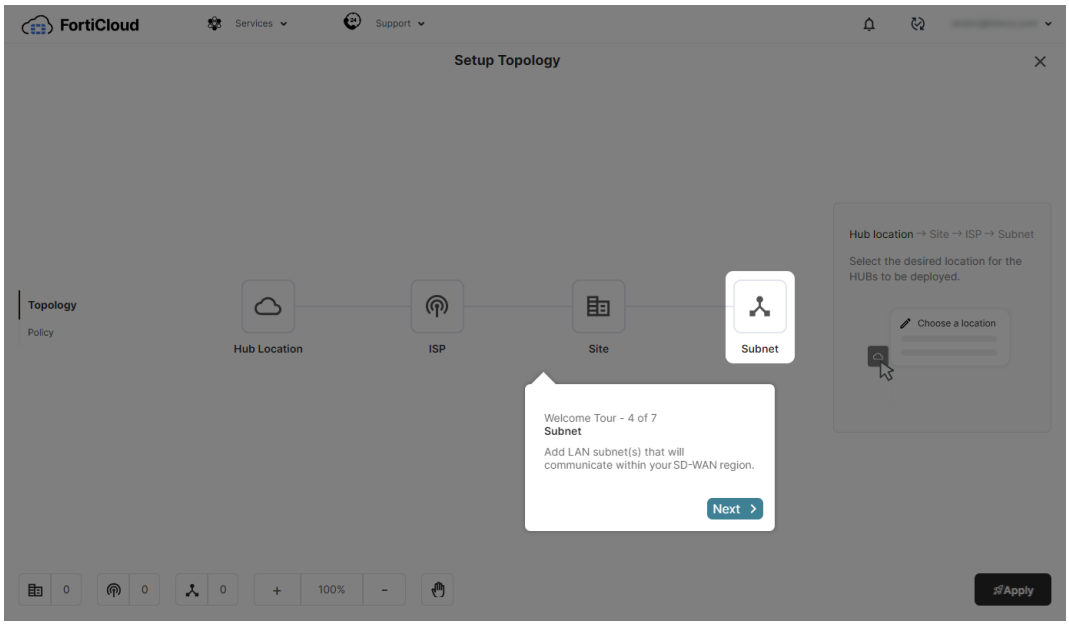
2. *Sites*: When selecting a *Site*, you are defining the SD-WAN device that will act as a site FortiGate.



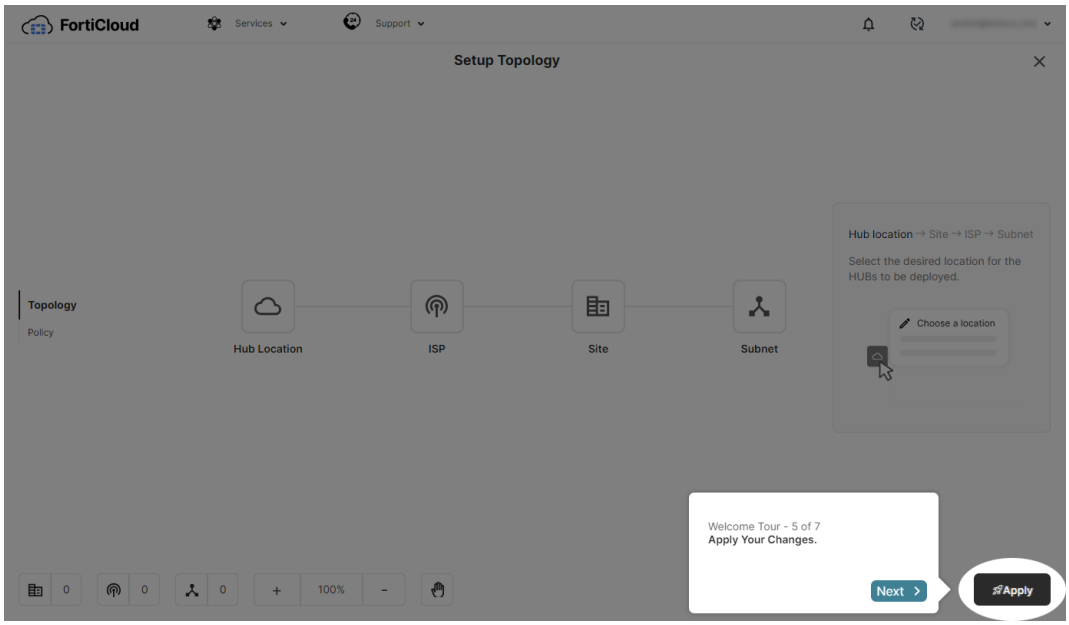
3. *ISP*: The ISP configured between the *Hub Location* and *Site* defines the external access link between the hub FortiGate and site FortiGate.



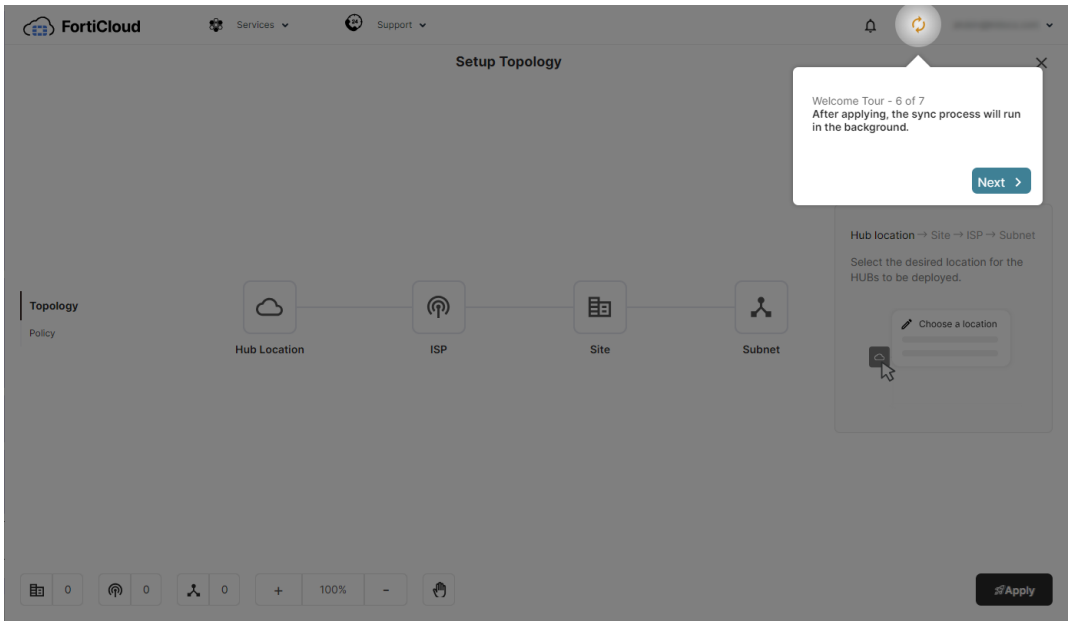
4. *Subnet*: You will then need to define any LAN subnets communicating within the SD-WAN region.



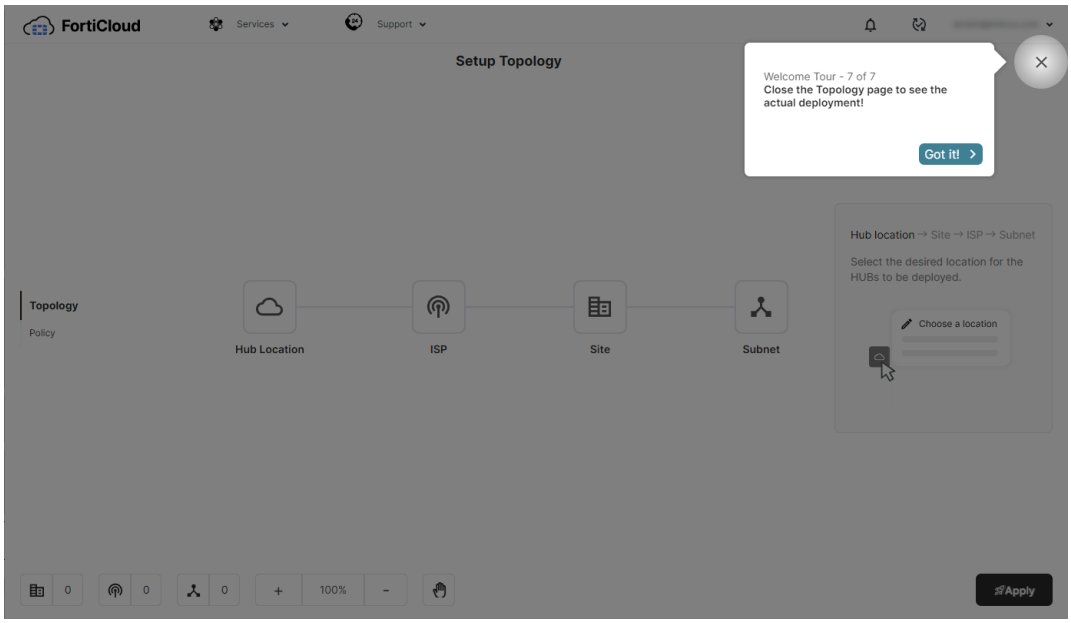
5. *Apply Your Changes*: Select *Apply* to create your initial topology and deployment.



6. *Sync*: The deployment will sync automatically once your apply the changes.



7. *Close*: Once you close the *Topology* page, you can view the OaaS deployment in the *Home* page.

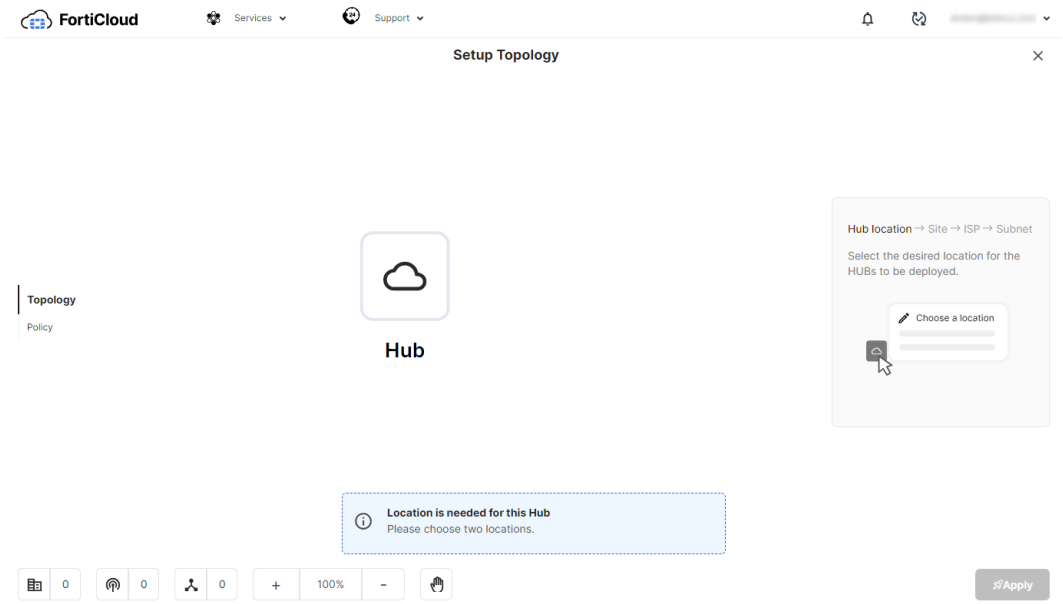


Creating the initial topology

When you first access the Overlay-as-a-Service portal, you can configure the OaaS deployment from the *Topology* page. Before you configure the topology, a walk through will display the general steps needed to complete the deployment. See Welcome tour on page 15.

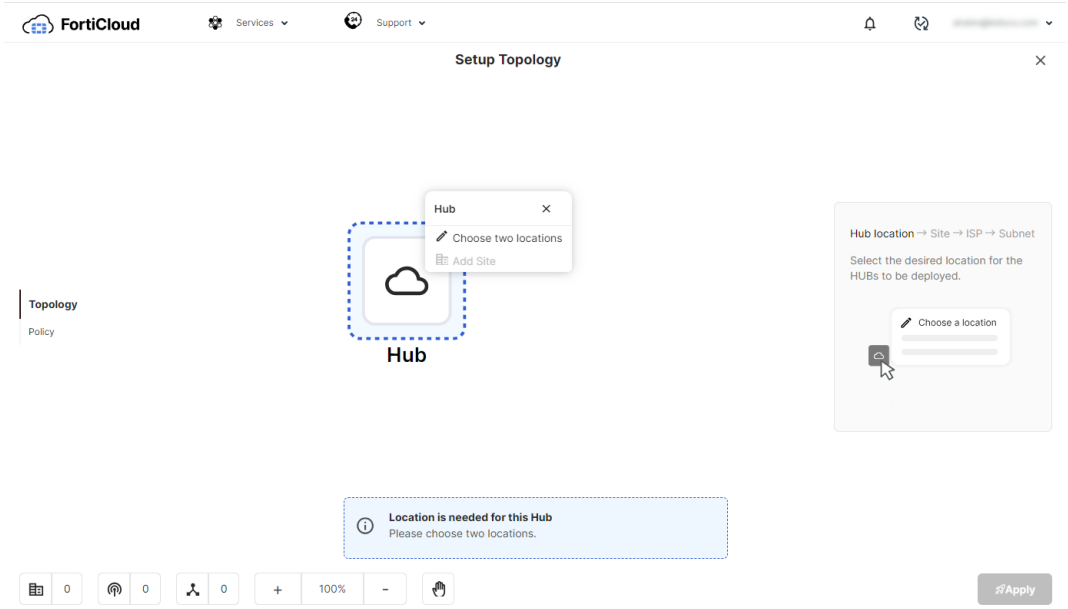
To create the initial topology:

1. Go to *Topology*. The *Setup Topology* page is displayed.

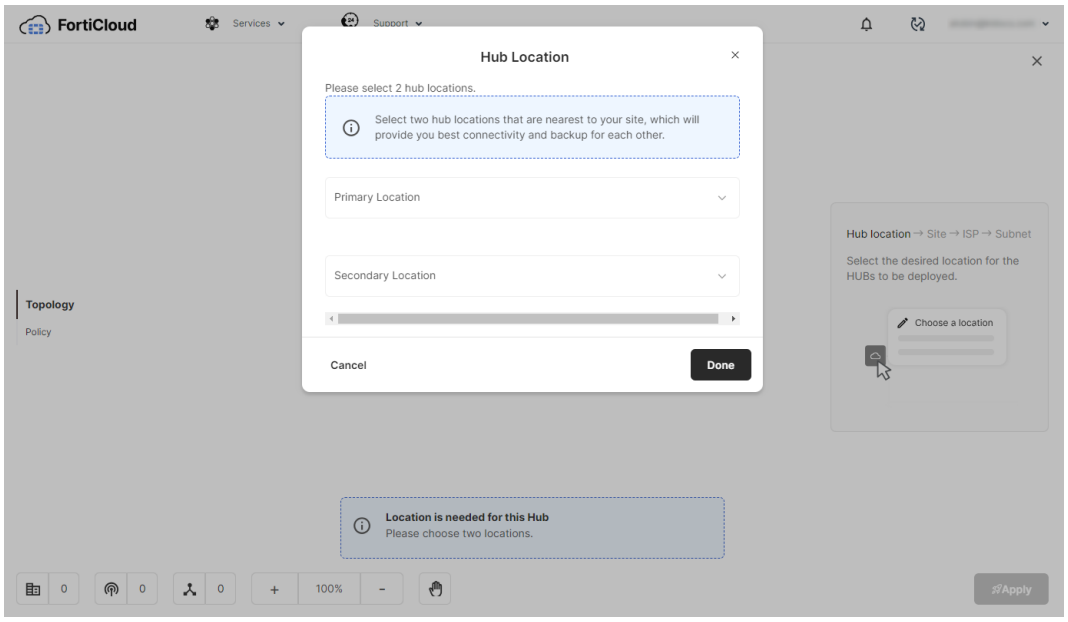


2. Set up the hub locations:

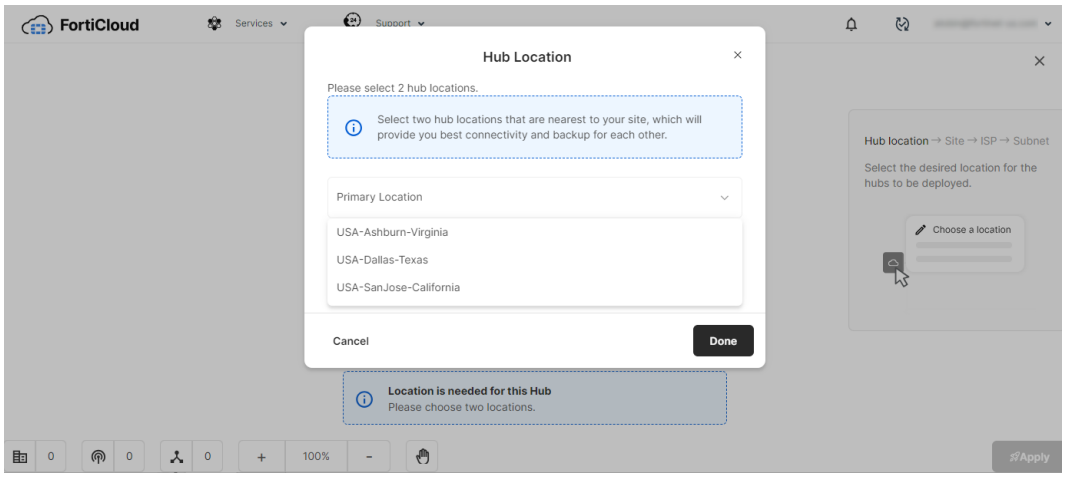
a. Click the *Hub*.



b. Click *Choose two locations*. The *Hub Location* dialog opens.



c. Use the *Primary Location* and *Secondary Location* dropdown lists to select your locations.

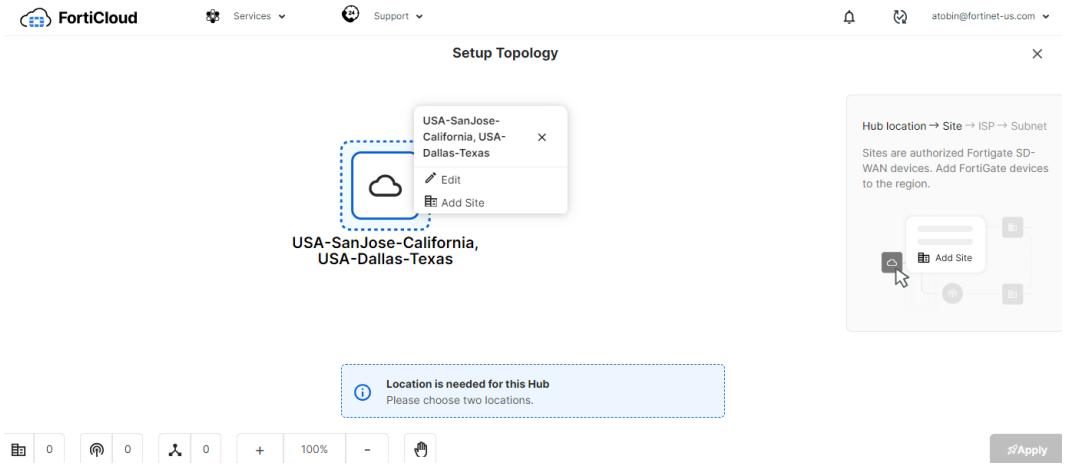


Select locations that are nearest to your site as this will provide the best connectivity and backup.

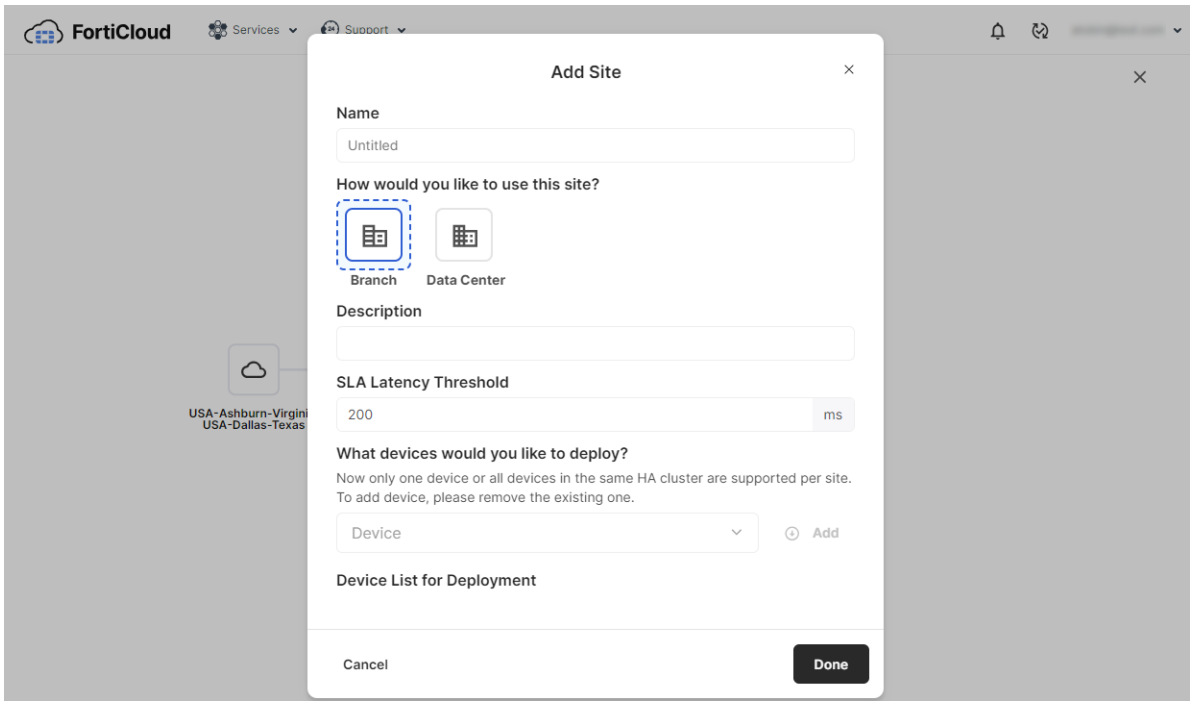
d. Click *Done*.

3. Add a site:

a. Click the *Hub*.



b. Select *Add Site*. The *Add Site* dialog opens.



c. Enter a *Name* for the site.

d. Set the site as either a *Branch* or *Data Center*.

Branch and *Data Center* sites affect how the site is displayed on the *Home* and *Topology* pages. OaaS configuration and management is not affected.

e. (Optional) Enter a *Description*.

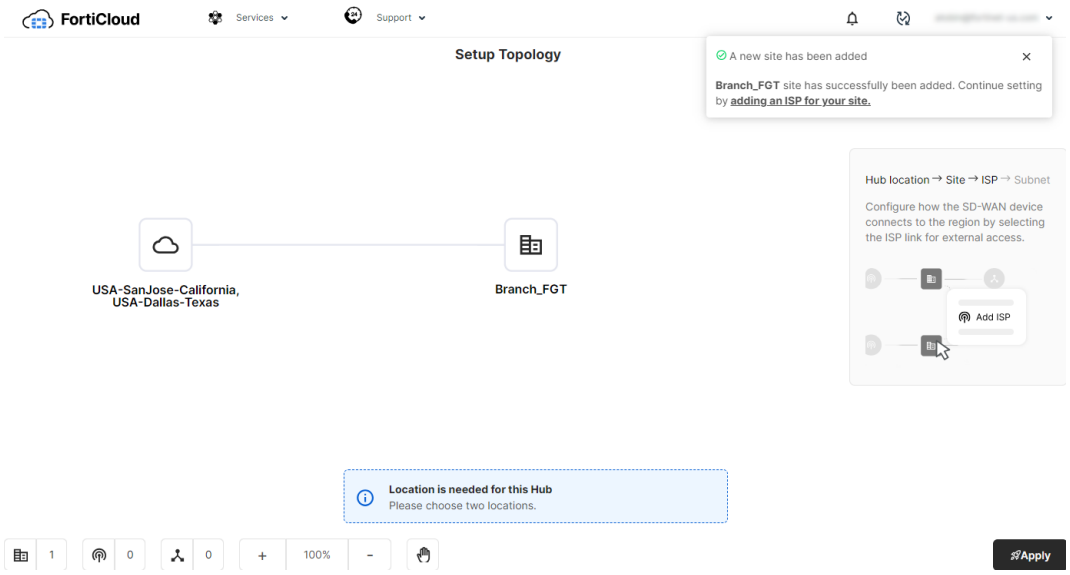
f. Enter the *SLA Latency Threshold*.

g. Select the FortiGate device to deploy from the *Device* dropdown menu.

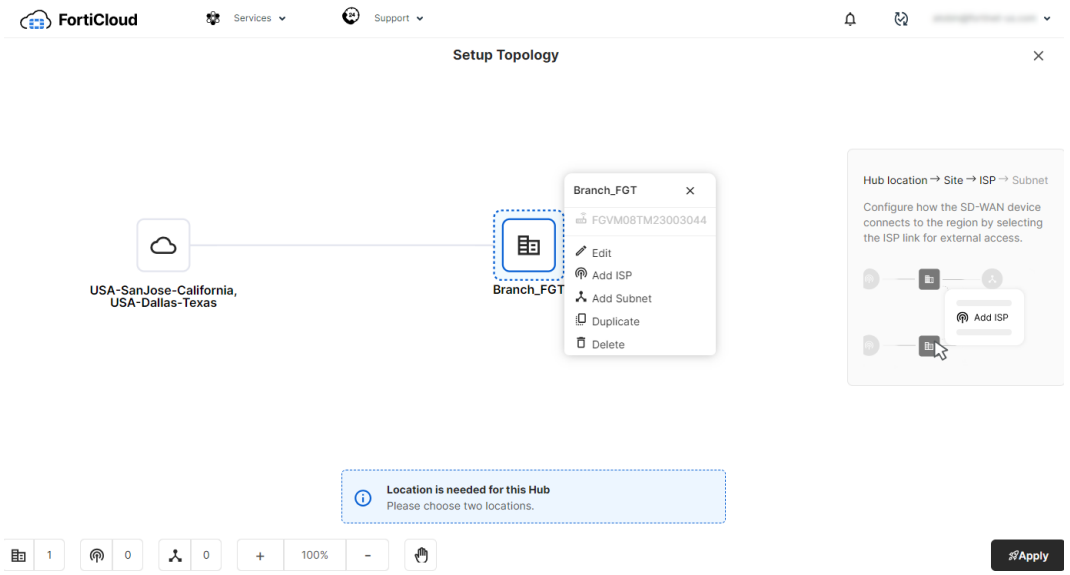
Single FortiGates or HA clusters can be added to a site. See Adding HA clusters to sites on page 27.

h. Click *Add*.

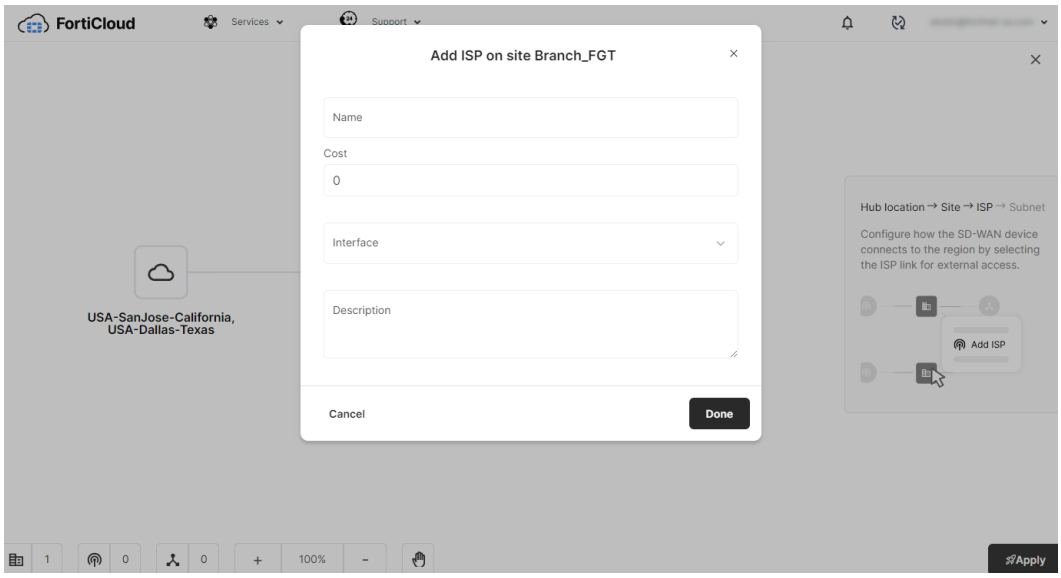
i. Click *Done*. The FortiGate is added to the topology as a site.



4. Add an ISP:
   a. Click the site.



   b. Select *Add ISP*. The *Add ISP on site <Site>* dialog opens.



c. Enter a *Name* for the ISP.

