SD-WAN Orchestrator MEA - Administration Guide

Version 6.4.1 r2

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

August 13, 2020
SD-WAN Orchestrator MEA 6.4.1 r2 Administration Guide
02-641r2-609779-20200813

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-13	Initial release of 6.4.1 r2.

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 r2 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 Release Notes on the Docs Library.

This section contains the following topics:

- Key concepts
- How SD-WAN Orchestrator MEA works with FortiManager

Key concepts

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

- FortiGate devices on page 6
- Regions and links on page 7
- Normalized interfaces on page 8
- Underlay and overlay links on page 8
- Profiles on page 8
- Configuration installation on page 9
- Global routing on page 9
- Global analysis and visibility on page 9
- Device analysis and visibility on page 9
- Business rules on page 9

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 9.

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 29 and Importing devices on page 32.

Regions and links

A region refers to a cluster of devices in one geographical location. Each region consists of exactly one hub device and one or more edge devices.

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

Links between hubs

SD-WAN Orchestrator MEA automatically builds full-mesh overlay links between all hub devices.

Links between hub and edge devices in the same region

In the same region, the connection between a hub device and its edge devices depends on the VPN mode. The VPN mode is configured in profiles, and a profile is assigned to each 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 device and its edge devices in the same region. Edge devices from the same region communicate with each other by forwarding packets through their region's hub.
Dialup VPN	Overlay links are one-to-one between the hub device and its 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 its hub device. 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.

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 hub and edge devices. After creating a profile, you can apply it to multiple FortiGate devices. In a profile, you can configure settings for VPN mode, system resources, network settings, and business rules.

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 enabled.

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.

Upgrade

Upgrade of SD-WAN Orchestrator MEA 6.4.0 to 6.4.1 r2 is supported. SD-WAN Orchestrator MEA is automatically upgraded to 6.4.1 r2 after you upgrade the host FortiManager to 6.4.1.

SD-WAN Orchestrator MEA 6.4.1 r2 requires FortiManager 6.4.1 or later, and you must be in a 6.4 ADOM to access SD-WAN Orchestrator MEA.

Although upgrade to SD-WAN Orchestrator MEA 6.4.1 r2 is supported, a new deployment of SD-WAN Orchestrator MEA 6.4.1 r2 is recommended.

This section covers the following upgrade scenarios:

- Upgrading from FortiManager, SD-WAN Orchestrator MEA, and FortiOS 6.4.0 to 6.4.1 on page 11
- Upgrading from FortiManager and SD-WAN Orchestrator MEA 6.4.0 and FortiOS 6.2.x to 6.4.1 on page 12

Upgrading from FortiManager, SD-WAN Orchestrator MEA, and FortiOS 6.4.0 to 6.4.1

In this scenario, you are starting the upgrade with the following items:

- FortiManager 6.4.0 with ADOMs enabled.
- SD-WAN Orchestrator MEA 6.4.0
- FortiGates running FortiOS 6.4.0

In FortiManager, a 6.4 ADOM contains the FortiGates.

To upgrade SD-WAN Orchestrator MEA:

1. Upgrade FortiManager to 6.4.1.
   After FortiManager reboots, SD-WAN Orchestrator MEA is automatically upgraded to 6.4.1.
2. In FortiManager, upgrade FortiOS from 6.4.0 to 6.4.1.
   a. Go to *Device Manager > Firmware*.
      The *Upgrade Available* column displays 6.4.1.
   b. Select the FortiGates, and click *Upgrade*.
      When the firmware upgrade completes, click *Close*.
3. Initiate the creation of normalized interfaces and new policy blocks by going to *Management Extensions > SD-WAN Orchestrator MEA*.
   In FortiManager, you can view the new policy blocks by going to *Policy & Objects > Policy Packages*, and expanding the *Policy Blocks* tree menu. The following policy blocks are created:
   - SDWAN_Overlay_PB_EDGE
   - SDWAN_Overlay_PB_HUB

You can view normalized interfaces by going to *Policy & Objects* > *Object Configuration* > *Normalized Interface*.
The following normalized interfaces with per-platform mappings are created:

- overlay_edge2hub
- overlay_hub2edge
- overlay_hub2hub
- underlay
- sdwan_loopback

The interfaces are used by the automatically-generated policy blocks or by other custom policies.

