SD-WAN Orchestrator MEA - Administration Guide

Version 6.4.1.r5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 22, 2021
SD-WAN Orchestrator MEA 6.4.1.r5 Administration Guide
02-641r5-609779-20210122

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Simplified SD-WAN deployment 6
SD-WAN Orchestrator MEA use cases 7
Key concepts 7
FortiGate devices 8
Regions and links 8
Normalized interfaces 10
Underlay and overlay links 10
Profiles 10
Configuration installation 10
Global routing 10
Global analysis and visibility 11
Device analysis and visibility 11
Business rules 11
How SD-WAN Orchestrator MEA works with FortiManager 11
Quick start **12**
Enabling SD-WAN Orchestrator MEA 12
Planning your network 13
Creating shared resources 13
Creating profiles for all roles 14
Adding devices to FortiManager 14
Adding devices to SD-WAN Orchestrator MEA and installing configurations 14
Installing firewall policies 15
Monitoring devices and network traffic 15
Monitor **16**
Dashboard 16
Viewing devices on the world map 16
Viewing device topology 17
Viewing shortcut overlays (ADVPN) 18
Viewing hub devices 18
Viewing regions 19
Traffic 21
Viewing global network traffic reports 21
Exporting global traffic reports 22
SLA 23
Devices 24
Viewing device overviews 24
Viewing device link reports 24
Viewing device traffic reports 25
Viewing device SLA 26
Logs 26

Configuration **28**
Device 28
Adding devices 29
Adding devices in HA clusters 30
Adding model devices 31
Adding model devices in HA clusters 32
Adding regions 34
Adding unauthorized devices 35
Installing configuration changes 35
Importing devices 36
Viewing configuration status 37
Overriding device settings 37
Adding static routes 38
Updating regions 39
Deleting regions 40
Monitoring devices 40
Replacing FortiGate serial numbers 40
Profile 41
Creating profiles for hub devices 42
Creating profiles for edge devices 43
Creating profiles for HA devices 44
Creating new WAN settings 45
Creating new LAN settings 47
Attaching a FortiSwitch model to FortiGate 49
Adding a FortiAP model device 54
Creating new DMZ settings 59
Creating business rules 60
Cloning profiles 60
Updating profiles 61
Deleting profiles 62
Profile options described 62
Shared resources 69
Intranet Addresses 69
Network 69
SLA 73
System 73
Health Threshold 75
Global routing 75
Maintenance **77**
Upgrade 77
Configuration 77
Debug 78
More information **79**

Change Log

Date	Change Description
2020-12-22	Initial release of 6.4.1.r5.
2021-01-22	Added information about device location changes and anti-theft to Changing network settings on page 71.

Introduction

When enabled, SD-WAN Orchestrator MEA is installed on FortiManager. SD-WAN Orchestrator MEA is a management extension application (MEA) that is released and signed by Fortinet to run on FortiManager.

SD-WAN Orchestrator MEA 6.4.1.r5 requires FortiManager 6.4.1 or later, and you must be in a 6.4 ADOM to access SD-WAN Orchestrator MEA.

You can use SD-WAN Orchestrator MEA to configure and monitor SD-WAN networks on FortiGates that are managed by FortiManager. SD-WAN Orchestrator MEA is available only with FortiManager, and it supports several FortiGate models. For a list of supported FortiGate models, see the SD-WAN Orchestrator MEA 6.4.1.r5 Release Notes on the Docs Library. The release notes also identify any limitations of SD-WAN Orchestrator MEA.

This section contains the following topics:

- Simplified SD-WAN deployment on page 6
- SD-WAN Orchestrator MEA use cases on page 7
- Key concepts
- How SD-WAN Orchestrator MEA works with FortiManager

Simplified SD-WAN deployment

SD-WAN Orchestrator MEA simplifies the configuration of an SD-WAN network by automating tasks and making some decisions for you. It is ideal for a multi-region enterprise network, where hub and edge devices interconnect to create a complex mesh of underlays and VPN overlays. SD-WAN Orchestrator MEA automates the configuration based on profiles that you define for hub and edge devices, allowing you to scale your SD-WAN deployment with ease.

This section describes what components contribute to the automation and when the automation occurs.

The first step is to create the following shared resources for SD-WAN Orchestrator MEA to use for its automation:

- Profile for primary hub devices
- Profile for secondary hub devices, if using
- Profile for edge devices
- Region for hub and edge devices

When you add a FortiGate device to SD-WAN Orchestrator MEA, you specify whether it is a primary hub device, secondary hub device, or an edge device by selecting a profile, and you specify its region by selecting a region. SD-WAN Orchestrator MEA uses this information to automatically perform the following tasks:

- Create full-mesh overlay links between all hub devices
- Create VPN tunnels between hub and edge devices in the same region
- Apply policy templates for SD-WAN from the profiles

After you install the configuration to FortiGate devices, you can monitor the SD-WAN network by using the *Monitor* tab in SD-WAN Orchestrator MEA. On the *Monitor* tab, you have real-time visibility across regions, and you can view network performance.

Another way to use automation is zero-touch provisioning. With zero-touch provisioning, you can add a model device to SD-WAN Orchestrator MEA where you specify the profile and region and what action to take when the device first comes online. For example, you can set up the model device to automatically retrieve and install the configuration and upgrade to the accepted firmware version before automatically joining the overlay mesh of the SD-WAN network. Alternately with zero-touch provisioning, you can allow administrators to approve the device when it first comes online before it automatically joins the SD-WAN network.

SD-WAN Orchestrator MEA use cases

Although SD-WAN Orchestrator MEA is available with FortiManager, FortiManager also includes SD-WAN network configuration options. You can access the two SD-WAN configuration methods in FortiManager as follows:

- *FortiManager > Device Manager > SD-WAN*
- *FortiManager > Management Extensions > SD-WAN Orchestrator MEA*

Each SD-WAN configuration method has its strengths and limitations. The following table summarizes the strengths and limitations of each method and identifies when to use each method.

	FortiManager SD-WAN	SD-WAN Orchestrator MEA
Strengths	• Full SD-WAN feature set • Scales to 10K plus sites • No additional license required	• VPN overlay and routing automatically configured • Simplified provisioning workflow • Better SD-WAN charts and graphs
Limitations	• VPN and routing need separate configurations	• Supports up to 1000 sites • Does not expose all configurations • Flexible per appliance license
Best suited to	• Large, complex SD-WAN deployments • Customers requiring advanced WAN remediation • NOC and SOC team collaboration • Large enterprise, MSSP, and carrier customers	• Simple SD-WAN deployments • Customers looking for intelligent traffic steering • Mid-sized enterprise customers

Key concepts

This section contains information about the following key concepts and features of SD-WAN Orchestrator MEA:

- FortiGate devices on page 8
- Regions and links on page 8
- Normalized interfaces on page 10

- Underlay and overlay links on page 10
- Profiles on page 10
- Configuration installation on page 10
- Global routing on page 10
- Global analysis and visibility on page 11
- Device analysis and visibility on page 11
- Business rules on page 11

FortiGate devices

SD-WAN Orchestrator MEA supports FortiGate devices. For SD-WAN Orchestrator MEA to configure and manage SD-WAN networks on FortiGate devices, the devices must be added to both FortiManager and SD-WAN Orchestrator MEA.

After the FortiGate devices are added to both products, SD-WAN Orchestrator MEA works with FortiManager to configure and monitor SD-WAN networks on the devices. See also How SD-WAN Orchestrator MEA works with FortiManager on page 11.

In general, you should add devices to both products in the following order:

1. FortiManager
2. SD-WAN Orchestrator MEA

However, in some cases you can add FortiGate devices to SD-WAN Orchestrator MEA first. For example, see Adding model devices on page 31 and Importing devices on page 36.

SD-WAN Orchestrator MEA supports FortiGate devices in high availability (HA) active-passive (AP) mode.

Regions and links

Each region can have a primary hub, secondary hub, and multiple edge devices. The secondary hub is optional and provides redundancy.

SD-WAN Orchestrator MEA automatically creates links between devices based on settings in the assigned profiles.

Links between hub devices

SD-WAN Orchestrator MEA automatically builds full-mesh overlay links between all primary and secondary hub devices. Primary hubs have higher priority than secondary hubs.

When a hub receives incoming traffic destined to the edge subnet of a local region, but links between hub and edge devices are down, SD-WAN Orchestrator MEA uses the links to forward traffic to another hub.

If LAN port communication is also configured between hubs in a region, the LAN port is also used.

Links between hub and edge devices in the same region

In the same region, the connection between the hub devices (primary and secondary hubs) and edge devices depends on the VPN mode. The VPN mode is configured in profiles, and a profile is assigned to each primary hub, secondary hub, and edge device when you add it to SD-WAN Orchestrator MEA. The following VPN modes are available:

- Site-to-site VPN
- Dialup VPN

The following table summarizes how the VPN modes affect the connection between hub and edge devices:

VPN Mode	Description
Site-to-site VPN	Overlay links are full-mesh between the hub devices and edge devices in the same region. Edge devices from the same region communicate with each other by forwarding packets through their region's hubs.
Dialup VPN	Overlay links are one-to-one between hub devices and edge devices in the same region. In other words, one WAN port on each edge device establishes an IPsec tunnel only with one WAN port on hub devices. In DialUP VPN mode, ADVPN is supported to create shortcut tunnels between edge devices. On hub devices, select one of the following options: • *NONE* - ADVPN is disabled. Edge devices from the same region will communicate with each other by forwarding packets through their region's hub. • *INSIDE_REGION* - Shortcut tunnels are triggered by traffic and established only inside a region. On edge devices, toggle *ADVPN* on to enable ADVPN. Toggle off to disable ADVPN.

When a region contains both a primary hub and secondary hub, edge devices establish overlay links with both hubs in the region. Overlay links between edge devices and the primary hub have higher priority than overlay links between edge devices and secondary hubs.

When overlay links between edge devices and the primary hub are down, links between the edge device and the secondary hub are used to forward traffic.

When incoming traffic destined to an edge device subnet of the local region is received by one hub, but links between the hub and edge devices are down, the hub uses the overlay links to forward traffic to another hub.

If LAN port communication is configured between primary and secondary hubs in a region, traffic is forwarded by using the LAN port communication.

Edge device communication between regions

When site-to-site VPN mode is enabled, edge devices in one region can communicate with devices in another region by using the following method:

1. Edge devices send packets to their region's hub.
2. The hub forwards the packet to the hub of the destination region.
3. The hub from the destination region forwards the packet to the final destination.

Normalized interfaces

SD-WAN Orchestrator MEA 6.4.1 and later automatically creates the following normalized interfaces with per-platform mappings in FortiManager:

- overlay_edge2hub
- overlay_hub2edge
- overlay_hub2hub
- underlay
- sdwan_loopback

You can view normalized interfaces in FortiManager by going to *Policy & Objects* > *Object Configuration* > *Normalized Interface*.

The normalized interfaces are used by the policy blocks that SD-WAN Orchestrator MEA automatically creates. You can also use normalized interfaces with custom policies.

Underlay and overlay links

Underlay links are data links rented or bought from an ISP. These links consist of Internet, MPLS, and 3G/LTE links.

Overlay links are virtual tunnels built on top of underlay links. These links form an IPsec secured connection between two FortiGate devices.

You specify underlay and overlay links when you configure profiles.

Profiles

Profiles are templates that you can use to define settings for primary hub, secondary hub, and edge devices. You can also define settings for FortiGate devices in high availability (HA) clusters in active-passive (AP) mode. In a profile, you can configure settings for VPN mode, system resources, network settings, and business rules.

After creating a profile, you can apply it to multiple FortiGate devices.

You can override profile settings for individual devices.

Configuration installation

You can configure profiles of configuration settings on SD-WAN Orchestrator MEA before setting up a device. Once the device is set up, you can install the profile of configuration settings via SD-WAN Orchestrator MEA to the device.

Global routing

SD-WAN Orchestrator MEA automatically maintains the LAN and static subnet routes for all the devices it manages.

Global analysis and visibility

SD-WAN Orchestrator MEA collects and aggregates information from connected FortiGate devices to provide a global traffic and health status view for the SD-WAN network.

Device analysis and visibility

SD-WAN Orchestrator MEA provides you with information on device resource usage, underlay and overlay traffic, network health status, as well as traffic statistics based on source IP, destination IP, applications, and event logs.

Business rules

Business rules define routing policies between subnets in SD-WAN networks or how traffic from SD-WAN subnets accesses the Internet. SD-WAN Orchestrator MEA includes predefined business rules in profiles. You can also create business rules.

How SD-WAN Orchestrator MEA works with FortiManager

SD-WAN Orchestrator MEA works with FortiManager to configure and monitor SD-WAN networks on FortiGates.

You use SD-WAN Orchestrator MEA to configure SD-WAN networks and assign configurations to FortiGate devices. When you use SD-WAN Orchestrator MEA to apply the configuration to FortiGates, SD-WAN Orchestrator MEA uses the following method to work with FortiManager to install the configurations to FortiGates:

1. SD-WAN Orchestrator MEA automatically generates CLI scripts of the configuration.
   You can view the scripts in FortiManager on the *Device Manager* > *Scripts* pane.
2. SD-WAN Orchestrator MEA installs the CLI scripts to the *Device Manager* database in FortiManager.
3. FortiManager receives the CLI scripts, and FortiManager installs the configurations to the FortiGates.
   When the configuration is installed to FortiGates, the overlay and underlay links between all devices in the SD-WAN network are automatically created.

   SD-WAN Orchestrator MEA creates the normalized interfaces for generated tunnel interfaces. The normalized interfaces use per-platform mapping interface, and you can use them in FortiManager when you create policies. SD-WAN Orchestrator MEA also creates two policy blocks in FortiManager: one for hub devices and one for edge devices. The policy blocks include the necessary firewall policies to allow health check traffic through the VPN tunnels. You can view the policy blocks in FortiManager by going to *Policy & Objects* > *Policy Packages*.

You should use SD-WAN Orchestrator MEA for all configuration and monitoring of SD-WAN networks. You should not use FortiManager to configure SD-WAN networks on FortiGates when SD-WAN Orchestrator MEA is already enabled and configured.

However you can use FortiManager to configure firewall policies and objects for the FortiGate units in the SD-WAN network after SD-WAN is configured.

Quick start

SD-WAN Orchestrator MEA is a flexible application. Although you must add FortiGate devices to both SD-WAN Orchestrator MEA and FortiManager, you can add the devices using several different methods, depending on need. This section describes one method, which is to add the FortiGate device to FortiManager first, and then add the device to SD-WAN Orchestrator MEA second. See also FortiGate devices on page 8.

This section provides a summary of how to get started with SD-WAN Orchestrator MEA:

1. Enable SD-WAN Orchestrator MEA. See Enabling SD-WAN Orchestrator MEA on page 12.
2. Plan your SD-WAN network. See Planning your network on page 13.
3. Create shared resources. See Creating shared resources on page 13.
4. Create profiles for hub and edge devices. See Creating profiles for all roles on page 14.
5. Add FortiGate devices to FortiManager. See Adding devices to FortiManager on page 14.
6. Add devices to SD-WAN Orchestrator MEA and install SD-WAN configurations. See Adding devices to FortiManager on page 14.
7. Install firewall policies to FortiGate devices in SD-WAN networks. See Installing firewall policies on page 15.
8. Monitor the SD-WAN network. See Monitoring devices and network traffic on page 15.

Enabling SD-WAN Orchestrator MEA

FortiManager provides access to the SD-WAN Orchestrator MEA application that is released and signed by Fortinet.

Only administrators with a *Super_User* profile can enable management extensions.
A CA certificate is required to install management extensions on FortiManager.

To enable SD-WAN Orchestrator MEA:

1. Ensure you are using ADOM version 6.4 or later.
2. Go to *Management Extensions*.
3. Click the grayed out tile for SD-WAN Orchestrator MEA to enable the application.
   Grayed out tiles represent management extensions. In the following example, *SD-WAN Orchestrator MEA* is enabled, and *Wireless Manager* is disabled.

4. Click *OK* in the dialog that appears. It may take some time to install the application.

Planning your network

While individual network requirements might vary, you should consider the following principles when planning your network topology:

- Regions - Depending on how your network is structured geographically, you might need multiple regions.
- Devices - Each FortiGate device should be added to its corresponding region. In addition, each FortiGate device must be able to connect to FortiManager.
- Hub and edges - You can identify one FortiGate device from each region to act as a primary hub and another to act as a secondary hub. Each region can have one primary hub device and one secondary hub device, but multiple edge devices are allowed in each region.
  SD-WAN Orchestrator MEA automatically establishes overlay links between all hubs. Each hub also establishes tunnels to every edge device in the same region.

  If you choose not to identify a hub device, SD-WAN Orchestrator MEA does not set up an overlay network for the region.

Creating shared resources

Before you create profiles, you can create a number of shared resources that you can select in profiles. You can create the following shared resources:

- Network resources, such as DHCP servers, DHCP relays, DNS servers, intranet IP pools, SNMP hosts, and VPN address pools.
  It is recommended to create intranet IP pools that SD-WAN Orchestrator MEA can use when it creates the SD-WAN network for selected devices.

  ISP links are automatically created when a WAN port is enabled in a profile.
- Service level agreements (SLA), such as quality levels and servers.
- Servers, such as NTP, FortiGuard, and email, that SD-WAN Orchestrator MEA can use.
- Health threshold settings

For more details, see Shared resources on page 69.

Creating profiles for all roles

Profiles are templates that define general, system, network, and business policies for devices in SD-WAN networks. It is recommended to create the following profiles at a minimum:

- Profile for primary hub devices and secondary hub devices - see Creating profiles for hub devices on page 42
- Profile for edge devices - see Creating profiles for edge devices on page 43

See also Profile on page 41.

Adding devices to FortiManager

Devices must be added to FortiManager and SD-WAN Orchestrator MEA. For details about adding devices to FortiManager, see the *FortiManager Administration Guide*.

Adding devices to SD-WAN Orchestrator MEA and installing configurations

After you have planned the network, created shared resources, created profiles, and added FortiGate devices to FortiManager, you are ready to add the FortiGate devices to SD-WAN Orchestrator MEA. When you add FortiGate devices to SD-WAN Orchestrator MEA, you select profiles and install configurations to the devices to automatically create the SD-WAN network. This step executes your network plan.

Following is a summary of the process:

1. Ensure that you have created profiles for hub and edge devices.
   You should create a profile for the primary hub role and a profile for the edge role. If you are using secondary hub devices, ensure you have created a profile for the secondary hub role too.
2. Ensure that you have added FortiGate devices to FortiManager.
3. Add the FortiGate devices to SD-WAN Orchestrator MEA by adding a region.
   When you add a region to SD-WAN Orchestrator MEA, you can specify a region name, and select the devices for hub and edge roles. You can also select profiles for each device in the region.

   When you finish adding a region, SD-WAN Orchestrator MEA works with FortiManager to automatically install the configurations to the devices and create the SD-WAN network. For more information, see How SD-WAN Orchestrator MEA works with FortiManager on page 11.