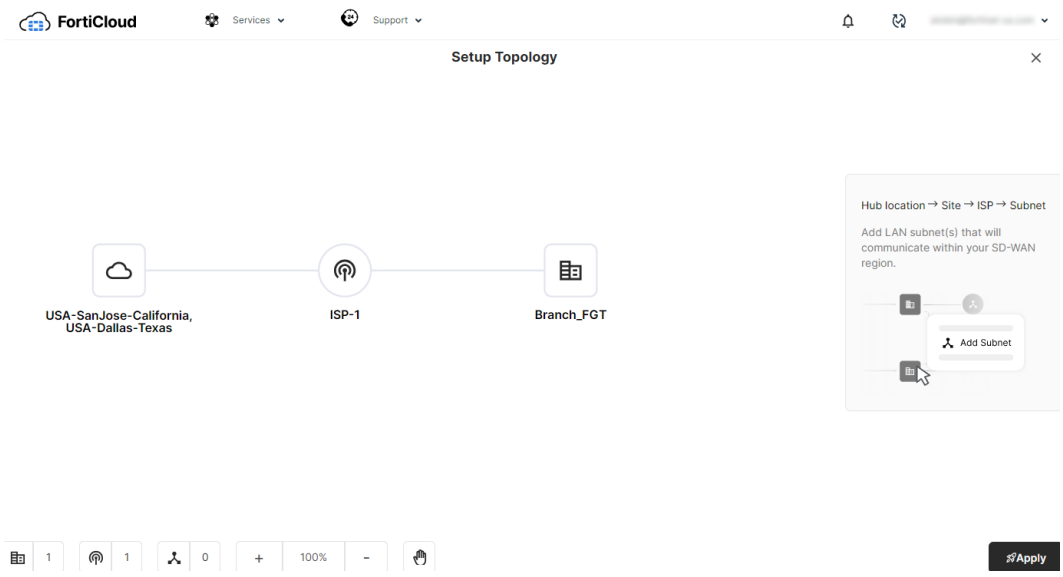
d. Enter the cost assigned to the ISP in the *Cost* field.

You can leave *Cost* as the default value of zero.

e. Select the interface from the *Interface* dropdown list.

f. (Optional) Enter a *Description*.

g. Click *Done*. The ISP is added between the hub and site.

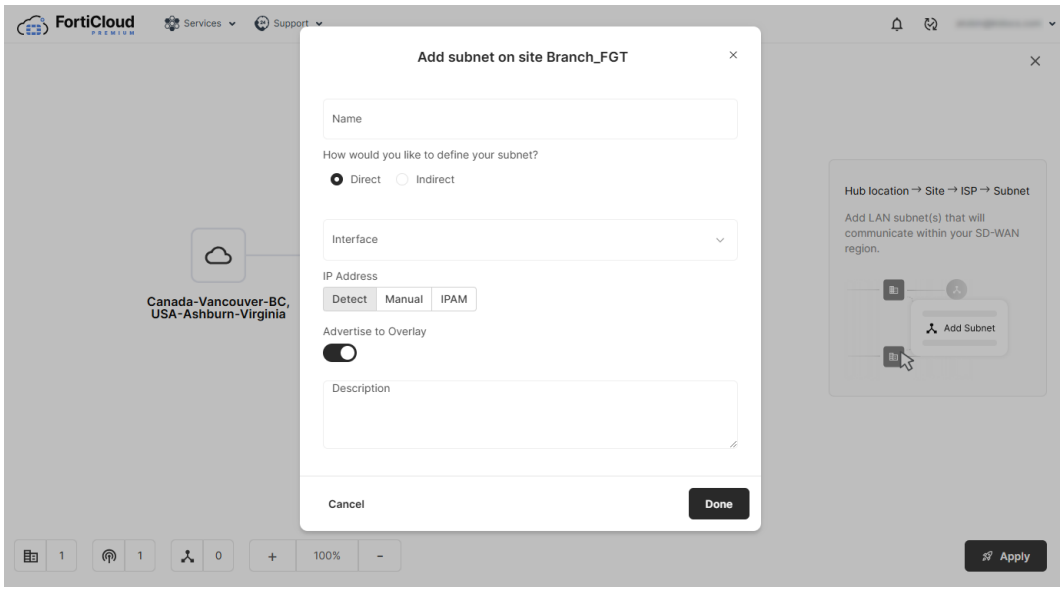


h. Repeat the above steps to add another ISP configuration. OaaS allows a maximum of three ISPs for each site.

5. Add a subnet:

a. Click the site.

b. Select *Add Subnet*. The *Add subnet on site <Site>* dialog opens.



c. Enter a *Name*.

d. Select *Direct* or *Indirect* for the subnet definition.

If an Indirect subnet is selected, the *CIDR* field is displayed.

---

e. Select the interface from the *Interface* dropdown list.

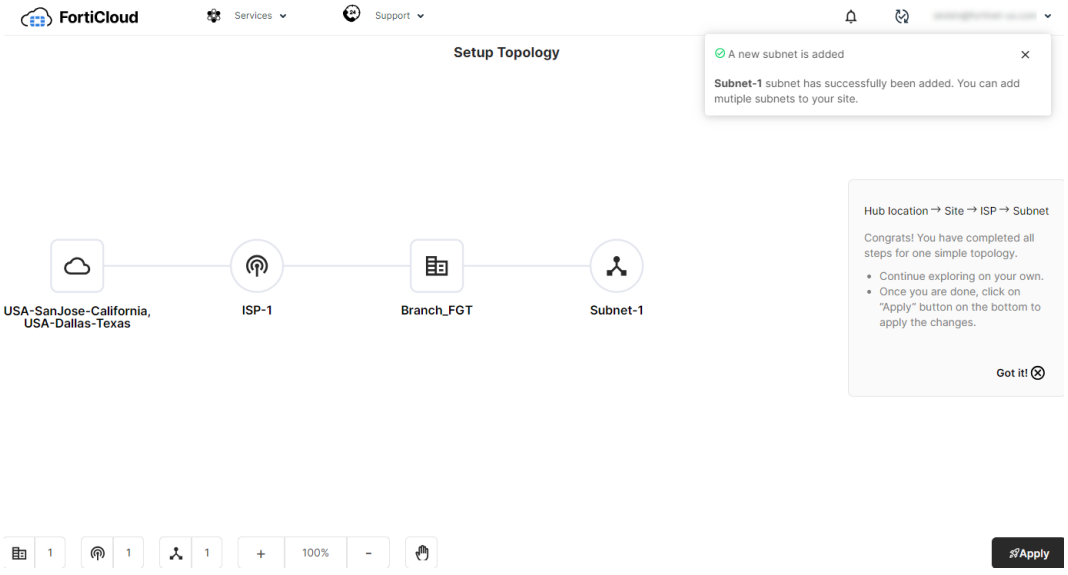
f. Select the *IP Address* method.

g. Configure the IP address information, as needed. Fields will differ depending on the *IP Address* selected.

h. Enable or disable *Advertise to Overlay*.

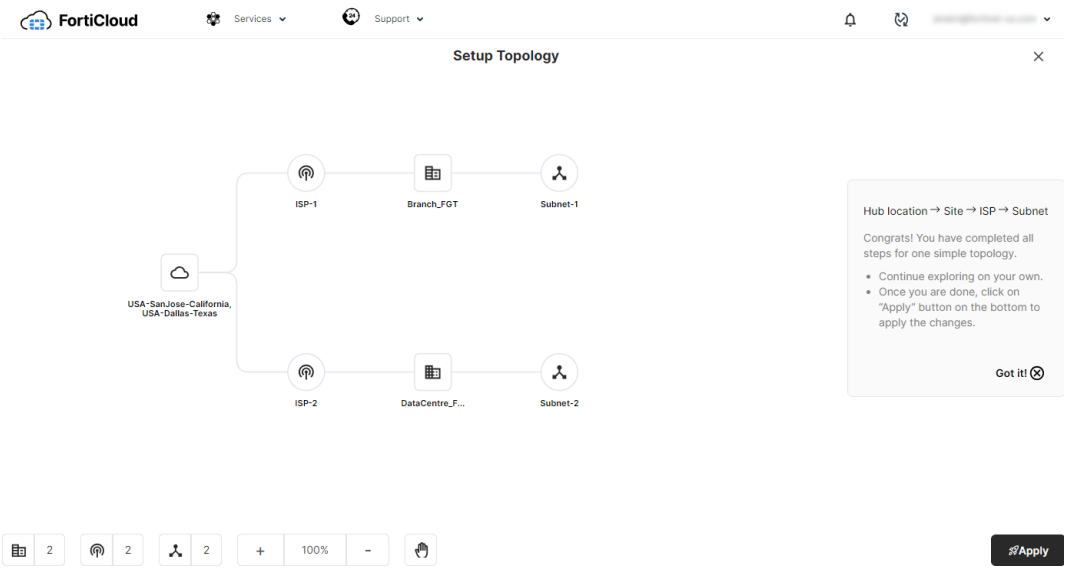
i. (Optional) Enter a *Description*.

j. Click *Done*. The subnet is added to the topology.

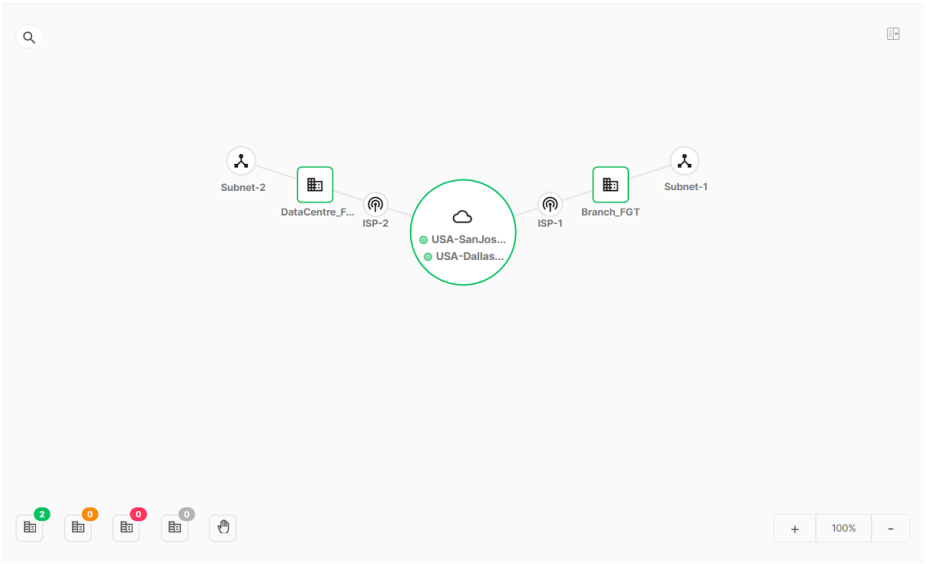


6. Repeat these steps to add another site configuration.

Not all FortiGate sites must be configured at once. You can add new sites, ISPs, and LAN subnets after you apply the initial configuration. See Adding a new site to a hub on page 26, Adding an ISP for the site on page 28, Adding a subnet for the site on page 29, and Deploying the SD-WAN configuration to your sites and viewing Task Status on page 30.



7. Click *Apply* to save changes the configuration.
8. Select the *X* to close the *Topology* page. The deployment is displayed in the *Home* page.



Adding a new site to a hub

SD-WAN sites are authorized FortiGate devices. Use OaaS to add your FortiGate devices to the site. You can assign the site as:

- *Branch*: Organization sites that need to access headquarter applications.
- *Data Center*: Organization headquarters that maintain business applications.

The hub locations must be set before you can add a new site. See Creating the initial topology on page 19.

You can also configure the site, ISP, and LAN subnet simultaneously from the *Site* page. See Creating a site on page 44.

To add a new site:

1. Go to *Topology*.
2. Click the *Hub*.
3. Select *Add Site*.
4. Enter a *Name* for the site.
5. Set the site as either a *Branch* or *Data Center*.
6. (Optional) Enter a *Description*.
7. Enter the *SLA Latency Threshold*.
8. Select the FortiGate device to deploy from the *Device* dropdown menu.

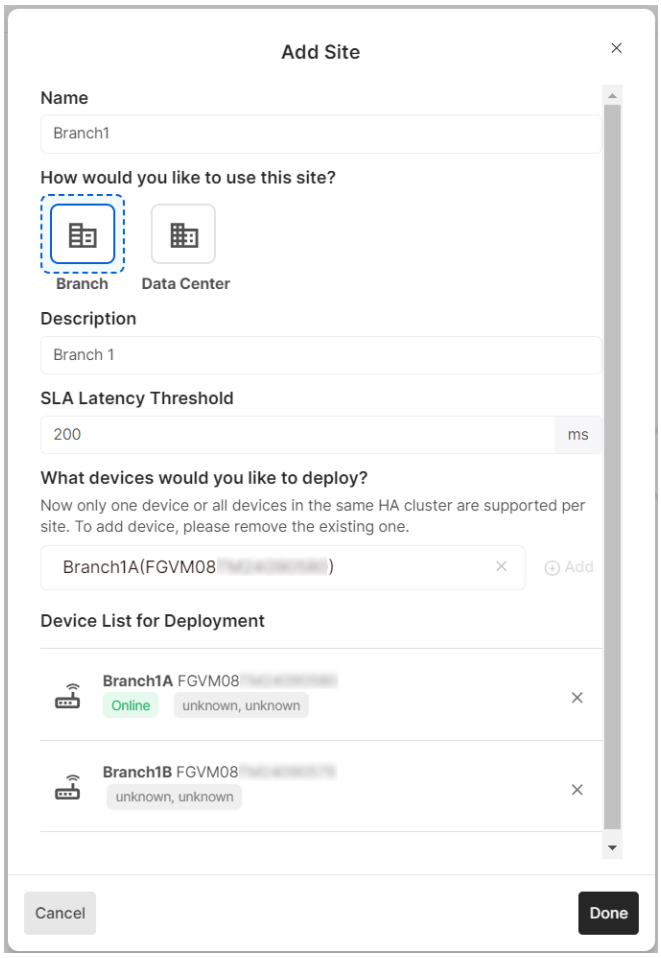
It is critical for the added FortiGate device to appear with a status of *Online*. If the device lacks a status of *Online*, check whether the device is:

- Powered on.
- Activated or logged in to FortiGate Cloud.
- Configured and properly connected to its ISP's WAN link.

9. Click *Add*.
10. Click *Done*. The FortiGate is added to the topology as a site.
11. If this there are no other configurations, click *Apply*. See Deploying the SD-WAN configuration to your sites and viewing Task Status on page 30.

Adding HA clusters to sites

HA clusters that have been set up outside of Overlay-as-a-Service can be added to a site when selecting the *Device*. To implement an HA cluster in Overlay-as-a-Service, select the primary FortiGate as the *Device* when adding a site. The secondary FortiGate in the HA cluster will be added to the *Device List for Deployment*.



See High Availability in the FortiOS Administration guide for more information on HA clusters.

Adding an ISP for the site

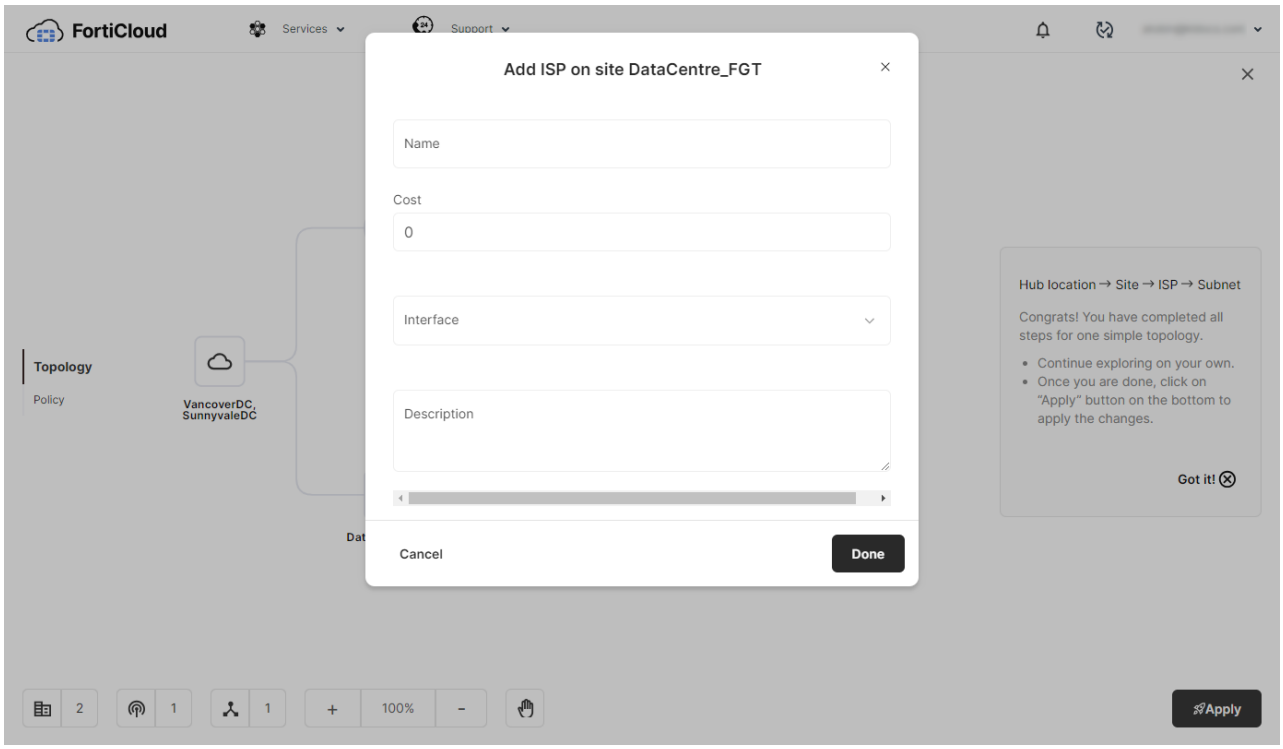
Configure how the SD-WAN device connects to the region by selecting the ISP link for external access.

The hub locations and site must be set before you can add a new ISP. See Creating the initial topology on page 19 and Adding a new site to a hub on page 26.

You can also configure the site, ISP, and LAN subnet simultaneously from the *Site* page. See Creating a site on page 44.

To add an ISP for your site:

1. Go to *Topology*.
2. Click the site.
3. Select *Add ISP*. The *Add ISP on site <Site>* dialog opens.



4. Enter a *Name* for the ISP.
5. Enter the cost assigned to the ISP in the *Cost* field.
6. Select the interface from the *Interface* dropdown list.
7. (Optional) Enter a *Description*.
8. Click *Done*. The ISP is added between the hub and site.
9. Repeat the above steps to add another ISP configuration. OaaS allows a maximum of three ISPs for each site.
10. If there are no other configurations, click *Apply*. See Deploying the SD-WAN configuration to your sites and viewing Task Status on page 30.

Adding a subnet for the site

You can add LAN subnets that will communicate within your SD-WAN region from the *Home* page. You can define subnets as either *Direct* or *Indirect*:

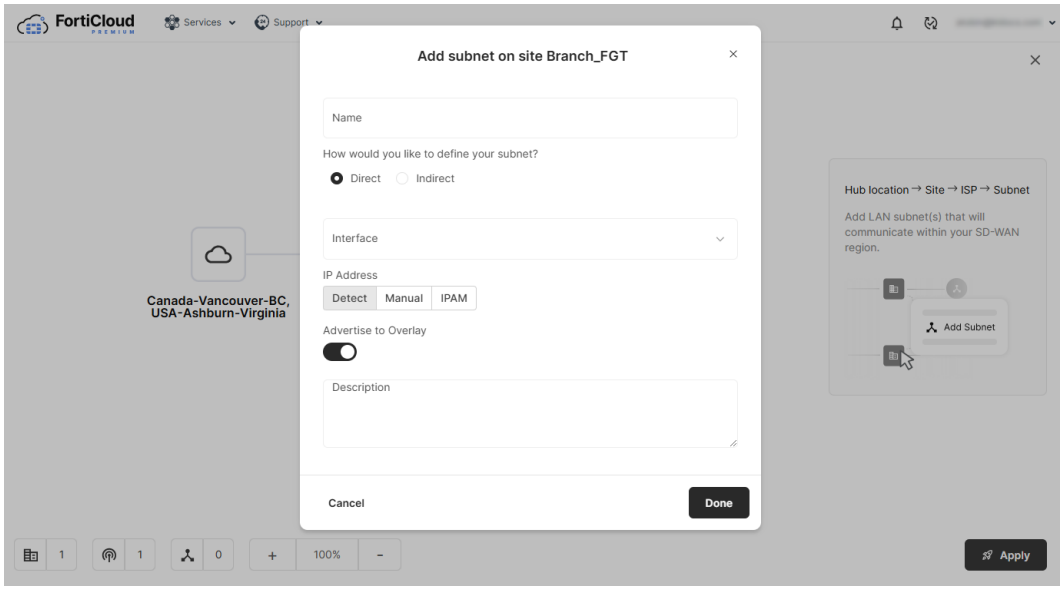
- *Direct*: Directly select the subnet assigned to a FortiGate interface.
- *Indirect*: Use a Classless Inter-Domain Routing (CIDR) prefix to input a network summary address behind the interface. You can create multiple indirect subnets behind the same interface, if needed.

The hub locations, site, and ISP should be set before you can add a new subnet. See Creating the initial topology on page 19, Adding a new site to a hub on page 26, and Adding an ISP for the site on page 28.

You can also configure the site, ISP, and LAN subnet simultaneously from the *Site* page. See Creating a site on page 44.

To add a subnet for your site:

1. Click the site.
2. Select *Add Subnet*. The *Add subnet on site <Site>* dialog opens.



3. Enter a *Name*.
4. Select *Direct* or *Indirect* for the subnet definition.
5. Select the interface from the *Interface* dropdown list.
6. Select the *IP Address* method.
7. Configure the IP address information, as needed. Fields will differ depending on the *IP Address* selected.
8. Enable or disable *Advertise to Overlay*.
9. (Optional) Enter a *Description*.
10. Click *Done*. The subnet is added to the topology.
11. If this there are no other configurations, click *Apply*. See Deploying the SD-WAN configuration to your sites and viewing Task Status on page 30.

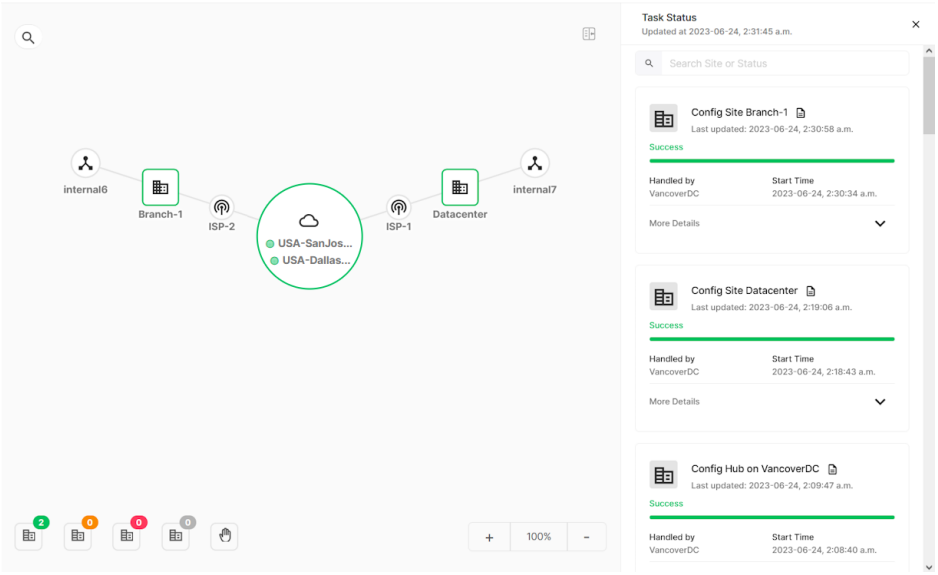
Deploying the SD-WAN configuration to your sites and viewing Task Status

You can add several sites with their corresponding ISP and subnets in the *Topology* page. When you apply the changes, the configuration is deployed to the FortiGates, and the SD-WAN network is configured. The status of each configuration within the topology is displayed in the *Task Status*.

To apply changes and view Task Status:

1. Go to *Topology*.
2. Add the desired sites and their corresponding configuration. See Adding a new site to a hub on page 26, Adding an ISP for the site on page 28, and Adding a subnet for the site on page 29.

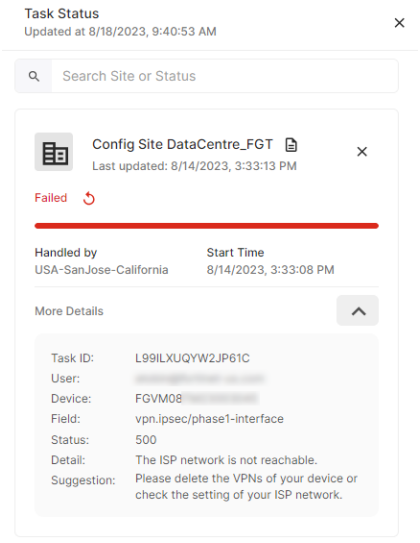
3. Click *Apply*. After clicking *Apply*, the sync process runs in the background.
4. Click the *X* at top-right to close the *Setup Topology* page and view the deployment.
5. Next to the FortiCloud username at the top-right of the screen, click the *Task Status* icon to view the status of each configuration task.



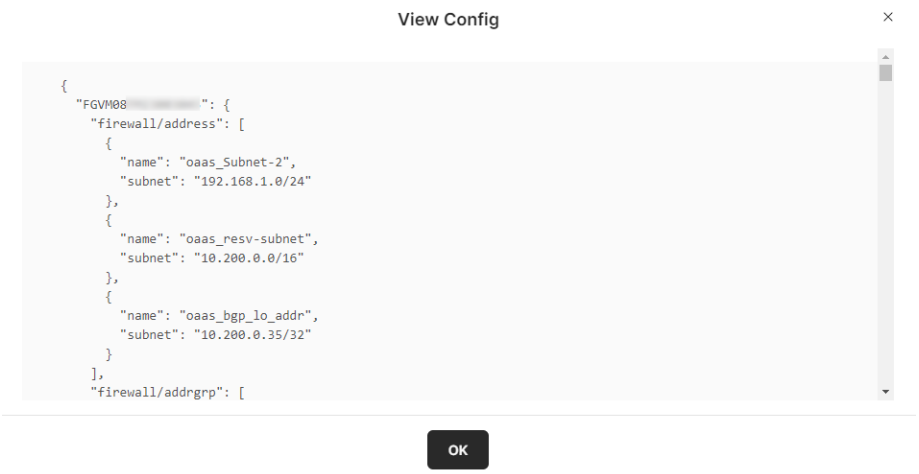
Failed configurations

If a configuration in the topology fails, the configuration will appear as red in the *Task Status*. You can review information on the configuration to identify troubleshooting scenarios:

- For suggestions on how to successfully connect an asset, select *Details*.



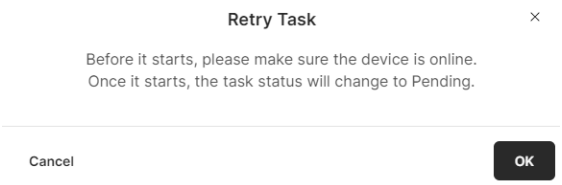
- For information on the configuration, click *View Config*.



You can retry the connection for each asset from the *Task Status* in case the issue has been resolved.

To retry a failed connection:

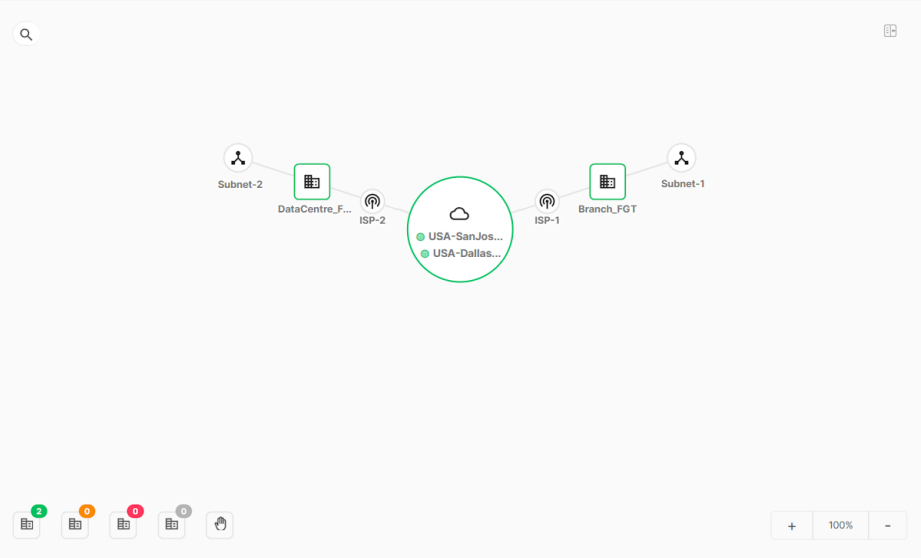
1. Next to the FortiCloud username at the top-right of the screen, click the *Task Status* icon.
2. Identify the failed connection.
3. Click *Retry*. The *Retry Task* dialog is displayed.