4. In FortiManager, append new policy blocks to policy packages used by hub and spoke devices.
   a. Go to *Policy & Objects* > *Policy Packages*.
   b. In the tree menu, select the policy package for the hub device, and from the *Policy Block* menu, select *Append Policy Block*.
      The *Insert Policy Block* dialog box appears.
   c. From the list, select the policy block for hub devices, and click *OK*.
   d. Repeat this procedure for edge devices, if necessary.
   e. Delete from the policy package the policy block named *SDWAN_Overlay_PB* that was created in 6.4.0.
   f. Add other policies if necessary.
5. In SD-WAN Orchestrator MEA, install all configurations.
   a. Go to *Management Extensions* > *SD-WAN Orchestrator MEA*.
   b. Go to *Configuration* > *Device*, and click the *Install all configuration* button.
6. In FortiManager, install policy packages to hub and edge devices.
7. Check the configuration on FortiGate for the following changes:
   - SD-WAN configuration is migrated to `config system sdwan`.
   - New SD-WAN zones are created, and member interfaces have been added to corresponding zones.
   - Business rules remain unchanged, and SLA is up.
   - Firewall policies have been updated.

Upgrading from FortiManager and SD-WAN Orchestrator MEA 6.4.0 and FortiOS 6.2.x to 6.4.1

In this scenario, you are starting the upgrade with the following items:

- FortiManager 6.4.0 with ADOMs enabled.
- SD-WAN Orchestrator MEA 6.4.0
- FortiGates running FortiOS 6.2.x

In FortiManager, a 6.2 ADOM contains the FortiGates.

To upgrade SD-WAN Orchestrator MEA:

1. Upgrade FortiManager to 6.4.1.
   After FortiManager reboots, SD-WAN Orchestrator MEA is automatically upgraded to 6.4.1 r2.

2. In FortiManager, upgrade FortiOS from 6.2.x to 6.4.1.
   a. Go to *Device Manager* > *Firmware*.
      The *Upgrade Available* column displays 6.4.1.
   b. Select the FortiGates, and click *Upgrade*.
      When the firmware upgrade completes, click *Close*.
3. In FortiManager, upgrade the ADOM from version 6.2 to 6.4.

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 6.

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 14.
2. Plan your SD-WAN network. See Planning your network on page 15.
3. Create shared resources. See Creating shared resources on page 15.
4. Create profiles for hub and edge devices. See Creating profiles for all roles on page 16.
5. Add FortiGate devices to FortiManager. See Adding devices to FortiManager on page 16.
6. Add devices to SD-WAN Orchestrator MEA and install SD-WAN configurations. See Adding devices to FortiManager on page 16.
7. Install firewall policies to FortiGate devices in SD-WAN networks. See Installing firewall policies on page 16.
8. Monitor the SD-WAN network. See Monitoring devices and network traffic on page 17.

Enabling SD-WAN Orchestrator MEA

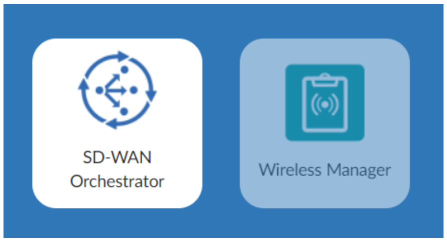
FortiManager provides access to the SD-WAN Orchestrator MEA application that is released and signed by Fortinet.

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 hub. Each region can have only one hub device, but multiple edge devices are allowed in each region.
  SD-WAN Orchestrator MEA automatically establishes overlays 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 58.

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 hub devices - see Creating profiles for hub devices on page 37
- Profile for edge devices - see Creating profiles for edge devices on page 38

See also Profile on page 36.

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 hub role and a profile for the edge role.
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 9.

   For more details about adding devices, see Device on page 27.
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 18.

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 18, Traffic on page 21 and SLA on page 23.
- For device analysis and visibility, see Devices on page 23.

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 18
- Traffic on page 21
- SLA on page 23
- Devices on page 23
- 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*.