   For more details about adding devices, see Device on page 28.
4. After the configurations are installed, the SD-WAN network is configured between the devices, and you can monitor the global network as well as individual devices. For details, see Monitor on page 16.

Installing firewall policies

Although SD-WAN Orchestrator MEA is used to configure SD-WAN networks, you use FortiManager to define and install firewall policies to the FortiGates in an SD-WAN network. It is recommended to configure the SD-WAN network before you install firewall policies to FortiGate devices.

Before installing firewall policies, it is recommended to insert the policy block *SDWAN_Overlay_PB_EDGE* and *SDWAN_Overlay_PB_HUB* to policy packages, and move the policy blocks to the top. The policy block is automatically maintained by SD-WAN Orchestrator MEA. The policy block allows health-check packets and negotiation packets for IPsec tunnels between devices.

For details about using FortiManager to install firewall policies, see the *FortiManager Administration Guide*.

Monitoring devices and network traffic

After the configurations are installed, the SD-WAN network is configured between the devices, and you can monitor the global network and individual devices:

- For global analysis and visibility, see Dashboard on page 16, Traffic on page 21 and SLA on page 23.
- For device analysis and visibility, see Devices on page 24.

Monitor

After you have configured an SD-WAN network, you can monitor the global network as well as individual devices in the network by using the *Monitor* tree menu.

From the *Monitor* tree menu, you can access the following panes:

- Dashboard on page 16
- Traffic on page 21
- SLA on page 23
- Devices on page 24
- Logs on page 26

Dashboard

The *Dashboard* pane provides global analysis and visibility into all connected devices in the SD-WAN network. From the *Dashboard* pane, you can switch between the *Topology View*, *Map View* and *HubView*.

This section contains the following topics:

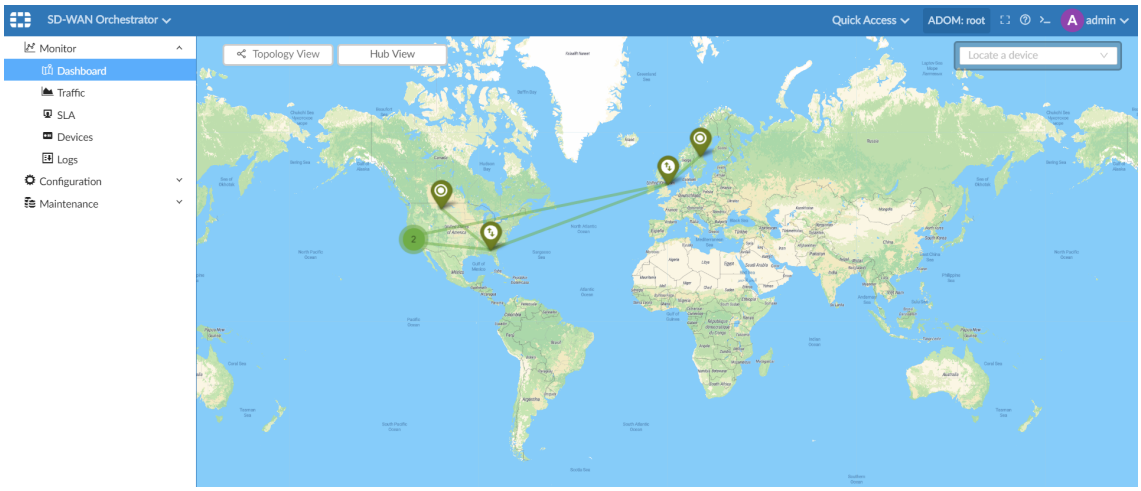
- Viewing devices on the world map on page 16
- Viewing device topology on page 17
- Viewing shortcut overlays (ADVPN) on page 18
- Viewing hub devices on page 18
- Viewing regions on page 19

When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the maps. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

If you want to view details about individual devices in the SD-WAN network, see Devices on page 24.

Viewing devices on the world map

Map View is the default, global view when you open SD-WAN Orchestrator MEA. Map view displays connected devices across the globe. You can move device icons by clicking and dragging them across the map.

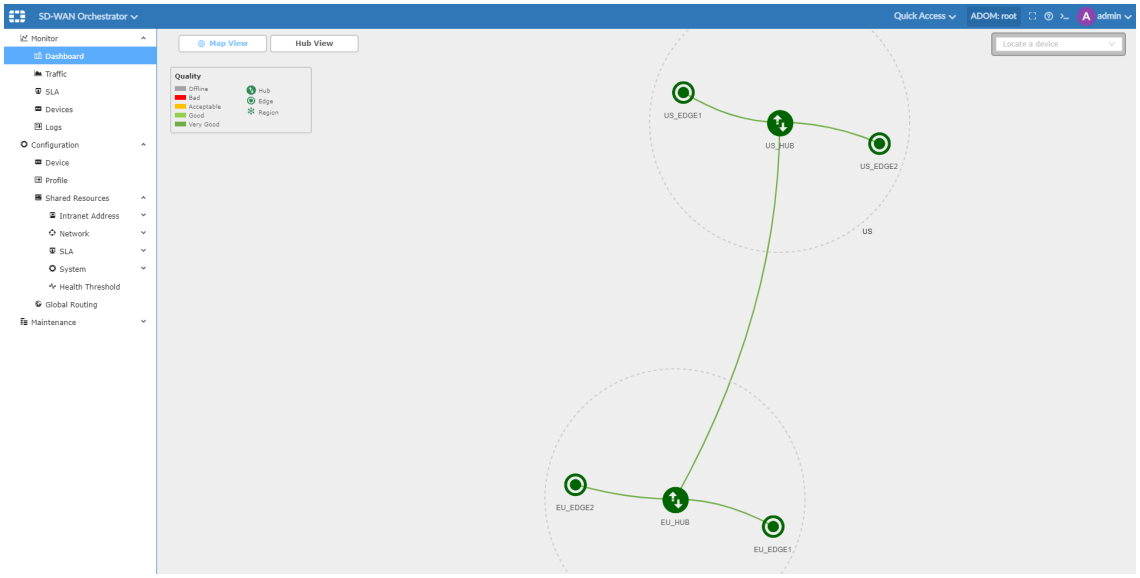


Viewing device topology

The *Topology View* displays all connected devices across the globe in the SD-WAN network, regardless of geographical distance.

To view device topology:

1. Go to *Monitor* > *Dashboard*, and click *Topology View* at the top of the map.
   The following example shows the topology view of two regions and two hubs. The color shows the quality, and the lines show the VPN tunnels between the devices. The width of the lines indicates the amount of traffic passing through the tunnel.



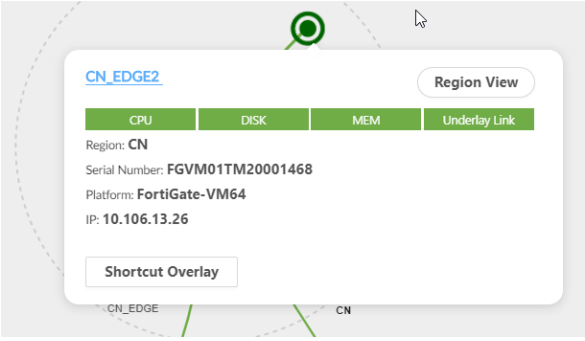
2. Click the lines to view link information, including the inbound and outbound bandwidth.

Viewing shortcut overlays (ADVPN)

From the *Topology View*, you can view the shortcut overlay for an edge device.

To view shortcut overlays (ADVPN):

1. Go to *Monitor* > *Dashboard*, and click *Topology View* at the top of the map.
   The topology is displayed.
2. In the topology, click an edge device.
   A summary of the device is displayed.



3. Click the *Shortcut Overlay* button.
   The shortcut view is displayed.
4. Click the *Exit Shortcut View* button to exit the view.

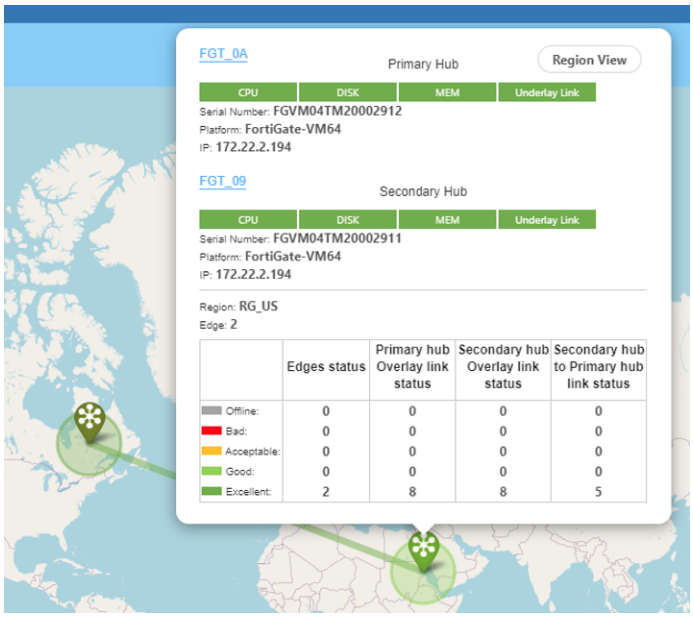
Viewing hub devices

You can view all hub devices across the globe in the SD-WAN network on the *Hub View* pane.

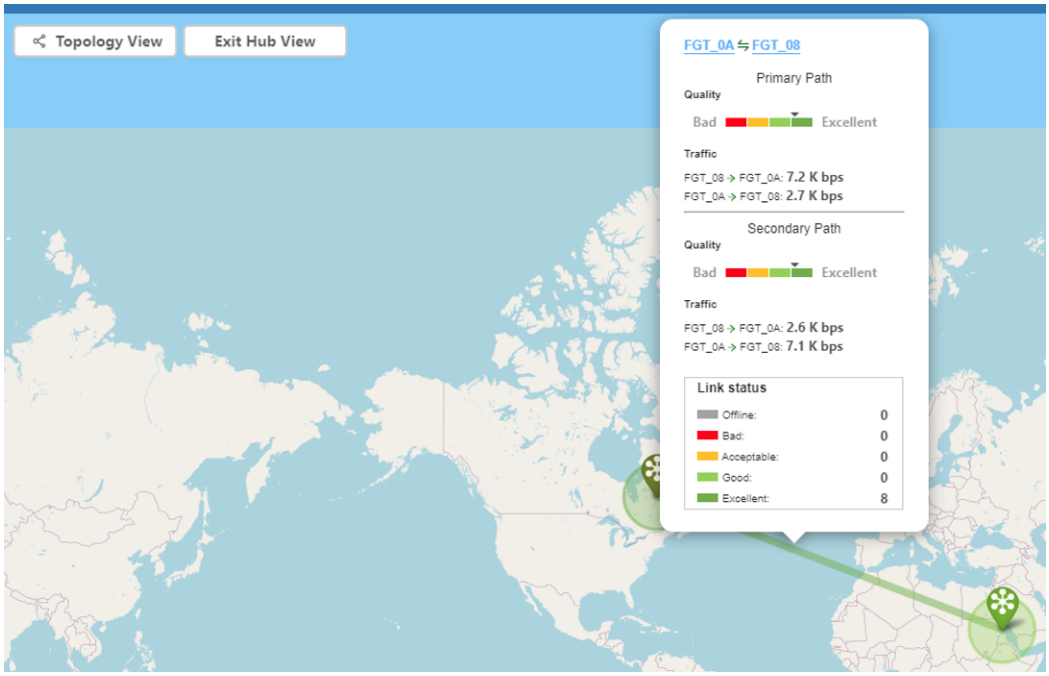
When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the map. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

To view hub devices:

1. Go to *Monitor* > *Dashboard*, and click *Hub View*.
2. Click a hub to view status information, including *Edges status* and *Overlay link status*.
   When the region includes both a primary hub and a secondary hub, the status displays information for both hubs. In the following example, *FGT_0A* is the primary hub, and *FGT_09* is the secondary hub.



3. Click the lines between hubs to view link information.
When the region includes both a primary hub and a secondary hub, information about links for both hubs is displayed. In the following example, information about the *Primary Path* and the *Secondary Path* is displayed.



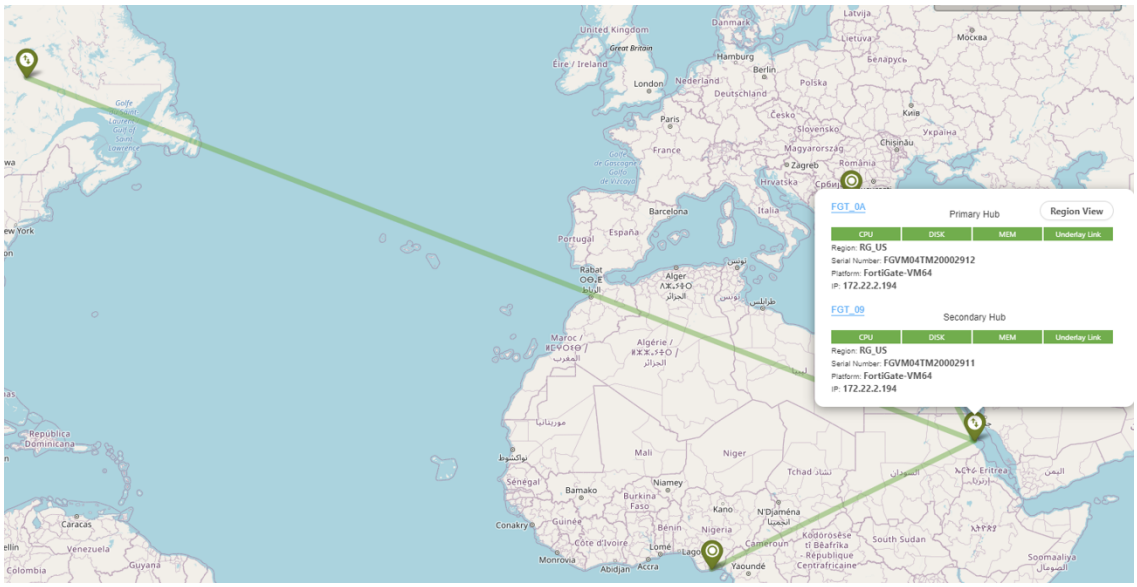
Viewing regions

You can view the details of each region in the SD-WAN network.

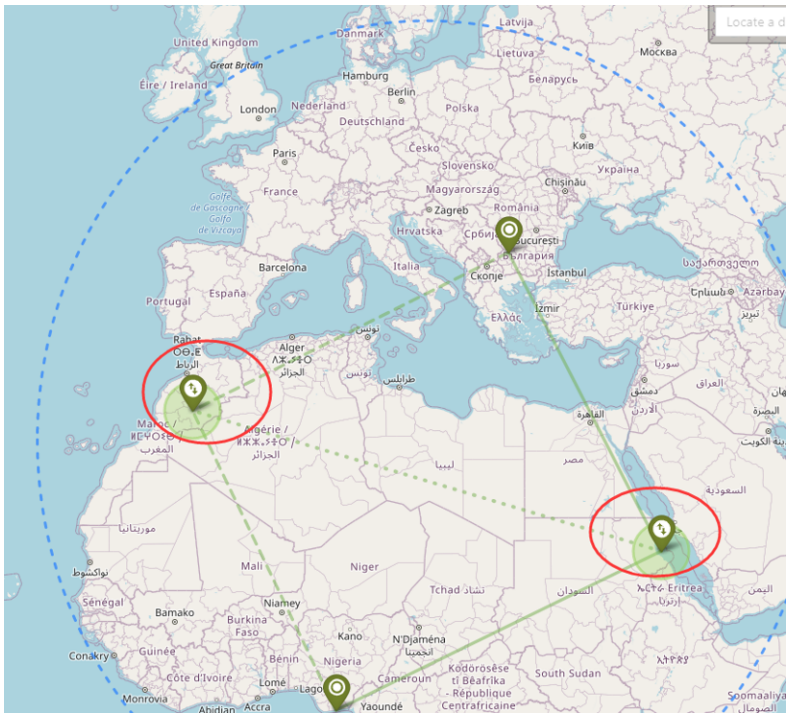
When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the map. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

To view regions:

1. Go to *Monitor* > *Dashboard*, and click *Hub View*.
2. Click a hub to view status information.
   Status information is displayed, and the dialog box includes a *Region View* button.



3. In the dialog box, click *Region View*.
   Details about the region are displayed. In the following example, the region includes both a primary hub and a secondary hub.



Traffic

You can view global traffic reports for all devices in the SD-WAN network by using the *Traffic* tree menu. You can also export traffic reports to PDF.

This section includes the following topics:

- Viewing global network traffic reports on page 21
- Exporting global traffic reports on page 22

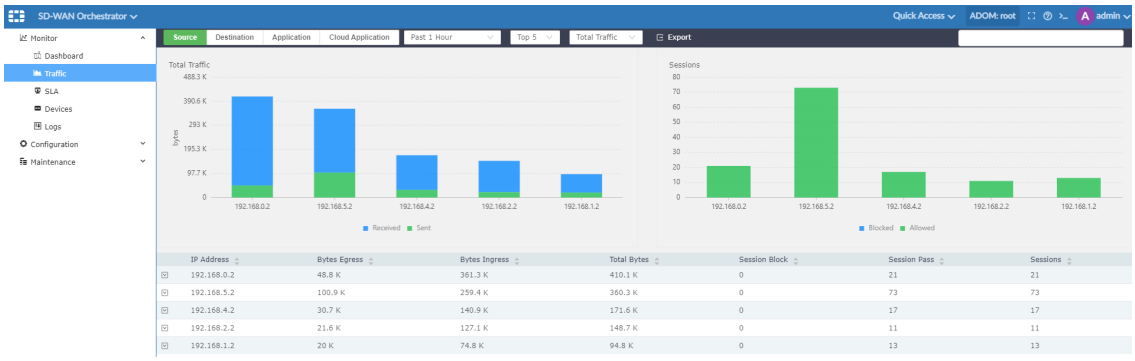
Viewing global network traffic reports

You can view several types of reports and filter data for all traffic in the network. You can also search global traffic for specific values.

After navigating and filtering the desired traffic statistics, you can export the report to PDF. See Exporting global traffic reports on page 22.

To view network traffic reports:

1. Go to *Monitor* > *Traffic*.
2. Click each of the following tabs to display information about the different types of traffic: *Source*, *Destination*, *Application*, *Cloud Application*.
   Each tab contains charts and tables.