4. Click *OK*.

Home

In the *Home* page, you can view the completed topology and the status of the sites.

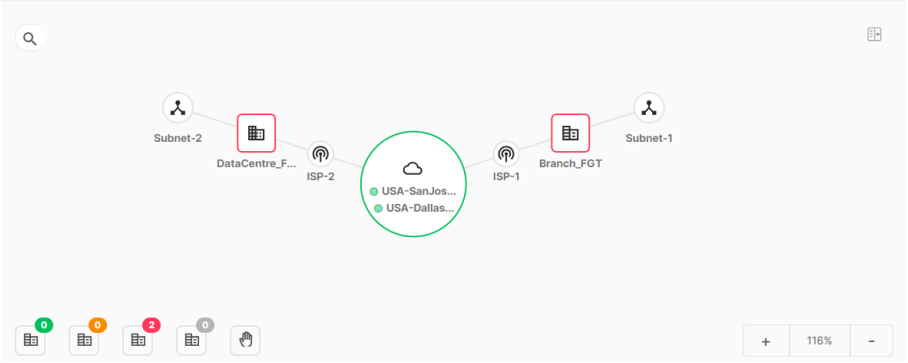


This section includes:

Topology status

The color of the device outline and icons at the bottom of the page define the status indicators:

- *Green*: Number of devices in the All Pass state, where all overlays are connected.
- *Orange*: Number of devices in the Operational state, where some overlays are connected. When either the tunnel to primary or secondary hub is down, a device falls into the Operational state.
- *Red*: Number of devices in the Disconnected state. The state of the site falls to Disconnected when both tunnels of the FortiGate device in the site are down.
- *Grey*: Number of devices in the Unmanaged state. The state of the site falls to Unmanaged when the OaaS portal loses communication with the FortiGate device.

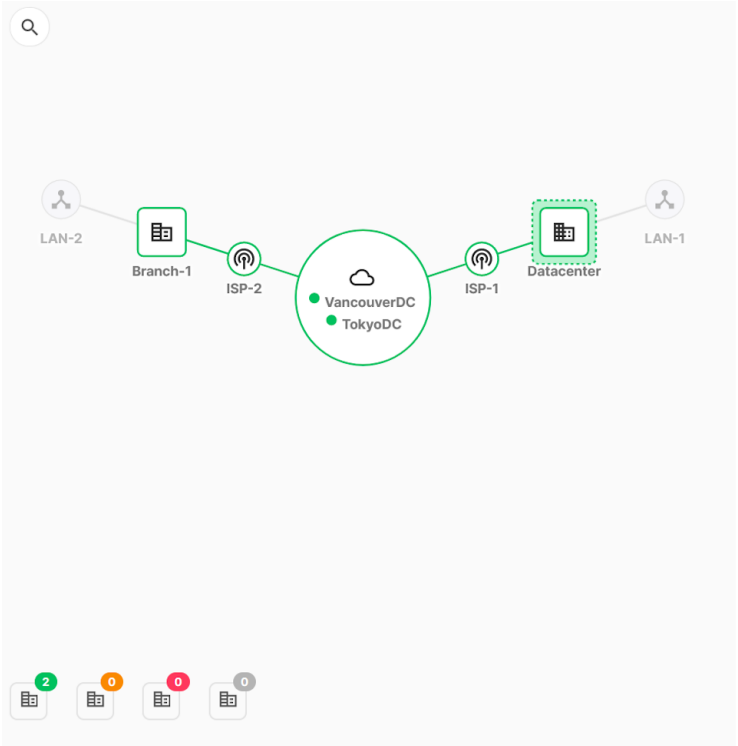


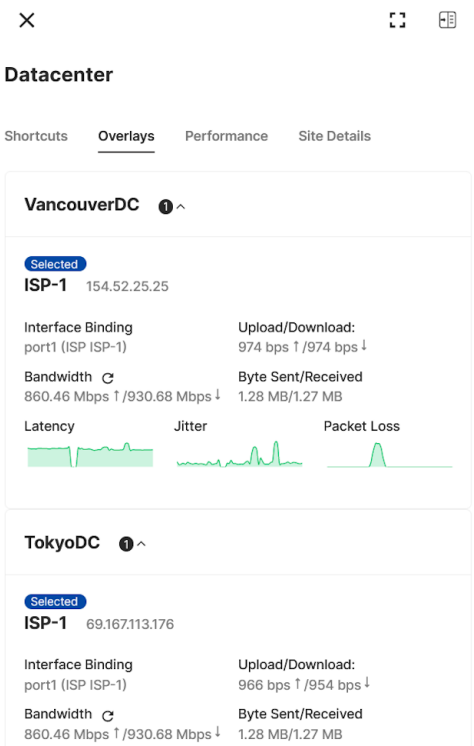
Monitoring link performance and quality across SD-WAN devices in OaaS

You can monitor link performance and quality across SD-WAN devices in OaaS from the *Home* page.

To monitor link performance and quality:

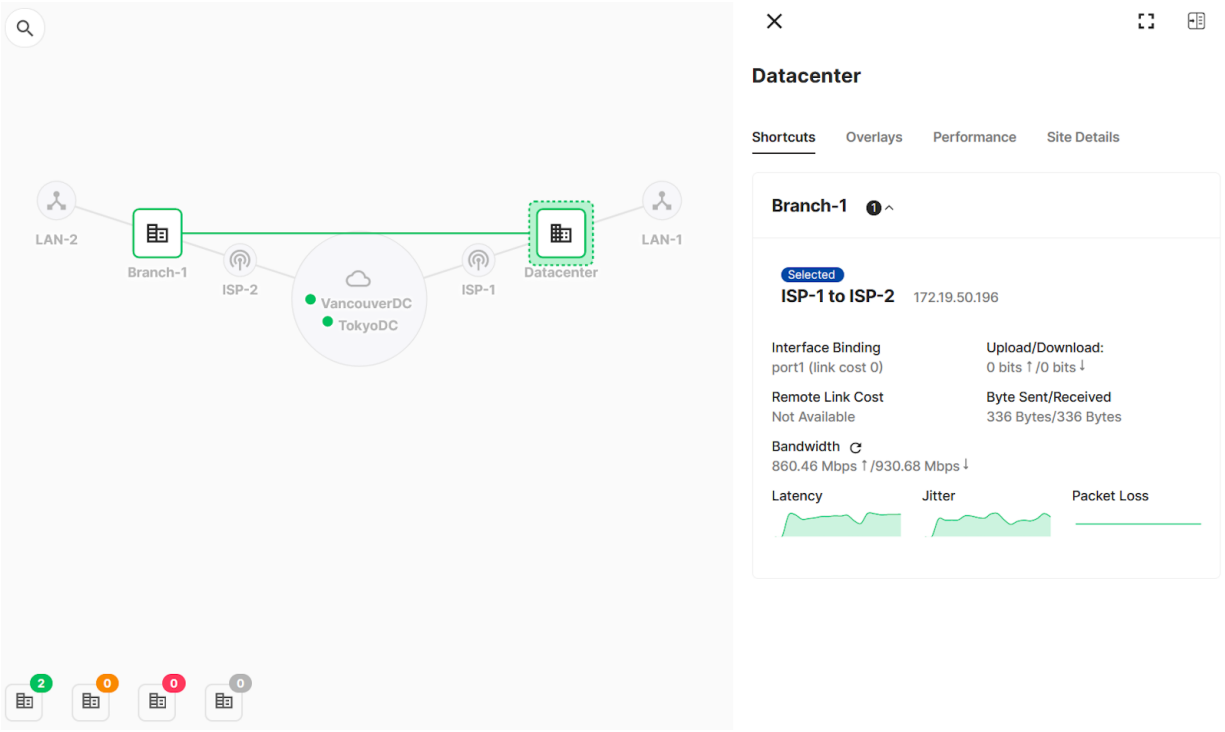
1. Select any of the sites in the diagram or enter a site name in the *Search* field to monitor the health of their overlays, monitor their performance, and view site details.



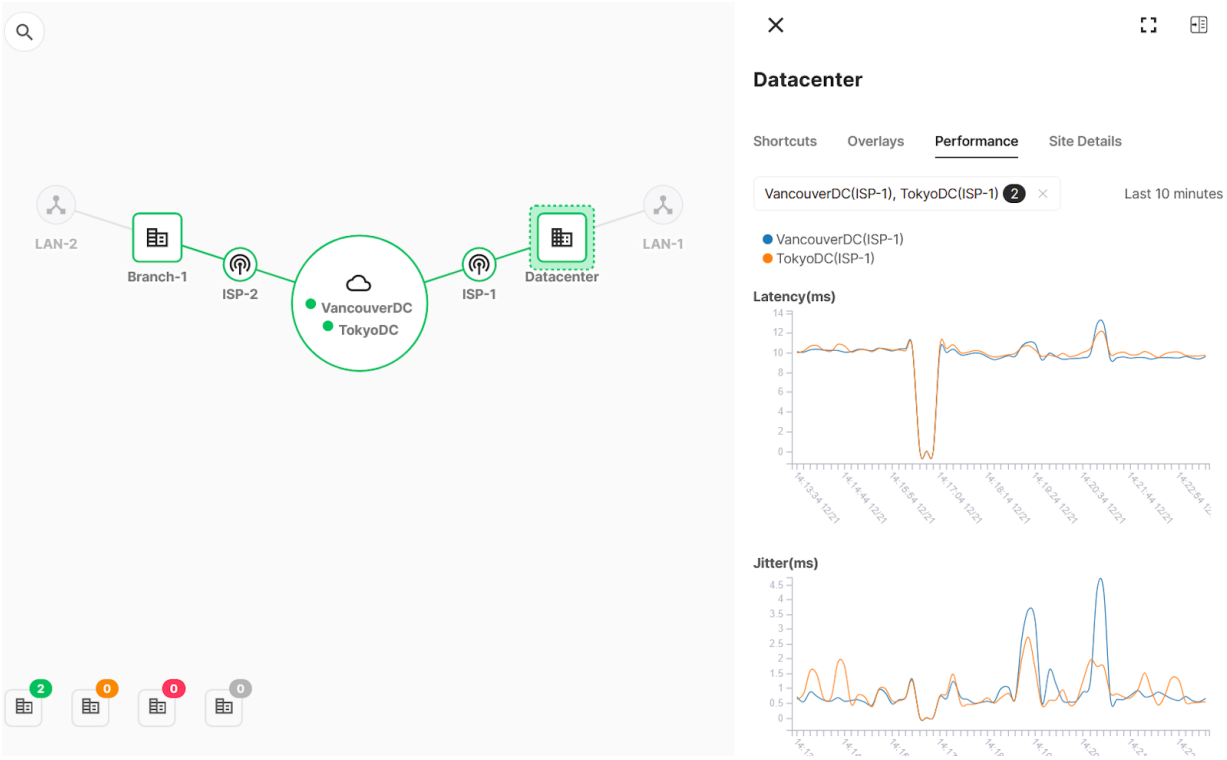


If bandwidth displays as *Not Available*, it can be determined by performing a speed test. See Performing bandwidth speed tests on page 38.

2. Select *Shortcuts* to monitor the health of the shortcut tunnels between sites.

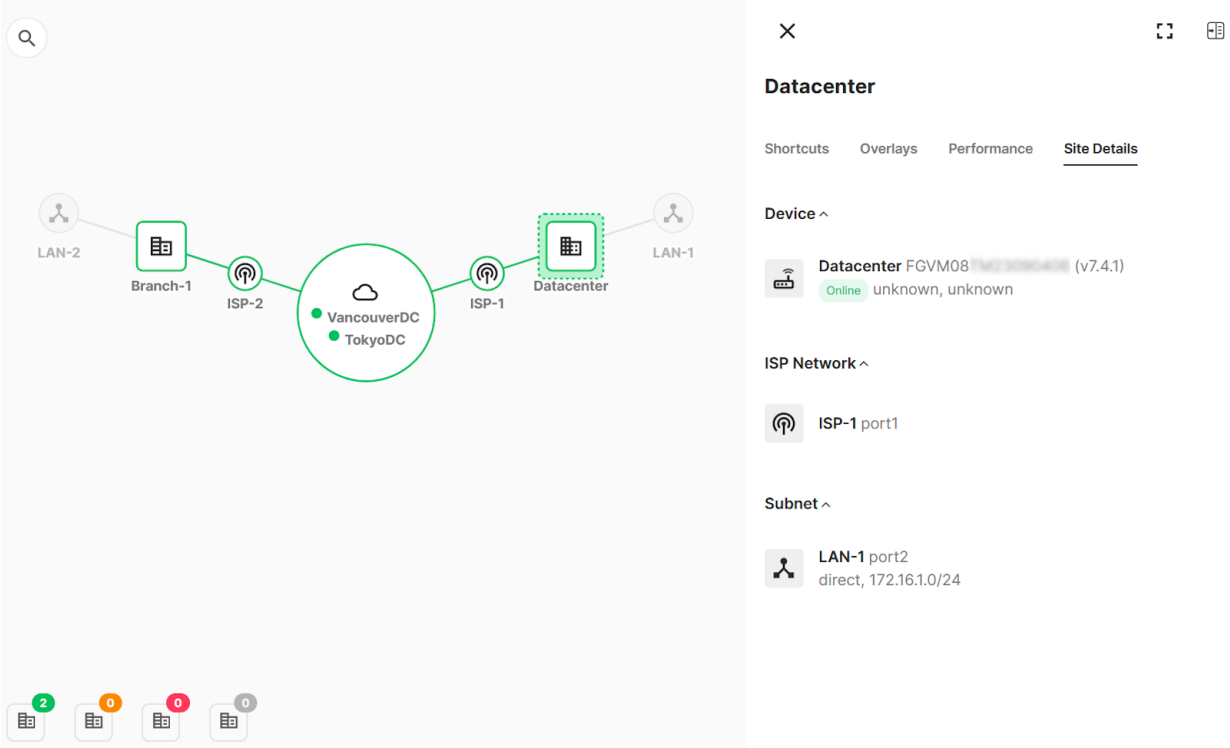


3. Select *Performance*, and then use the graphs to monitor the latency, jitter, and packet loss. Select a time stamp to view the values for the hub locations and remote sites on the graphs.



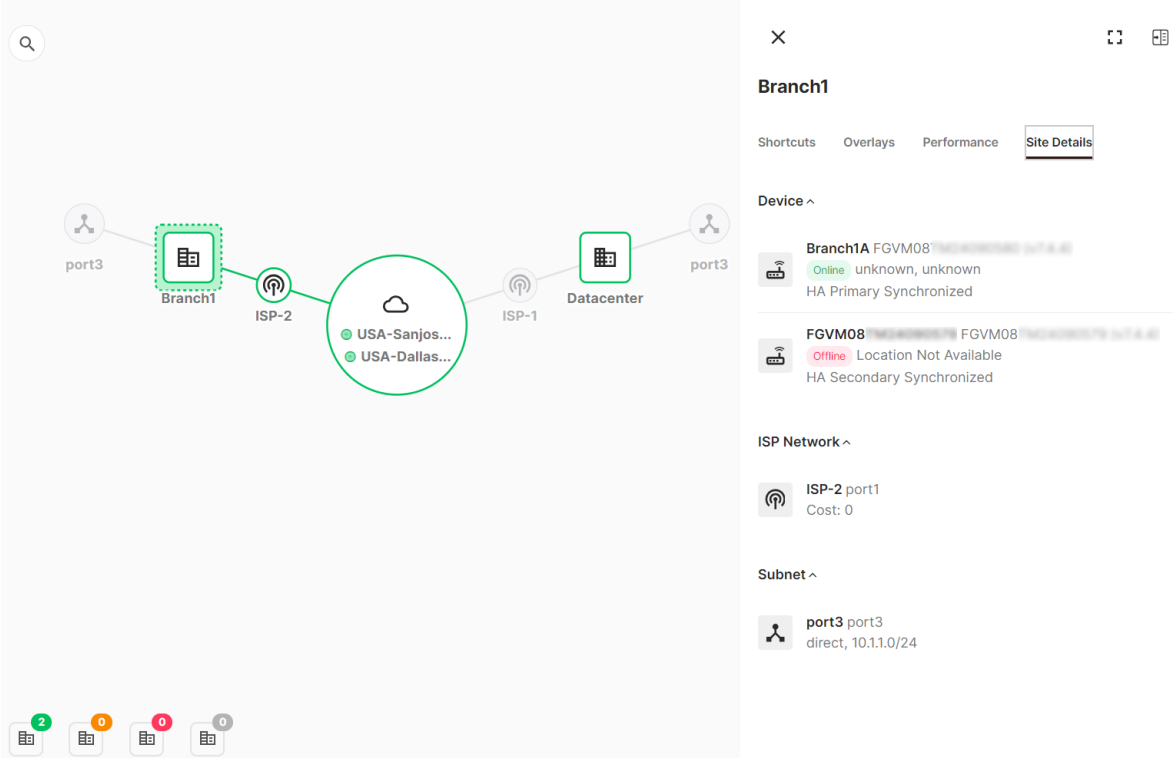
4. Select *Site Details* to review details about the selected site.

The image version of the FortiGate device is displayed in the *Site Details*. If the image version does not meet OaaS requirements, a warning message will be displayed.



Site details of HA clusters

If a site is configured with an HA cluster, the *Site Details* will include information on both FortiGates devices that are included in the cluster.



See High Availability in the FortiOS Administration guide for more information on HA clusters.

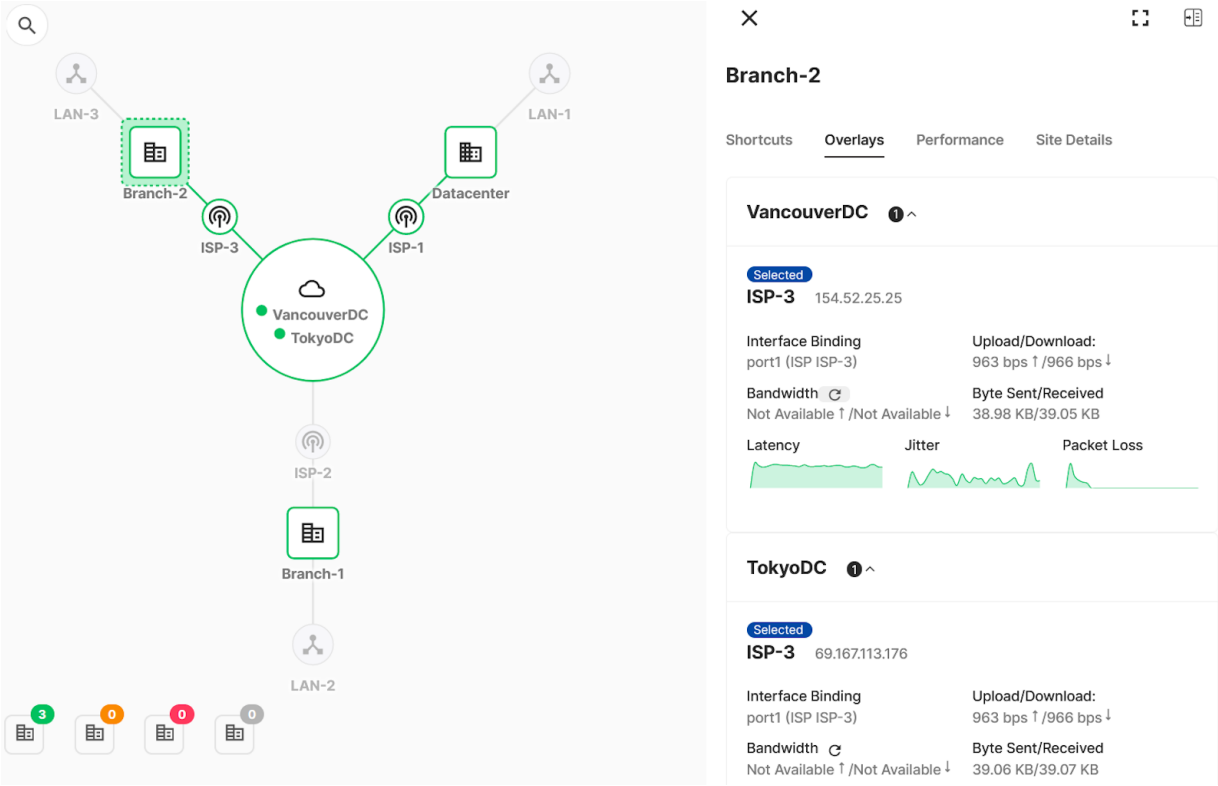
Performing bandwidth speed tests

When viewing the site Overlays, a speed test is required for obtaining the bandwidth of an interface. The bandwidth will appear an *Not Available* if a speed test has not been performed.

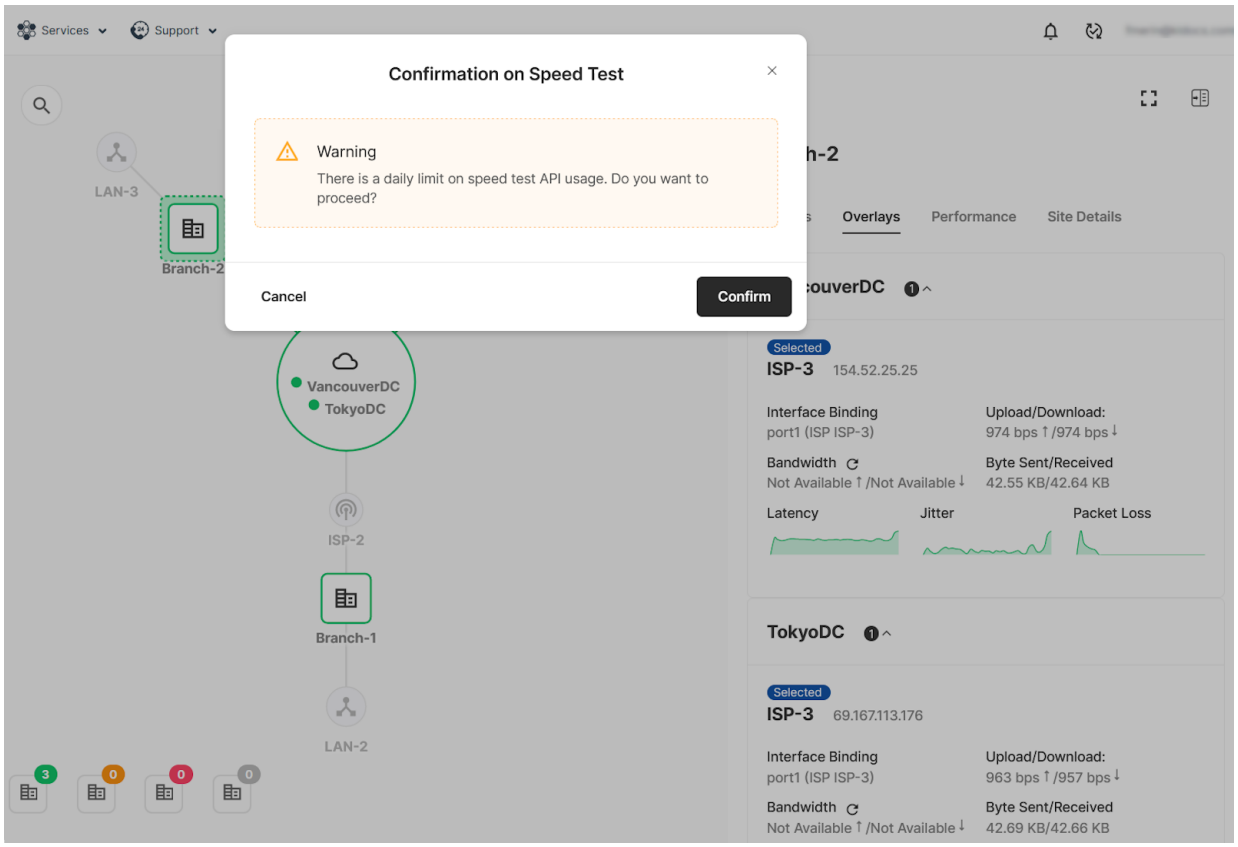
The speed test is per port and can only be performed a limited number of times per day. It can lasts for approximately 10-20 seconds and utilizes the full capacity of a network port.

To perform a speed test:

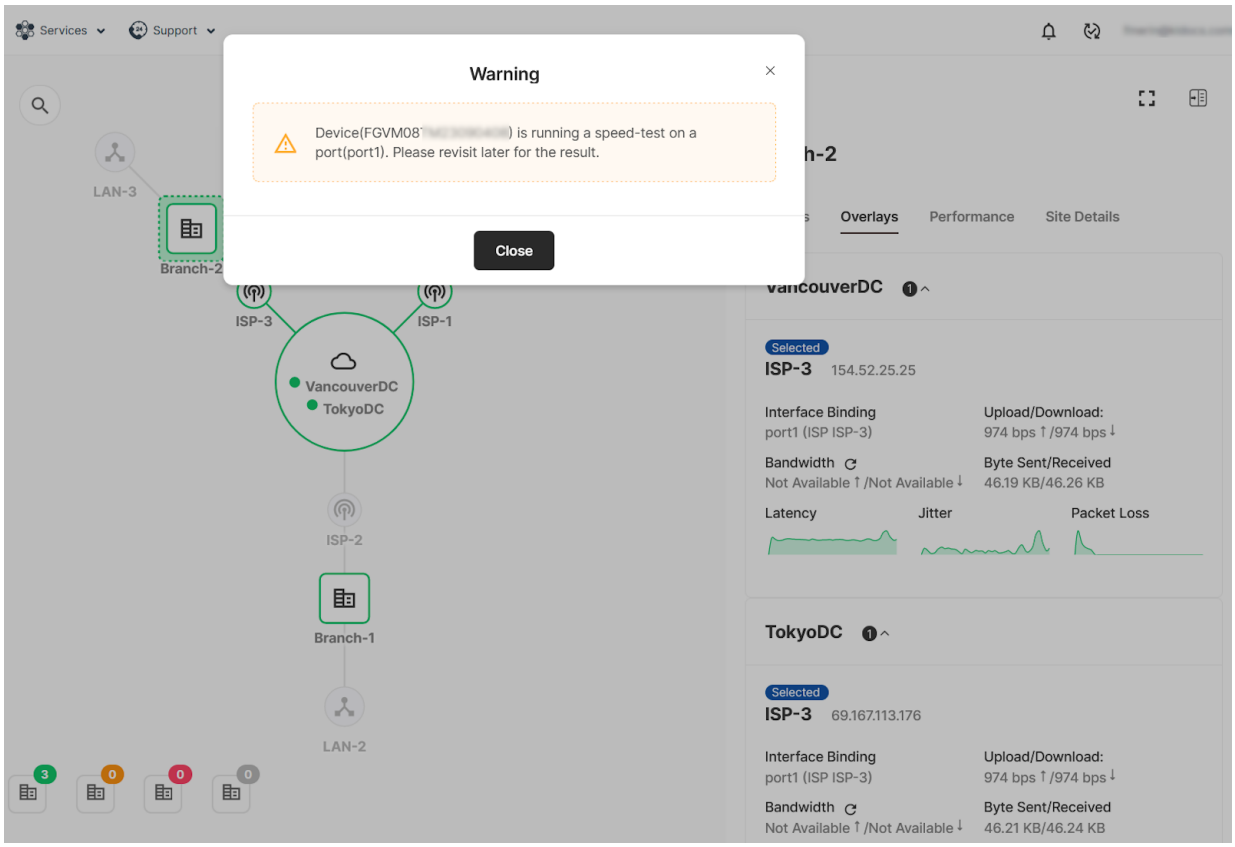
1. Go to *Home* and select the site you want to review.