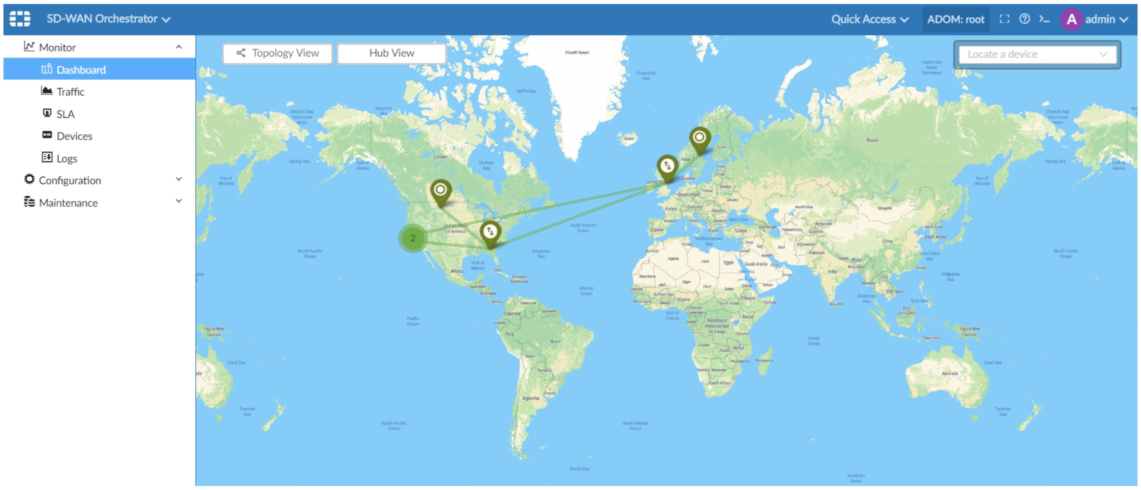
This section contains the following topics:

- Viewing devices on the world map on page 18
- Viewing device topology on page 19
- Viewing shortcut overlays (ADVPN) on page 20
- Viewing hub devices on page 20

If you want to view details about individual devices in the SD-WAN network, see Devices on page 23.

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.

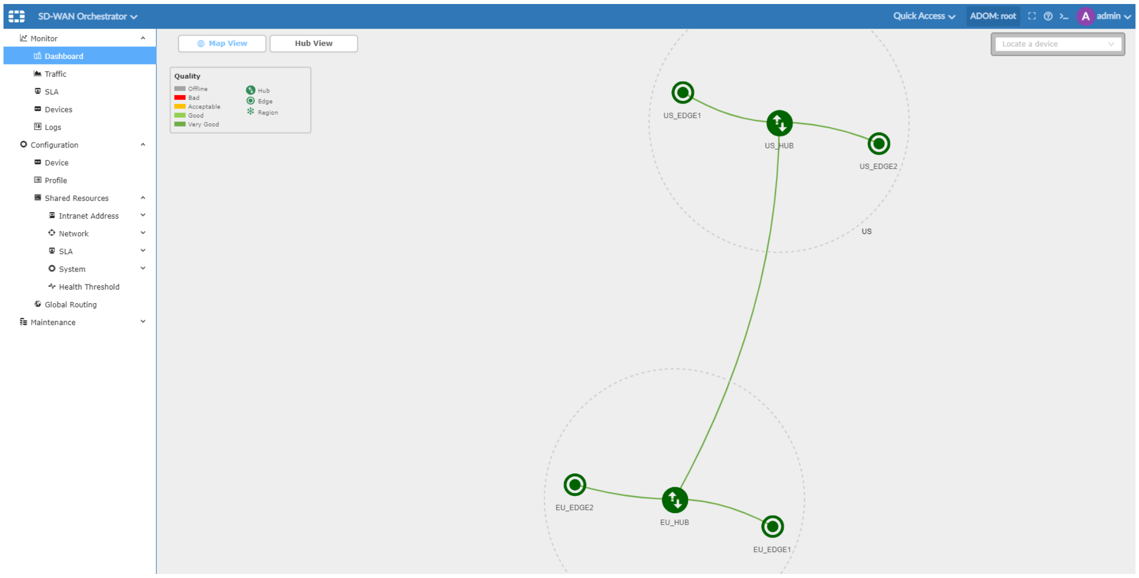


Viewing device topology

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.



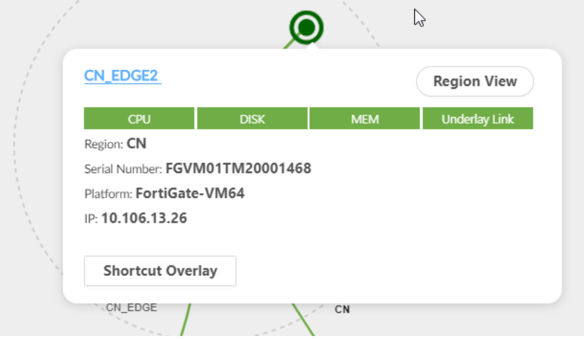
2. Click the lines to view link information, including the inbound and outbound bandwidth.

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.