Report	Description
Source	The statistics generated in the report are based on the source IP of the traffic. The report contains two statistical charts (*Total Traffic* and *Session*), and a statistical table. Click *Source* in the table to view drill-down information. You can filter the report by time frame, top sources, and total traffic.
Destination	The *Destination* pane reports the destination traffic information for all the devices deployed on the SD-WAN network. The pane contains two statistical charts (*Total Traffic* and *Sessions*), and a statistical table. Click a destination in the table to view drill-down information. You can filter the report by time frame and top destinations, and sort the report by total traffic or sessions.
Application	The statistics generated in the report are based on application traffic. The pane contains two statistical charts (*Total Traffic* and *Sessions*), and a statistical table. Click an application name in the table to view drill down information. You can filter the report by time frame and top sources, and sort the report by total traffic or sessions.
Cloud Application	The statistics generated in the report are based on application traffic. The report contains four statistical charts (*File size*, *File number*, *Sessions*, and *Videos Number*), as well as a statistical table. Click an application name in the table to view drill down information. You can filter the statistics by time frame and top applications, and sort the report by total traffic or sessions.

3. Hover over the charts to display additional details.
4. Expand the rows for each application to display additional details.
5. Click the predefined values in the toolbar to filter the charts based on time, priority, and all traffic or sessions.
6. Click the search box to select a filter, and type a value to search for.

Exporting global traffic reports

After you display the desired traffic details on the *Traffic* pane, you can export the traffic report to PDF.

To export traffic reports:

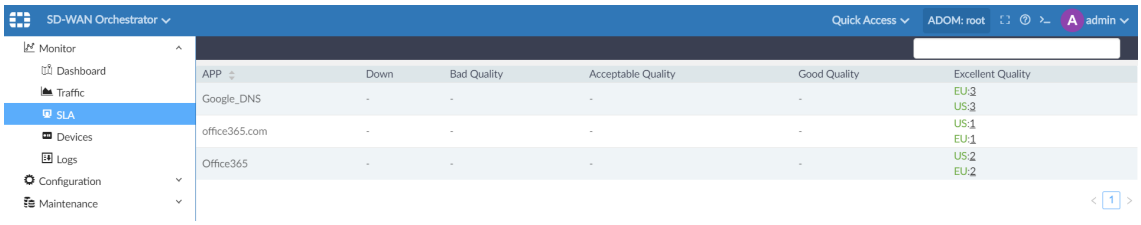
1. Go to *Monitor* > *Traffic*.
2. Display the desired traffic report. See Viewing global network traffic reports on page 21.
3. In the toolbar, click *Export*.
   A PDF of the traffic report is exported to your computer.

SLA

You can view information about service level agreements for all regions in the SD-WAN network by using the *SLA* tree menu.

To view SLA:

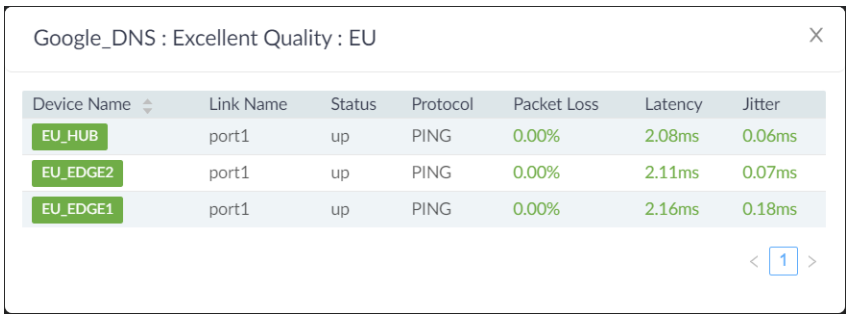
1. Go to *Monitor* > *SLA*.
   The quality rating for the devices in each region is displayed by application. The number of devices in each region is displayed as <region name>:<number of devices>, for example *EU:3*.



   The following table identifies the SLA criteria for each rating.

SLA quality rating	SLA criteria
Down	Down
Bad Quality	-
Acceptable Quality	Meets low criteria
Good Quality	Meets medium criteria
Excellent Quality	Meets high criteria

2. Click the <number of devices> to view details.
   A dialog box with information about *Link Name*, *Status*, *Protocol*, *Packet Loss*, *Latency*, and *Jitter* is displayed.



3. Click *X* to close the dialog box.

Devices

You can view information about each device in the SD-WAN network by using the *Devices* tree menu.

This section contains the following topics:

- Viewing device overviews on page 24
- Viewing device link reports on page 24
- Viewing device traffic reports on page 25
- Viewing device SLA on page 26

If you want to view information about all devices in the SD-WAN network, see Dashboard on page 16.

Viewing device overviews

You can use the *Devices* > *Overview* tab to monitor SD-WAN rules utilization, performance status, disk utilization, traffic, and more for each device in the SD-WAN network.

When a device is part of an HA cluster, information about the devices in the cluster is displayed.

To view device overviews:

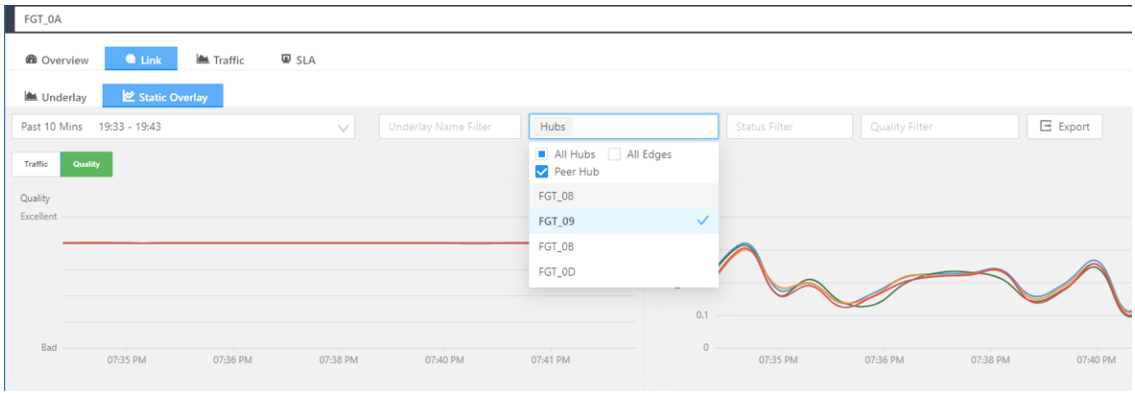
1. Go to *Monitor* > *Devices* > *Overview*.
   You can switch between devices by using the dropdown menu in the toolbar at the top of the page.
2. Hover over each chart to display additional detail.
3. You can also filter data in some charts by selecting a filter from the drop-down menu.

Viewing device link reports

The *Devices* > *Link* tab contains information about the underlay, static overlay, and shortcut overlay links.

To view device link reports:

1. Go to *Monitor* > *Devices* > *Link*.
   The *Static Overlay* tab displays for the selected device. You can also click the *Underlay* or *Shortcut Overlay* tabs.
   You can switch between devices by using the dropdown menu in the toolbar at the top of the page.



Report	
Static Overlay	The *Static Overlay* pane is the default view of the *Link* page and includes the views: • **Quality**: Contains reports of quality evaluation, jitter, latency, and packet loss in the device overlay links. • **Traffic**: Contains reports about the total inbound/outbound throughput and session.
Underlay	The Underlay pane includes the following views: • **Traffic**: Contains reports about the total inbound and outbound throughput, and session ramp-up of the SD-WAN underlay links. The table features information about the device's status, inbound/outbound bytes, and session of the underlay link.**Quality**: Contains reports about performance status, packet loss, jitter, and latency for the device overlay links.
Shortcut Overlay	Available when ADVPN is enabled on devices, and shortcut links are established. The charts monitor the total inbound and outbound throughput of the shortcut overly links. The table features information about peer devices, inbound/outbound bytes, and bandwidth.

2. Select the time frame to filter data by time.
   On the *Static Overlay* tab, you can also display data by traffic or quality.
3. Click the *Hubs* box to filter by *All Hubs*, *All Edges*, or *Peer Hubs*.
4. Click the *Export* button to export the report to PDF.

Viewing device traffic reports

The *Devices* > *Traffic* tab displays traffic reports for the selected device in the SD-WAN network.

For more information about traffic reports, see Viewing global network traffic reports on page 21.

To view device traffic reports:

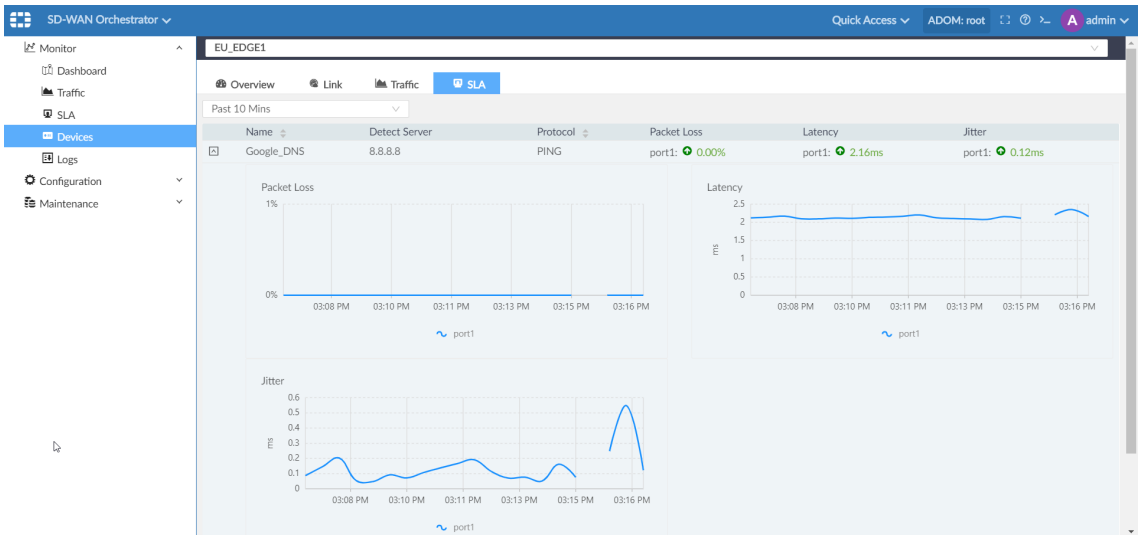
1. Go to *Monitor* > *Devices* > *Traffic*.
   The *Source* tab displays for the selected device. You can also click the *Destination*, *Application*, *Cloud Application*, and *Internet Service* tabs to display additional reports for the selected device.
   You can switch between devices by using the dropdown menu in the toolbar at the top of the page.
2. After you display the desired traffic details, you can export the report to PDF by clicking *Export*.
   A PDF of the traffic report is exported to your computer.

Viewing device SLA

The *Devices* > *SLA* tab displays information about service level agreements for the selected device in the SD-WAN network.

To view device SLA:

1. Go to *Monitor* > *Devices* > *SLA*.
   The *SLA* tab displays for the selected device.
   You can switch between devices by using the dropdown menu in the toolbar at the top of the page.
   You can select a different history range from the dropdown menu in the *SLA* content pane. The default is *Past 10 Mins*.



Logs

Some logs are visible only in the root ADOM, and the root ADOM must be version 6.4.

You can view event logs for SD-WAN Orchestrator MEA by using the *Logs* tree menu. The log displays the time, type, sub type, and message for events.

To view logs:

1. Go to *Monitor* > *Logs*.
2. Select a *Start* and *End* date to filter the logs.
3. (Optional) From the *Type* dropdown, select the log type to filter the results.
   You can select multiple log types. A checkmark displays beside the selected log types.
   Click the checkmark to remove a filter.
4. (Optional) From the *Device* dropdown, select a device.

Configuration

You can configure SD-WAN networks by using the *Configuration* tree menu. From the *Configuration* tree menu, you can access the following panes:

- Device on page 28
- Profile on page 41
- Shared resources on page 69
- Global routing on page 75

Device

You can add devices and regions to an SD-WAN network by using the *Device* tree menu. When you add a device to SD-WAN Orchestrator MEA, you assign a profile of configuration settings to it, and then install the configuration.

You can use several different methods to add devices to SD-WAN Orchestrator MEA.

It is recommended to configure profiles before you add devices to SD-WAN Orchestrator MEA. See Profile on page 41.

This section contains the following topics:

- Adding devices on page 29
- Adding devices in HA clusters on page 30
- Adding model devices on page 31
- Adding model devices in HA clusters on page 32
- Adding regions on page 34
- Adding unauthorized devices on page 35
- Installing configuration changes on page 35
- Importing devices on page 36
- Viewing configuration status on page 37
- Overriding device settings on page 37
- Adding static routes on page 38
- Updating regions on page 39
- Deleting regions on page 40
- Monitoring devices on page 40
- Replacing FortiGate serial numbers on page 40

Adding devices

When you add a device to SD-WAN Orchestrator MEA, you also define the configuration and control when to install the configuration to the device.

Before you use this method to add devices to SD-WAN Orchestrator MEA, you must add the devices to FortiManager.

After you add the device, you can change the settings by editing the assigned profile or by overriding settings for each device.

To add a device:

1. Ensure that you have created profiles for hub and edge devices. See Profile on page 41.
2. Go to *Configuration* > *Device*.
3. In the toolbar, click + *Device*.
   The *Device* dialog box opens.

4. On the *General* tab, configure the following settings:

Option	Description
Device Name	Enter the name of the device.
Host Name	Enter the host name.
Profile Name	Select a profile from the dropdown, or click *Create* to create a new profile.
First Online Action	Specify how to manage device configuration when the device comes online for the first time. Choose from: • *NONE*: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • *RETRIEVE_CONFIG*: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • *SYNC_CONFIG*: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Serial Number	Enter the device serial number.
Type	The model is displayed after you enter the device serial number.
Region	Select a region from the dropdown, or click *Create Region* to create a new region.
Password	The *Password* option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from: • No change: Keep the original password of the newly added device. • Manual: Specify the password of the device. • Auto: Generate a random password for the device automatically. Click the eye icon to view the password.

5. Click *OK*.

Adding devices in HA clusters

You can add managed FortiGates in a high availability (HA) cluster in active-passive (AP) mode to SD-WAN Orchestrator MEA.

Before you use this method to add an HA cluster to SD-WAN Orchestrator MEA, you must add the devices in the HA cluster to FortiManager.

Ensure that you have created profiles for devices in the HA cluster before you add the cluster to SD-WAN Orchestrator MEA. The profile defines the interface settings, and the *HA Monitor* and *Heartbeat Interface* settings in the profile should match the same settings in FortiManager.

After you add the cluster to SD-WAN Orchestrator MEA, you cannot change the cluster name or cluster members.

If the HA cluster is in a VM environment, ensure that you enable *Promiscuous mode* and *Mac address changes* in the vswitch.

To add devices in HA clusters:

1. Ensure you have created profiles for devices in HA clusters. See Creating profiles for HA devices on page 44.
2. Perform a factory reset on the FortiGates in the HA cluster.
3. Add the managed devices to SD-WAN Orchestrator MEA. See Adding devices on page 29.

Adding model devices

You can add an offline FortiGate device to SD-WAN Orchestrator MEA by using its serial number. This is called adding a model device.

When you add a model device to SD-WAN Orchestrator MEA, the model device is added to FortiManager too.

To add devices by serial number:

1. Ensure that you have created profiles for hub and edge devices. See Profile on page 41.
2. Go to *Configuration* > *Device*.
3. In the *Device* menu, select *+ Model Device*.
   The *+ Model Device* dialog box opens.

4. Configure the following settings:

Option	Description
Serial Number	Enter the serial number for the device.
Device Name	Enter a name for the device.
Host Name	Enter the host name.
Type	The model is displayed after you enter the device serial number.
Profile Name	Select a profile from the dropdown, or click *Create* to create a new profile.
Region	Select a region from the dropdown, or click *Create Region* to create a new region.
First Online Action	Specify how to manage device configuration when the device comes online for the first time. Choose from: • *NONE*: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • *RETRIEVE_CONFIG*: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • *SYNC_CONFIG*: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Enforce Firmware Version	(Optional) Select the required FortiOS version for the device when it comes online.
Password	The *Password* option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from: • No change: Keep the original password of the newly added device. • Manual: Specify the password of the device. • Auto: Generate a random password for the device automatically. Click the eye icon to view the password.
HA Mode	Select *STANDALONE* to disable HA mode. Select *AP* to enable active-passive HA mode.

5. Click *OK*.

Adding model devices in HA clusters

SD-WAN Orchestrator MEA supports active-passive (AP) HA mode, and the FortiGates in the cluster must be the same type of model.

You can add two or more offline FortiGate devices to a high availability (HA) cluster by using the device serial numbers. When you add model devices to SD-WAN Orchestrator MEA, the model devices are added to FortiManager too.

Interfaces for the HA cluster are defined in profiles, and you select a profile when you add model devices to SD-WAN Orchestrator MEA.

If you choose a profile without HA interface definitions, default ports are used.

To add model devices to HA clusters:

1. Ensure that you have created profiles for HA devices. See Creating profiles for HA devices on page 44.
2. Go to *Configuration* > *Device*.
3. In the *Device* menu, select + *Model Device*.
   The + *Model Device* dialog box opens.
4. Configure the following settings for the primary device and cluster:

Option	Description
Serial Number	Enter the serial number for the primary device in the HA cluster.
Device Name	Enter a name for the primary device.
Host Name	Not available when *HA Mode* is set to *AP*.
Type	The model is displayed after you enter the device serial number.
Profile Name	Select a profile for HA devices from the dropdown, or click *Create* to create a new profile.
Region	Select a region from the dropdown, or click *Create Region* to create a new region.
First Online Action	Specify how to manage device configuration when the device comes online for the first time. Choose from: • *NONE*: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • *RETRIEVE_CONFIG*: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • *SYNC_CONFIG*: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Enforce Firmware Version	(Optional) Select the required FortiOS version for the device when it comes online.
Password	The *Password* option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from: • No change: Keep the original password of the newly added device. • Manual: Specify the password of the device. • Auto: Generate a random password for the device automatically. Click the eye icon to view the password.
HA Mode	Select *STANDALONE* to disable HA mode.

Option	Description
	Select *AP* to enable active-passive HA mode.
Cluster Name	Available when *HA Mode* is set to *AP*. Type a name for the HA cluster. Minimum length is 1 character, and maximum length is 21 characters. The *#,(,)* characters are not supported.
HA Password	(Optional) Available when *HA Mode* is set to *AP*. Specify a password for the HA cluster. Maximum length is 128 characters.
Priority	Type a high number between 0-255 to set the priority for the primary HA member.
HA Secondaries	Available when *HA Mode* is set to *AP*. Click *Add* to add a secondary model device to the HA cluster by serial number. In the *SerialNumber #1* box, type the serial number for the FortiGate device in the HA cluster. It should be the same type of serial number as the primary FortiGate in the HA cluster. In the *Priority* box, type the priority restriction for the device in the HA cluster. Type a number between 0 and 255.

5. Under *HA Secondaries*, add one or more secondary devices.
   a. Click *+Add*.
      A row of options for the first secondary device is displayed.
   b. In the *SerialNumber #1* box, type the serial number for a secondary device in the HA cluster.
   c. In the *Priority* box, type a number between 0-255 that is lower than the priority for the primary device.
      Configuration of the secondary device is complete.
   d. (Optional) *Click +Add* to add and configure another secondary device.
6. Click *OK*.