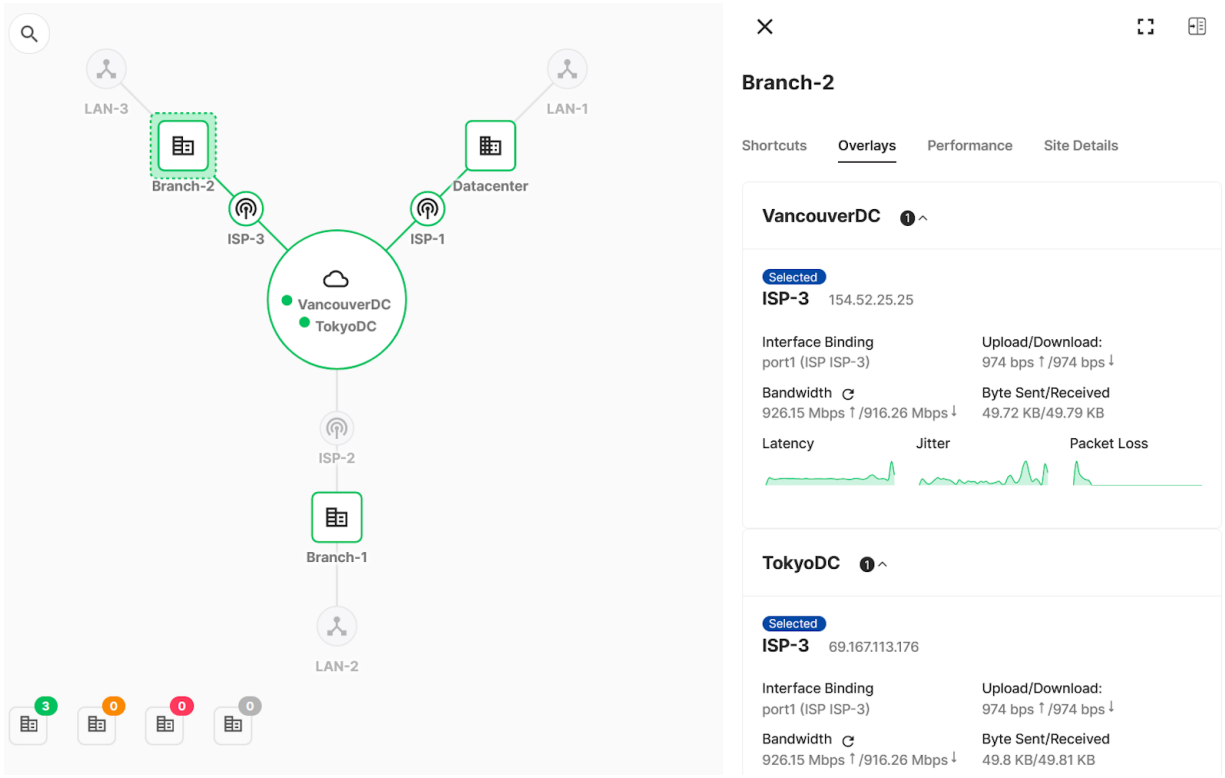
2. In the *Overlays* tab, refresh the *Bandwidth* field. A message displays to indicate the daily API usage limit.



3. Click *Confirm*. The speed test will begin and a warning will display to indicate that the speed test is currently ongoing.

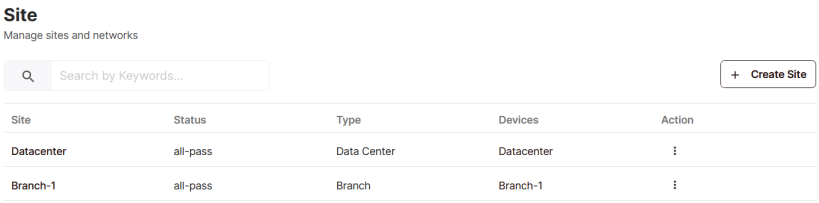


4. Click *Close*. When the speed test is complete, the *Bandwidth* field will update.



Site

In the *Site* page, you can view a table of the sites that have been added. You can also add more sites by clicking *Create Site* to enter the *Add Site* dialog.



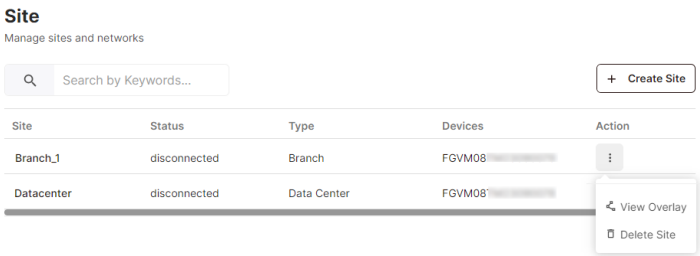
This section includes:

Viewing site overlay

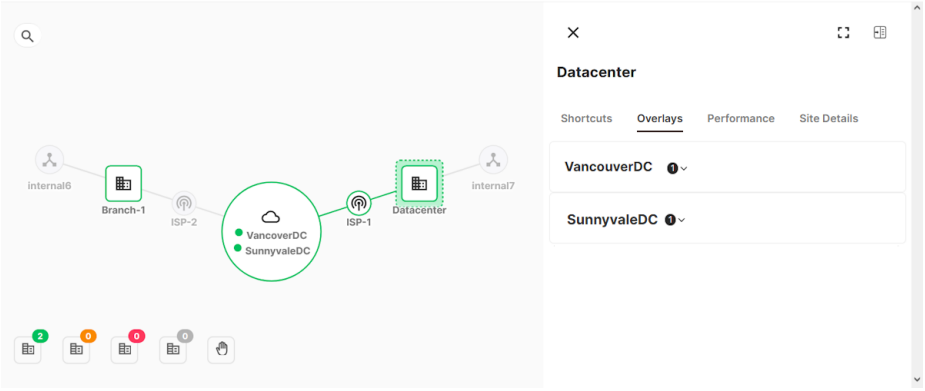
You can monitor link performance and quality from the *Site* page. See Monitoring link performance and quality across SD-WAN devices in OaaS on page 34 for more information.

To view site overlay:

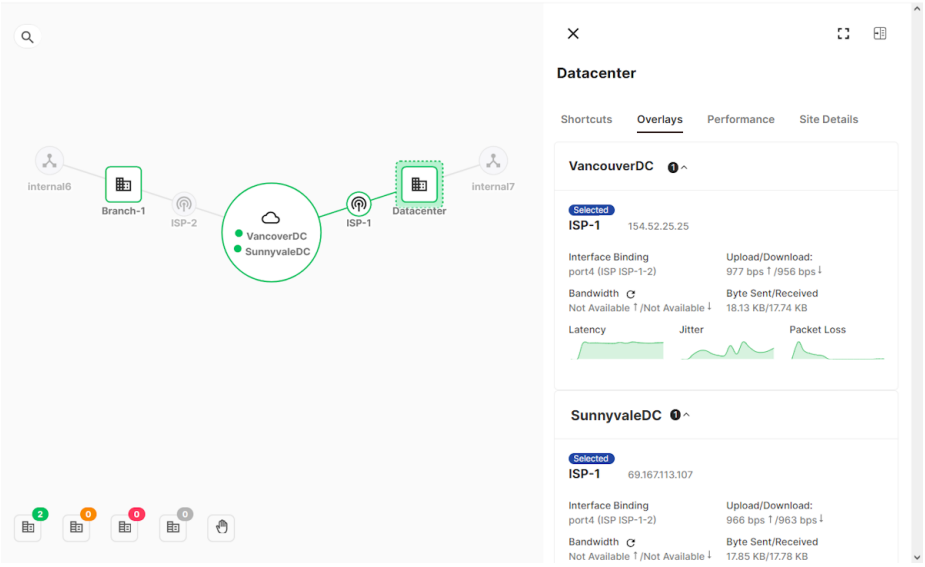
1. Go to *Site* and identify the site you want to review.
2. Select *Action* > *View Overlay*.



The site *Overlay* pane opens.

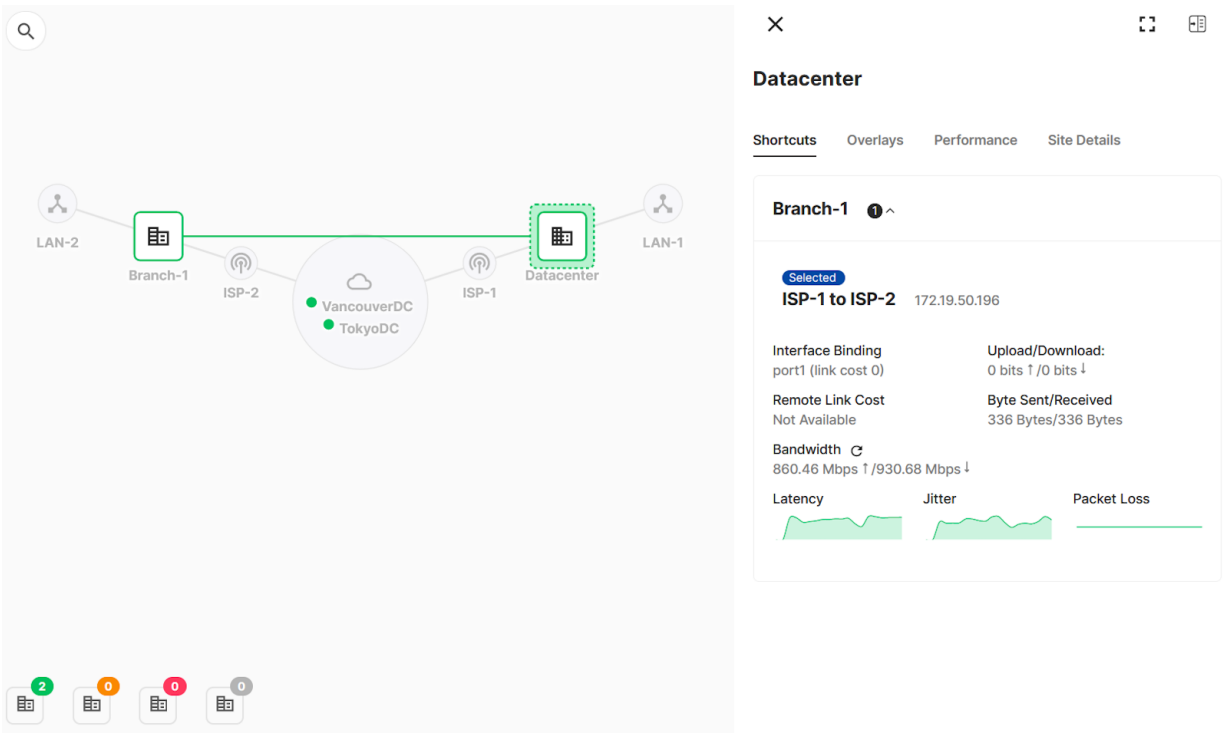


Select the Hub names to expand for more details.



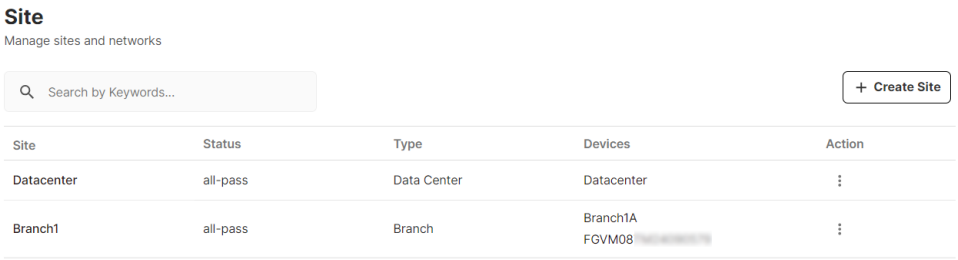
Bandwidth can be determined by performing a speed test. See Performing bandwidth speed tests on page 38.

3. Select *Shortcuts* to monitor the health of the shortcut tunnels between sites.



Viewing HA clusters

Sites that have been configured with HA cluster FortiGates can be reviewed using the same method as sites with single FortiGate associations. The primary and secondary HA FortiGates will display in *Devices*.



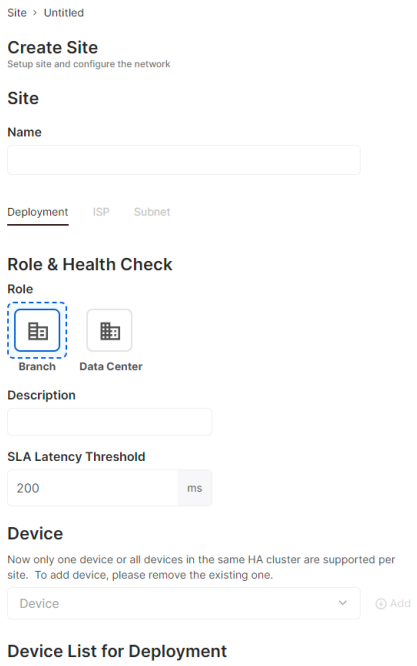
See High Availability in the FortiOS Administration guide for more information on HA clusters.

Creating a site

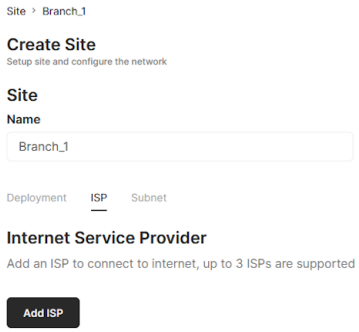
You can create a new site and define the ISP and LAN subnet simultaneously from the *Site* page.

To create a new site:

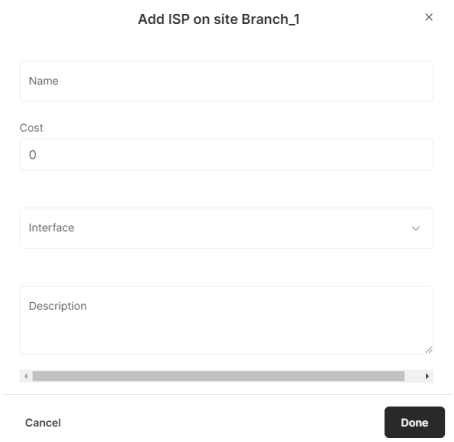
1. Go to *Site*.
2. Click *Create Site*.



3. Enter the *Name*.
4. Configure the site details in the *Deployment* tab. See Adding a new site to a hub on page 26 for more information.
5. Select the *ISP* tab.

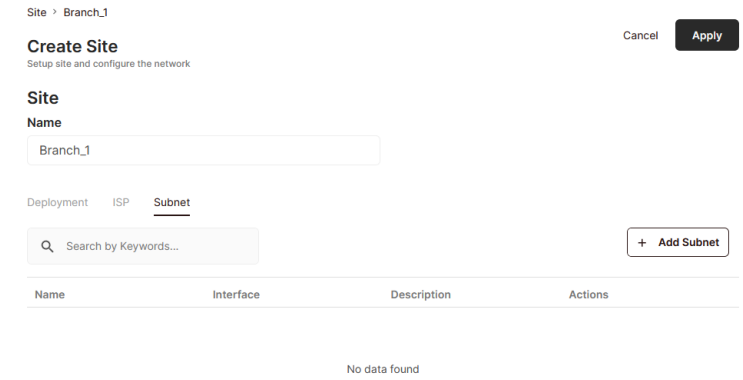


6. Click *Add ISP*. The *Add ISP on site <Branch>* dialog is displayed.

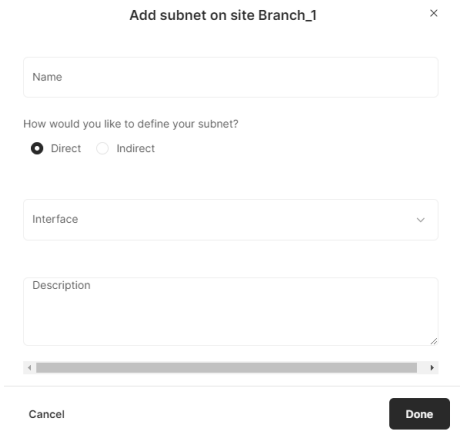


7. Configure the ISP details. See Adding an ISP for the site on page 28 for more information.

8. Select the *Subnet* tab.



9. Click *Add Subnet*. The *Add subnet on site <Branch>* dialog is displayed.



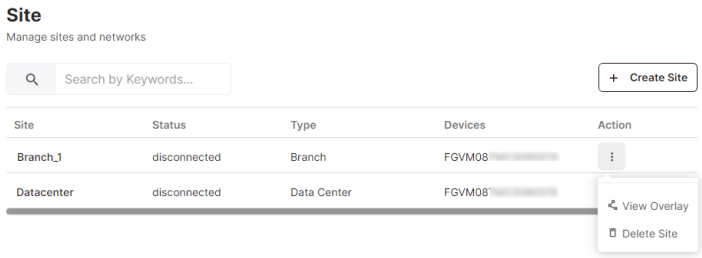
10. Configure the subnet details. See Adding a subnet for the site on page 29 for more information.
11. Click *Apply*.

Deleting sites

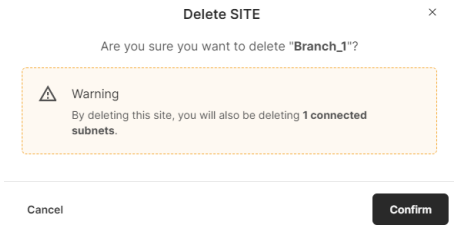
You can permanently remove a site FortiGate and connected LAN subnets from the *Site* page.

To delete a site:

1. Go to *Site* and identify the site you want to delete.
2. Select *Action* > *Delete Site*.



The *Delete SITE* confirmation message is displayed.

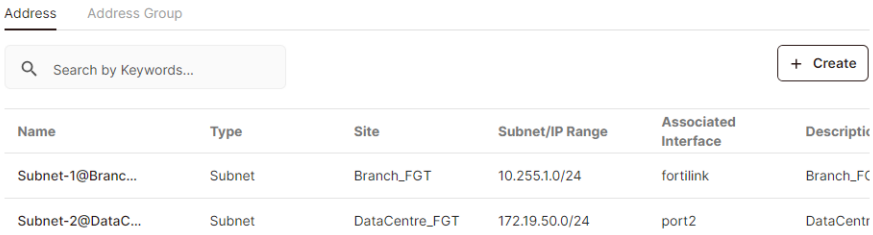


3. Click *Confirm*.

Address

Address objects and groups can be creating and managed in the *Address* pages. The addresses can be used in an OaaS policy to identify the source and destination of the traffic flow. For more information about address objects and groups, see Address objects in the FortiOS Administration Guide.

Subnet addresses will be automatically added to the address list when you add a subnet to your topology. See Creating the initial topology on page 19 and Adding a subnet for the site on page 29 for more information.

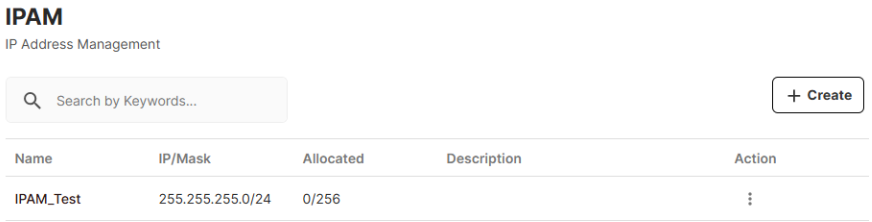


This section includes:

IPAM

This feature requires a site to be running FortiOS 7.4.5 and above. Major version 7.6.0 and above is not currently supported.

IP address management (IPAM) can be configured in the *Address* > *IPAM* page. For information on IPAM, see Configure IPAM locally on the FortiGate in the FortiOS Administration Guide.

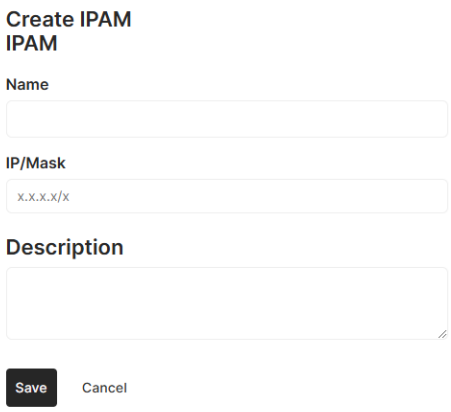


Configuring IPAM

New IPAM can be configured in the *Address* > *IPAM* page.

To configure IPAM:

1. Go to *Address* > *IPAM*.
2. Click *Create*.



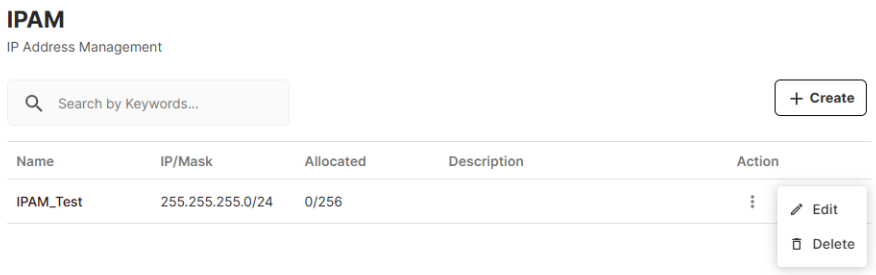
3. Enter the *Name*.
4. Enter the *IP/Mask*.
5. Enter a *Description*, if desired.
6. Click *Save*.

Managing IPAM

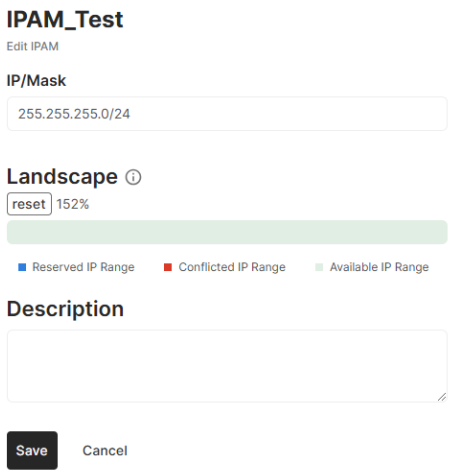
You can edit and delete existing IPAM instances from the *Address* > *IPAM* page. When editing an IPAM instance, you can aslo reset the IPAM landscape.

To edit an IPAM instance:

1. Go to *Address* > *IPAM*.
2. Select the IPAM *Action*.



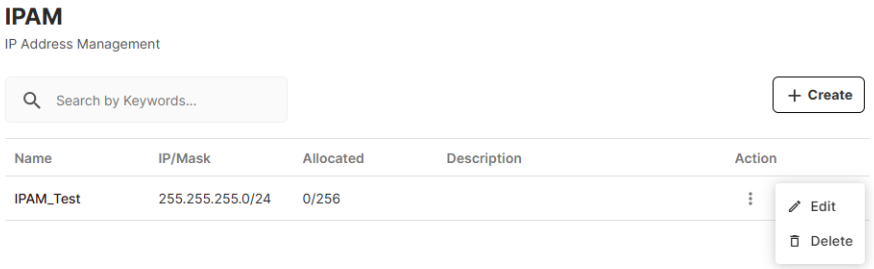
3. Click *Edit*.
4. Edit the configuration.



5. Click *Save*.

To delete an IPAM instance:

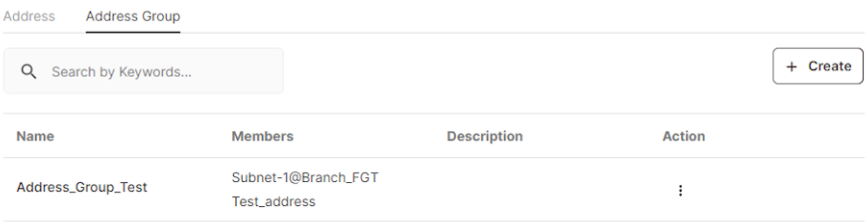
1. Go to *Address* > *IPAM*.
2. Select the IPAM *Action*.



3. Click *Delete*. A confirmation dialog is displayed.
4. Click *Confirm*.

Addresses

Addresses created in the *Address* > *Addresses* page can be added to address groups in the *Address Group* tab.



This section includes:

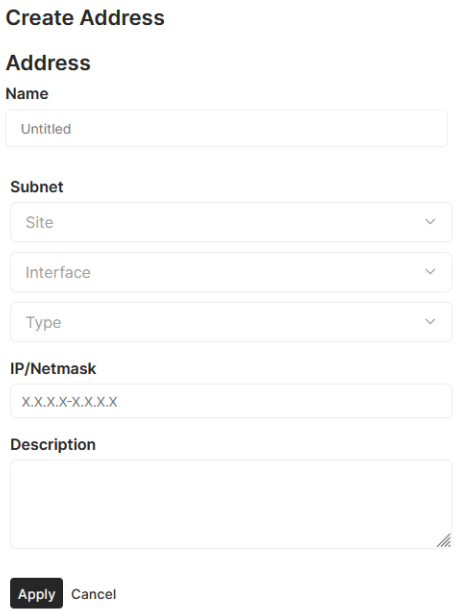
Creating an address

You can create new addresses to add to OaaS policies in the *Address* > *Addresses* page.

You can implement addresses in an address group. See Creating an address group on page 52.

To create a new address:

1. Go to *Address* > *Addresses*.
2. Select the *Address* tab.
3. Click *Create*.



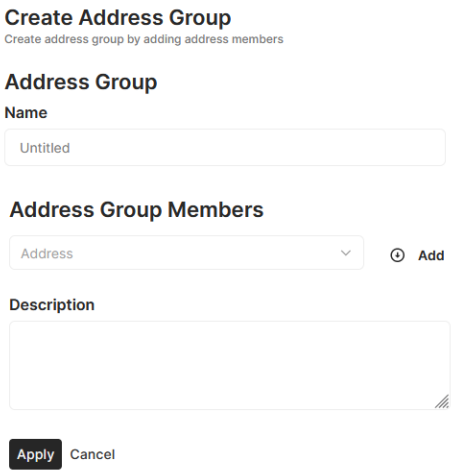
4. Enter a *Name*.
5. Define the subnet:
   a. Select the *Site* from the dropdown list.
   b. Select the *Interface* from the dropdown list.
   c. Select the *Type* from the dropdown list.
      i. If you selected *IP Range*, enter the IP address range in the *IP/Netmask* field.
6. (Optional) Enter a *Description* for the address.
7. Click *Apply*.

Creating an address group

You can create a new address group to be used in an OaaS policy in the *Address* > *Addresses* page. An address group is a group of address objects that can be used in an OaaS policy to identify the source and destination of traffic flow.

To create a new address group:

1. Go to *Address* > *Addresses*.
2. Select the *Address Group* tab.
3. Click *Create*.



4. Enter a *Name*.
5. Add address objects:
   a. Select an *Address* from the dropdown list.

   For information on creating addresses that can be added to an address group, see Creating an address on page 51.

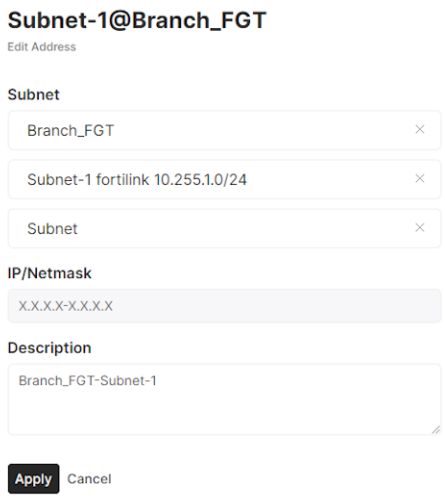
   b. Click *Add*.
   c. Repeat these steps to add other address objects to the address group.
6. (Optional) Enter a *Description* for the address group.
7. Click *Apply*.

Managing address objects and groups

You can edit or delete existing addresses and address groups in the *Address* > *Addresses* page.

To edit an address:

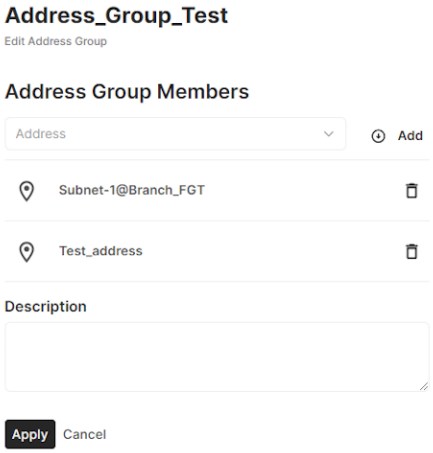
1. Go to *Address* > *Addresses*.
2. Select the *Address* tab.
3. For the address you want to edit, select *Action* > *Edit*.



4. Make your updates.
5. Click *Apply*.

To edit an address group:

1. Go to *Address* > *Addresses*.
2. Select the *Address Group* tab.
3. For the address group you want to edit, select *Action* > *Edit*.



4. Make your updates.
5. Click *Apply*.

To delete an address:

1. Go to *Address* > *Addresses*.
2. Select the *Address* tab.
3. For the address you want to delete, select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

You cannot delete an address if it is being used in an address group.

To delete an address group:

1. Go to *Address* > *Addresses*.
2. Select the *Address Group* tab.
3. For the address you want to delete, select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

Policy

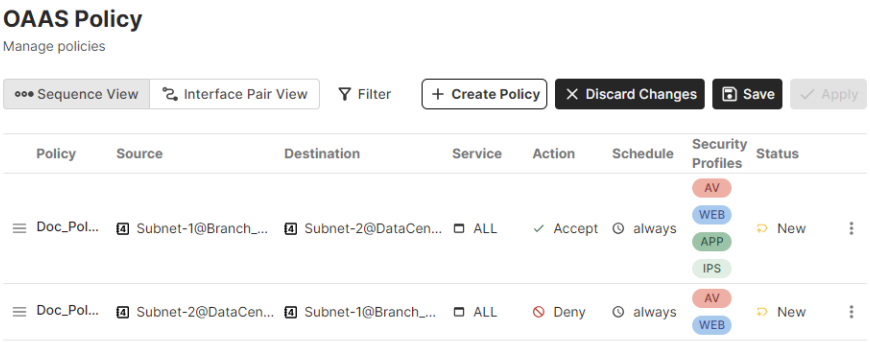
In the *Policy* pages, you can create and define centralized management policies for the FortiGates managed in Overlay-as-a-Service. Policies can be created based on intention and connected FortiGates will receive appropriate firewall policies based on this intention. Once the FortiGates participate in the OaaS central policy management, you cannot configure individual firewall policies for the FortiGates.