Region: CN
Serial Number: FGVM01TM20001468
Platform: FortiGate-VM64
IP: 10.106.13.26

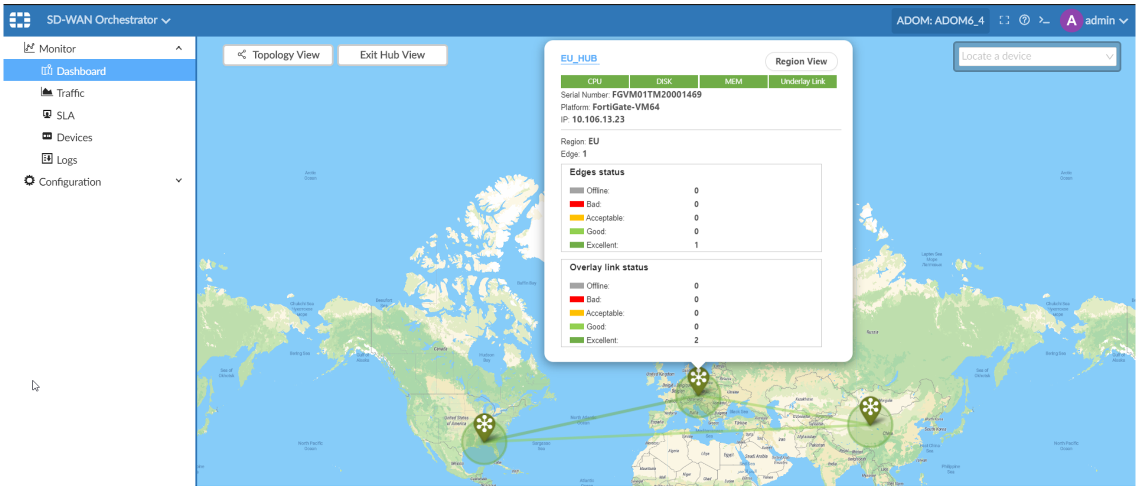
3. Click the *Shortcut Overlay* button.
   The shortcut view is displayed.
4. Click the *Exit Shortcut View* button to exit the view.

Viewing hub devices

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

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*.