Adding regions

A region refers to a cluster of devices in one geographical location. Each region has one primary hub device that is connected to one or more edge devices. You can also configure an optional secondary hub device in the region for redundancy.

When you create a region, you select the devices, assign the profiles of configuration settings, and install configurations to all devices in the region.

To create a region:

1. Ensure that you have created profiles for hub and edge devices. See Profile on page 41.
2. Go to *Configuration* > *Device*.
3. In the toolbar, click + *Region*.
4. In the *Name* field, type a name for the region.
5. In the *Hub* table, select a device from the list.
6. In the *Edges* table, select one or more devices to connect to the hub.
7. (Optional) In the *Description* field, enter a description of the region.

8. Click *OK*.
   It may take a while to complete the configuration.

Adding unauthorized devices

When unauthorized devices have been added to FortiManager, you can add them to SD-WAN Orchestrator MEA. Unauthorized devices are devices that have been added to *Device Manager* in FortiManager, but not yet authorized for management by FortiManager.

The + *Add Unauthorized Device* option is hidden in SD-WAN Orchestrator MEA when no unauthorized devices are available in FortiManager.

To add unauthorized devices:

1. Go to *Configuration* > *Device*.
2. In the toolbar, click + *Unauthorized Device*.
   The *Add Unauthorized Devices* dialog box opens.
3. Configure the following settings:

Option	Description
ADOM	Select the ADOM that contains the unauthorized device.
Unauthorized	Click the box, and select the device.

4. Click *OK*.

Installing configuration changes

You can install configuration changes to all regions, to all devices in each region, or to individual devices.

A FortiGate managed by SD-WAN Orchestrator MEA must have a corresponding SD-WAN Orchestrator MEA license. Otherwise installation will fail with a warning message.

To install configuration changes:

1. Go to *Configuration* > *Device*.
2. Perform one of the following actions:

Goal	Method
Install all configuration updates for all regions and devices.	In the toolbar, click *Install all configuration*.
Install all configuration changes	For a region name, click the *Install Region Configuration* button.

Goal	Method
for all devices in a region.	
Install configuration changes to a device.	For a device, click the *Install Configuration* button.

Importing devices

You can import one or more devices to SD-WAN Orchestrator MEA by downloading a template in CSV format, adding devices to the CSV file, and then uploading the CSV file to SD-WAN Orchestrator MEA.

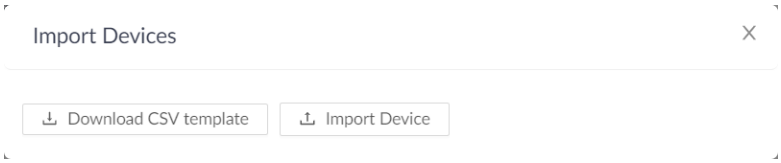
The CSV file uses the following fields:

Region Name	If regions are used, specify the name of the region defined in SD-WAN Orchestrator MEA.
Serial Number	Specify the serial number for the FortiGate.
Device Name	Specify the FortiGate model, such as FortiGate-100E.
Profile Name	Specify the name of the SD-WAN Orchestrator MEA profile to assign to the device.
Sync First Time Online	Specify how to manage device configuration when the device comes online for the first time. Choose from: • *NONE*: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • *RETRIEVE_CONFIG*: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • *SYNC_CONFIG*: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Host Name	Specify the host name for the FortiGate.

Each row in the CSV file identifies one device. Add a row of fields to the CSV file for each device that you want to import.

To import a device:

1. Ensure that you have created profiles for hub and edge devices. See Profile on page 41.
2. Go to *Configuration* > *Device*.
3. In the *Device* menu, select *Import Devices*.
   The *Import Devices* dialog box opens.



4. Click *Download CSV template*.
   A `TEMPLATES_IMPORT_DEVICES.csv` file is downloaded to your computer. The template contains details about devices already added to SD-WAN Orchestrator MEA.
5. Open the CSV file in Microsoft Excel, add a new row for each additional device you want to import, and save the file.
6. Click *Import Device*, select the `.csv` file, and click *Open*.

Viewing configuration status

You can view the SD-WAN configuration status for each region and each device in the SD-WAN network.

When a configuration is synchronizing, status information also displays in the SD-WAN Orchestrator MEA banner.

To view configuration status:

1. Go to *Configuration* > *Device*.
   The list of regions is displayed as well as the synchronization status.
2. Expand each region to view the devices in each region.
   The *Config Status* column displays the status for each device.

Overriding device settings

When you add a device to SD-WAN Orchestrator MEA, you assign a profile to the device. After the device is added to SD-WAN Orchestrator MEA, you can override profile settings for each device.

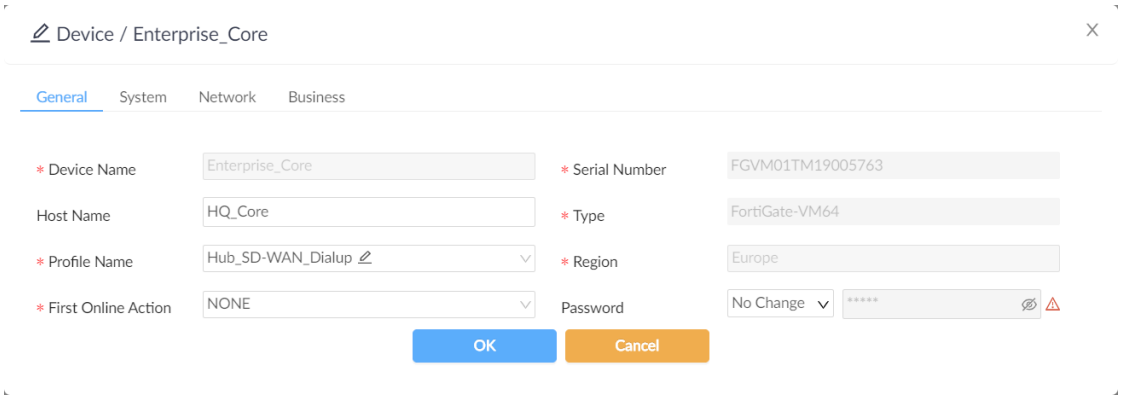
This topic describes how to override the NTP setting. You can also override network settings.

Any changes you make apply only to the device.

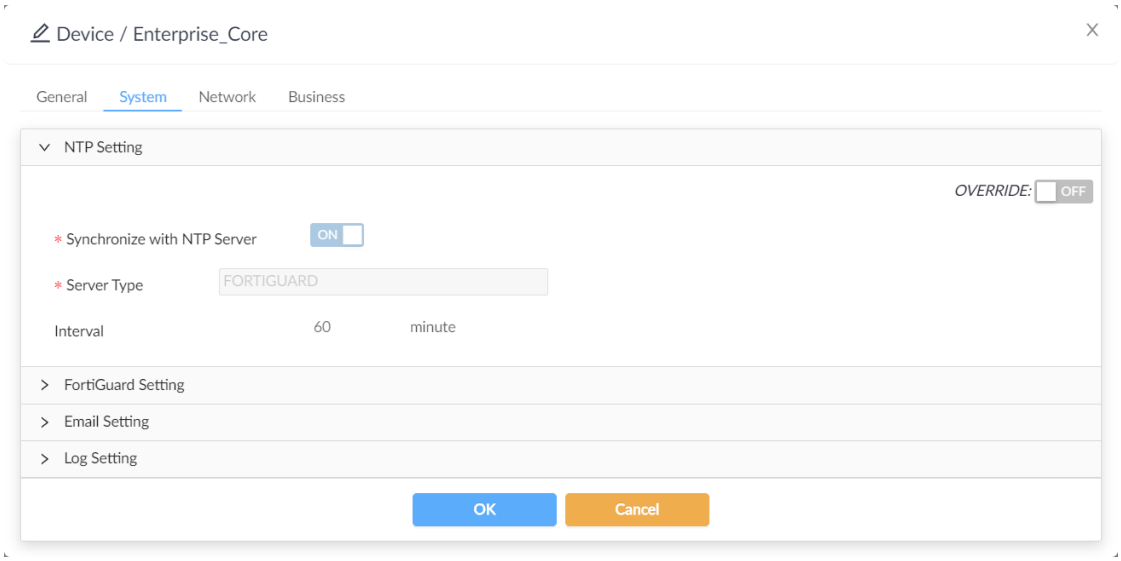
See also Adding static routes on page 38 and Creating business rules on page 60.

To override device settings:

1. Go to *Configuration* > *Device*.
2. Expand the region.
   The devices in the region are displayed.
3. Double-click the device to open it for editing.
   The *Device / <name>* dialog box is displayed.



4. Click the *System* tab.
   The *System* settings are displayed.



5. Expand the setting that you want to override, such as *NTP Setting*, and toggle on the *Override* button.
   A confirmation dialog box displays.
6. Click *OK* to confirm the desire to enable an override, and select the settings you want to override.
7. Click *OK* to save the changes.
8. Install the configuration changes. See Installing configuration changes on page 35.

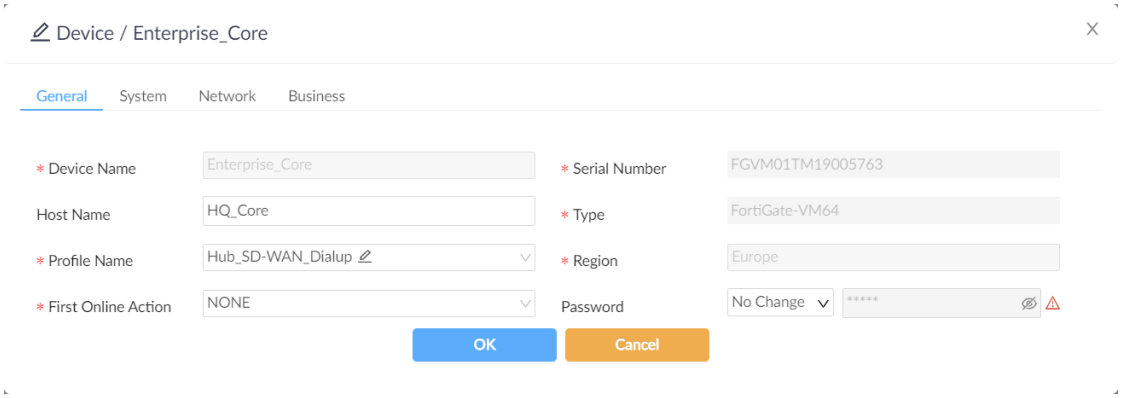
Adding static routes

After the device is added to SD-WAN Orchestrator MEA, you can override profile settings for each device. For example, you can add a static route. The static route applies only to the device.

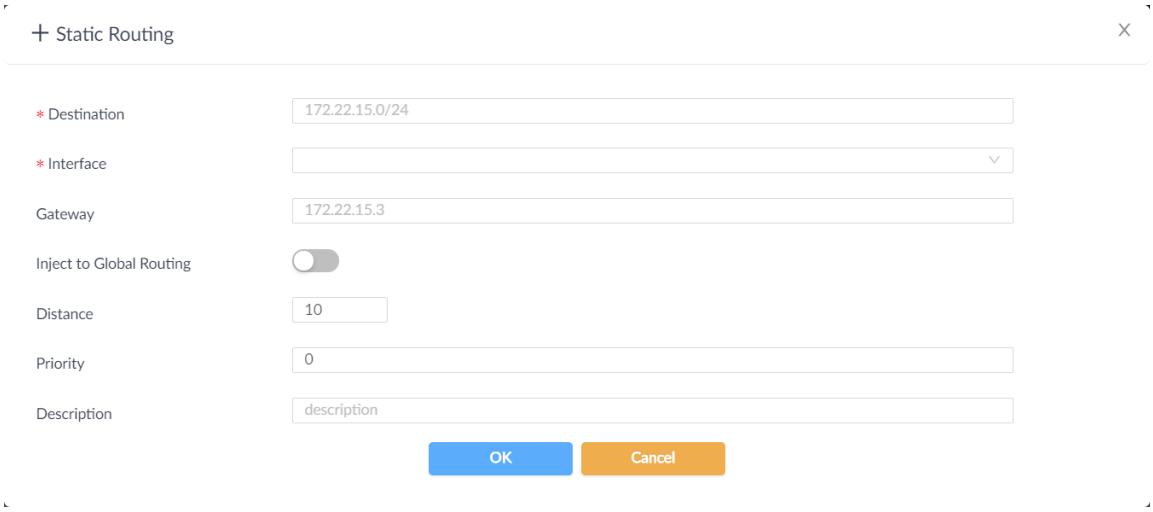
To add static routes:

1. Go to *Configuration* > *Device*.
2. Expand the region.
   The devices in the region are displayed.

3. Double-click the device to open it for editing.
   The *Device / <name>* dialog box is displayed.



4. Click the *Network* tab, and expand the *Static Routing* section.
5. Click *Create New*.
   A + *Static Routing* dialog box displays.



6. Configure the options, and click *OK*.
   The static route is created.
7. Click *OK* to save the changes.
8. Install the configuration changes. See Installing configuration changes on page 35.

Updating regions

After you create regions, you can delete devices from the region, change profile assignments, and specify whether to synchronize profile settings when the device comes online for the first time.

To update a region:

1. Go to *Configuration* > *Device*.
2. Beside the region name, click the *Update* button.
3. Select a device, and click *Delete* to remove the device from the region.

4. Select a device, and click *Assign Profile* to change the profile.
5. Select a device, and click *Sync First Time Online* to change the setting.
6. Click *OK*.
   The configuration changes are saved to the region.
7. Install the configuration changes. See Installing configuration changes on page 35.

Deleting regions

You can delete a region and all its devices from SD-WAN Orchestrator MEA.

To delete a region:

1. Go to *Configuration* > *Device*.
2. Beside the region name, click *Delete*.

Monitoring devices

You can access the device monitoring panes from the *Device* tree.

To monitor a device:

1. Go to *Configuration* > *Device*.
2. Expand the region to view details about each device.
   When the device is part of an HA cluster, an HA icon displays in the *Status* column. You can hover over the icon to view details about the HA cluster.
3. Click the *monitor* button beside the device you want to monitor.
   The *Devices* > *Overview* tab is displayed. For more information, see Viewing device overviews on page 24.

Replacing FortiGate serial numbers

You can use this procedure to replace one FortiGate with another FortiGate by updating the serial number in SD-WAN Orchestrator MEA.

It is recommended to use the same WAN IP for the new and old FortiGates, regardless of whether a static IP or DHCP is used.

To replace FortiGate serial numbers:

1. In SD-WAN Orchestrator MEA, go to *Configuration* > *Device*, and ensure that the *Config Status* for the device is *Synched*.
2. Turn off the FortiGate device that you want to replace.
3. Edit the serial number in SD-WAN Orchestrator MEA
   a. Go to *Configuration* > *Device*, and double-click the device to open it for editing.
   b. Beside the *Serial Number* box, click the *Pencil* icon.
      The *Serial Number* box becomes editable.
   c. In the *Serial Number* box, type the new serial number, and click *Confirm*.

   d. Click *OK*.
      The serial number is updated.
4. In FortiManager, download a configuration revision for the FortiGate device you are replacing.
   a. Go to *Device Manager* > *Device & Groups*, and select the device in the lower tree menu.
      The *System: Dashboard* is displayed in the content pane.
   b. In the *Configuration and Installation* widget, click the *Revision History* button.
      The *Configuration Revision History* dialog box is displayed.
   c. Select the revision, and select *Download Revision* from the *More* menu.
   d. Select the *Regular Download*, and click *OK*.
      The configuration is downloaded to your computer.
5. Open the downloaded configuration file in a text editor, and remove the FortiManager IP address from the `central-management` configuration section.
   The change ensures that the new FortiGate device isn't registered as a new device.
6. Turn on the new FortiGate.
7. Go to FortiOS, and restore the configuration.
8. Go to FortiManager, and replace the serial number by using the following CLI.

```
#diag dvm device list
#exec device replace sn <device name> <serial number>
```

<serial number> is case-sensitive. Letters used in Fortinet product serial numbers are capitalized.

Profile

You can create and edit profiles by using the *Profile* tree menu. Profiles are templates that define general, system, network, and business policies for devices in SD-WAN networks. You can create one profile and assign it to multiple devices.

This section contains the following topics:

- Creating profiles for hub devices on page 42
- Creating profiles for edge devices on page 43
- Creating profiles for HA devices on page 44
- Creating new WAN settings on page 45
- Creating new LAN settings on page 47
- Attaching a FortiSwitch model to FortiGate on page 49
- Adding a FortiAP model device on page 54
- Creating new DMZ settings on page 59
- Creating business rules on page 60
- Cloning profiles on page 60
- Updating profiles on page 61
- Deleting profiles on page 62
- Profile options described on page 62

Creating profiles for hub devices

Before you create a profile, you should create all of the needed shared resources, so you can select them in the profile. See Shared resources on page 69.

Each region can have one primary hub and one secondary hub. The secondary hub is for redundancy and is optional.

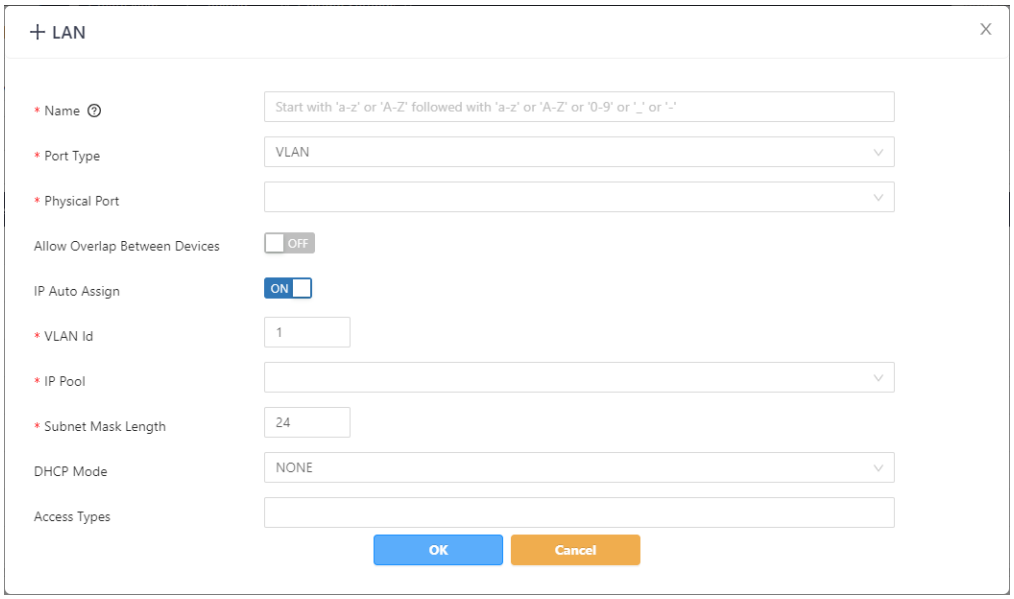
You should create a profile for each device type in the SD-WAN network. If plan to use primary and secondary hubs, should create a profile for primary hubs and a profile for secondary hubs.