For more information on policies, see Policy and Objects in the FortiOS Administration Guide.

The *Policy* section includes the following pages:

OaaS Policy

Centralized OaaS policies can be created and managed in the *Policy* > *OaaS Policy* page. OaaS policies are policies whose source and destination can be in different sites, crossing overlay networks. For more information on policies, see Policies in the FortiOS Administration Guide.



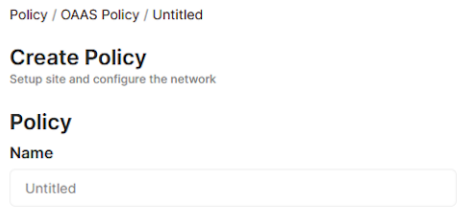
This section includes:

Creating a policy

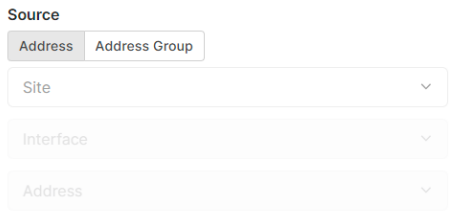
You can create new central policies from the *Policy* > *OaaS Policy* page.

To create a new policy:

1. Go to *Policy* > *OaaS Policy*.
2. Click *Create Policy*.
3. Enter a *Name*.



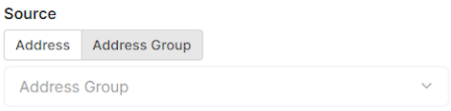
4. Define the source:
   - To define a source address, select *Address*:



     i. Select the *Site* from the dropdown list.
     ii. Select the *Interface* from the dropdown list.
     iii. Select the *Address* from the dropdown list.

> You can create a new address in the *Policy* > *Address* page. See Creating an address on page 51.

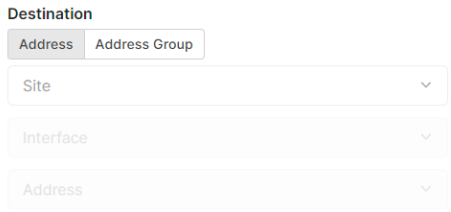
   - To define a source address group, select *Address Group*:



     i. Select the *Address Group* from the dropdown menu.

> If there are no address groups listed, you can create a new address group in the *Policy* > *Address* page. See Creating an address group on page 52.

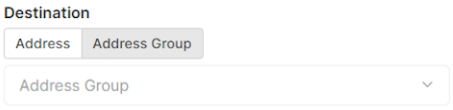
5. Define the destination:
   - To define a destination address, select *Address*:



     i. Select the *Site* from the dropdown list.
     ii. Select the *Interface* from the dropdown list.
     iii. Select the *Address* from the dropdown list.

> You can create a new address in the *Policy* > *Address* page. See Creating an address on page 51.

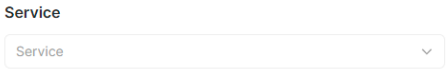
   - To define a destination address group, select *Address Group*:



     i. Select the *Address Group* from the dropdown menu.

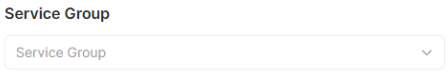
> If there are no address groups listed, you can create a new address group in the *Policy* > *Address* page. See Creating an address group on page 52.

6. Select the *Service* from the dropdown list.



> You can create a new service in the *Policy* > *Service* page. See Creating a service on page 68.

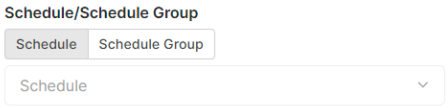
7. Select the *Service Group* from the dropdown list.



> If there are no service groups listed, you can create a new service group in the *Policy* > *Service* page. See Creating a service group on page 69.

8. Define the schedule of the policy:

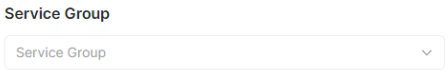
- To define the schedule, select *Schedule*:



  i. Select the *Schedule* from the dropdown list.

> You can create a new schedule in the *Policy* > *Schedule* page. See Creating a recurring schedule on page 73 and Creating a one-time schedule on page 74.

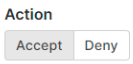
- To define the schedule group, select *Schedule Group*:



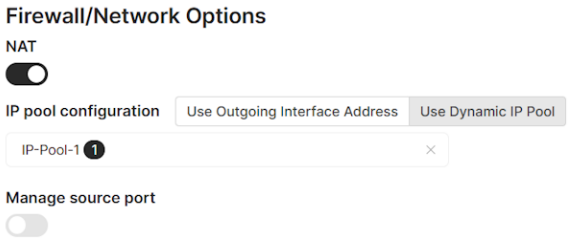
  i. Select the *Schedule Group* from the dropdown list.

> If there are no schedule groups listed, you can create a new schedule group in the *Policy* > *Schedule* page. See Creating a schedule group on page 74.

9. Set the *Action* as *Accept* or *Deny*.



10. Define the *Firewall/Network Options*:
    a. Enable *NAT*.
    b. Select the *IP pool configuration* option:
       - *Use Outgoing Interface Address*: Uses the address of the outgoing interface as the source address.
       - *Use Dynamic IP Pool*: Select an IP pool configured in *Policy* > *IP Pools* to perform source NAT.



    c. Enable *Manage source port* and select the source port option:
       - *Fixed port*: Enables the fixed port range of the selected IP pool.
       - *Preserve source port*: Use the same source port for services that expect traffic to come from a specific source port.

All *Firewall/Network Options* are only available for configuration if:

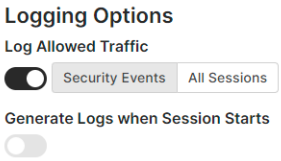
- The *Source* and *Destination* are set to the same site.
- The *Destination Interface* is set to an ISP port.

To support the *IP pool configuration* > *Use Dynamic IP Pool* option in an OaaS policy, a site must be running FortiOS version 7.4.5 and above. Major version 7.6.0 and above is not currently supported. See IP Pools on page 78.
To support the *Manage source port* > *Fixed port option* in an OaaS policy, a site must be running FortiOS version 7.4.5 and above.

11. Select the *Security Profiles*.

Security profiles can be configured in the *Policy* > *Security Profiles* page. See Security Profiles on page 80.

12. Define the *Logging Options*:



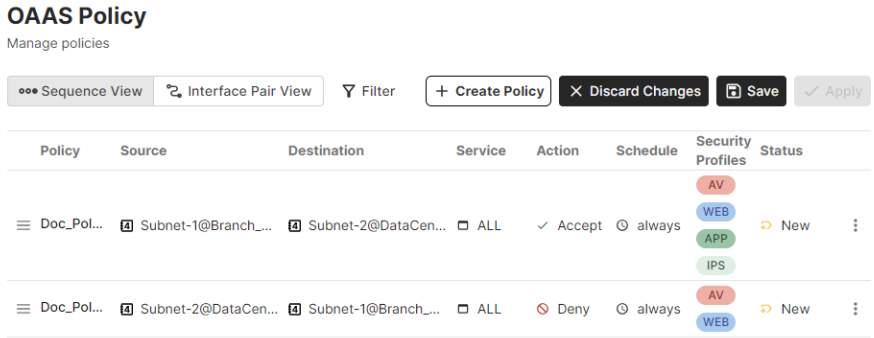
   a. Toggle *Log Allowed Traffic* and select *Security Events* or *All Sessions* to define which events to log.
   b. Enable *Generate Logs when Session Starts*, if needed.
13. (Optional) Enter a description for the policy.
14. Toggle *Enable this policy* to enable or disable the policy.
15. Click *Save*.

Once a policy has been created, it will appear in the *Policy* > *OaaS Policy* list with the *Unsaved* status. You must save and apply the policy to the spoke FortiGates before they will take effect. See Applying policies on page 61.

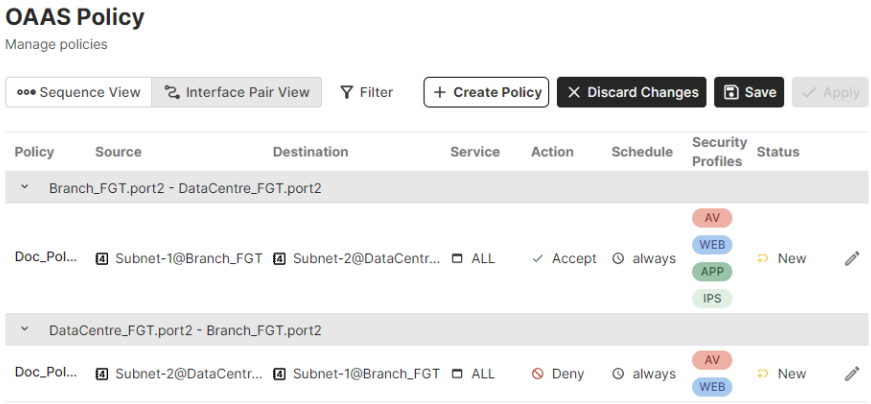
Viewing policies

OaaS policies are displayed in the in the *Policy* > *OaaS Policy* page. Policies can be viewed in:

- *Sequence View*: Displays policies in the order that they are checked for matching traffic. The order can be changed by dragging and dropping policies into a new location in the list.



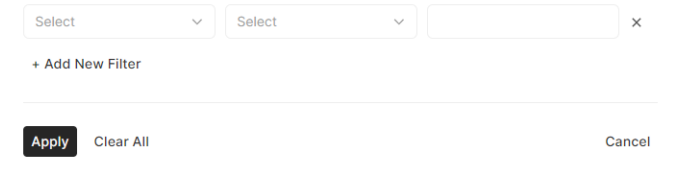
- *Interface Pair View*: Displays policies in the order by the pairs of incoming and outgoing interfaces in collapsible sections.



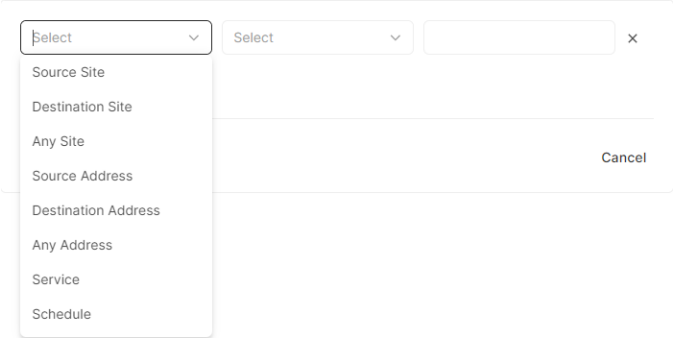
For more information on *Sequence View* and *Interface Pair View*, see Policy views in the FortiOS Administration Guide.

To filter policies:

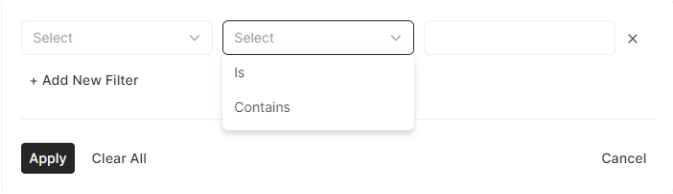
1. Go to *Policy* > *OaaS Policy*.
2. Click *Filter*.



3. Select the filter criteria from the dropdown list.



4. Select the filter definition from the dropdown list.



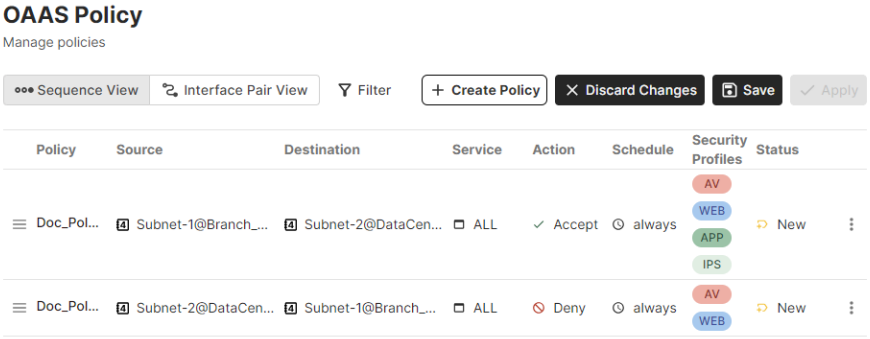
5. Enter the filter value.
6. Click *Add New Filter* to add another criteria.
7. Click *Apply*.

Applying policies

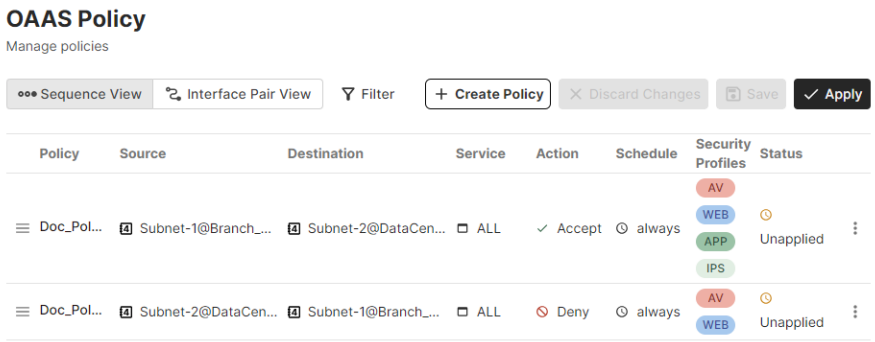
The OaaS policies must be saved and applied to the spoke FortiGates before they can take effect. Any edits made to a policy will not be pushed to the spokes until they have been applied.

To apply a policy:

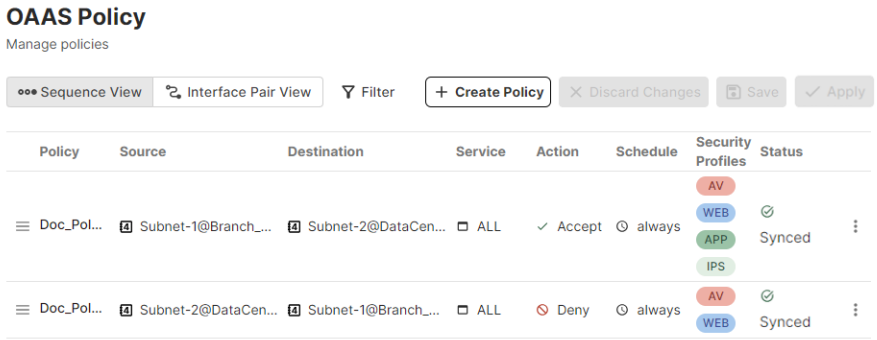
1. Go to *Policy* > *OaaS Policy*.



2. Click *Save*. The *Status* will change to *Unapplied*.



3. Click *Apply*. The *Status* will change to *Synced*.

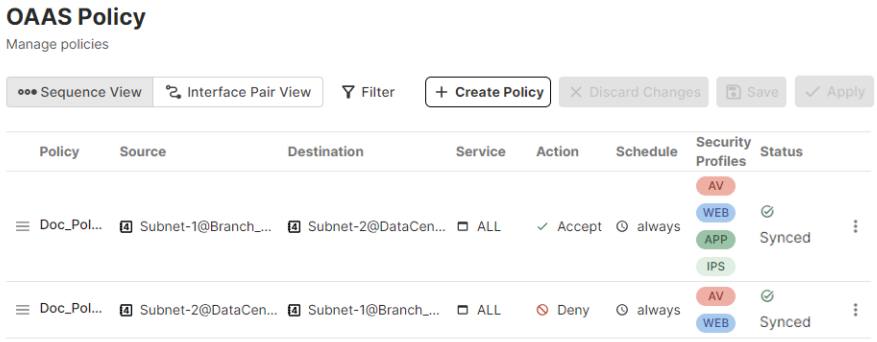


Managing policies

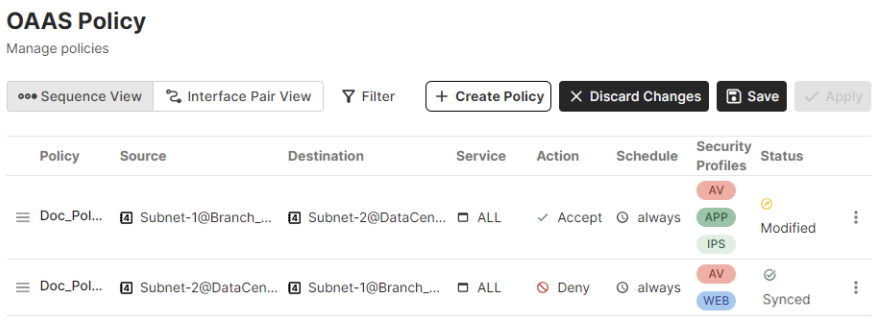
Policies can be edited and deleted in the *Policy* > *OaaS Policies* page.

To edit a policy:

1. Go to *Policy* > *OaaS Policy*.

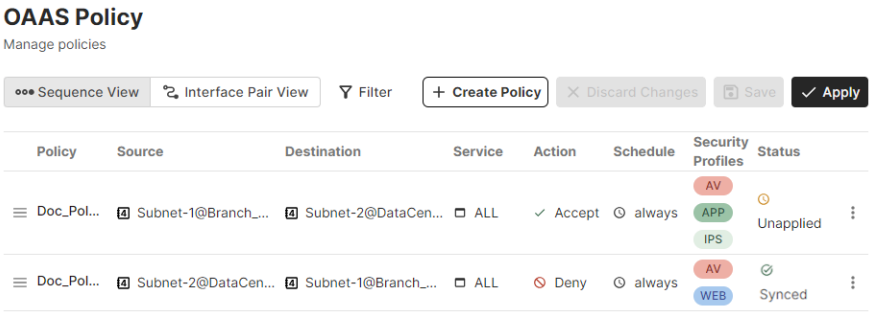


2. Find the policy you want to update can select *Edit*.
3. Make the edits and click *Save*. The Status will change to *Modified*.

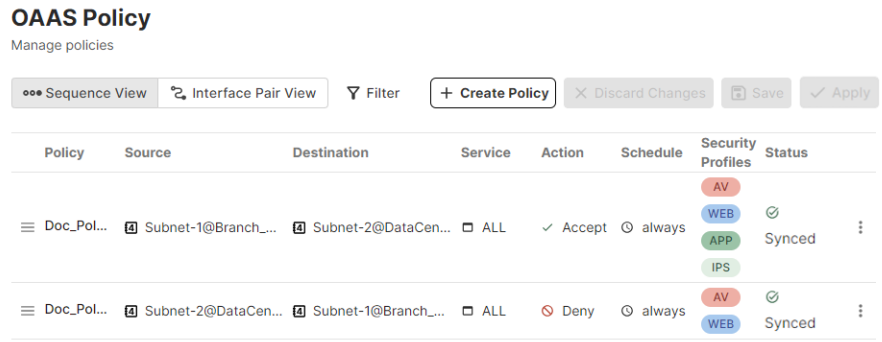


Select *Discard Changes* to undo any edits made.

4. Click *Save*. The *Status* will change to *Unapplied*.



5. Click *Apply*. The *Status* will change to *Synced*.



To delete a policy:

1. Go to *Policy* > *OaaS Policy*.
2. In *Sequence View*, find the policy you want to delete.
3. Click *Delete*.
4. Click *Confirm* in the confirmation dialog.

Policy example

Given a topology that has already been previously orchestrated using the OaaS portal, the following example demonstrates how to create OaaS policies between two FortiGate sites in that topology using these steps:

1. Configure an OaaS policy to allow traffic from the Datacenter LAN (10.1.100.0/24) to the Branch 1 LAN (10.1.1.0/24).
2. Test and verify connectivity from the Datacenter LAN to the Branch 1 LAN.
3. Test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the OaaS policy configured in Step 1.
4. Configure an OaaS policy to allow traffic from the Branch 1 LAN (10.1.1.0/24) to the Datacenter LAN (10.1.100.0/24).
5. Test and verify connectivity from the Branch 1 LAN to the Datacenter LAN.

For granularity, OaaS policies are destined for the source and destination specified only. Therefore, an OaaS policy from site A crossing overlay networks to site B does not automatically allow traffic in the opposite direction from site B to site A. You must create a separate OaaS policy for traffic in the opposite direction between sites.

To configure an OaaS policy to allow traffic from the Datacenter LAN to the Branch 1 LAN:

1. Go to *Policy* > *OAAS Policy*.
2. Configure the policy as follows:

Name		DCport3-to-Br1port3
Source		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Destination		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24
	Address	port3@Branch-1
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always
Action		Accept
Security Profiles		
	AntiVirus	Default

	Web Filter	Default
	Application Control	Default
	Intrusion Prevention	Default
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions
	Generate Logs when Session Starts	Disabled
	Description	DC port3 to Br1 port3
Enable this policy		Enabled

3. Click *Save*.
4. In *Policy* > *OAAS Policy*:
   a. Status is *Unsaved*. Click *Save*.
   b. Status is *Unsynced*. Click *Apply*.
   c. Status is *Synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Datacenter LAN to the Branch 1 LAN:

1. Run these CLI commands on the Datacenter FortiGate:

```
# execute ping-options source <IP address in Datacenter LAN>
# execute ping <IP address in Branch 1 LAN>
```

2. Observe the following output:

```
Datacenter# execute ping-options source 10.1.100.1

Datacenter# execute ping 10.1.1.99
PING 10.1.1.99 (10.1.1.99): 56 data bytes
64 bytes from 10.1.1.99: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 10.1.1.99: icmp_seq=1 ttl=255 time=2.7 ms
64 bytes from 10.1.1.99: icmp_seq=2 ttl=255 time=1.2 ms
64 bytes from 10.1.1.99: icmp_seq=3 ttl=255 time=1.9 ms
64 bytes from 10.1.1.99: icmp_seq=4 ttl=255 time=0.6 ms

--- 10.1.1.99 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.4/2.7 ms
```

To test and verify connectivity from the Branch 1 LAN and the Datacenter LAN is not allowed by the OaaS policy:

1. Run these CLI commands on the Branch 1 FortiGate:

```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes

--- 10.1.100.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

To configure an OaaS policy to allow traffic from the Branch 1 LAN to the Datacenter LAN:

1. Go to *Policy* > *OAAS Policy*.
2. Configure the policy as follows:

Name		Br1port3-to-DCport3
Source		Address
	Site	Branch-1
	Interface	port3 10.1.1.0/24
	Address	port3@Branch-1
Destination		Address
	Site	Datacenter
	Interface	port3 10.1.100.0/24
	Address	port3@Datacenter
Service		ALL
Service Group		
Schedule/Schedule Group		Schedule
Schedule		always
Action		Accept
Logging Options		
	Log Allowed Traffic	Enabled, All Sessions
	Generate Logs when Session Starts	Disabled

	Description
Enable this policy	Enabled

3. Click *Save*.
4. In *Policy* > *OAAS Policy*:
   a. Status is *Unsaved*. Click *Save*.
   b. Status is *Unsynced*. Click *Apply*.
   c. Status is *Synced*. The policy has been applied to the FortiGate devices in the specified sites.

To test and verify connectivity from the Branch 1 LAN to the Datacenter LAN:

1. Run these CLI commands on the Branch 1 FortiGate:

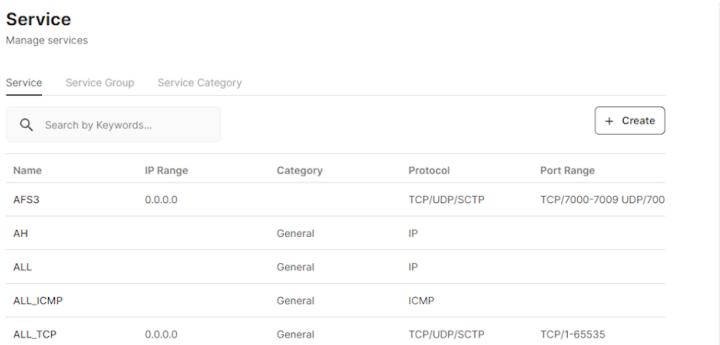
```
# execute ping-options source <IP address in Branch 1 LAN>
# execute ping <IP address in Datacenter LAN>
```

2. Observe the following output:

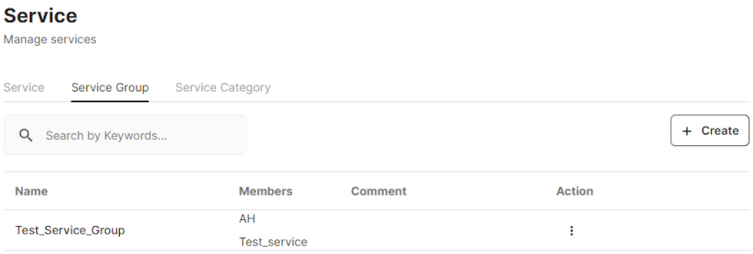
```
Branch-1# execute ping-options source 10.1.1.99