Serial Number: FGVM01TM20001469
Platform: FortiGate-VM64
IP: 10.106.13.23

Region: EU
Edge: 1

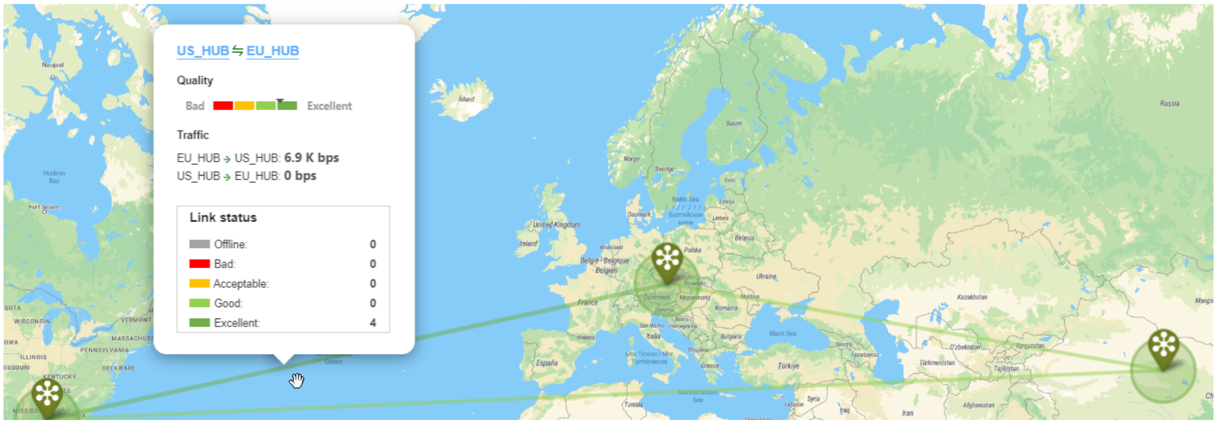
Edges status

Offline:	0
Bad:	0
Acceptable:	0
Good:	0
Excellent:	1

Overlay link status

Offline:	0
Bad:	0
Acceptable:	0
Good:	0
Excellent:	2

3. Click the lines between hubs to view link information.



US_HUB ⇋ EU_HUB

Quality

Bad 🟥🟧🟩🟩 Excellent

Traffic

EU_HUB → US_HUB: **6.9 K bps**
US_HUB → EU_HUB: **0 bps**

Link status

Offline:	0
Bad:	0
Acceptable:	0
Good:	0
Excellent:	4

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

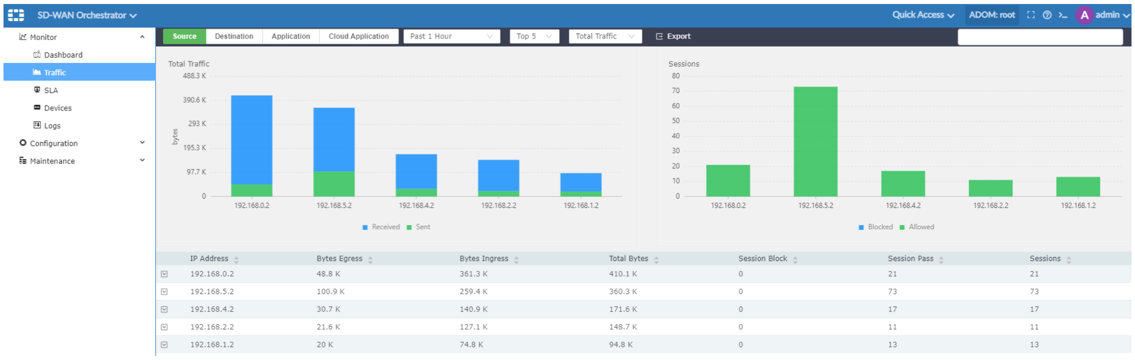
Viewing global network traffic reports

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.



IP Address	Bytes Egress	Bytes Ingress	Total Bytes	Session Block	Session Pass	Sessions
192.168.0.2	48.8 K	361.3 K	410.1 K	0	21	21
192.168.5.2	100.9 K	259.4 K	360.3 K	0	73	73
192.168.4.2	30.7 K	140.9 K	171.6 K	0	17	17
192.168.2.2	21.6 K	127.1 K	148.7 K	0	11	11
192.168.1.2	20 K	74.8 K	94.8 K	0	13	13

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:

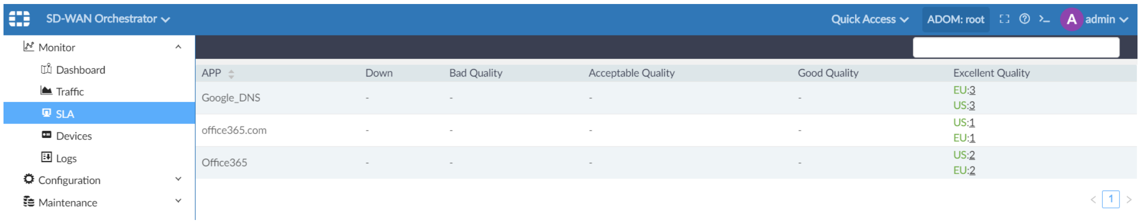
1. Go to *Monitor* > *Traffic*.
2. Display the desired traffic report. See Viewing global network traffic reports on page 21.
3. In the toolbar, click *Export*.
   A PDF of the traffic report is exported to your computer.

SLA

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

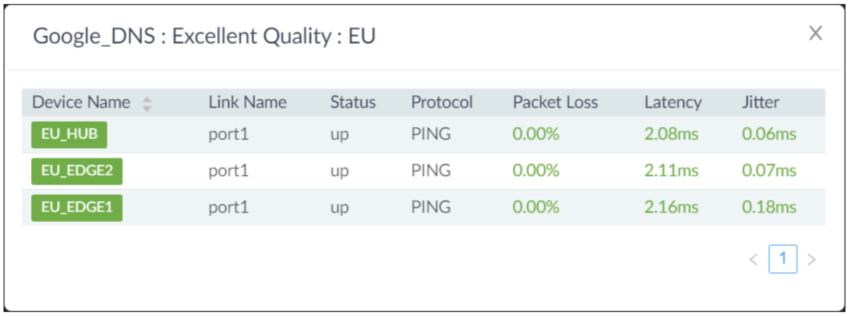
To view SLA:

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*.



APP	Down	Bad Quality	Acceptable Quality	Good Quality	Excellent Quality
Google_DNS	-	-	-	-	EU:3 US:3
office365.com	-	-	-	-	US:1 EU:1
Office365	-	-	-	-	US:2 EU:2

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.