To create profiles for hub devices:

1. Go to *Configuration* > *Profile*.
2. In the toolbar, click *+Create New*.
3. Configure the profile settings.

Option	Description
Name	Enter the profile name.
Platform	Select the platform that matches the device you intend to add.
Device Role	Select *PRIMARY_HUB* to create a profile for primary hubs. Select *SECONDARY_HUB* to create a profile for secondary hubs.
VPN Mode with Edge	Select one of the following options to connect the hub device with edge devices: • Select *SITE_TO_SITE* to create full-mesh overlay links between the hub device and its edge devices in the same region. • Select *DIAL_UP* to create one-to-one overlay links between the hub device and its edge devices. When you select *DIAL_UP*, you can enable ADVPN on the *Network* tab in the *WAN* settings.
Max Edge Count	Available when *VPN Mode with Edge* is set to *DIAL_UP*. Specify the maximum number of edge devices allowed to connect with the hub device.
Port Number	Specify the number of ports on the FortiGate. The number of ports in the FGT VM should be the same number as defined here. Otherwise conflict will occur.
Comments	(Optional) Type a comment about the profile.

4. Click *OK*. The profile is created, and the *System* tab opens.
5. Configure the *System* settings.
   For a description of the options on the *System* tab, see Profile options described on page 62.
6. Click the *Network* tab to configure the network settings.
   If you're using primary and secondary hubs in a region, you can optionally configure LAN port communication between the hubs. The LAN port communication is used in addition to the default full-mesh overlay link communication between the hubs.
   a. On the *Network* tab, expand the *LAN* section.
   b. Either click *Create New*, or double-click an interface to open it for updating.
      The LAN options are displayed.



c. Toggle *Connect to Peer Hub* to *ON*.
You must enable this option in the profile for the primary hub and the profile for the secondary hub.

d. For primary hub devices, toggle *Allow Overlap Between Devices* to *ON*.
In the *IP Address* box, type the IP address for the primary hub, and in the *Peer Hub's IP Address* box, type the IP address for the secondary hub.
This option is not available for secondary hubs.

e. Set the remaining options as desired, and click *OK* to save the WAN configuration.
For a description of the options on the *Network* tab, see Profile options described on page 62.

7. Click the *Business* tab to create business rules.
For a description of the options on the *Business* tab, see Profile options described on page 62.

8. Click *OK*.

Creating profiles for edge devices

Before you create a profile, you should create all of the needed shared resources, so you can select them in the profile. See Shared resources on page 69.

To create profiles:

1. Go to *Configuration* > *Profile*.
2. In the toolbar, click *+Create New*.
3. Configure the profile settings.

Option	Description
Name	Type a name for the profile.
Platform	Select the platform that matches the device you intend to add.
Device Role	Select *Edge* to designate the device as an edge.

Option	Description
VPN Mode with Hub	Select one of the following options to connect the edge devices to the hub in the region: • Select *SITE_TO_SITE* to create full-mesh overlay links between the hub device and its edge devices in the same region. • Select *DIAL_UP* to create one-to-one overlay links between the hub device and its edge devices. When you select *DIAL_UP*, you can enable ADVPN on the *Network* tab in the *WAN* settings.
Port Number	Specify the number of ports on the FortiGate. The number of ports in the FGT VM should be the same number as defined here. Otherwise conflict will occur.
Comments	(Optional) Type a comment about the profile.

4. Click *OK*.
   The profile is created, and the *System* tab opens.
5. Configure the *System* settings.
   For a description of the options on the *System*, *Network*, and *Business* tabs, see Profile options described on page 62.
6. Click the *Network* tab to configure the network settings.
7. Click the *Business* tab to create business rules.
8. Click *OK*.

Creating profiles for HA devices

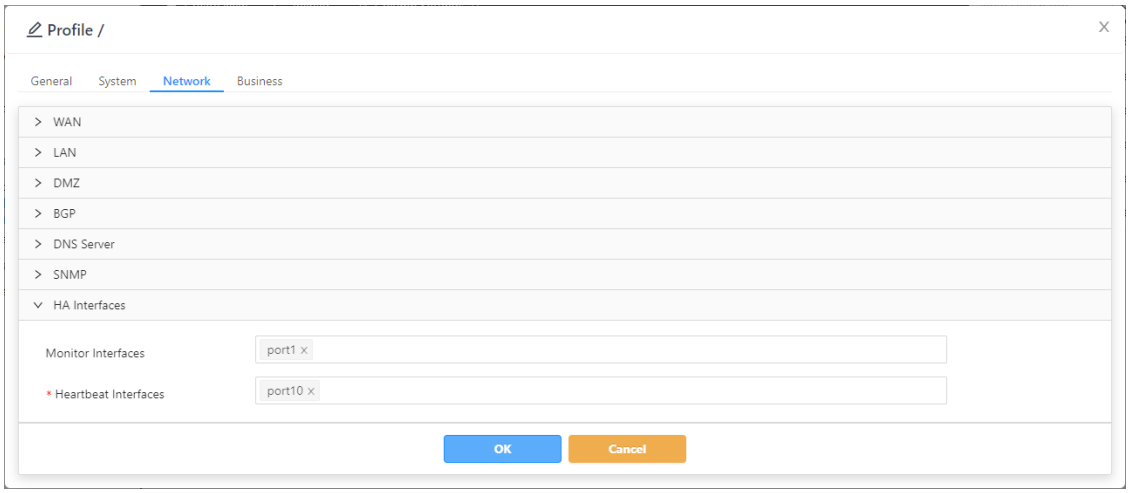
Before you create a profile, you should create all of the needed shared resources, so you can select them in the profile. See Shared resources on page 69.

Among other settings, use the profile to define high availability (HA) interfaces for devices. Once a profile refers to one or more devices, you cannot change HA interfaces in the profile.

To create profiles for HA devices:

1. Go to *Configuration* > *Profile*.
2. In the toolbar, click *+Create New*.
   The settings on the *General* tab are displayed.
3. Complete the settings on the *General* tab, and click *OK*.
   The profile is created, and the *System* tab opens.
4. Click the *Network* tab.
   The *Network* settings are displayed.
5. Configure options as needed.

6. Expand the *HA Interfaces* section at the bottom, and set the options.



   For a description of the options on the *Network* tab, see HA Interfaces on page 67.
7. Configure the options on the *System* and *Business* tabs as desired.
   For a description of the options on the *System* and *Business* tabs, see Profile options described on page 62.
8. Click *OK*.

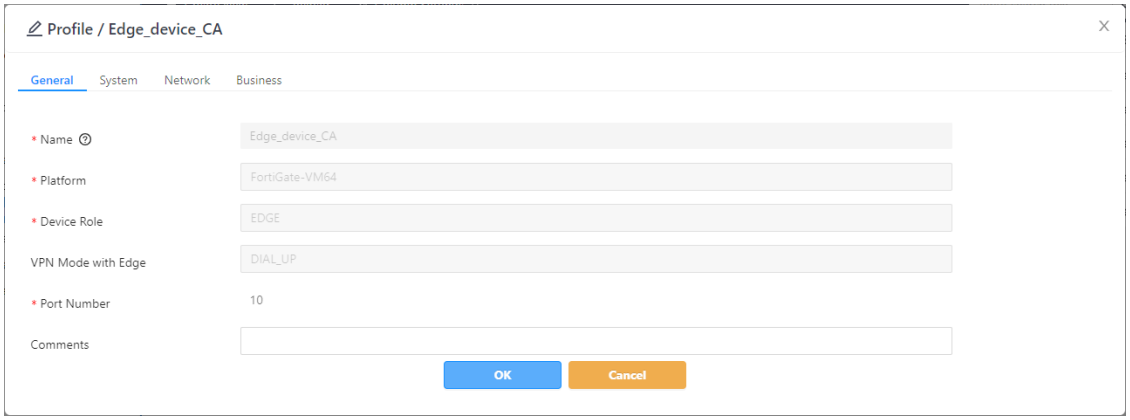
Creating new WAN settings

When creating a profile, you can also create new WAN settings.

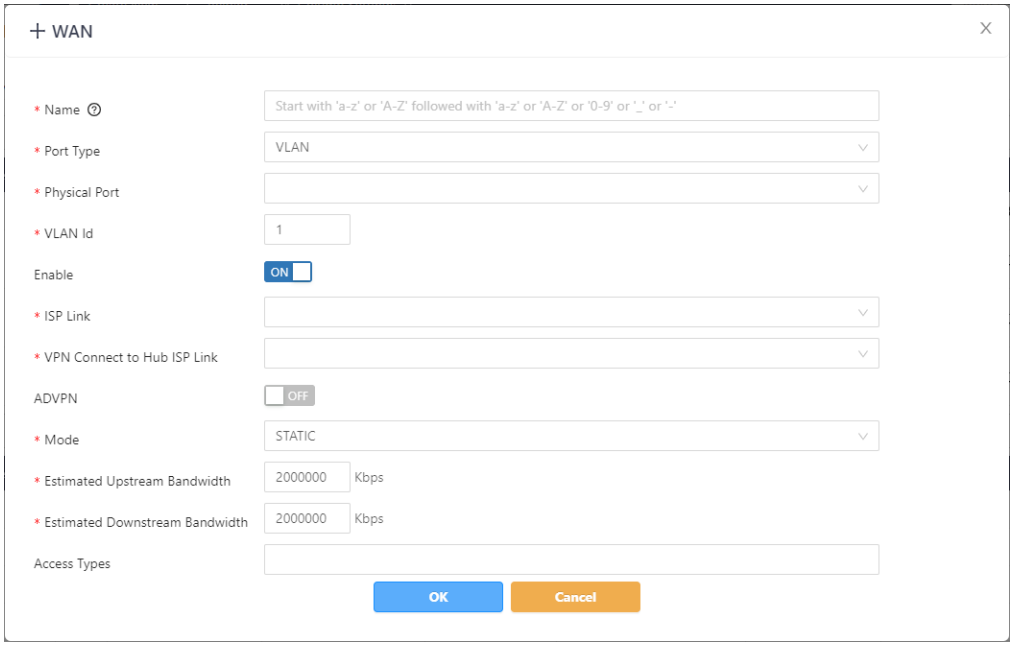
FortiGate 40F-3G4G model supports a special WAN interface for Wireless Wide Area Networks (WWAN). When you insert a 3G or 4G SIM card into the WWAN interface slot of the device, you can connect to the Internet by using telecommunication operators. If you add this type of FortiGate with WWAN enabled to SD-WAN Orchestrator MEA, a WWAN port is available for configuration.

To create new WAN settings:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
   The *Profile <name>* dialog box is displayed.



3. Click the *Network* tab.
   The *Network* pane is displayed. For a description of the options, see Network tab on page 65.
4. Expand the *WAN* section, and click *+Create New*.
   The WAN dialog box is displayed.



5. In the *Name* box, type a name for the WAN settings.
6. In the *Port Type* box, select the port, and complete the options.
   Choose between *VLAN* and *Aggregate*.
7. Complete the remaining options, and click *OK*.

Option	Description
Physical Port	Available when *Port Type* set to *VLAN*. Select the port number. Displays *wwan* for FortiGate 40F-3G4G models with enabled WWAN ports.
VLAN ID	Available when *Port Type* is set to *VLAN*. Type an ID for the VLAN.
Enable	Toggle on to enable the interface. Toggle off to disable the interface.
ISP Link	Available for edge devices when *VPN Mode with Hub* is set to *SITE_TO_SITE* on the *General* tab.
VPN Connect to Hub ISP Link	Available for edge devices when *VPN Mode with Hub* is set to *SITE_TO_SITE* on the *General* tab. When configuring WWAN interfaces, select an LTE type of ISP link, such as *DEFAULT_ISP_LTE_1*. Any other setting will disable the wwan feature.
ADVPN	Available for edge devices when *VPN Mode with Hub* is set to *DIAL_UP* on the *General* tab. On hub devices, select one of the following options:

Option	Description
	• *NONE* - ADVPN is disabled. Edge devices from the same region will communicate with each other by forwarding packets through their region's hub. • *INSIDE_REGION* - Shortcut tunnels are triggered by traffic and established only inside a region. On edge devices, toggle *ADVPN* on to enable ADVPN. Toggle off to disable ADVPN.
Mode	Select a mode.
Use VIP for VPN Connection	Toggle on to enable VIP mapping for the WAN port. This feature allows overlay tunnels to be established when FortiGate devices are deployed on Cloud platforms, such as AWS, Azure, and on. It also helps establish overlay links between devices when both devices are behind a NAT gateway.
VIP Address	Available when *Use VIP for VPN Connection* is on. Type the VIP address for the device. When enabled, tunnels are established with the VIP address instead of the intranet IP address. If the FortiGate is deployed on a Cloud platform, contact the Cloud operator to obtain the public IP address .
Estimated Upstream Bandwidth	Leave the default value, or specify an estimated value.
Estimated Downstream Bandwidth	Leave the default value, or specify an estimated value.
Access Types	Select one or more types of access.

The WAN settings are created.

8. If you set *Port Type* to *Aggregate*, open the WAN settings for editing, select interface members, and click *OK*. Interface members are added to the WAN settings.

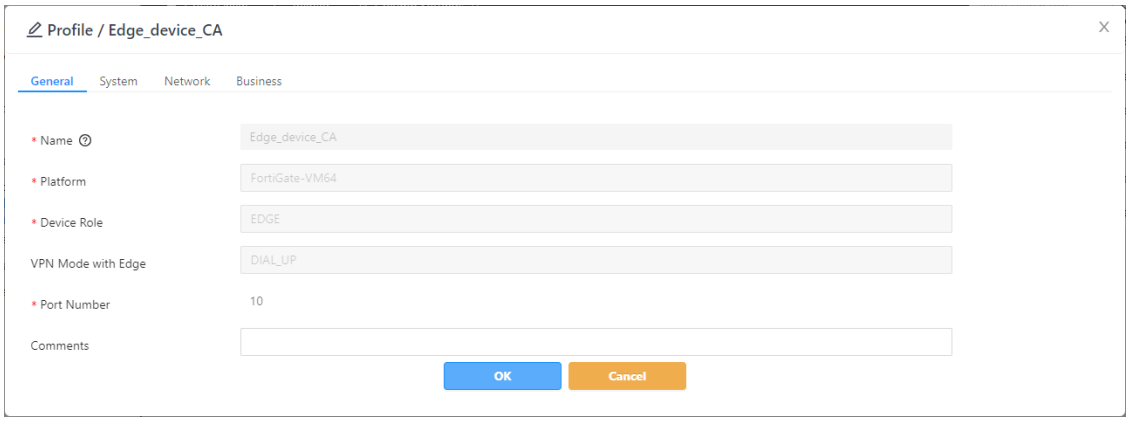
Creating new LAN settings

When creating a profile, you can also create new LAN settings.

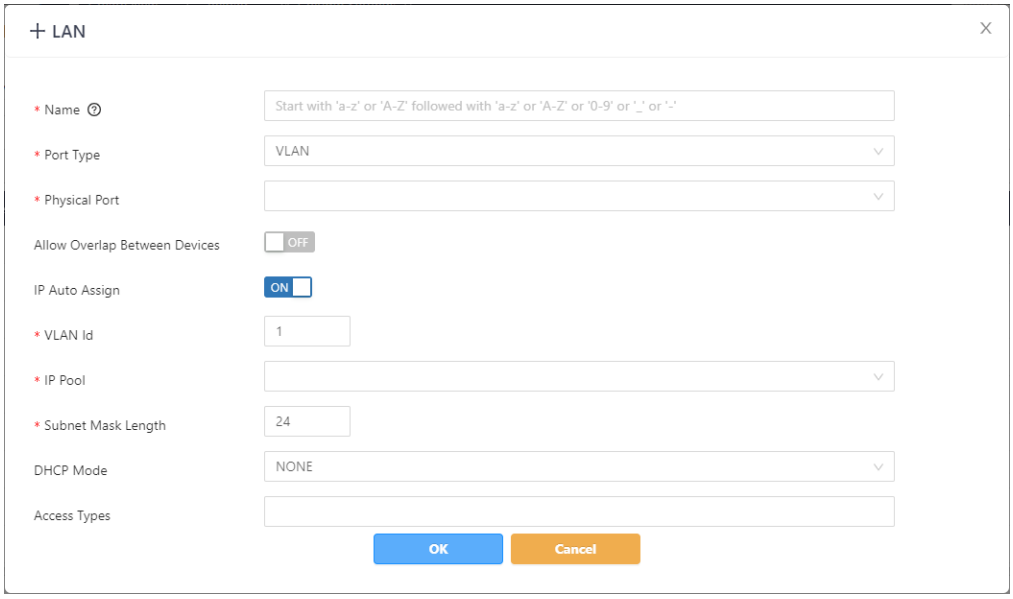
When creating profiles for primary hubs and secondary hubs in a region, you can optionally configure LAN ports for each hub to define communication between them by using the *Connect to Peer Hub* option. When LAN ports are configured for both hubs in a region, they are connected by site-to-site VPN and LAN, and the LAN port has higher priority than the VPN tunnels in business rules.

To create new LAN settings:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
   The *Profile* <*name*> dialog box is displayed.



3. Click the *Network* tab.
   The *Network* pane is displayed. For a description of the options, see Network tab on page 65.
4. Expand the *LAN* section, and click *+Create New*.
   The *LAN* dialog box is displayed.



5. In the *Name* box, type a name for the LAN settings.
6. In the *Port Type* box, select the port, and complete the options.
   Choose between *VLAN*, *WiFi_SSID*, and *Aggregate*.
7. Complete the remaining options, and click *OK*.

Option	Description
Connect to Peer Hub	Available when configuring profiles for primary or secondary hubs. Toggle on to configure LAN communication between a primary hub and a secondary hub in a region. You must enable this option in the profile for the primary hub and the profile for the secondary hub to enable communication for the interface.
Allow Overlap Between Devices	For edge devices, toggle on to allow overlap between devices. Toggle off to disable this feature.

Option	Description
	For primary hub devices, toggle on to configure the local address and peer hub address for the LAN port to communicate between the primary and secondary hubs. For secondary hubs, this feature is disabled and cannot be enabled.
IP Address	Available when *Allow Overlap Between Devices* is enabled.
Peer Hub's IP Address	Available when *Allow Overlap Between Devices* is enabled.
IP Auto Assign	Available when *Allow Overlap Between Devices* is disabled. Toggle on to automatically assign IP addresses. Toggle off to disable this feature.
IP Pool	Available when *IP Auto Assign* is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator MEA to automatically assign.
Subnet Mask Length	Available when *IP Auto Assign* is enabled. Specify the length of the subnet mask.
DHCP Mode	Choose from: • None • Server • Relay
Access Types	Select the types of access to allow on the interface.