Branch-1# execute ping 10.1.100.1
PING 10.1.100.1 (10.1.100.1): 56 data bytes
64 bytes from 10.1.100.1: icmp_seq=0 ttl=254 time=50.6 ms
64 bytes from 10.1.100.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.1.100.1: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 10.1.100.1: icmp_seq=3 ttl=255 time=0.7 ms
64 bytes from 10.1.100.1: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.1.100.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/10.5/50.6 ms
```

Service

Services can be managed from the *Policy* > *Service* page. See Firewall policy in the FortiOS Administration guide for more information on services.



Services created in the *Policy* > *Service* page can be implemented in service groups displayed in the *Service Group* tab.



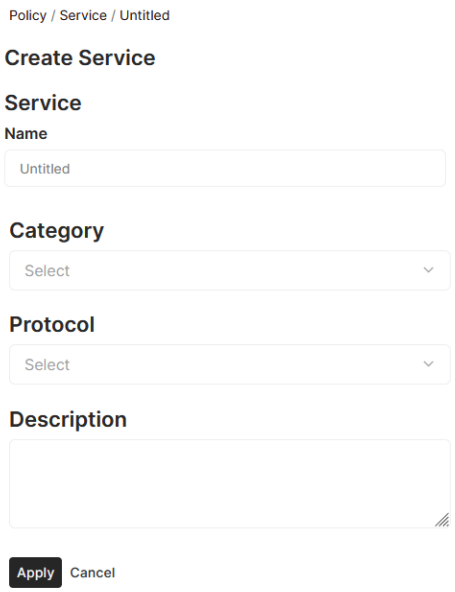
This section includes:

Creating a service

Service protocols can be created in the *Policy* > *Service* page.

To create a service:

1. Go to *Policy* > *Service*.
2. Select the *Service* tab.
3. Click *Create*.



4. Enter a *Name*.
5. Select a *Category* from the dropdown list.

Service categories can be created in the *Service Category* tab. See Creating a service category on page 70.

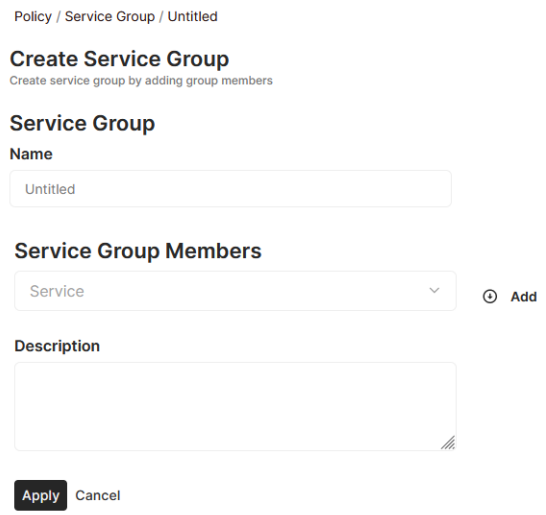
6. Select a *Protocol* from the dropdown list:
7. Enter the protocol particulars in the new fields.
8. (Optional) Enter a *Description* of the protocol.
9. Click *Apply*.

Creating a service group

Service protocols can be combined into a service group.

To create a service group:

1. Go to *Policy* > *Service*.
2. Select the *Service Group* tab.
3. Click *Create*.



4. Enter a *Name*.
5. Add service group members:
   a. Select a *Service* from the dropdown list.

      For information on creating services that can be added to a service group, see Creating a service on page 68.

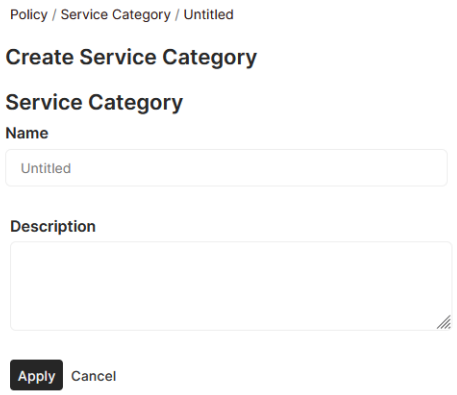
   b. Click *Add*.
   c. Repeat these steps to add other services to the service group.
6. (Optional) Enter a *Description* for the address group.
7. Click *Apply*.

Creating a service category

You can create new service categories to be used in service protocols.

To create a new service category:

1. Go to *Policy* > *Service*.
2. Select the *Service Category* tab.
3. Click *Create*.



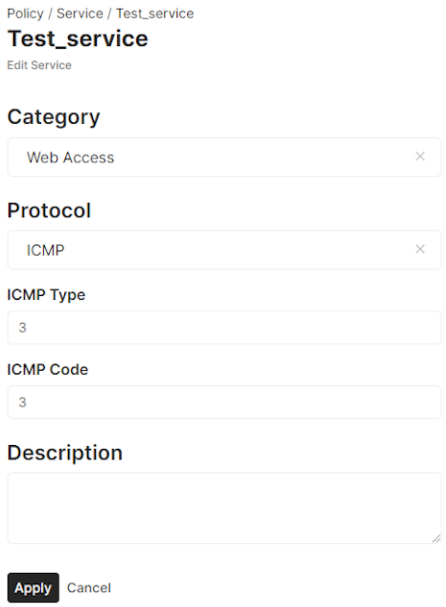
4. Enter a *Name*.
5. Enter a description of the service category.
6. Click *Apply*.

Managing services

You can edit or delete services, service groups, and service categories in the *Policy* > *Service* page.

To edit a service:

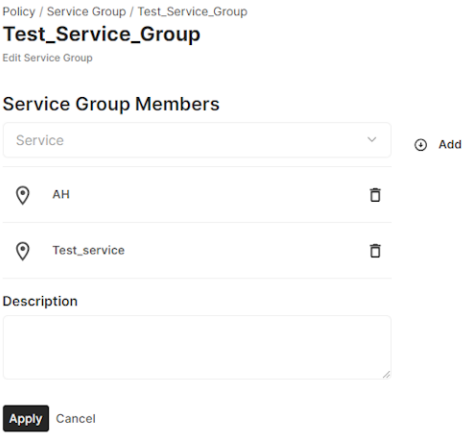
1. Go to *Policy* > *Service*.
2. Select the *Service* tab.
3. Find the service you want to edit and select *Action* > *Edit* or click on the name.



4. Make your updates.
5. Click *Apply*.

To edit a service group:

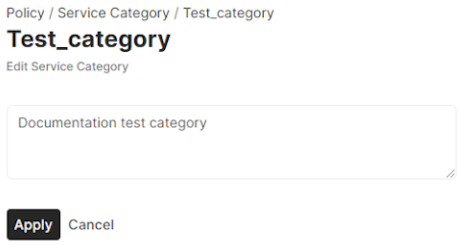
1. Go to *Policy* > *Service*.
2. Select the *Service Group* tab.
3. Find the service group you want to edit and select *Action* > *Edit* or click on the name.



4. Make your updates.
5. Click *Apply*.

To edit a service category:

1. Go to *Policy* > *Service*.
2. Select the *Service Category* tab.
3. Find the category you want to edit and select *Action* > *Edit* or click on the name.



4. Make your updates.
5. Click *Apply*.

To delete a service:

1. Go to *Policy* > *Service*.
2. Select the *Service* tab.
3. Find the service you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

You cannot delete a service if it is being used in a service group.

To delete a service group:

1. Go to *Policy* > *Service*.
2. Select the *Service Group* tab.
3. Find the service group you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

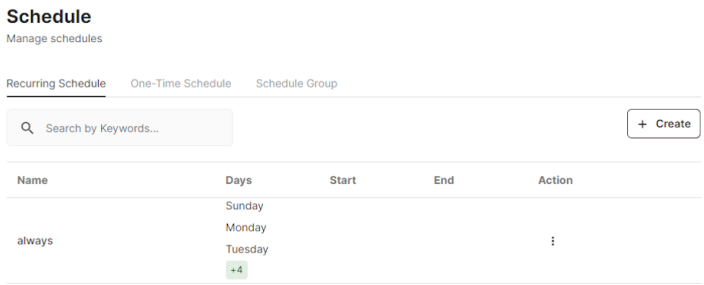
To delete a service category:

1. Go to *Policy* > *Service*.
2. Select the *Service Category* tab.
3. Find the category you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

You cannot delete a category if it is being used in a service.

Schedules

Policy schedules can be created and managed in the *Policy* > *Schedules* page. Schedules can be recurring or one-time occurrences, or a combination in a schedule group.



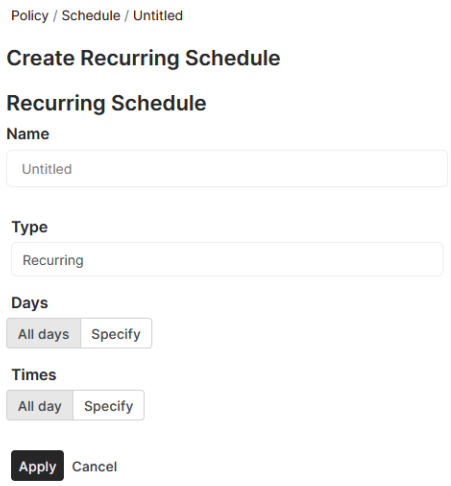
This section includes:

Creating a recurring schedule

You can create a policy schedule that recurs at specific days and times in the *Policy* > *Schedule* page. This schedule will continue to recur in the assigned policy until it is removed or edited.

To create a recurring schedule:

1. Go to *Policy* > *Schedules*.
2. Select the *Recurring Schedule* tab.
3. Click *Create*.



4. Enter a *Name*.
5. Specify the *Days*:
   - Select *All days* if the schedule should occurs every day of the week.
   - Select *Specify* to select specific days of the week for the schedule to occur.
6. Specify the *Times*:

- Select *All day* if the schedule should occurs for 24 hours.
- Select *Specify* to set a *Start* and *End* time.

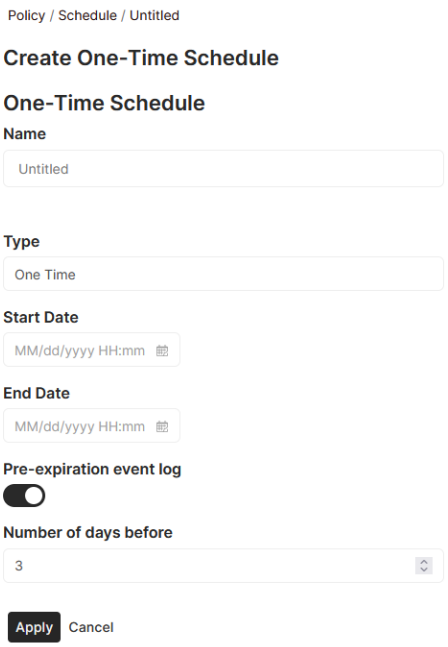
7. Click *Apply*.

Creating a one-time schedule

You can create a one-time schedule event in the *Policy* > *Schedule* page.

To create a one-time schedule:

1. Go to *Policy* > *Schedules*.
2. Select the *One-Time Schedule* tab.
3. Click *Create*.



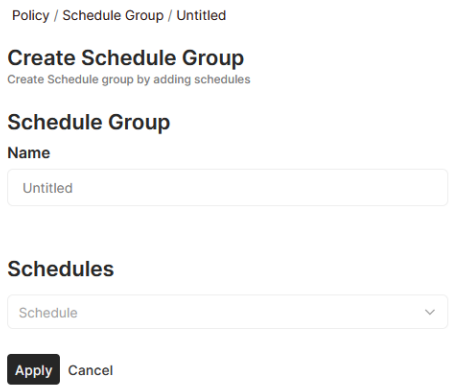
4. Enter a *Name*.
5. Specify the *Start Date* and time.
6. Specify the *End Date* and time.
7. If you would like an event log to occur before the expiration of the schedule, enable *Pre-expiration event log* and specify the *Number of days before* expiration.
8. Click *Apply*.

Creating a schedule group

You can create a schedule group from a combination of recurring and one-time schedules in the *Policy* > *Schedule* page.

To create a schedule group:

1. Go to *Policy* > *Schedules*.
2. Select the *Schedule Group* tab.
3. Click *Create*.



4. Enter a *Name*.
5. Select the *Schedules* from the dropdown list.

For information on creating schedules that can be added to an schedule group, see Creating a recurring schedule on page 73 and Creating a one-time schedule on page 74.

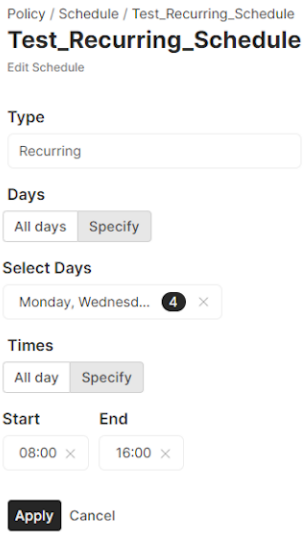
6. Click *Apply*.

Managing schedules

You can edit and delete schedules and schedule groups from the Policy > Schedule page.

To edit a recurring schedule:

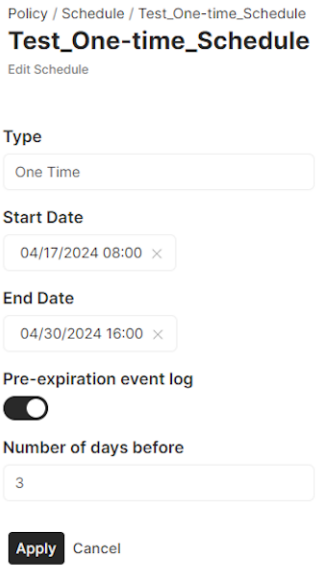
1. Go to *Policy* > *Schedules*.
2. Select the *Recurring Schedule* tab.
3. Find the schedule you want to edit and select *Action* > *Edit* or click on the name.



4. Make your updates.
5. Click *Apply*.

To edit a one-time schedule:

1. Go to *Policy* > *Schedules*.
2. Select the *One-Time Schedule* tab.
3. Find the schedule you want to edit and select *Action* > *Edit* or click on the name.

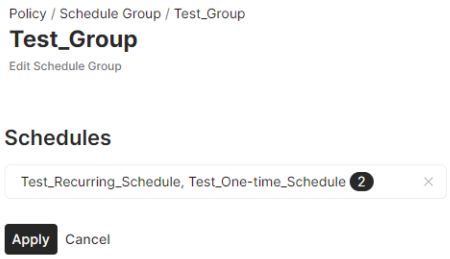


4. Make your updates.
5. Click *Apply*.

To edit a schedule group:

1. Go to *Policy* > *Schedules*.
2. Select the *Schedule Group* tab.

3. Find the schedule group you want to edit and select *Action* > *Edit* or click on the name.



4. Make your updates.
5. Click *Apply*.

To delete a recurring schedule:

1. Go to *Policy* > *Schedules*.
2. Select the *Recurring Schedule* tab.
3. Find the schedule you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

You cannot delete a schedule if it is being used in a schedule group.

To delete a one-time schedule:

1. Go to *Policy* > *Schedules*.
2. Select the *One-Time Schedule* tab.
3. Find the schedule you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

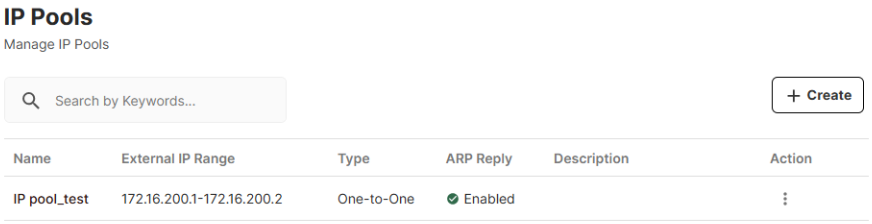
You cannot delete a schedule if it is being used in a schedule group.

To delete a schedule group:

1. Go to *Policy* > *Schedules*.
2. Select the *Schedule Group* tab.
3. Find the schedule group you want to delete and select *Action* > *Delete*.
4. Click *Confirm* in the confirmation dialog.

IP Pools

IP pools are a mechanism that allows sessions leaving the FortiGate firewall to use NAT. IP pools can be configured in the *Policy* > *IP Pools* page. For more information on IP pools, see Static SNAT, Dynamic SNAT, and Central SNAT in the FortiOS Administration Guide.



Once an IP pool is configured, it can be implemented when configuring OaaS policies to be applied to the FortiGate devices. See Creating a policy on page 55.

This feature requires a site to be running FortiOS 7.4.5 and above. Major version 7.6.0 and above is not currently supported.

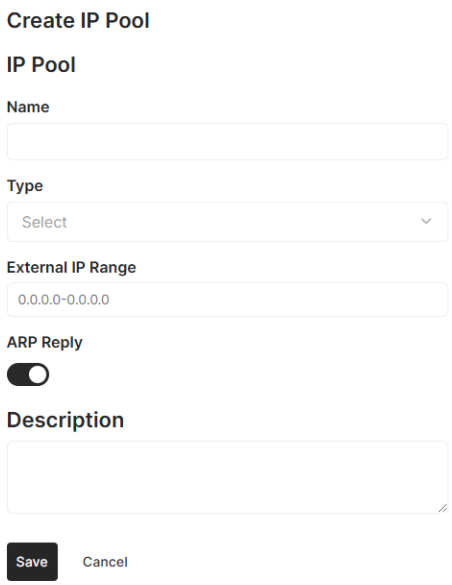
This section includes:

Creating an IP pool

You can create a new IP pool in the *Policy* > *IP Pools* page.

To create an IP pool:

1. Go to *Policy* > *IP Pools*.
2. Click *Create*.



3. Enter the *Name*.
4. Select the *Type*.
5. Enter the IP address and range information as needed.

The IP address and range field differ depending on the selected *Type*. For more information on each *Type*, see Dynamic SNAT in the FortiOS Administration Guide.

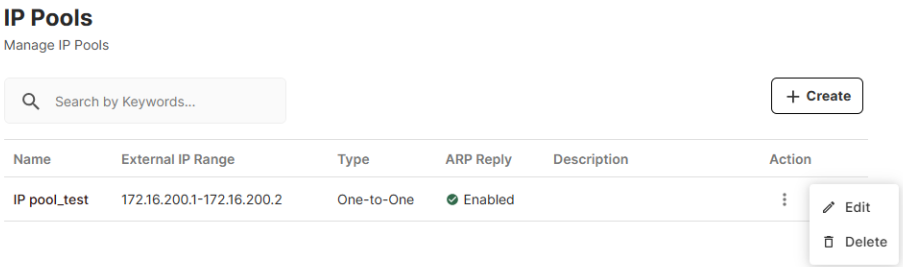
6. Enable or disabled *ARP Reply*.
7. Enter a *Description*, if desired.
8. Click *Save*.

Managing IP pools

You can edit or delete existing IP pools in the *Policy* > *IP Pools* page.

To edit an IP pool:

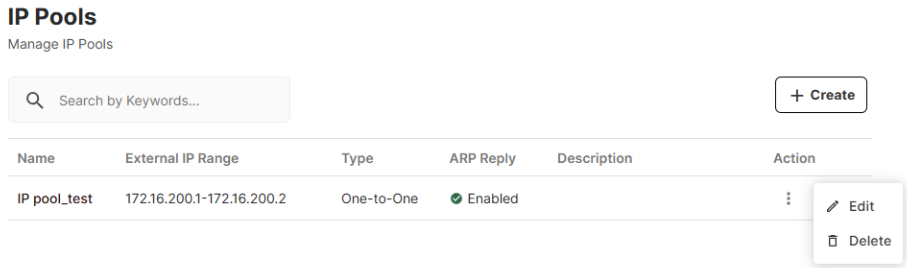
1. Go to *Policy* > *IP Pools*.
2. Select the IP pool *Action*.



3. Click *Edit*.
4. Edit the fields as desired.
5. Click *Save*.

To delete an IP pool:

1. Go to *Policy* > *IP Pools*.
2. Select the IP pool *Action*.



3. Click *Delete*. A confirmation dialog is displayed.
4. Click *Confirm*.

Security Profiles

Security profiles configurations can be managed from *Policy* > *Security Profiles*. See Security Profiles in the FortiOS Administration Gudide for more information.

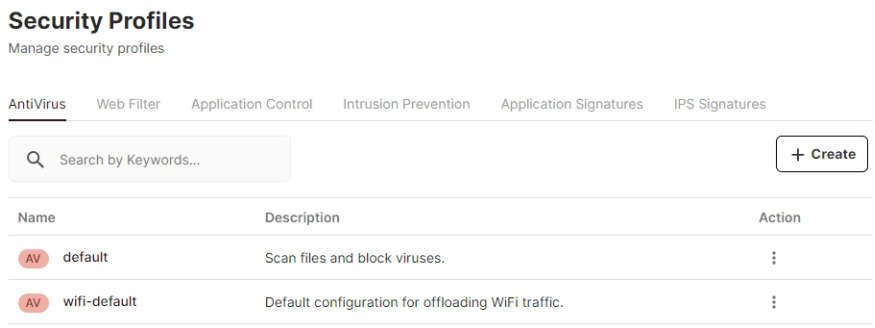
Sites must be running FortiOS 7.6.0 or later to support security profiles. See Prerequisites on page 6.

The security profiles available include:

- AntiVirus on page 80
- Web Filter on page 83
- Application Control on page 86
- Intrusion Prevention on page 89
- Application Signatures on page 92
- IPS Signatures on page 92

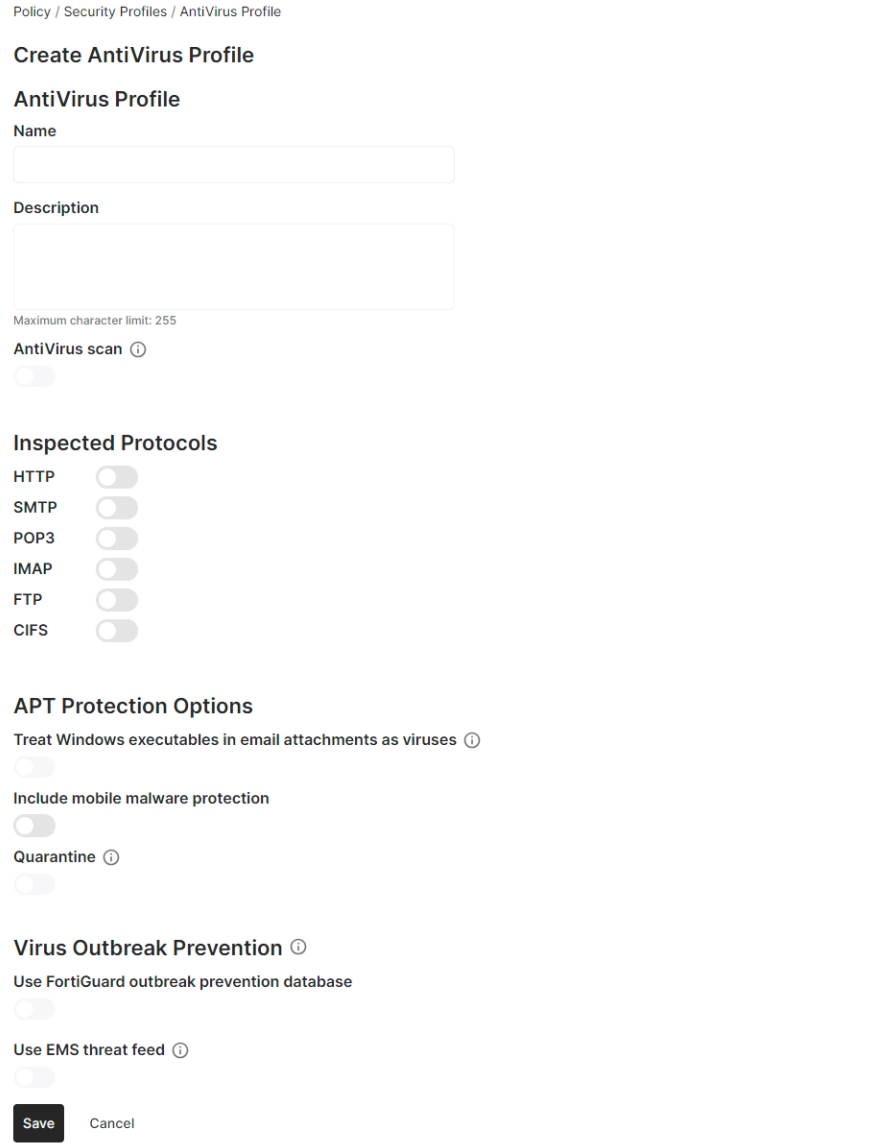
AntiVirus

Antivirus security profiles can be created and managed from *Policy* > *Security Profiles* > *AntiVirus* tab. See Antivirus in the FortiOS Administration Guide for more information.



To create an antivirus security profile:

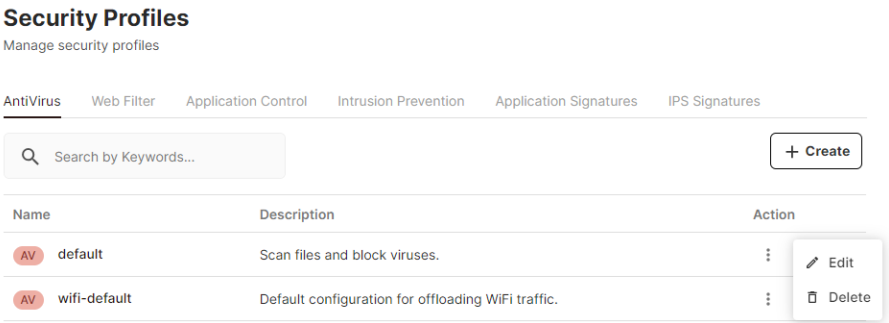
1. Go to the *Policy* > *Security Profiles* > *AntiVirus* tab.
2. Click *Create*. The *Create AntiVirus Profile* page is displayed.



3. Enter the *Name*.
4. Enter a *Description*.
5. Enable the desired *Inspected Protocols*. An error is displayed until the scan options are defined in the next step.
6. Enable *AntiVirus scan*. This feature cannot be enabled until the security profile is inspecting at least one protocol.
7. Enable the desired *APT Protection Options*.
8. Enable the desired *Virus Outbreak Prevention* fields.
9. Click *Save*.

To edit a security profile:

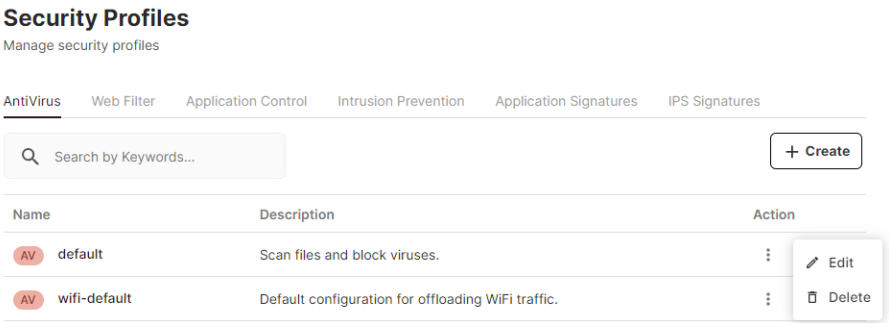
1. Go to the *Policy* > *Security Profiles* > *AntiVirus* tab.
2. Select the *Action* icon for the desired profile.



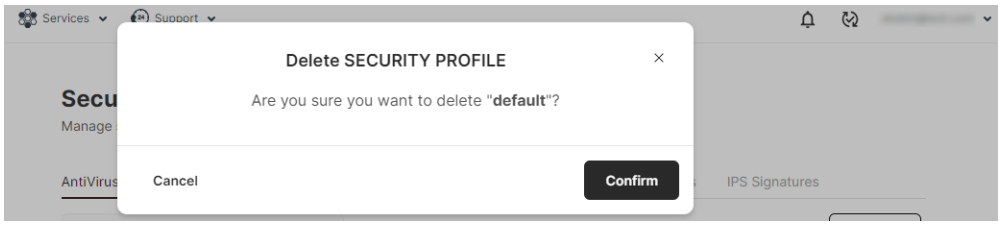
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *Save*.

To delete a security profile:

1. Go to the *Policy* > *Security Profiles* > *AntiVirus* tab.
2. Select the *Action* icon for the desired profile.



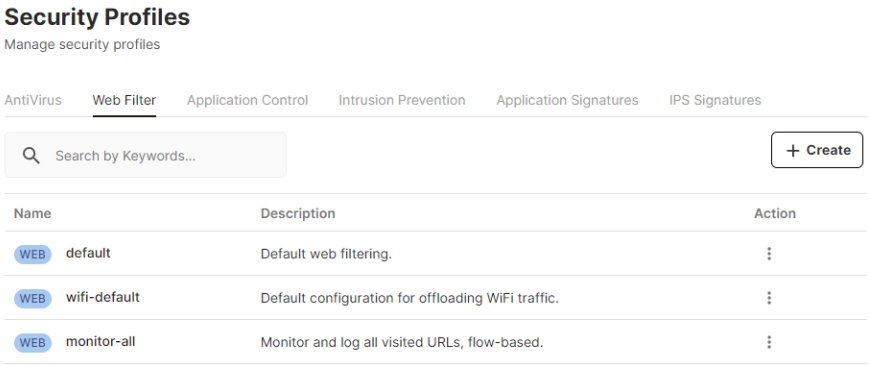
3. Click *Delete*. A confirmation dialog is displayed.



4. Click *Confirm*.

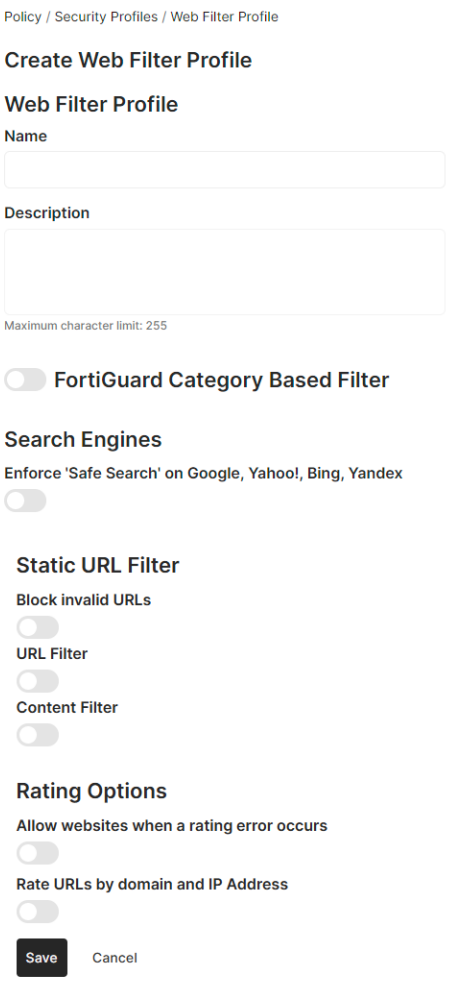
Web Filter

Web filter security profiles can be created and managed from *Policy* > *Security Profiles* > *Web Filter* tab. See Web filter in the FortiOS Administration Guide for more information.

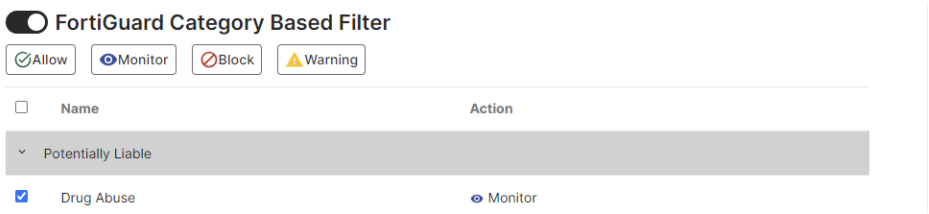


To create a new web filter security profile:

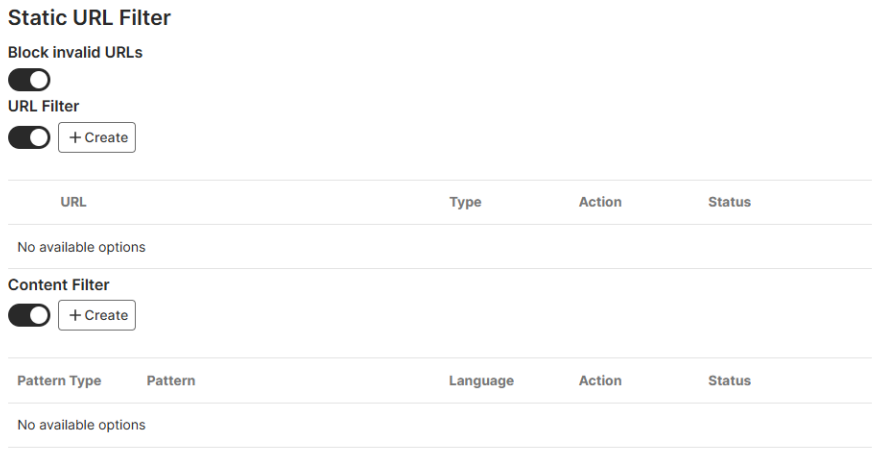
1. Go to the *Policy* > *Security Profiles* > *Web Filter* tab.
2. Click *Create*. The *Create Web Filter Profile* page is displayed.



3. Enter the *Name*.
4. Enter a *Description*.
5. Enable the *FortiGuard Category Based Filter* and configure the filters. See FortiGuard filter in the FortiOS Administration Guide.
   a. Select a category dropdown menu to view the available filters.
   b. Select a filter.



   c. Select the *Action* from the provided options if you would like to change the default.
6. Enable and configure the desired *Search Engine* parameters. See Search engines in the FortiOS Administration Guide.
7. Enable and configure the desired *Static URL Filter* parameters. See Static URL filter in the FortiOS Administration Guide.

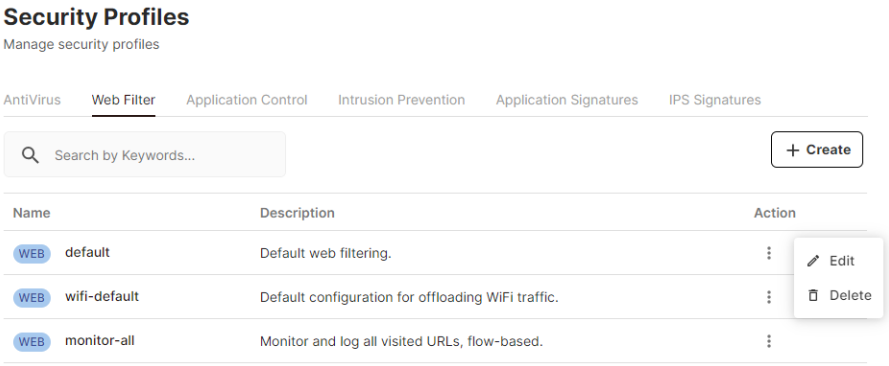


The *URL Filter* and *Content Filter* features require a site to be running FortiOS 7.4.6 and above. Major version 7.6.0 and above is not currently supported.

8. Enable the desired *Rating Options*.
9. Click *Save*.

To edit a security profile:

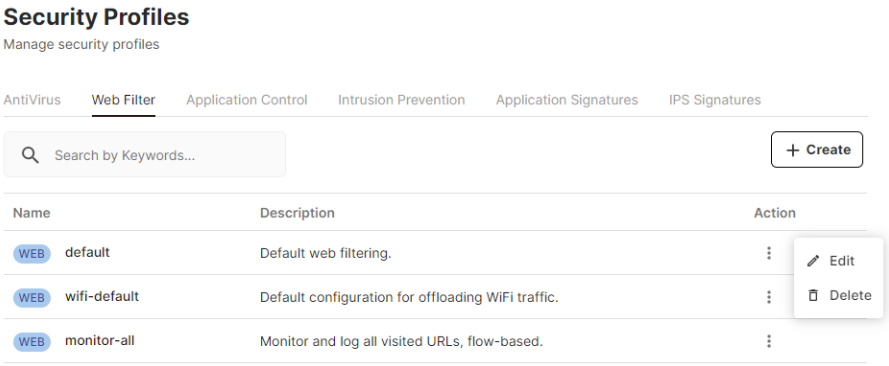
1. Go to the *Policy* > *Security Profiles* > *Web Filter* tab.
2. Select the *Action* icon for the desired profile.



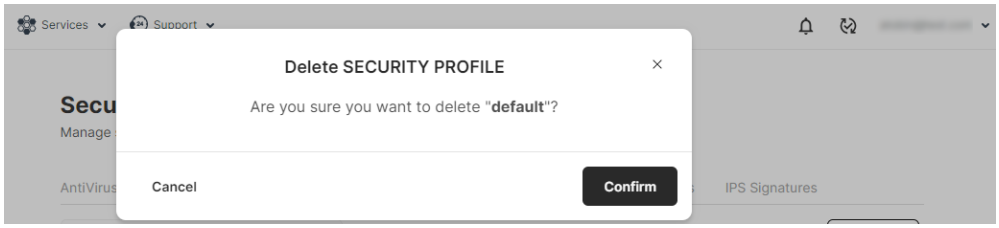
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *Save*.

To delete a security profile:

1. Go to the *Policy* > *Security Profiles* > *Web Filter* tab.
2. Select the *Action* icon for the desired profile.



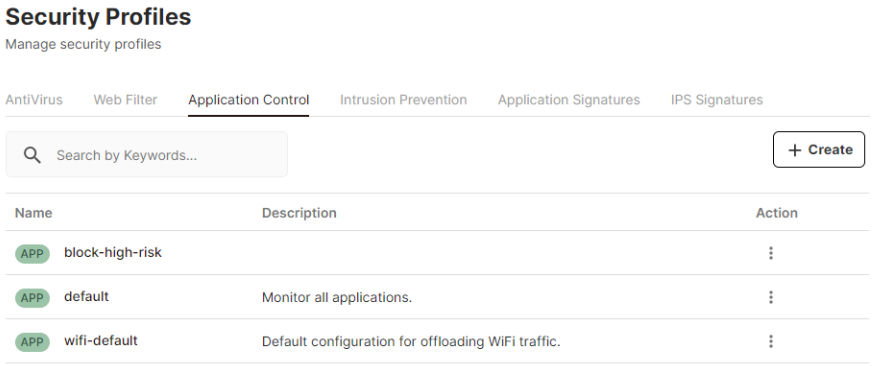
3. Click *Delete*. A confirmation dialog is displayed.



4. Click *Confirm*.

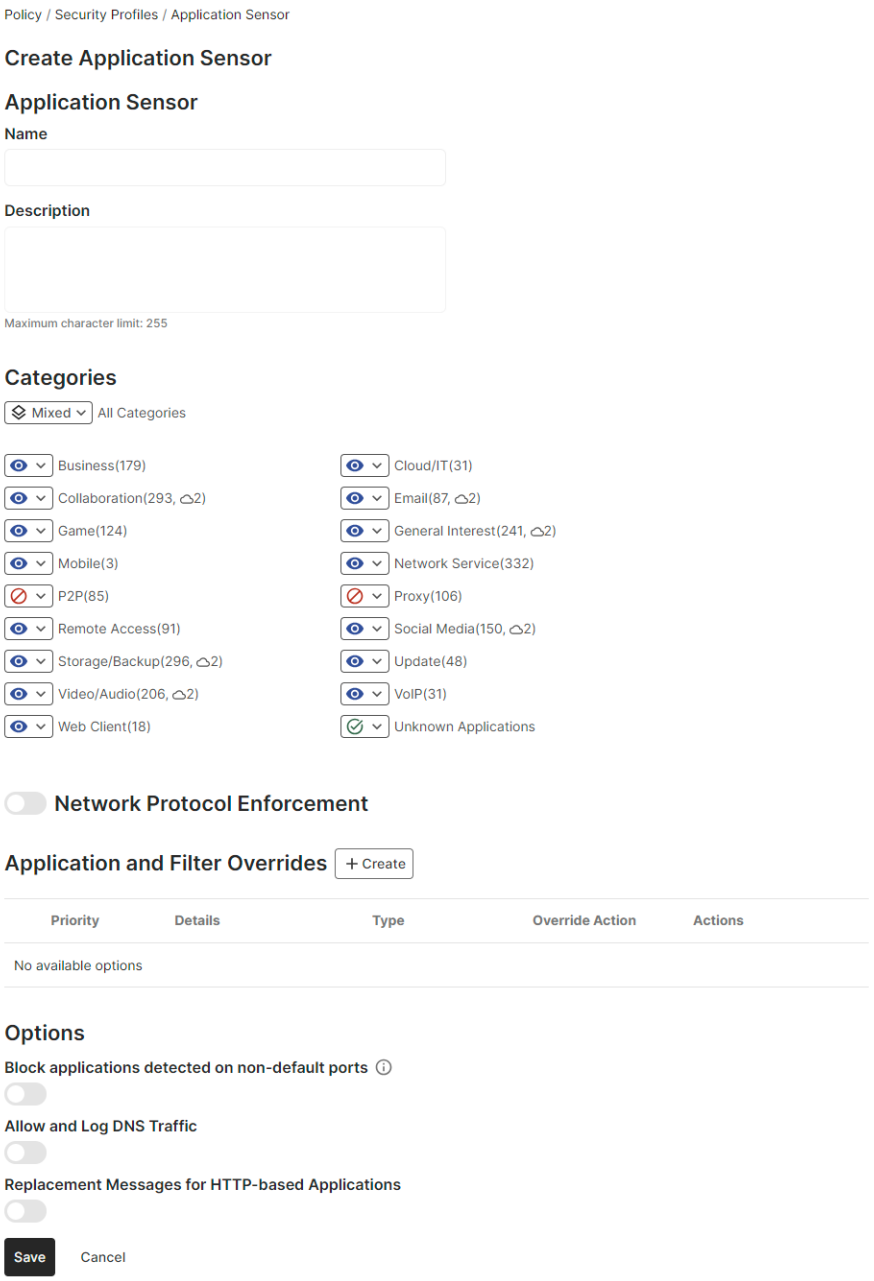
Application Control

Application control sensors can be created and managed from *Policy* > *Security Profiles* > *Application Control* tab. See Application control in the FortiOS Administration Guide for more information.

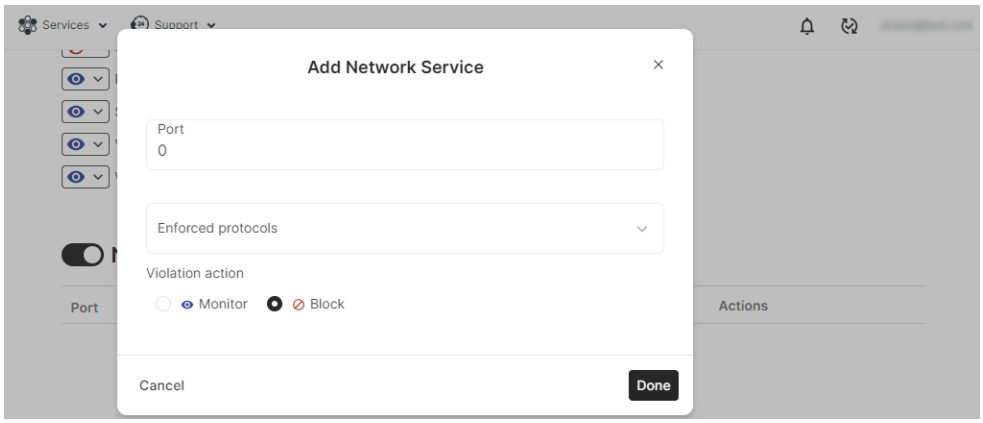


To create a new application control sensor:

1. Go to the *Policy* > *Security Profiles* > *Application Control* tab.
2. Click *Create*. The *Create Application Sensor* page is displayed.

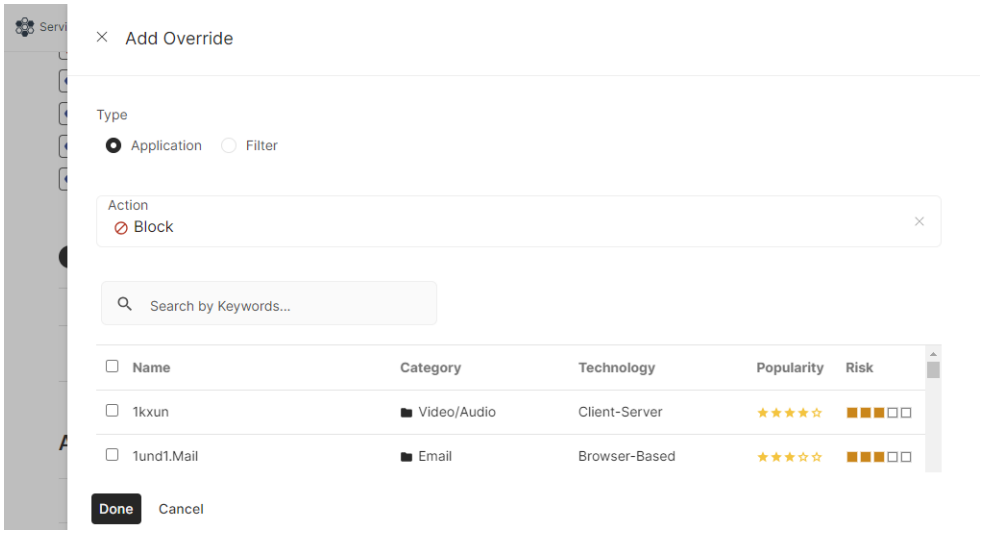


3. Enter the *Name*.
4. Enter a *Description*.
5. Edit the *Categories* as desired.
6. Enable *Network Protocol Enforcement*.
   a. Click *Create*.
   b. Configure the network service.



c. Click *Done*.