Google_DNS : Excellent Quality : EU

Device Name	Link Name	Status	Protocol	Packet Loss	Latency	Jitter
EU_HUB	port1	up	PING	0.00%	2.08ms	0.06ms
EU_EDGE2	port1	up	PING	0.00%	2.11ms	0.07ms
EU_EDGE1	port1	up	PING	0.00%	2.16ms	0.18ms

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 25

If you want to view information about all devices in the SD-WAN network, see Dashboard on page 18.

Viewing device overviews

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

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. You can switch the view between two categories: • **Quality** (default): 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 charts monitor 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 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 *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:

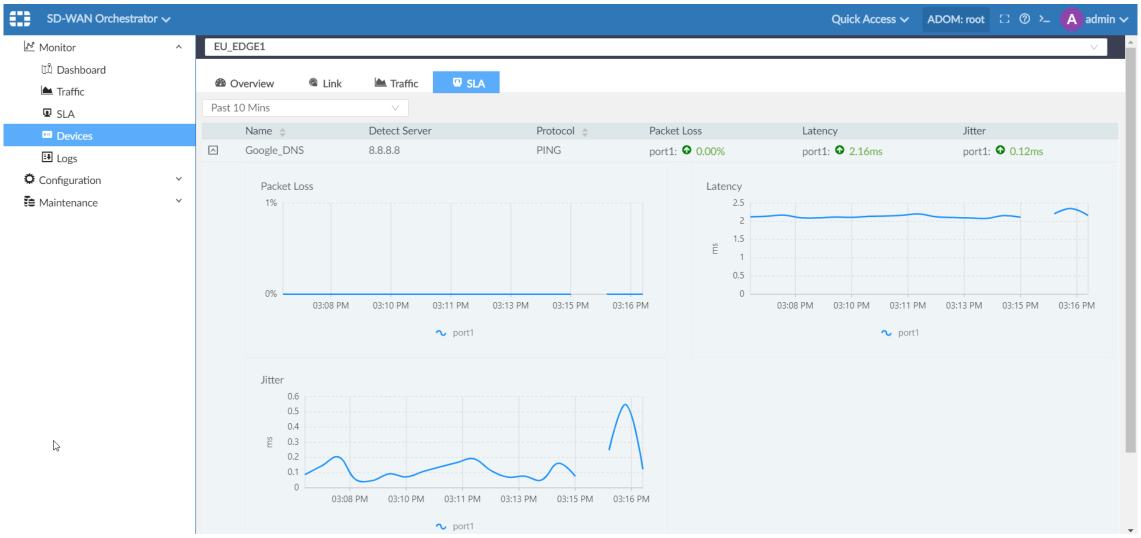
1. Go to *Monitor* > *Devices* > *Traffic*.
   The *Source* tab displays for the selected device. You can also click the *Destination*, *Application*, and *Cloud Application* tabs to display additional reports for the selected device.
   You can switch between devices by using the dropdown menu in the 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*.



Name	Detect Server	Protocol	Packet Loss	Latency	Jitter
Google_DNS	8.8.8.8	PING	port1: 0.00%	port1: 2.16ms	port1: 0.12ms

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 27
- Profile on page 36
- Shared resources on page 58
- Global routing on page 65

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 36.

This section contains the following topics:

- Adding devices on page 27
- Adding model devices on page 29
- Adding regions on page 30
- Adding unauthorized devices on page 31
- Installing configuration changes on page 31
- Importing devices on page 32
- Viewing configuration status on page 33
- Overriding device settings on page 33
- Adding static routes on page 34
- Updating regions on page 35
- Deleting regions on page 36
- Monitoring devices on page 36

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 36.
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, 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 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 36.
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.
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, 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.
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.
Device Name	Enter a name for the device.
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.
Enforce Firmware Version	(Optional) Select the required FortiOS version for the device when it comes online.

5. Click *OK*.

Adding regions

A region refers to a cluster of devices in one geographical location. Each region has one hub device that is connected to one or more edge devices.

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 36.
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.
New Name	(Optional) Type a name for 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 all devices in a region.	For a region name, click the *Install Region Configuration* button.
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.

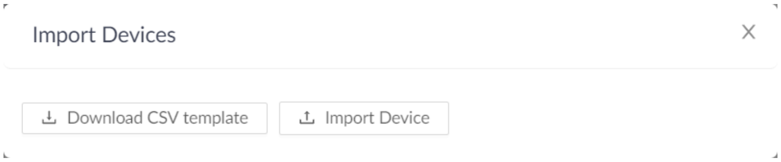
The CSV file uses the following fields:

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, 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 36.
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.