The LAN settings are saved.

8. If you set *Port Type* to *AGGREGATE*, open the LAN settings for editing, select interface members, and click *OK*. Interface members are added to the LAN settings.

Attaching a FortiSwitch model to FortiGate

When creating a profile, you can attach a model switch to a port on a FortiGate. This is called attaching FortiLink. When the switch comes online, it is managed by FortiGate and receives the configuration.

Do not connect FortiSwitch to the physical FortiGate port until the FortiSwitch profile is installed. See Install a profile on a device.

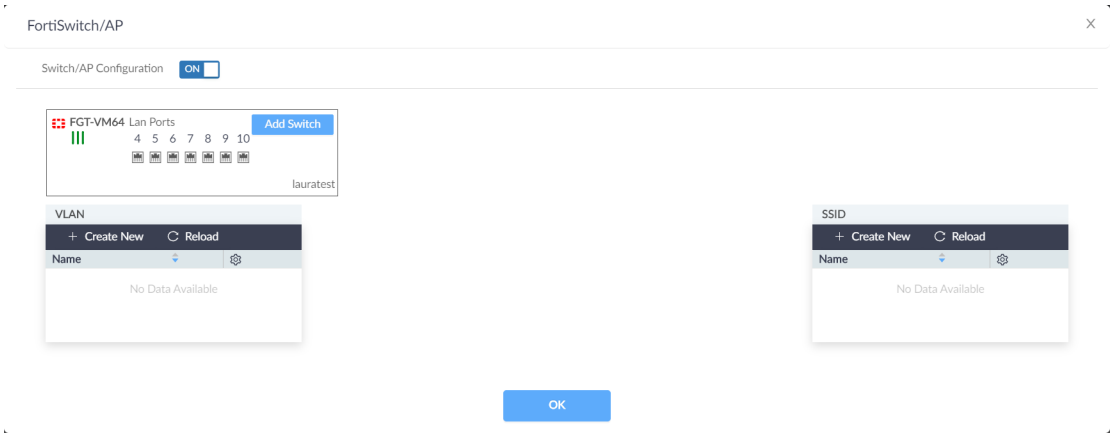
If FortiSwitch is already connected to FortiGate:

Configure and install the profile without FortiLink and FortiSwitch first. After the profile has successfully synchronized with FortiGate, add the FortiLink and FortSwitch configuration, and then install the profile again.

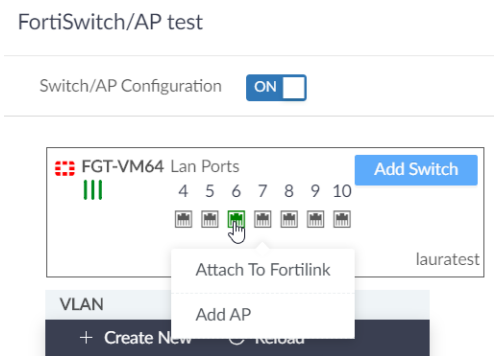
To attach a FortiGate port to a FortiSwitch:

1. Go to *Configuration* > *Profile*.
The list of profiles is displayed.

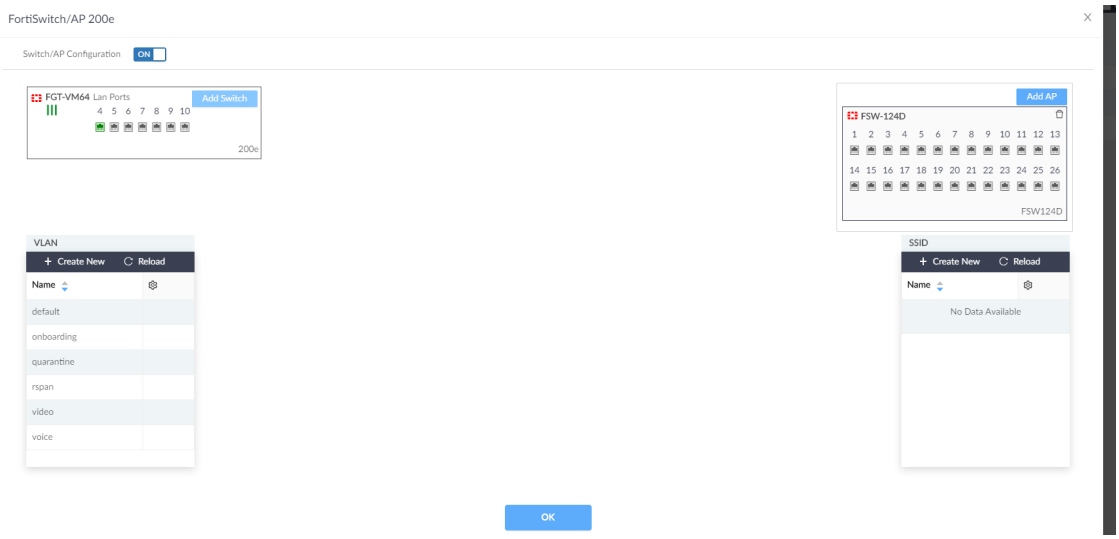
2. Create a new profile, or open a profile for updating.
   The *Profile / <Name>* dialog box is displayed.
3. Display the Switch/AP settings.
   a. Click the *Network* tab.
      The *Network* pane is displayed. For a description of the options, see Network tab on page 65.
   b. Expand the *LAN* section, and click *Switch/AP*.
      The *FortiSwitch/AP<Name>* dialog box is displayed.



4. Select the FortiGate port you want to connect to FortiSwitch, and click *Attach to FortiLink*.



   The port is attached, and the VLAN settings are created.
5. Add a platform model.
   a. Click *Add Switch*.
   b. In the *Name* field, enter a name for the FortiSwitch.
   c. From the *Platform* dropdown, select a FortiSwitch model.
   d. Click *OK*.
      The switch is added to the profile.

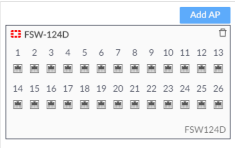


To assign a VLAN to ports in a switch template:

1. In the *VLAN* table, create a new VLAN or open a VLAN for updating.
   The *VLAN / <Name>* dialog box is displayed.
2. Configure the VLAN settings, and click *OK*.

Option	Description
Name	Type a name for the interface.
Allow Overlap Between Devices	Toggle on to allow overlap between devices. Toggle off to disable this feature.
VLAN Id	Enter a unique VLAN ID.
IP Auto Assign	Available when *Allow Overlap Between Devices* is disabled. Toggle on to automatically assign IP addresses. Toggle off to disable this feature.
IP Pool	Available when *IP Auto Assign* is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator to automatically assign.
Subnet Mask Length	Available when *IP Auto Assign* is enabled.
DHCP Mode	Choose from: • *None* • *Server* • *Relay*
Access Types	Select the types of access to allow on the interface.

3. Assign the VLAN to a switch template.
   a. Select a FortiSwitch port.

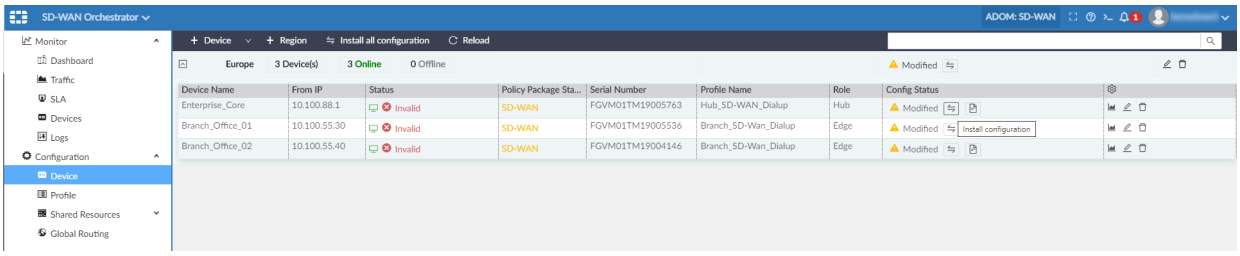


   The *More Configuration/ <port>* dialog box is displayed.
   b. Configure the port settings and click *OK*.

Option	Description
Native Vlan	Select the native VLAN from the available VLAN objects
Allowed Vlans	Select the allowed VLAN from the available VLAN objects.
Allowed Vlans-all	Select the allowed VLAN from the available VLAN objects.
Description	Enter a description of the VLAN.
DHCP Snooping	Choose TRUSTED or UNTRUSTED.
LIdp Profile	Choose *default* or *default-auto-isl*.
Loop Guard	Toggle on to enable Loop Guard for the port. Loop Guard cannot be applied to ports that are in trunks.
Port Security-policy	Select a port security policy from the dropdown.
Stp State	Toggle on to enable this feature.
stp Root-gaurd	Toggle on to enable STP Root Guard for the port.
Edge Port	Right-click to enable or disable Edge Port for the port.
stp bpdu-guard	Toggle on to enable STP BPDU Guard for the port.

To install a profile on a device:

1. Go to *Configuration* > *Device*.
   The device list is displayed.
2. Click *+Device* to add a device, or select a device to update.
   The *Device <Name>* dialog box is displayed.
3. From the *Profile Name* dropdown, select a profile and click *OK*.
4. In the *Config Status* column, click *Install Configuration*.

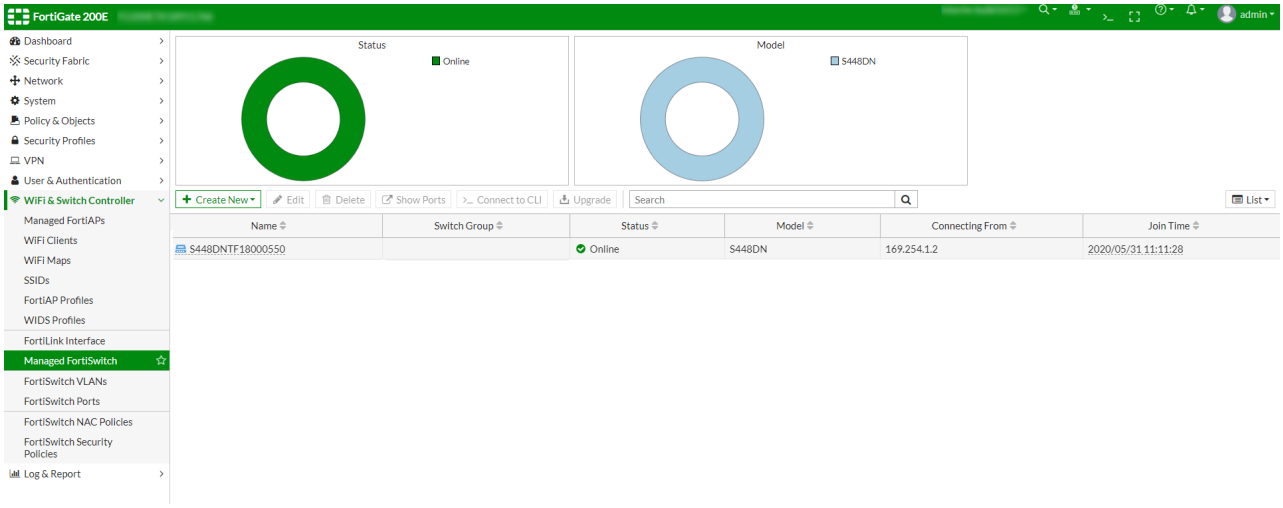


   Wait for the status to change to *Synchronized*.

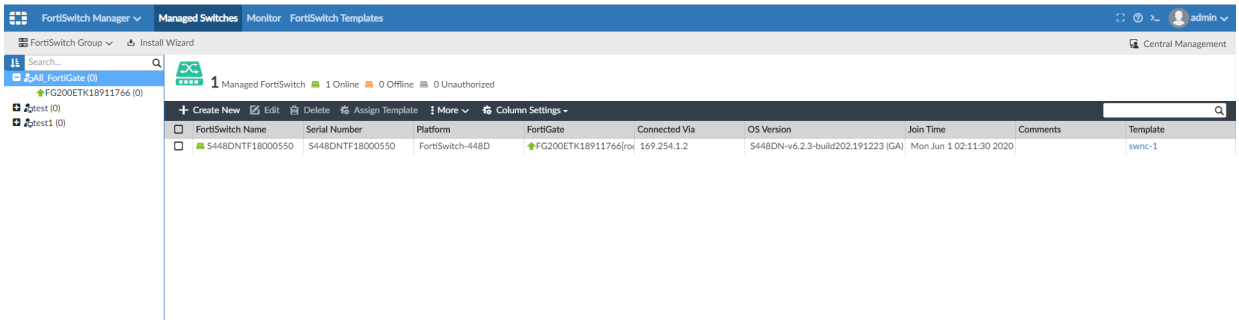
5. Connect the physical port on the FortiSwitch to the target port on FortiGate.
   Wait 10-15 minutes to allow the device to come online.

To verify the connection:

1. On FortiGate, go to *WiFi & Switch Control* > *Managed FortiSwitch*.
   Check the *Status* column to verify the device status is *Online*.

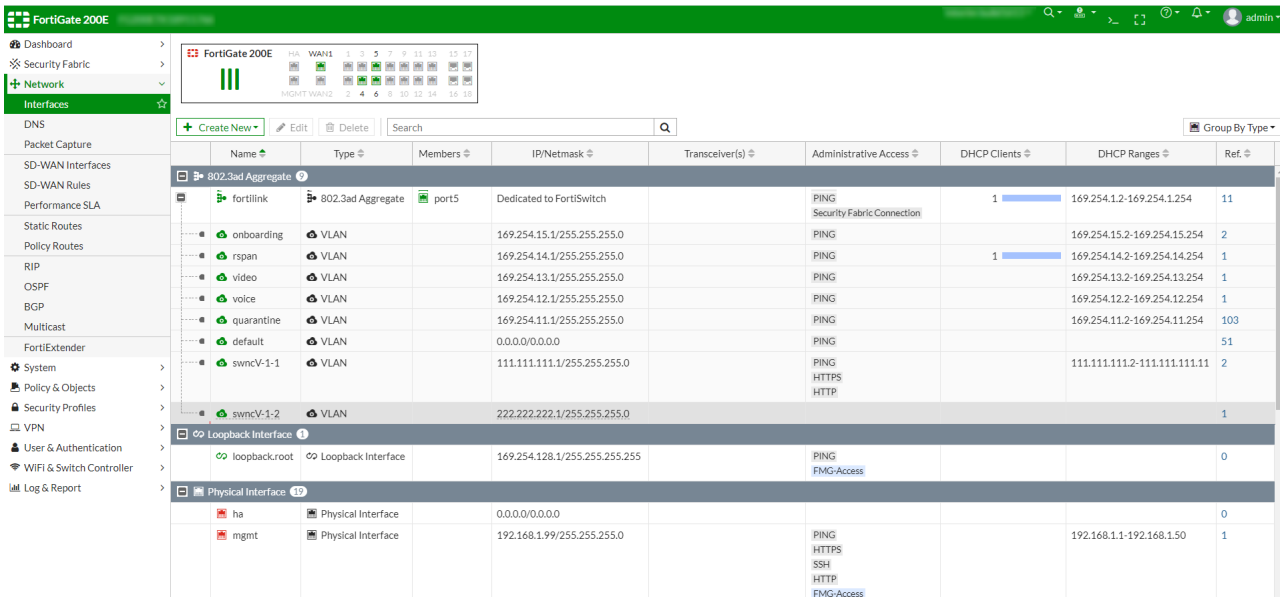


2. On FortiManager, go to *FortiSwitch Manager* > *Managed Switches* > *All_FortiGate* and select a device in the tree menu.
   Check the *FortiSwitch Name* column to verify the device is online.

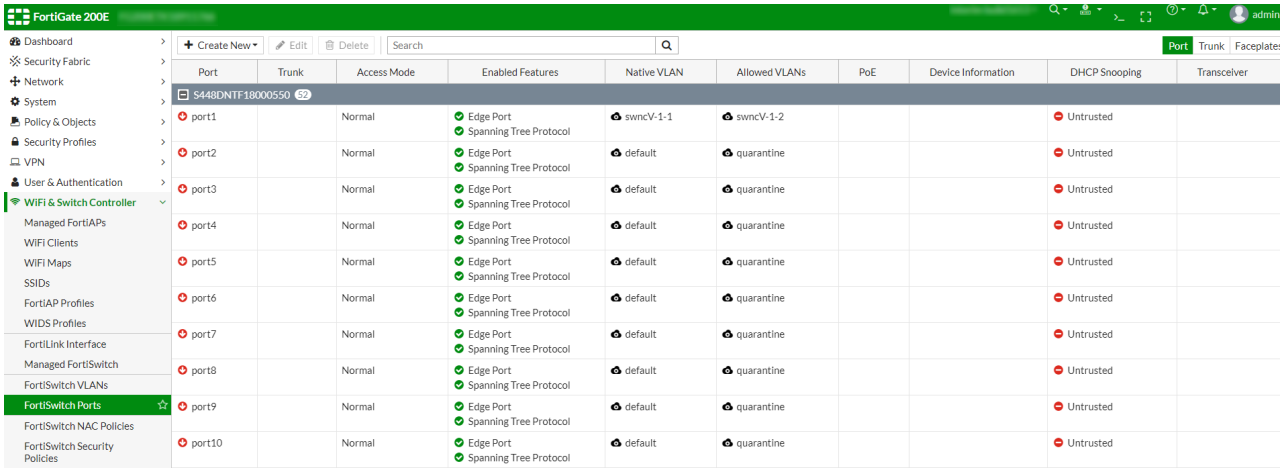


To verify the device received the configuration:

1. On FortiGate go to *Network* > *Interfaces*, and expand the interface in the table.
   In the *Name* column check that the target interface is set as *fortilink* member.
   In the *Type* column check that then VLANs in the controller profile are displayed.



2. Go to *WiFi & Switch Control* > *Managed FortiSwitch*.
   In the *Native VLAN* or *Allowed VLANs* columns, check that the VLANs are assigned to the FortiSwitch port.



Adding a FortiAP model device

When creating a profile, you can add a model FortiAP device to a FortiGate. When the access point comes online, it is managed by FortiGate and receives the configuration.

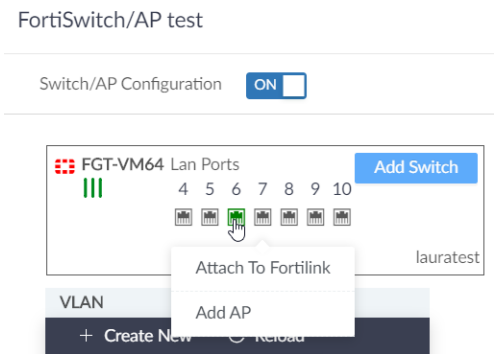
Requirements:

Connect the FortiAP LAN port to the target FortiGate port.