7. Click *Create* for *Application and Filter Overrides*. See Basic category filters and overrides in the FortiOS Administration Guide.
   a. Configure the override.

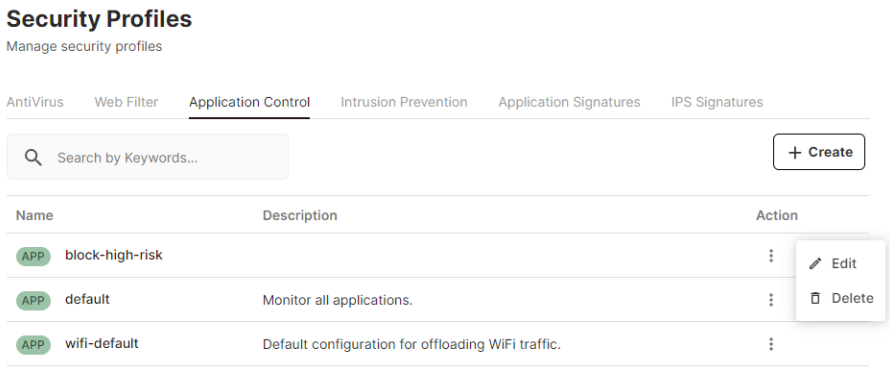


Application signatures can also be viewed in the *Policy* > *Security Profiles* > *Application Signatures* tab. See Application Signatures on page 92.

   b. Click *Done*.
8. Enable the desired *Options*.
9. Click *Save*.

To edit a sensor:

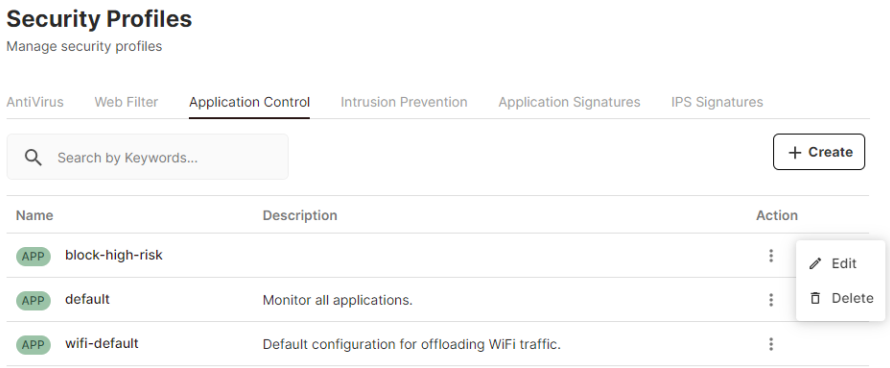
1. Go to the *Policy* > *Security Profiles* > *Application Control* tab.
2. Select the *Action* icon for the sensor.



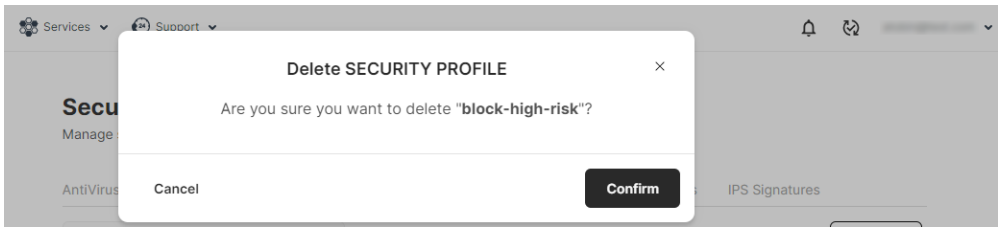
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *Save*.

To delete a sensor:

1. Go to the *Policy* > *Security Profiles* > *Application Control* tab.
2. Select the *Action* icon for the sensor.



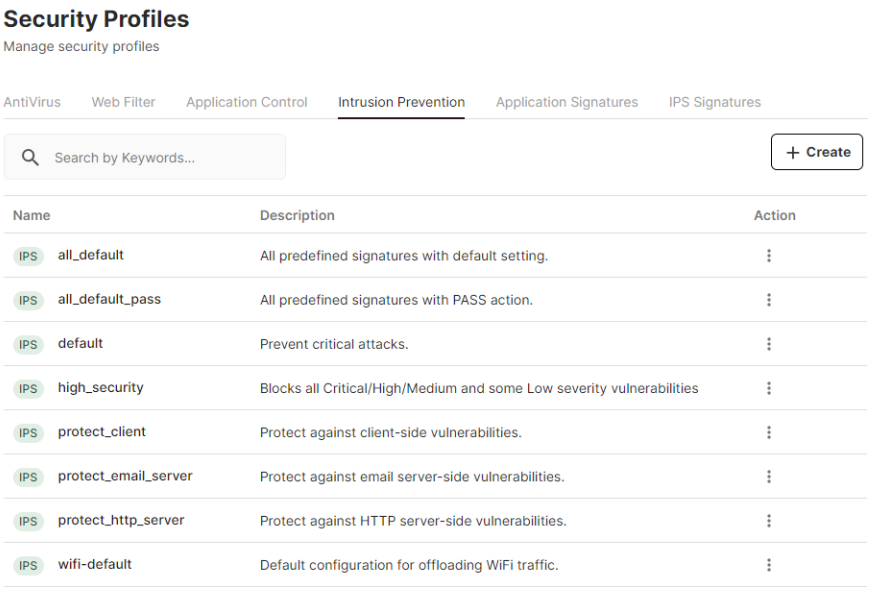
3. Click *Delete*. A confirmation dialog is displayed.



4. Click *Confirm*.

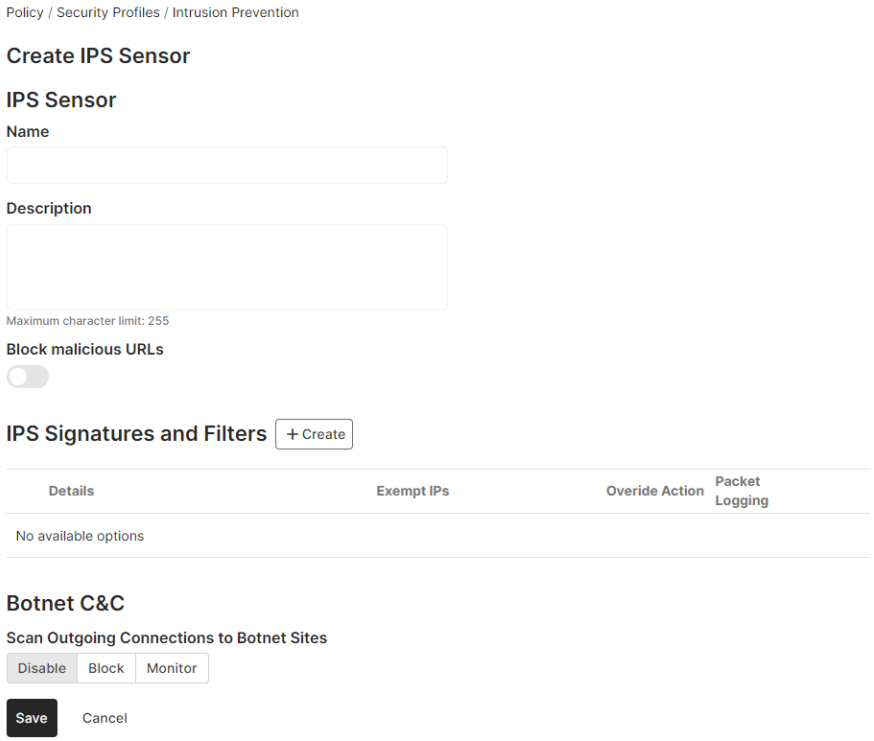
Intrusion Prevention

Intrusion prevention security profiles can be created and managed from *Policy* > *Security Profiles* > *Intrusion Prevention* tab. See Intrusion prevention in the FortiOS Administration Guide for more information.



To create a new IPS sensor:

1. Go to the *Policy* > *Security Profiles* > *Intrusion Prevention* tab.
2. Click *Create*. The *Create IPS Sensor* page is displayed.



3. Enter the *Name*.
4. Enter a *Description*.
5. Enable *Block malicious URLs*.
6. Click *Create* for *IPS Signatures and Filters*.

a. Select the *Type*.
b. Configure the filter or signature as required.

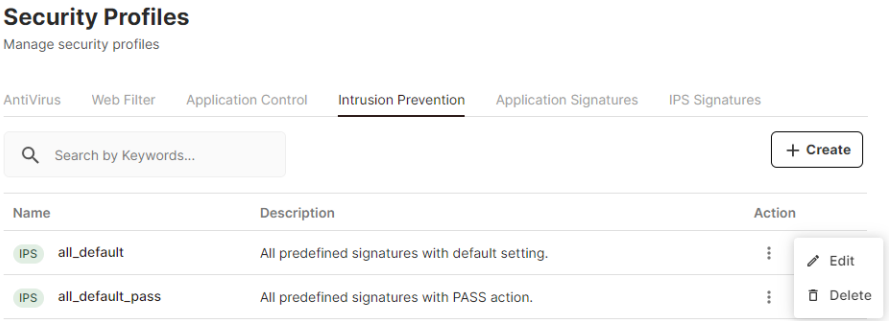
IPS signatures are also listed in the *Policy* > *Security Profiles* > *IPS Signatures* tab. See IPS Signatures on page 92.

c. Click *Done*.

7. Configure the *Botnet C&C* as desired.
8. Click *Save*.

To edit a sensor:

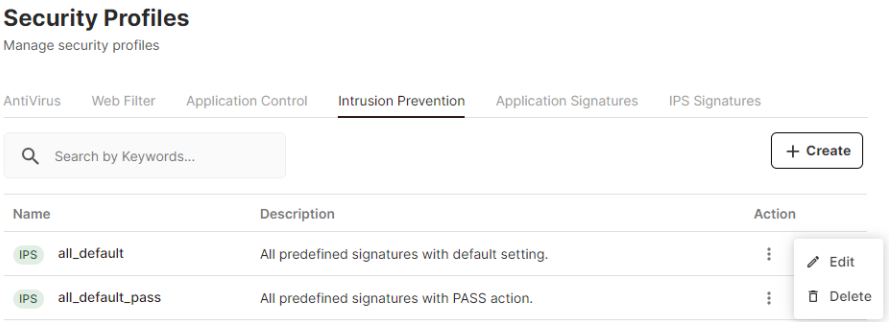
1. Go to the *Policy* > *Security Profiles* > *Intrusion Prevention* tab.
2. Select the *Action* icon for the desired profile.



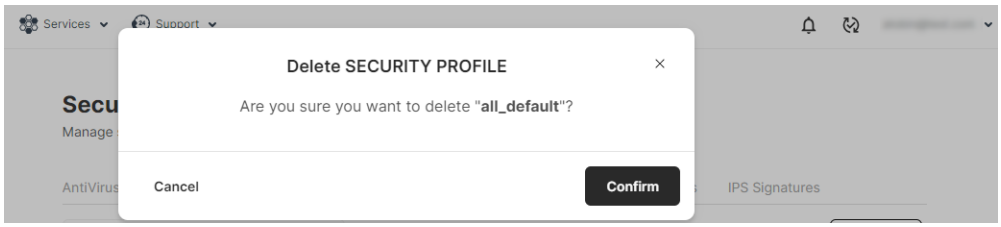
3. Click *Edit*.
4. Edit the security profile as desired.
5. Click *Save*.

To delete a sensor:

1. Go to the *Policy* > *Security Profiles* > *Intrusion Prevention* tab.
2. Select the *Action* icon for the desired profile.



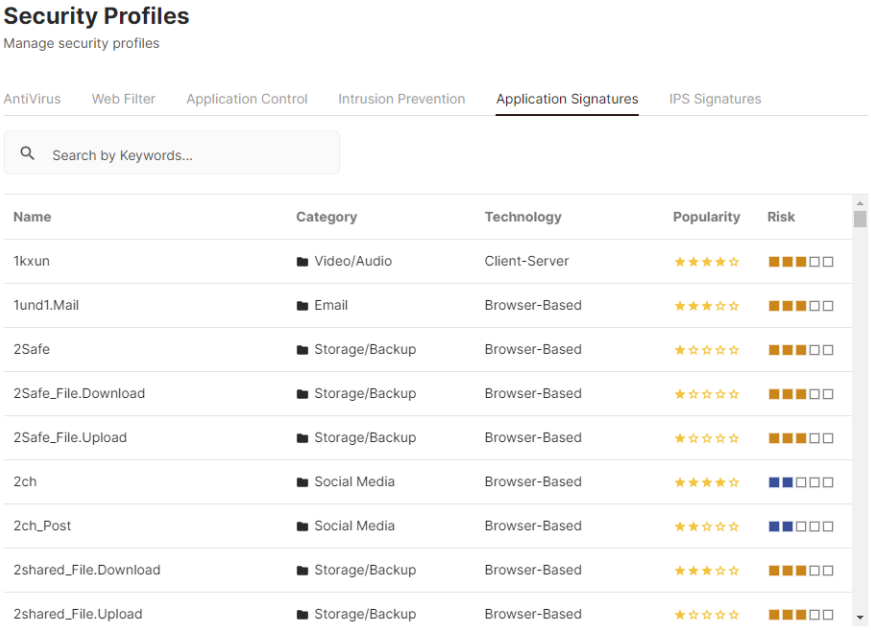
3. Click *Delete*. A confirmation dialog is displayed.



4. Click *Confirm*.

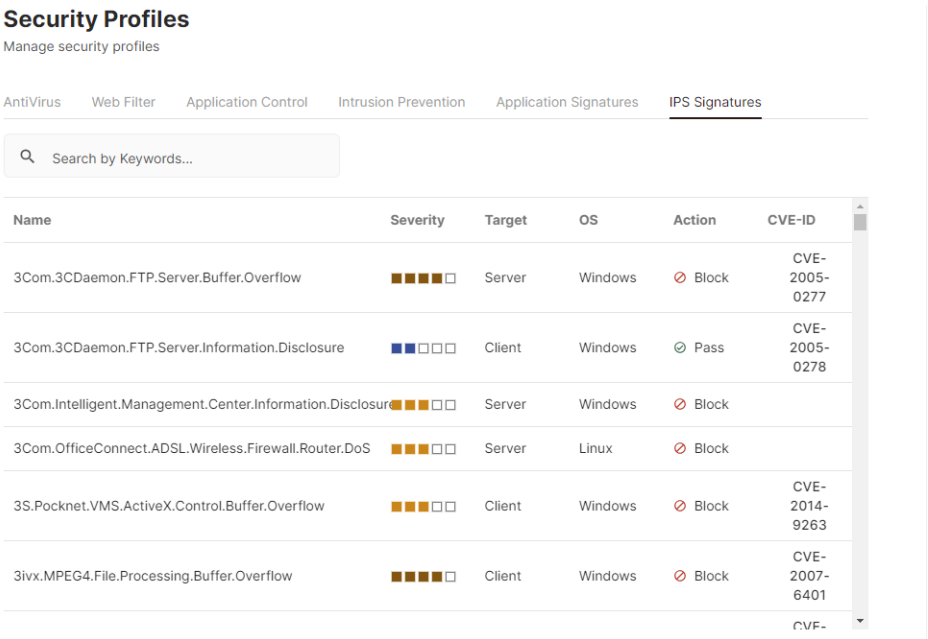
Application Signatures

Application signatures can be viewed in the *Policy* > *Security Profiles* > *Application Signatures* tab. Application signatures are required when configuring overrides in application control profiles. See Application Control on page 86.



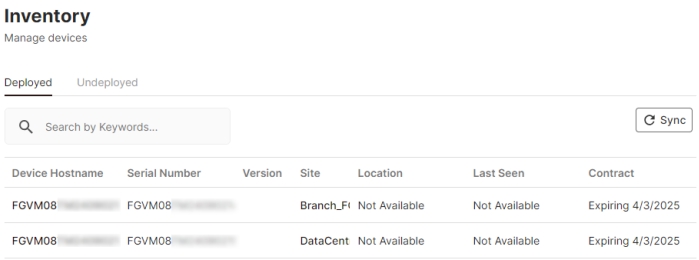
IPS Signatures

IPS signatures can be viewed in the *Policy* > *Security Profiles* > *IPS Signatures* tab. IPS signatures are required when configuring signatures in IPS sensors. See IPS Signatures on page 92.

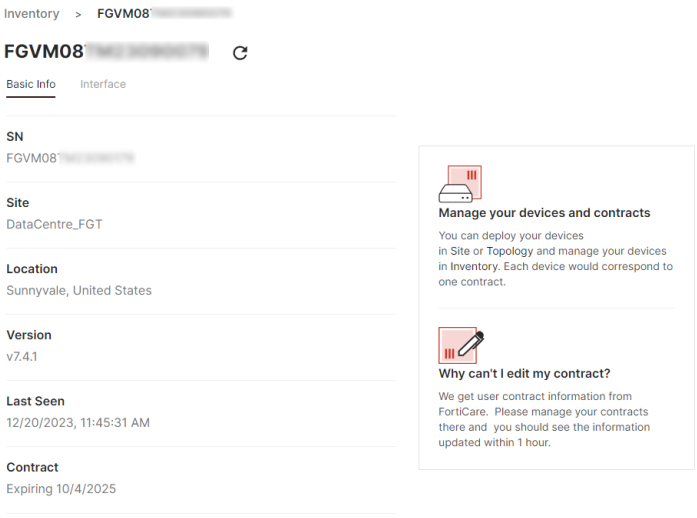

Security Profiles
Manage security profiles
AntiVirus
Web Filter
Application Control
Intrusion Prevention
Application Signatures
IPS Signatures
Search by Keywords...
Name
Severity
Target
OS
Action
CVE-ID
3Com.3CDaemon.FTP.Server.Buffer.Overflow
Server
Windows
Block
CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure
Client
Windows
Pass
CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure
Server
Windows
Block
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS
Server
Linux
Block
3S.Pocknet.VMS.ActiveX.Control.Buffer.Overflow
Client
Windows
Block
CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Overflow
Client
Windows
Block
CVE-2007-6401

Inventory

In the *Inventory* page, you can view a table with *Deployed* and *Undeployed* devices. Select *Sync* to manually sync the devices.



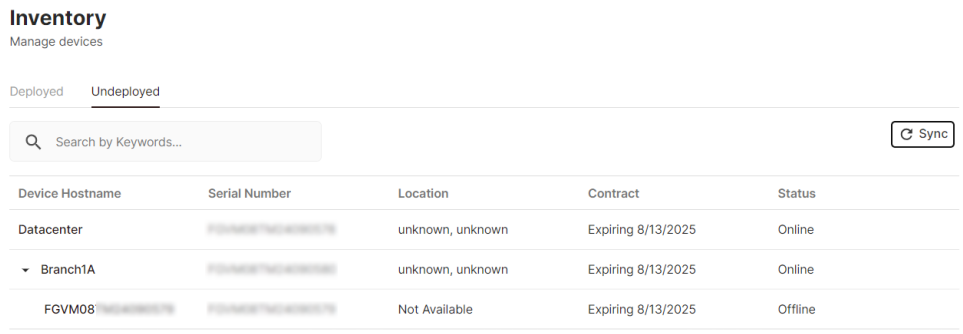
Select one of the device host names to view device details in the *Basic Info* and *Interface* tabs.



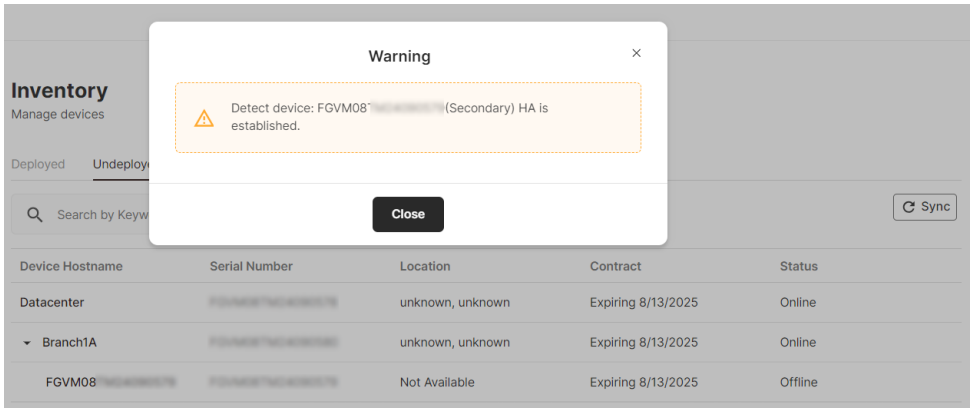
Click *Sync device with FortiCare* to update the device details, such as a new interface. For example, if you create a new interface in a FortiGate that is already deployed in the topology, you will need to sync the changes to retrieve the new interface information to the OaaS portal before you can deploy it in a subnet.

Spoke HA clusters in the Inventory

If two FortiGates are setup as an HA cluster, they will appear in the *Inventory* together. Select the dropdown icon in *Device Hostname* for the primary HA FortiGate to view information on the HA cluster FortiGates.



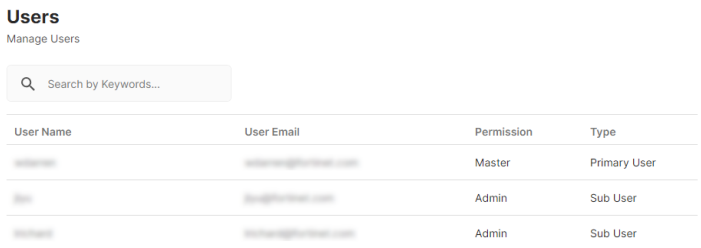
When an HA cluster is detected, a warning dialog is displayed to identify the secondary HA FortiGate.



See High Availability in the FortiOS Administration guide for more information on HA clusters.

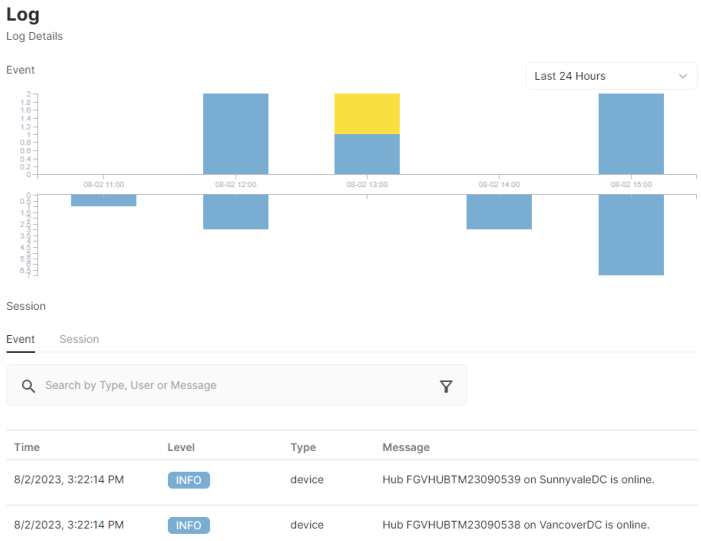
User

In the *User* page, you can view a table of user accounts associated with this FortiCloud account, including the FortiCloud administrator account and read-only user accounts created through the FortiCloud IAM portal. If there are multiple users, you can filter by entering user information in the *Search by Keywords* field.



Log

In the *Log* page, you can view graphs of the event log for the hub and spokes, and a session log for administrator actions. The top of the graph is for event logs, and the bottom of the graph is for session logs. You can navigate between *Event* and *Session* logs by selecting the desired tab.

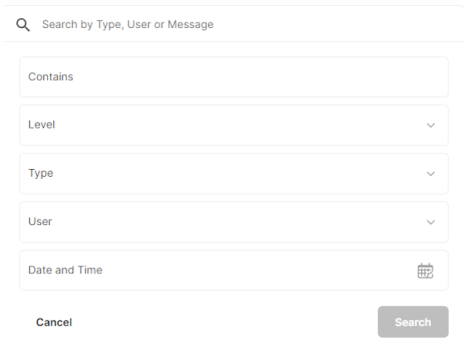


This section includes:

- Filtering logs on page 97

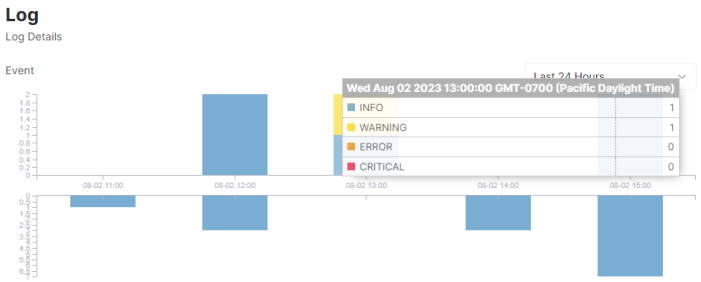
Filtering logs

You can filter event and session logs to view specific information. You can filter the *Event* and *Session* logs by selecting the filter icon or entering information in the *Search by Type, User or Message* field.



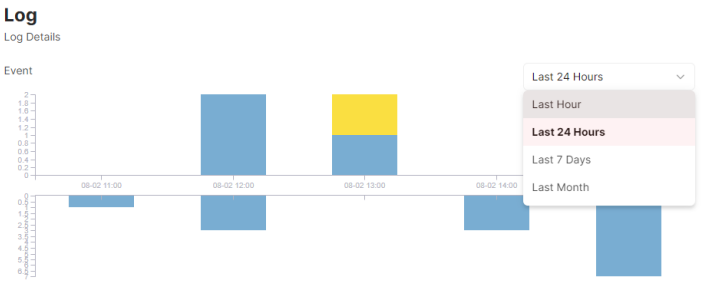
Filtering logs by type

Click the graph to display a list of filters: *Info*, *Warning*, *Error*, and *Critical*. Select a filter to display only those log entries in the table at the bottom of the view. For example, select *Info* to display only entries in the log labeled as information.



Viewing logs by time

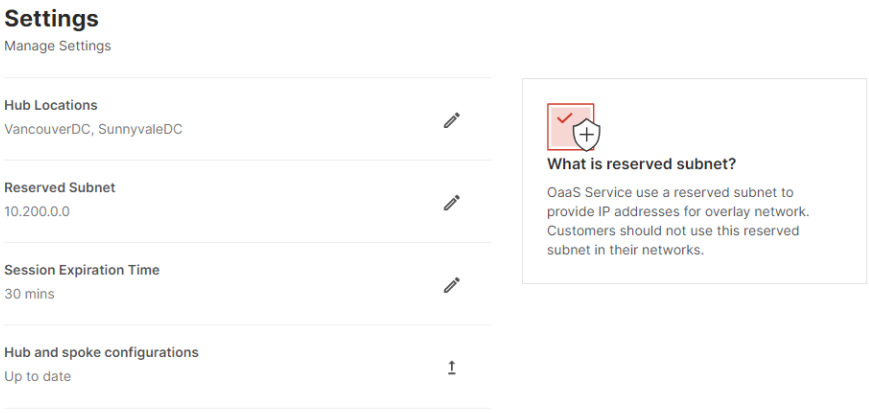
To view logs by a specific time frame, select the time frame from the graph dropdown menu.



Settings

In the *Settings* view, you can view the hub locations and the reserved subnet. You can modify settings as needed.

OaaS uses a reserved subnet to provide IP addresses for the overlay network. Customers should not use this reserved subnet in their networks.



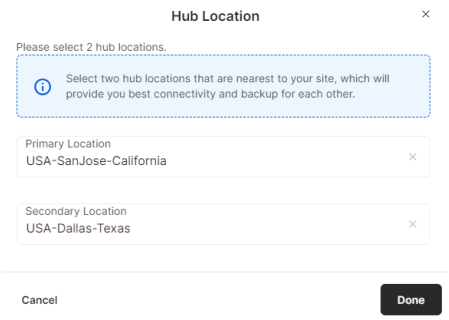
By default, OaaS has reserved 10.200.0.0/16 for overlay IP addressing of all spokes, and you should not use this network in either the LAN subnets or WAN network. If you have a network conflict, you can modify the reserved subnet in the *Settings* view within the OaaS portal. See Editing settings on page 99.

Editing settings

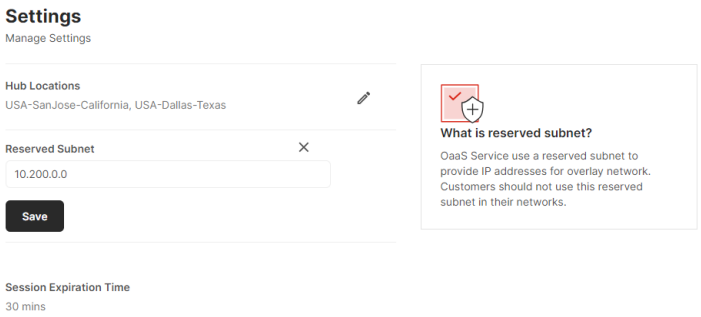
You can modify entries in the *Settings* page. Select the edit icon beside the setting you would like to modify.

Settings available for editing include:

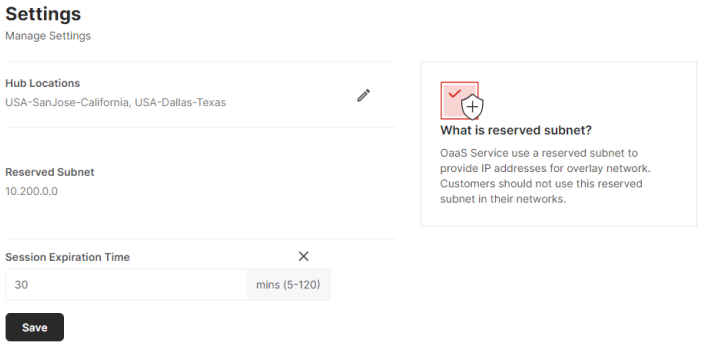
- *Hub Location*: Modify the primary and secondary locations using the dropdown menus.



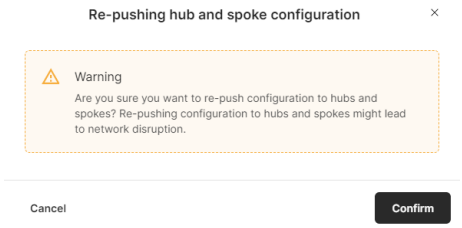
- *Reserved Subnet*: Assign a different subnet if you have a network conflict with the default reserved subnet.



- *Session Expiration Time*: Edit the idle timeout value for the Overlay-as-a-Service portal in minutes.



- *Hub and spoke configurations*: Push changes to the configuration of the hub and spokes.



Testing and verification on the FortiGate

You can verify the configurations created in the OaaS portal for the site FortiGates and test the connectivity between site devices.

Site deployment, updating, and deletion is conducted under the primary data center. If the primary data center is down, the network will continue to operate, but you will not be able to create, update, or delete site and subnets until the primary data center is back online.

This section includes:

Verifying firewall policies on a spoke

You can confirm that the spoke FortiGate's firewall policies have been configured on the spoke FortiGate's *Policy & Objects* > *Firewall Policy* page.

OaaS only creates and modifies configuration settings that it generates. OaaS does not affect any other FortiGate configuration settings. Therefore, the FortiGate spoke administrator is free to add firewall policies and other configuration settings as needed using the defined zone and address group objects created by OaaS.

OaaS creates firewall policies with wildcard address objects and services on the spoke FortiGates that allow all traffic. For some cases, these policies do not provide the necessary granularity to restrict overlay traffic to specific subnets or hosts.

OaaS will not affect any other FortiGate configuration settings and will only create and modify configuration settings that it generated. Therefore, the FortiGate spoke administrator is free to add firewall policies and other configuration settings as needed that only reference these specific configuration settings created by OaaS:

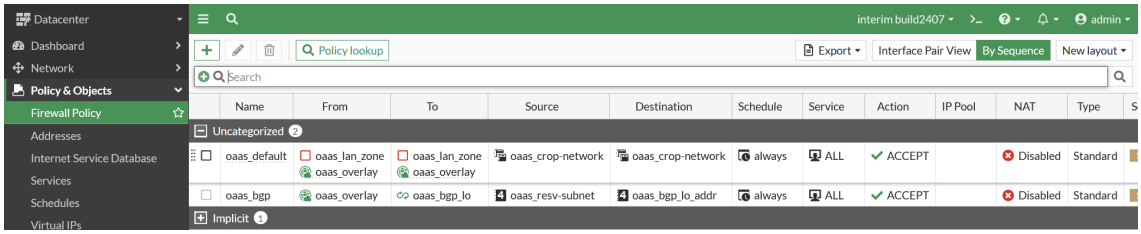
- `oaas_lan_zone` defined in `config system zone`
- `oaas_overlay` defined in `config zone` within `config system sdwan`
- `oaas_corp_network` defined in `config firewall addrgrp`

However, to ensure proper operation of OaaS with regards to topology changes and updates, ensure that you do not reference any other OaaS configuration settings in firewall policies and other configuration settings that you have added after installing settings orchestrated from OaaS.

For more information, see Firewall policy in the FortiOS Administration Guide.

To verify firewall policies on a spoke:

1. In FortiOS, on a spoke FortiGate, go to *Policy & Objects* > *Firewall Policy*.
2. Verify that firewall policies have been configured.



Verifying IPsec VPN tunnels on a spoke

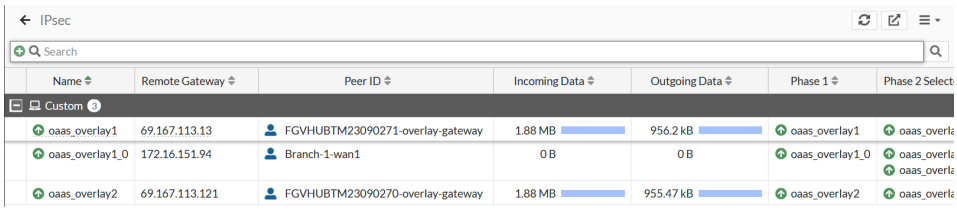
You can verify and identify the IPsec tunnels on a site in the spoke FortiGate.

In the following example, *oaas_overlay1* and *oaas_overlay2* are identified as the spoke's tunnels to the primary and secondary hubs, respectively. When there is spoke-to-spoke communication, a *_0* is added to the name of the shortcut tunnel to the hub. For example, *oaas_overlay1_0* is identified as the spoke's tunnel that was created for traffic from spoke 1 to spoke 2.

For more information on IPsec VPN tunneling, see Policy-based IPsec tunnel in the FortiOS Administration Guide.

To verify IPsec VPN tunnels on a spoke:

1. On the spoke FortiGate, go to *Dashboard* > *Network*, and click the IPsec widget to expand it.
2. Verify the IPsec tunnels that go back to the hub.



Verifying BGP routing on a spoke

You can confirm BGP routing on the spoke FortGates from the spoke FortiGate CLI and GUI. For more information on BGP routing, see BGP in the FortiOS Administration Guide.

To verify BGP routing on a spoke:

1. In the CLI on a spoke FortiGate:
   a. Check the BGP peering status:

      ```
      # get router info bgp summary
      ```

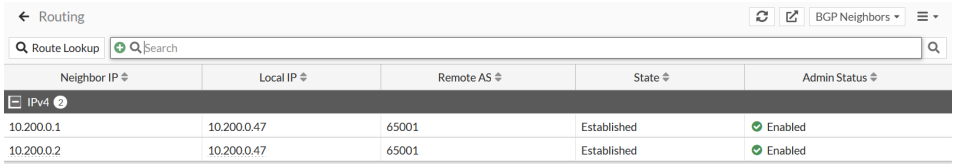
   b. Check the BGP advertised routes:

      ```
      # get router info bgp neighbors 10.200.0.1 advertised-routes
      ```

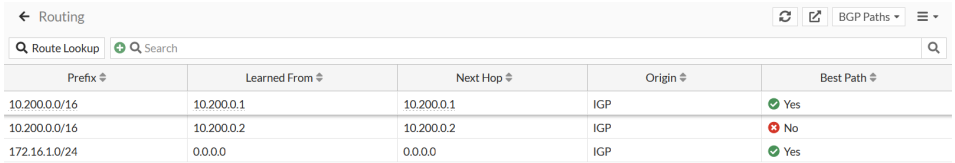
   c. Check the BGP learned routes:

      ```
      # get router info bgp neighbors 10.200.0.1 received-routes
      ```

2. In the GUI, go to *Dashboard* > *Network* and click the *Routing* widget to expand it.
3. In the dropdown, select *BGP Neighbors*.



4. In the dropdown, select *BGP Paths*.



Verifying the performance SLAs on a spoke

You can verify the performance SLA on a spoke FortiGate from *Network* > *SD-WAN*.

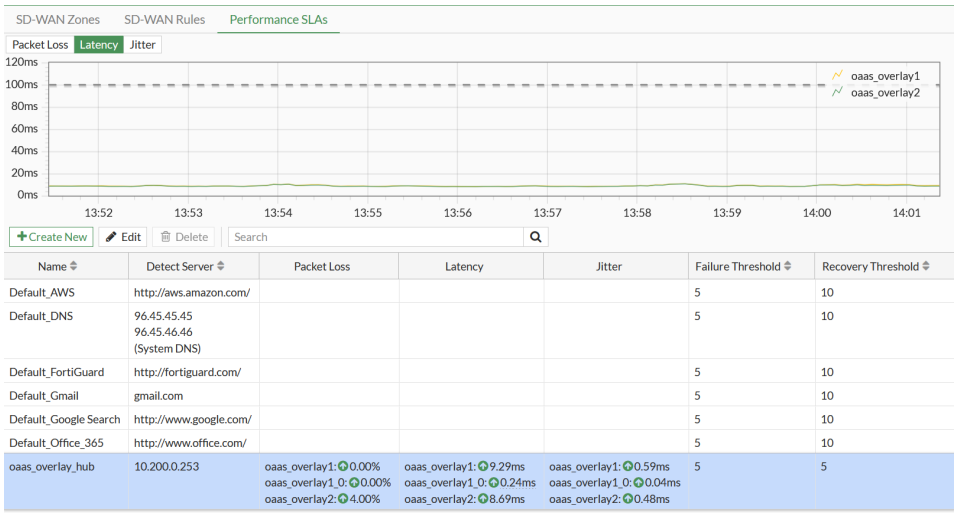
In the following example, when verifying performance SLAs, there is a new entry (*oaas_overlay_hub*) in the *Performance SLAs* tab:

- The performance SLAs to the primary and secondary hubs are denoted by *oaas_overlay1* and *oaas_overlay2*, respectively.
- The performance SLA to the spoke is denoted by *oaas_overlay1_0*.

For more information, see Performance SLA in the FortiOS Administration Guide.

To verify the performance SLAs on a spoke:

1. On the spoke FortiGate, go to *Network* > *SD-WAN*, and select the *Performance SLAs* tab.
2. Verify that the performance SLA is automatically created for the hub FortiGate.



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_AWS	http://aws.amazon.com/				5	10
Default_DNS	96.45.45.45 96.45.46.46 (System DNS)				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
oaas_overlay_hub	10.200.0.253	oaas_overlay1: 0.00% oaas_overlay1_0: 0.00% oaas_overlay2: 4.00%	oaas_overlay1: 9.29ms oaas_overlay1_0: 0.24ms oaas_overlay2: 8.69ms	oaas_overlay1: 0.59ms oaas_overlay1_0: 0.04ms oaas_overlay2: 0.48ms	5	5

Once a shortcut tunnel is established, it is also monitored using the performance SLA. If the performance SLA of the shortcut tunnel exceeds the specified thresholds during operation, then the shortcut tunnel will be removed as the best route learned using BGP in the routing table. Therefore, traffic for the destination spoke will be forwarded by the source spoke through the hub, which is not ideal.

Verifying spoke-to-spoke ADVPN communication

OaaS and the spokes rely on Auto-Discovery VPN (ADVPN), which allows the central hub to dynamically inform spokes about a better path for traffic between two spokes. You can confirm spoke-to-spoke shortcuts from the data centre FortiGate to a branch FortiGate. For more information on ADVPN communication, see ADVPN in the FortiOS Administration Guide.

To verify spoke-to-spoke ADVPN communication:

1. From the data center FortiGate, ping branch FortiGate:

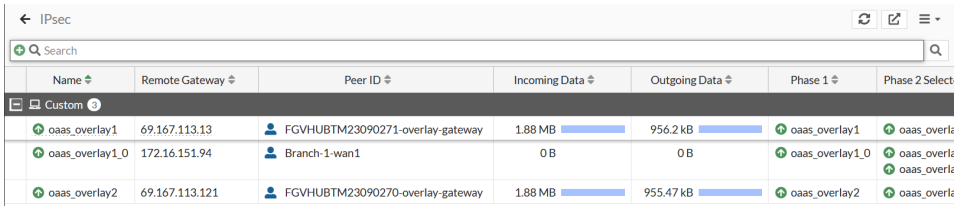
```
# execute ping-options source <Datacentre IP address>
# execute ping <Branch IP address>
```

2. Verify the IPsec tunnel summary:

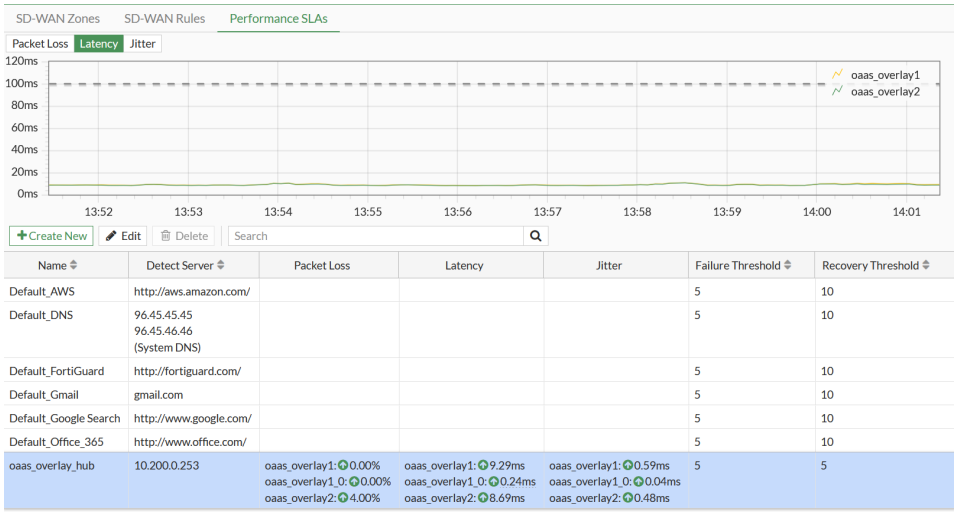
- In the CLI, enter the following:

  ```
  # get vpn ipsec tunnel summary
  ```

- In the GUI, go to *Dashboard* > *Network*, and click the *IPsec* widget to expand it.



3. Verify that the performance SLA was updated by going to *Network* > *SD-WAN*, and select the *Performance SLAs* tab. See Verifying the performance SLAs on a spoke on page 103.



Verifying SD-WAN rules on a spoke FortiGate

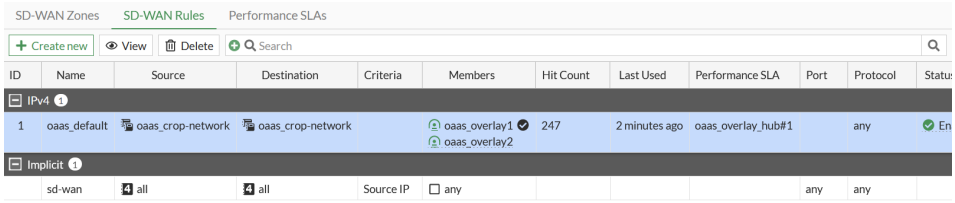
On each spoke, OaaS automatically creates a performance SLA that corresponds to the hub FortiGate. An SD-WAN rule has been configured on the spoke FortiGates to direct traffic to the hub FortiGate using this performance SLA.

You can create additional SD-WAN rules. Configure and place new rules below the *oaas_default* rule. See SD-WAN rules in the FortiOS Administration Guide for more information.

To verify SD-WAN rule on a spoke FortiGate:

1. On a spoke FortiGate, go to *Network* > *SD-WAN*, and select the *SD-WAN Rules* tab.
2. View the SD-WAN rule created by OaaS named *oaas_default* that corresponds to the performance SLA named

oaas_overlay_hub#1.



Verifying the OaaS agent for uninterrupted spoke traffic

To ensure FortiGate spoke traffic remains uninterrupted when configuration is orchestrated from OaaS, support for an OaaS agent on the FortiGate is available. The OaaS agent communicates with the OaaS controller in FortiCloud, validates and compares the FortiOS configuration, and applies the FortiOS configuration to the FortiGate as a transaction when it has been orchestrated from the OaaS portal. Secure communication between the OaaS agent and the OaaS controller is achieved using the FGFM management tunnel.

If any configuration change fails to be applied, then the OaaS agent rolls back all configuration changes that were orchestrated. The OaaS status on the spoke FortiGate can be acquired using `get oaas status`.

To determine the status of OaaS:

```
# get oaas status
Account ID: 78992
Account: admin@domain.com
Site: site1
Configuration version: 4
Configuration sync status: SUCCESS
    Target version: 4
    Task ID: xxxxxxxxx
    Error:
```

www.fortinet.com