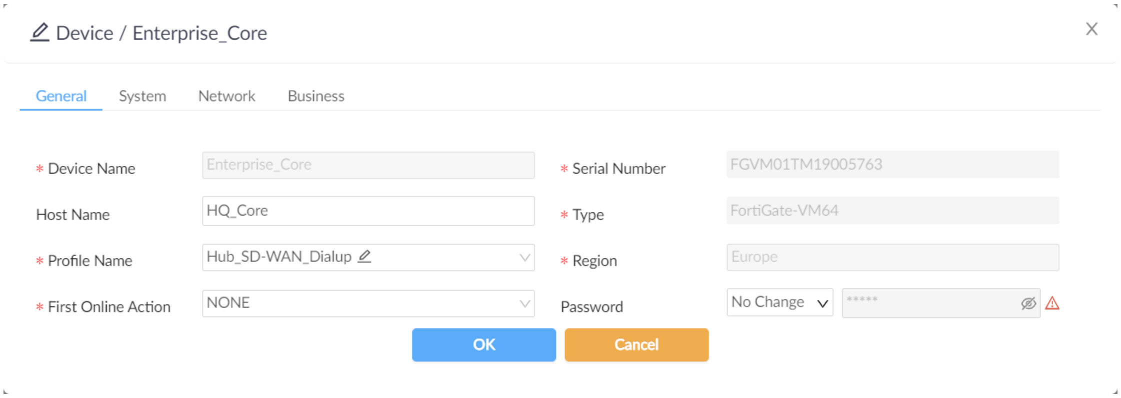
This topic describes how to override the NTP setting. You can also override network settings.

Any changes you make apply only to the device.

See also Adding static routes on page 34 and Creating business rules on page 51.

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.

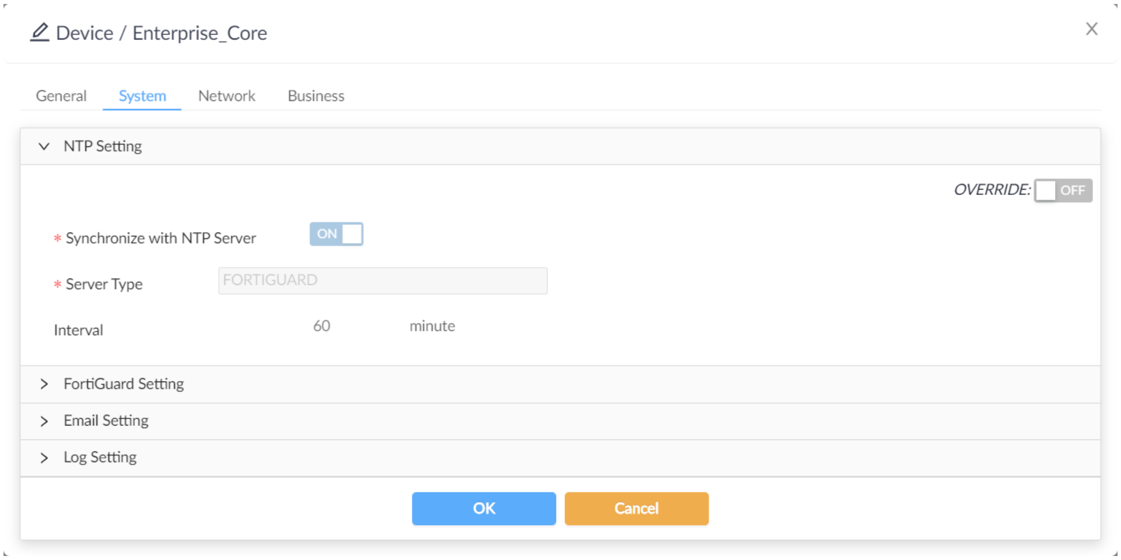


Device / Enterprise_Core

General | System | Network | Business

* Device Name	Enterprise_Core	* Serial Number	FGVM01TM19005763
Host Name	HQ_Core	* Type	FortiGate-VM64
* Profile Name	Hub_SD-WAN_Dialup	* Region	Europe
* First Online Action	NONE	Password	No Change *****

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



Device / Enterprise_Core

General | System | Network | Business

NTP Setting

OVERRIDE: OFF

* Synchronize with NTP Server	ON	
* Server Type	FORTIGUARD	
Interval	60	minute

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 31.