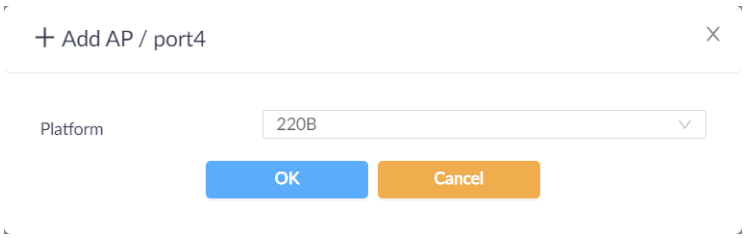
To add a model FortiAP to a FortiGate:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Create a new profile, or select a profile to update.

3. Display the FortiSwitch/AP settings.
   a. Click the *Network* tab.
   b. Expand the *LAN* section, and click *Switch/AP*.
      The *FortiSwitch/AP <Name>* dialog box is displayed.
4. Select a FortiGate port, and click *Add AP*.



   The *+Add AP <Name>* dialog box is displayed.
5. From the *Platform* dropdown, select a FortiAP model you want to manage .

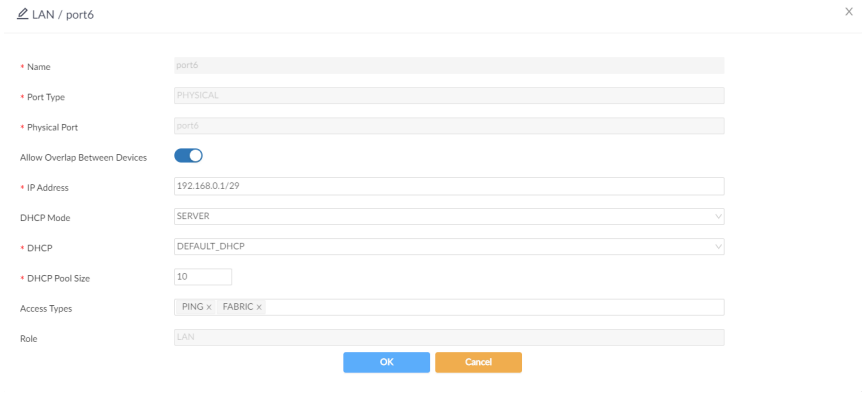


6. Click *OK*.
   The AP model is added to the profile.

To install a profile on the target device:

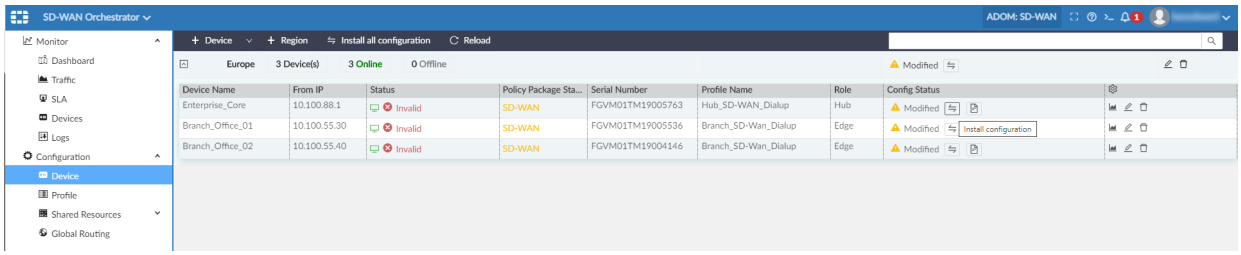
1. Enable DHCP on the port so the connected AP will receive the IP address from the DHCP server.
   a. Go to *Configuration* > *Device*.
      The device list is displayed.
   b. Select a device to update.
      The *Device / <Name>* dialog box is displayed.
   c. Click the *Network* tab.
   d. Expand the *LAN* section, and select a port to update.
      The *LAN<port>* dialog box is displayed.

e. Configure the DHCP settings, and click *OK*



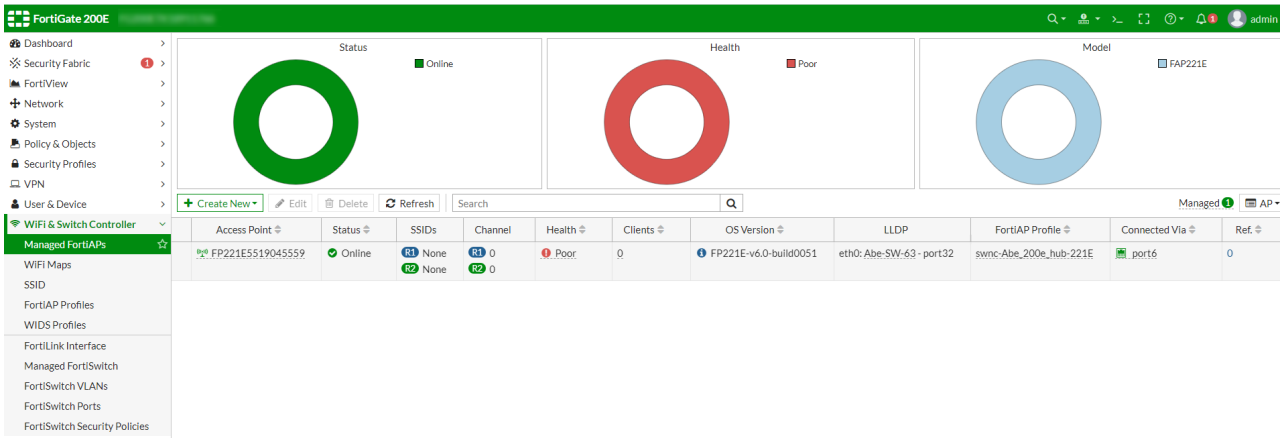
f. Click OK again.

2. In the *Device* pane, click *Install Configuration*.



The configuration is synchronized with FortiGate. Wait 10-15 minutes for the device to come online.

3. To verify the connection in FortiGate, go to *WiFi & Switch Controller* > *Manager FortiAPs*.
Check the *Status* column to verify the device is *Online*.
Check the *FortiAP Profile* column to ensure the correct profile was deployed.



4. To verify the connection in FortiManager, go to *AP Manager* > *Managed APs*.
Check the *Access Point* column to verify the device is online.
Check the *AP Profile* column to verify the correct profile was deployed.

To add an SSID profile to a ports AP profile:

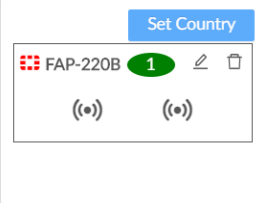
1. In the SSID table, create a new profile or select a profile to update.
   The *+SSID* dialog box is displayed.
2. Configure the SSID settings, and click *OK*.

Option	Description
Name	Enter a name for the SSID profile.
SSID	Type the wireless service set identifier (SSID), or network name, for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
Security Mode	Select a security mode: • *Open* • *WPA2_PERSONAL* • *WPA3_SAE* • *WPA3_SAE_TRANSITION*
Pre-shared Key	Enter the pre-shared key for the SSID. This option is only available when the security mode includes *WPA2 _PERSONAL* and *WPA3_SAE_TRANSITION*.
SAE Password	Enter the password for the SSID. This option is only available when the security mode includes *WPA3_SAE* and *WPA3_SAE_TRANSITION*.
Client Limit	The maximum number of clients that can simultaneously connect to the AP (0 - 4294967295, default = 0, meaning no limitation).
Broadcast SSID	Enable/disable broadcasting the SSID (default = enable). Broadcasting enables clients to connect to the wireless network without first knowing the SSID. For better security, do not broadcast the SSID.
Block Intra-SSID Traffic	Enable/disable blocking communication between clients of the same AP (default = disable).
Quarantine Host	Enable/disable station quarantine (default = enable).
Allow Overlap between Device	Toggle on to allow overlap between devices. Toggle off to disable this feature.
IP Auto Assign	Available when *Allow Overlap Between Devices* is disabled. Toggle on to automatically assign IP addresses. Toggle off to disable this feature.
IP Pool	Available when *IP Auto Assign* is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator to automatically assign.
Subnet Mask Length	Available when *IP Auto Assign* is enabled. Specify the length of the subnet mask.

Option	Description
DHCP Mode	Choose from: • *None* • *Server* • *Relay*
DHCP	Choose the DHCP server.
DHCP Pool Size	Enter the DHCP pool size.
Access Types	Select the types of access to allow on the interface.

To configure an AP profile:

1. In the AP profile table, click *Edit*.

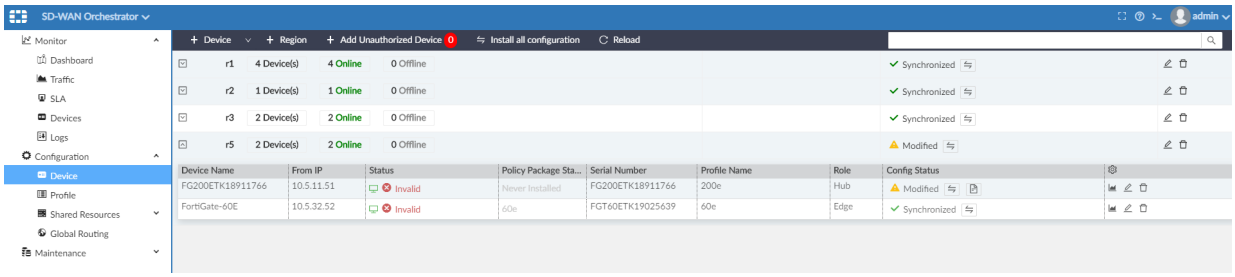


   The *AP<Name>* dialog box is displayed.
2. Configure the settings and click *OK*.

Option	Description
AllowAccess	Choose from: • *HTTPS* • *SSH* • *SNMP*
Login Password Change	Choose from: • *LEAVE_UNCHANGED* • *SET* • *SET_EMPTY*
Mode	Choose from: • *DISABLED* • *AP* • *MONITOR*
Wids Profile	Choose from: • *default* • *default-wids-apscan-enabled*
Radio Resource Provision	Select to enable radio resource provisioning. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point.

Option	Description
Band	Select the wireless protocol from the dropdown list. The available bands depend on the selected platform. In two radio devices, both radios cannot use the same band.
Short Guard-interval	Select to enable the short guard interval.
Auto TX Power Control	Enable automatic adjustment of transmit power.
TX Power (%)	If *Auto TX Power Control* is disabled, enter the TX power in the form of the percentage of the total available power. If *Auto TX Power Control* is enabled, enter the *TX Power Low (dBm)* and *TX Power High (dBm)* power levels.
SSIDs Auto Assign	Disable to manually assign the SSIDs that APs using this profile will carry, or let them be selected automatically.
Monitor Channel Utilization	Enable/disable monitoring channel utilization.

3. To verify the profile was updated, go to *Configuration* > *Device*.
Check the *Config Status* column to verify the profile is *Modified*.



4. Click *Install Configuration* to synchronize the profile on the device.

Creating new DMZ settings

When creating a profile, you can also create new DMZ settings.

To create new DMZ settings:

1. Go to *Configuration* > *Profile*.
The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
The *Profile <name>* dialog box is displayed.
3. Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see Network tab on page 65.
4. Expand the *DMZ* section, and click *+Create New*.
The *DMZ* dialog box is displayed.

Option	Description
Name	Type a name for the interface.
Port Type	Select the type of port. Choose from *VLAN* or *AGGREGATE*.
Physical Port	Available when *Port Type* is set to *VLAN*. Select the port number.
VLAN ID	Available when *Port Type* is set to *VLAN*. Type an ID for the VLAN.
Access Types	Select the types of access to allow on the interface.

5. Complete the options, and click *OK*.
   The DMZ setting is created.
6. If you set *Port Type* to *AGGREGATE*, open the DMZ settings for editing, select interface members, and click *OK*.
   Interface members are added to the DMZ settings.

Creating business rules

You can create or update a business rule in a profile from the *Business* tab.

To create a business rule:

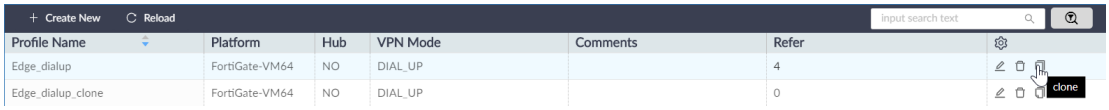
1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
   The *Profile <name>* dialog box is displayed.
3. Click the *Business* tab.
   The *Business* pane is displayed.
4. Click *+Create New*.
   The *Business Rule* dialog box is displayed.
5. Complete the options, and click *OK*.
   The business rule is created.

Cloning profiles

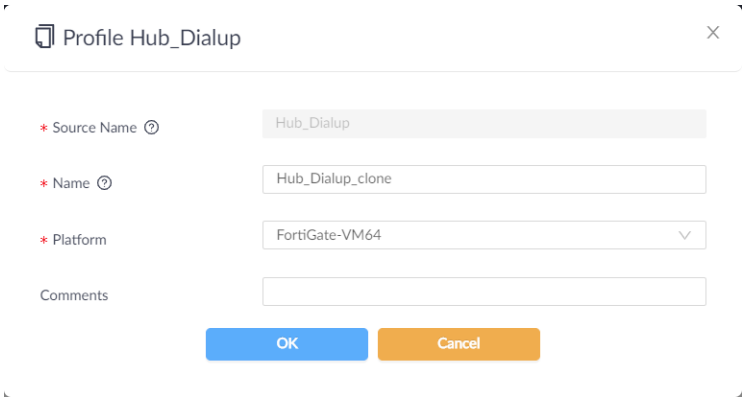
You can clone profiles, and then edit the settings to save time.

To clone profiles:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Click the *Clone* icon for the profile.

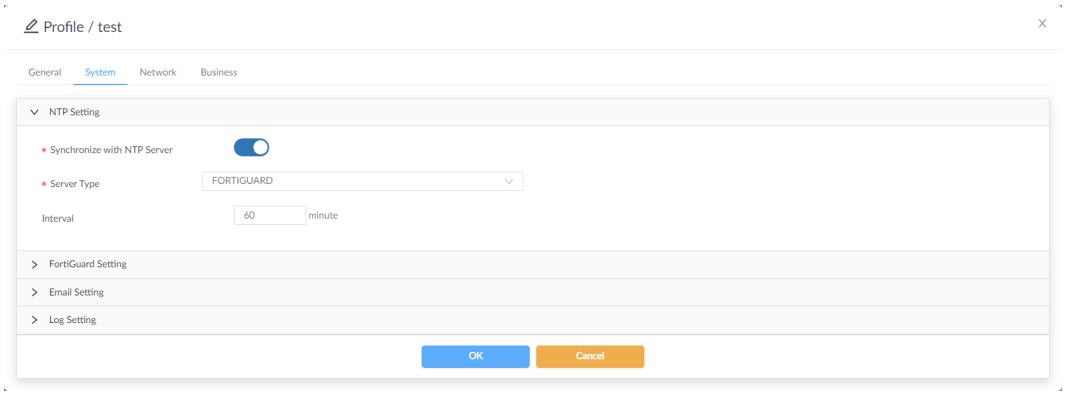


   The *Profile <name>* dialog box is displayed.



3. Set the following options, and click *OK*.
   a. In the *Name* box, type a unique name.
   b. In the *Platform* list, select the platform.

   The cloned profile opens for editing.



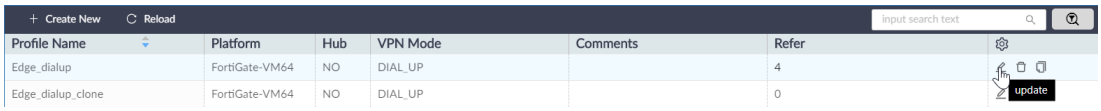
4. Set the options on the *System*, *Network*, and *Business* tabs, and click *OK*.

Updating profiles

You can update profiles after you create them. Updated profile settings are synchronized to associated devices.

To update profiles:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Click the *Update* icon for the profile.
   Alternately, you can double-click the profile to open it for updating.



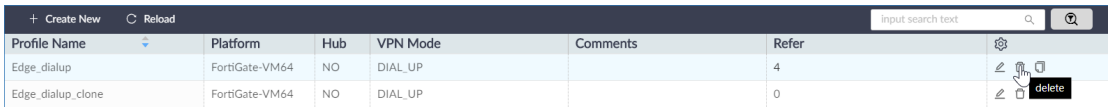
   The *Profile <name>* dialog box opens.
3. Edit the settings, and click *OK*.
4. Install profile changes. See Installing configuration changes on page 35.

Deleting profiles

You can delete profiles when they are no longer used by devices or regions.

To delete profiles:

1. Go to *Configuration* > *Profile*.
   The list of profiles is displayed.
2. Click the *Delete* icon for the profile.



   A confirmation dialog box is displayed.
3. Click *OK*.
   The profile is deleted.

Profile options described

This section describes the options available when you configure a profile. The options are organized into the following tabs:

- General tab on page 62
- System tab on page 63
- Network tab on page 65
- Business tab on page 67

General tab

The *General* tab contains the following sections:

Option	Description
Name	Type a name for the profile. You can use lowercase and uppercase letters, numbers 0 to 9, underscores, and dashes.
Platform	Select a platform for the profile settings.
Device Role	Select *PRIMARY_HUB* to create a profile for primary hubs. Select *SECONDARY_HUB* to create a profile for secondary hubs.
VPN Mode with Hub	Available with *Hub* is toggled off. Select one of the following options to connect the edge devices to the hub in the region: • Select *SITE_TO_SITE* to create full-mesh overlay links between the hub device and its edge devices in the same region. • Select *DIAL_UP* to create one-to-one overlay links between the hub device and its edge devices. When you select *DIAL_UP*, you can enable ADVPN on the *Network* tab in the *WAN* settings.

Option	Description
VPN Mode with Edge	Available with *Hub* is toggled on. Select one of the following options to connect the hub device with edge devices: • Select *SITE_TO_SITE* to create full-mesh overlay links between the hub device and its edge devices in the same region. • Select *DIAL_UP* to create one-to-one overlay links between the hub device and its edge devices. When you select *DIAL_UP*, you can enable ADVPN on the *Network* tab in the *WAN* settings.
Max Edge Count	Available with *Hub* is toggled on and *VPN Mode with Edge* is set to *DIAL_UP*. Specify the maximum number of edge devices allowed to connect with the hub device.
Port Number	Specify the number of ports on the FortiGate. The number of ports in the FGT VM should be the same number as defined here. Otherwise conflict will occur.
Comments	(Optional) Type a comment about the profile.

System tab

The *System* tab contains the following sections:

- NTP on page 63
- FortiGuard on page 63
- Email on page 64
- Log on page 64

NTP

Expand *NTP Setting* to view the following options:

Option	Description
Synchronize with NTP Server	Toggle on to enable synchronization with an NTP server, and then specify the server. Toggle off to disable this feature.
Server Type	Choose between the following options: • *FortiGuard* • *Specify* When you select *Specify*, you must also select an NTP server.
NTP Servers	Available when *Server Type* is set to *Specify*. Select an NTP server that you added to SD-WAN Orchestrator MEA.
Interval	Specify how often in minutes to synchronize time with the NTP server.

FortiGuard

Expand *FortiGuard Setting* to view the following options:

Option	Description
Enable FortiGuard Security Updates	Toggle on to enable security updates from FortiGuard. Toggle off to disable this feature.
Servers	Select a FortiGuard server that you added to SD-WAN Orchestrator MEA.
Include Worldwide FortiGuard servers	Toggle on to include FortiGuard servers from around the world. Toggle off to disable this feature.

Email

Expand *Email Setting* to view the following options:

Option	Description
Server name	Select the server to use for email notifications. You must add a server to SD-WAN Orchestrator MEA before you can select it.

Log

Expand *Log Setting* to view the following logging options:

- Send Logs to FortiAnalyzer / FortiManager
- Send logs to Syslog

You can configure devices to send logs to FortiAnalyzer/FortiManager or a syslog server.

Option	Description
Send logs to FortiAnalyzer / FortiManager	Toggle on to enable logging to FortiAnalyzer or FortiManager. Toggle off to disable this feature.
Server Type	Select one of the following options: • *This FortiManager or managed FortiAnalyzer*: Sets the IP of the FortiAnalyzer to be the same as the FortiManager to which the FortiGate is connected. Use this option when FortiAnalyzer features are enabled on FortiManager. • *Specify IP Address*: Specify an IP address for FortiAnalyzer when the IP address for FortiAnalyzer is different from the FortiManager to which the FortiGate is connected.
Upload option	Specify how often to upload logs from devices to FortiManager or FortiAnalyzer.
Encrypt Log Transmission	Specify the level of encryption for log transmission.
Reliable logging to FortiAnalyzer	Toggle on to enable reliable logging to FortiAnalyzer. Toggle off to disable this feature.
Send Logs to Syslog	Toggle on to enable logging to a syslog server. Toggle off to disable this feature.
Server IP/Name	Type the IP address or FQDN of the syslog server that you added to SD-WAN Orchestrator MEA.
Mode	Select a mode for transmitting logs. Choose from:

Option	Description
	• UDP • Legacy reliable • Reliable
Port	Specify which port to use.
Minimum Log Level	Specify the minimum level of logs to include.
Format	Specify the log format.

Network tab

The *Network* tab contains the following sections:

- WAN on page 65
- LAN on page 66
- DMZ on page 66
- BGP on page 67
- DNS Server on page 67
- SNMP on page 67
- HA Interfaces on page 67

WAN

Expand *WAN* to view the following options:

Option	Description
Create New	Click *Create New* to define a new WAN interface. You can define the port type as *VLAN* or *AGGREGATE*. When the port type is *AGGREGATE*, you must save the WAN configuration, and then open it for editing to add interface members. See also Creating new WAN settings on page 45.
Interface	Displays the interface name.
Interface Members	Displays the interface members for an aggregate interface.
Vlan	Displays whether VLAN is used.
ISP Link	Displays the name of the ISP link.
WAN Type	Displays the type of WAN used.
Private Wire	Displays whether a private wire is used.
Mode	Displays the mode used by the interface.
Enable	Indicates whether the interface is enabled.
Access	Displays the types of access to allowed for the interface.
Update	Click the *Update* icon to edit the settings.

LAN

Expand *LAN* to view the following options:

Option	Description
Create New	Click *Create New* to define a new LAN interface. You can define the port type as *VLAN*, *WiFi_SSID*, or *AGGREGATE*. When the port type is *AGGREGATE*, you must save the LAN configuration, and then open it for editing to add interface members. See also Creating new LAN settings on page 47.
Switch/AP	Click *Switch/AP* to define settings for FortiSwitch and FortiAP devices.
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
Interface Members	Displays the interface members for an aggregate interface.
Subnet Type	Displays the type of subnet.
IP Address	Displays the IP address.
DHCP Server/Relay	Displays the DHCP mode
DHCP Pool Size	Displays the DHCP pool size.
Access	Displays the types of access to allowed for the interface.
Update	Click the *Update* icon to edit the settings.

DMZ

Expand *DMZ* to view the following options:

Option	Description
Create New	Click *Create New* to define a new DMZ interface. You can define the port type as *VLAN* or *AGGREGATE*. When the port type is *AGGREGATE*, you must save the DMZ configuration, and then open it for editing to add interface members.
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
Interface Members	Displays the interface members for an aggregate interface.
Enable	Indicates whether the interface is enabled.
Access	Displays the types of access to allowed for the interface.
Update	Click the *Update* icon to edit the settings.

BGP

Expand *BGP* to view the following options:

Option	Description
Create New	Click *Create New* to define a new BGP interface.
Type	Displays the type of BGP network.
Subnet	Displays the physical port.
Update	Click the *Update* icon to edit the settings.

DNS Server

Expand *DNS Server* to view the following options:

Option	Description
Server Name	Select a DNS server that you added to SD-WAN Orchestrator MEA.

SNMP

Expand *SNMP* to view the following options:

Option	Description
SNMP Agent	Toggle on to enable an SNMP agent. Toggle off to disable this feature.

HA Interfaces

Expand *HA Interfaces* to view the following options:

Option	Description
Monitor Interfaces	Select a port for monitoring interfaces. You can use the same port as the FortiManager heartbeat interface.
Heartbeat Interfaces	Select a port to use for the heartbeat. You can use the same port as the FortiManager monitor interface.

When a profile without HA interface definitions is assigned to a device in an HA cluster, default ports are used. For *Monitor Interfaces*, WAN1 is used, and for *Heartbeat Interfaces*, the last LAN port is used.

Business tab

The *Business* tab contains the following options:

Option	Description
Create New	Click *Create New* to create a new business rule.

Option	Description
Name	Type a name for the business rule.
Criteria	
Valid	Displays whether the rule is valid. A checkmark indicates a valid rule.
Source Address	Select the source address or address group.
Users	Select or create users.
User Groups	Select or create user groups
Destination Type	Select the type of destination for the traffic.
Dest Address	Select or create the destination address or address group.
Service	Select or create the Internet service.
Enable	Toggle *ON* to enable the rule, and Toggle *OFF* to disable the rule.
Link Policy	
Group Type	For hub devices, choose from *UNDERLAY* or *OVERLAY*. For edge devices, choose from *UNDERLAY*, *OVERLAY*, or *ALL*.
Path	When *Group Type* is set to *OVERLAY*, displays the path. When *Group Type* is set to *UNDERLAY*, choose from *SINGLE_PATH*, *MULTIPLE_PATH*, or *ALL_PUBLIC_LINE*.
Load Policy	When *Group Type* is set to *Overlay*, choose from *LOW_COST*, *HIGH_QUALITY*, or *HIGH_THROUGHPUT*. When *Group Type* is set to *Underlay* for hub devices, choose from *LOW_COST*, *HIGH_QUALITY*, *HIGH_THROUGHPUT*, or *MANUAL*.
SLA Quality Level	Displays the minimum quality level.
Dual Hub Load Mode	Available for dual hubs when *Group Type* is set to *OVERLAY*. Choose from *ACTIVE_PASSIVE* or *ACTIVE_ACTIVE*. When you choose *ACTIVE_PASSIVE*, the business rule is split and deployed to FortiGate as two rules: • One rule is for the primary hub, and includes all overlay links to the primary hub as priority members. • The other rule is for secondary hub, and includes all overlay links to the secondary hub as priority members. When you choose *ACTIVE_ACTIVE*, a business rule is deployed to FortiGate as one rule. The priority members include all overlay links between the edge and both hubs.
SLA Server Type	When *Group Type* is set to *Overlay*, select the type of SLA server.
SLA Server	Select the SLA server.
Backhaul to Group	When *Group Type* is set to *Overlay* for hub devices, choose the backhaul route to the group.

Shared resources

You can define resources once, and then select them in multiple profiles by using the *Shared Resources* tree menu. You can create the following shared resources:

- Intranet addresses
- Network resources, such as DHCP servers
- SLA quality levels and servers
- Servers used by SD-WAN Orchestrator MEA, such as NTP servers, FortiGuard servers, and email servers
- Health thresholds

Intranet Addresses

You can view the internal addresses and address groups that SD-WAN Orchestrator MEA automatically generates for your network.

You can use these auto-generated addresses and address groups to implement business rules to manage the traffic between different devices and groups.

If you wan to create your own addresses and add them to an address group, you must add them by using the *Policy & Objects* module in FortiManager.

To view intranet addresses:

1. Go to *Configuration* > *Shared Resources* > *Intranet Address*.
2. Click *IPv4 Address* or *IPv4 Address Group*.
3. In the toolbar click *Reload*.

Network

From the *Network* tree menu, you can create and manage servers, relays, hosts, and IP Pools.

This section contains the following topics:

- Creating DHCP servers on page 70
- Creating DHCP relays on page 70
- Creating DNS servers on page 70
- Creating intranet IP pools on page 71
- Creating SNMP hosts on page 71
- Changing network settings on page 71
- Creating ISP links on page 72

Creating DHCP servers

To create DHCP servers:

1. Go to *Configuration* > *Shared Resources* > *Network* > *DHCP Server*.
2. In the toolbar, click *+Create New*.
   The *DHCP Server* dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the DHCP server.
TFTP Server	Enter the IP address for the TFTP server.
DNS Server Res Type	Select *Default* or *Local* from the dropdown.

Creating DHCP relays

To create DHCP relays:

1. Go to *Configuration* > *Shared Resources* > *Network* > *DHCP Relay*.
2. In the toolbar, click *Create New*.
   The *DHCP Relay* dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the DHCP server.
Primary Relay IP	Enter the primary relay IP address.
Secondary Relay IP	Enter the secondary relay IP address.

Creating DNS servers

To create DNS servers:

1. Go to *Configuration* > *Shared Resources* > *Network* > *DNS*.
2. In the toolbar, click *+Create New*.
   The *DNS Server* dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the DHCP server.
Primary Server	Enter the IP address for the primary server.

Option	Description
Secondary Server	Enter the IP address for the secondary server.

Creating intranet IP pools

To create intranet IP pools:

1. Go to *Configuration* > *Shared Resources* > *Network* > *Intranet IP Pool*.
2. In the toolbar, click *+Create New*.
   The *IP Pool* dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the Intranet IP pool.
Pool	Enter the IP address for the pool.

Creating SNMP hosts

You must create an SNMP host before you can add it to SD-WAN Orchestrator MEA.

To create SNMP hosts:

1. Go to *Configuration* > *Shared Resources* > *Network* > *SNMP Host*.
2. In the toolbar, click *+Create New*.
   The SNMP dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the SNMP Host.
Version	Select the version from the dropdown.
Host Type	Select the host type from the dropdown.
IP	Enter the IP address for the SNMP host.
Query Port	Enter the query port number.
Trap Remote Port	Enter the trap remote port number.
Community Name	Enter a name for SNMP community.

Changing network settings

In the network settings, you can change VPN address pool, loopback address pool, and enable anti-theft protection.

To change network settings:

1. Go to *Configuration* > *Shared Resources* > *Network* > *Network Settings*.
2. Configure the settings, and click *OK*.

Option	Description
VPN Addr Pool	Enter the IP address for the VPN address pool.
Loopback Address Pool	Enter the IP address for the loopback address pool.
Auth After Location Change	Toggle *On* to enable anti-theft protection. When a device is disconnected from the SD-WAN network and reappears in a different geographic location or in a different network topology, access to the overlay is blocked, and information is displayed about the device location change. Administrators can choose whether manually approve access to the network. Toggle *Off* to disable anti-theft protection.

Creating ISP links

To create ISP links:

1. Go to *Configuration* > *Shared Resources* > *Network* > *ISP Link*.
2. In the toolbar, click *+Create New*.
   A dialog box is displayed.
3. Configure the settings, and click *OK*.

Option	Description
Name	Enter a name for the ISP link.
Type	From the dropdown, select one of the following options: • *Internet*: An Internet ISP link with a public IP can both initiate or respond IPsec negotiation with peer devices. • *MPLS*: If a WAN port is set as *MPLS* link type with *Private Wire* on, it can only establish IPsec tunnels with other devices' WAN ports that are also configured as MPLS. • *LTE*: Usually used when local WAN port is behind NAT or without a public IP address. If a WAN port is set as *LTE*, it can only be IPSec initiator but not responder.
Cost	From the dropdown, select *Low*, *Medium*, or *High*. • *High* sets cost to 3. • *Medium* sets cost to 2. • *Low* sets cost to 1. For example, if the Load Policy is LOW_COST, FortiGates usually choose links with lower cost first. As a result, the interface with the lowest assigned cost of 1 is selected.
Public IP	Toggle *On* if the IP is public.

SLA

The service level agreements in SD-WAN Orchestrator MEA help you monitor SD-WAN performance.

This section contains the following topics:

- Adding SLA quality levels on page 73
- Adding SLA servers on page 73

Adding SLA quality levels

To add SLA quality levels:

1. Go to *Configuration* > *Shared Resources* > *SLA* > *SLA Quality*.
2. In the toolbar, click *+Create New*.
   The *SLA Quality Level* dialog box is displayed.
3. Configure the following settings, and click *OK*.

Option	Description
Name	Enter a name for the quality level.
Latency	Enter the latency threshold (in milliseconds).
Jitter	Enter the jitter threshold (in milliseconds).
Packet Loss	Enter the packet loss threshold (in percent).

Adding SLA servers

You must create an SLA server before you can add it to SD-WAN Orchestrator MEA.

To add SLA servers:

1. Go to *Configuration* > *Shared Resources* > *SLA* > *SLA Server*.
2. In the toolbar, click *Create New*.
3. Configure the SLA server settings, and click *OK*.

Option	Description
Name	Enter a name for the SLA server.
Protocol	From the dropdown select the detection method (*Ping* or *HTTP*).
Servers	Type the IP address or FQDN of the SLA server to probe.

System

The *System Settings* tree menu lets you add servers for SD-WAN Orchestrator MEA to use. SD-WAN Orchestrator MEA supports the following servers: NTP, FortiGuard, and email. See:

- Adding NTP servers on page 74
- Adding FortiGuard servers on page 74
- Adding email servers on page 75

Adding NTP servers

You can add an NTP server to SD-WAN Orchestrator MEA, and then select the server in profiles and devices.

To add NTP servers:

1. Go to *Configuration* > *Shared Resources* > *System* > *NTP Server*.
2. In the toolbar, click *Create New*.
3. Configure the NTP server settings, and click *OK*.

Option	Description
Name	Enter a name for the NTP server.
Address Type	From the dropdown, select *IP* or *FQDN*.
Address	Enter the server's IP address or host name.
NTP v3	Toggle *On* to enable NTP v3.
Authentication	Toggle *On* to enable authentication.
Key	Available when *Authentication* is enabled.
Key ID	Available when *Authentication* is enabled.

Adding FortiGuard servers

You can add a FortiGuard server to SD-WAN Orchestrator MEA, and then select the server in profiles and devices.

To add FortiGuard servers:

1. Go to *Configuration* > *Shared Resources* > *System* > *FortiGuard Server*.
2. In the toolbar, click *Create New*.
3. Configure the FortiGaurd server settings, and click *OK*.

Option	Description
Name	Enter a name for the NTP server.
Server Type	From the dropdown, select *Update* or *Rating*.
Address Type	From the dropdown, select *IP4*, *IP6*, or *FQDN*.
Address	Enter the device's IP address or host name.

Adding email servers

You can add an email server to SD-WAN Orchestrator MEA, and then select the server in profiles and devices.

To add email servers:

1. Go to *Configuration* > *Shared Resources* > *System* > *Email Server*.
2. In the toolbar, click *Create New*.
3. Configure the email server settings and click *OK*.

Option	Description
Name	Enter a name for the email server.
Address Type	From the dropdown, select *IPv4* or *FQDN*.
Address	Enter the email server's IP address or host name.
Authentication	Toggle *On* to enable authentication, then enter the *Username* and *Password*.
Username	Available when *Authentication* is enabled.
Password	Available when *Authentication* is enabled.
Port	Enter the port number.
Reply To	Enter the email address users can reply to.
Security	From the dropdown, select *None*, *STARTTLS*, or *SMTPS* .
SSL Version	From the dropdown, select the SSL version.
Validate Server	Toggle *On* to enable validation.

Health Threshold

Quality of devices (indicated by color in *Monitor* > *Dashboard and Monitor* > *Devices*) in the SD-WAN network are valued according to the defined health threshold.

To update health thresholds:

1. Go to *Configuration* > *Shared Resources* > *Health Threshold*.
2. In the *Tools* column, click the *Update* icon for the health threshold.
   The *Health Threshold* dialog box is displayed.
3. Update the settings, and click *OK*.

Global routing

You can view the subnet, next hop, and type information for global routing.

To view global routing:

1. Go to *Configuration* > *Global Routing*.
   The subnet, next hop, and type information is displayed for global routing.

Maintenance

The *Maintenance* tree menu is available only in the root ADOM, and the root ADOM must be version 6.4.

You can maintain SD-WAN Orchestrator MEA by using the *Maintenance* tree menu. You can perform the following tasks:

- Upgrade firmware for SD-WAN Orchestrator MEA. See Upgrade on page 77.
- Back up and restore configurations for SD-WAN Orchestrator MEA. See Configuration on page 77.
- Export a zip file of debug information for SD-WAN Orchestrator MEA. See Debug on page 78.

Upgrade

You can upgrade firmware for SD-WAN Orchestrator MEA when updates are available.

To upgrade firmware:

1. Go to *Maintenance* > *Upgrade*.
2. Click *Check for updates*.

Configuration

You can back up all configurations from SD-WAN Orchestrator MEA, and then store them for safe keeping. You can also restore the configurations by uploading a backup file.

If devices managed by SD-WAN Orchestrator MEA are changed or removed from FortiManager after you back up an SD-WAN Orchestrator MEA configuration, restoring the SD-WAN Orchestrator MEA backup file does not work well. Instead it's recommend to back up and restore in FortiManager. When you restore a FortiManager backup file, SD-WAN Orchestrator MEA is restored as well.

To back up configurations:

1. Go to *Maintenance* > *Configuration*.
2. Click *Backup*.
   A `controller-store.config` file is downloaded to your computer.
3. Store the backup file in a safe location.

To restore configurations:

1. Go to *Maintenance* > *Configuration*.
2. Click *Restore*.
   The *Upload* window opens.
3. Click *Select File*.
4. Select your backup file, and click *Open*.

Debug

You can export debug information about SD-WAN Orchestrator MEA. The export process produces a zip file that contains the following folders of information that you can use:

- etc
- logs
- stat

To export debug information:

1. Go to *Maintenance* > *Debug*.
2. Click *Export Debug Info Zip File*.
   A `debug-info.zip` file is downloaded to your computer.

More information

SD-WAN Orchestrator MEA is available as a management extension application with FortiManager. For information about SD-WAN Orchestrator MEA, see the FortiManager page on the Document Library.