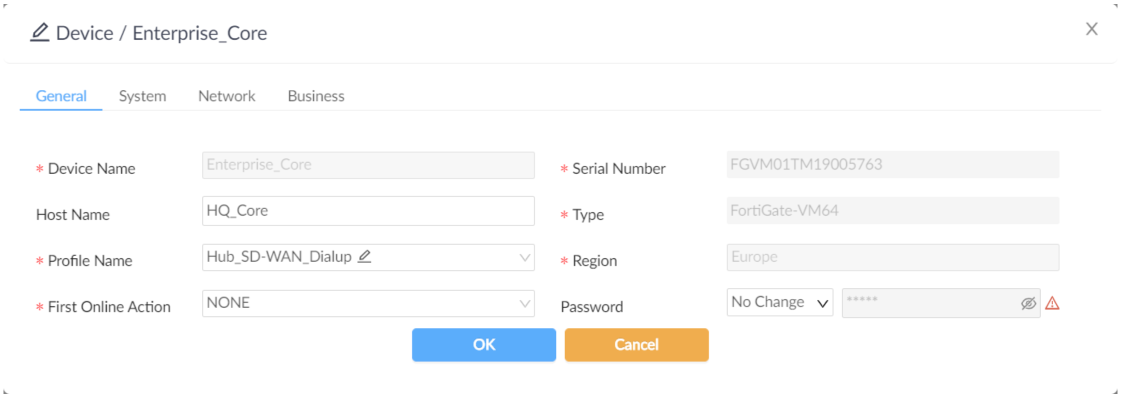
Adding static routes

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.

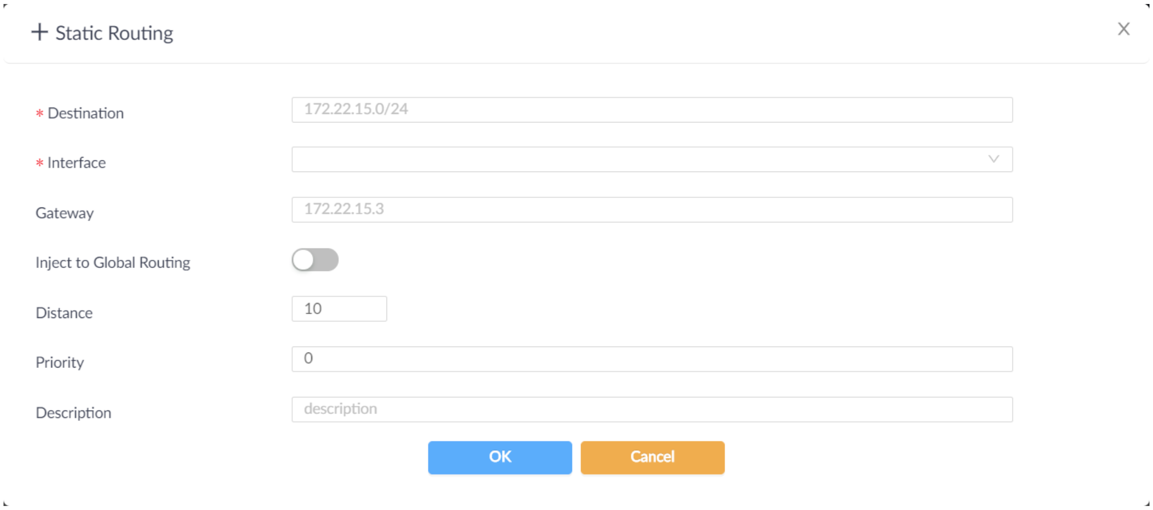
3. Double-click the device to open it for editing.
   The *Device / <name>* dialog box is displayed.



Device / Enterprise_Core

* Device Name	Enterprise_Core	* Serial Number	FGVM01TM19005763
Host Name	HQ_Core	* Type	FortiGate-VM64
* Profile Name	Hub_SD-WAN_Dialup	* Region	Europe
* First Online Action	NONE	Password	No Change *****

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



+ Static Routing

* Destination	172.22.15.0/24
* Interface	
Gateway	172.22.15.3
Inject to Global Routing	
Distance	10
Priority	0
Description	description

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 31.

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 31.

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, and 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.

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 new WAN settings on page 38
- Creating business rules on page 51
- Profile options described on page 53

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 58.

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.
Hub	Toggle on to designate the device as a hub.
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*, *Network*, and *Business* tabs, see Profile options described on page 53.
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 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 58.

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.
Hub	Toggle off to designate the device as an edge.
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.
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 53.
6. Click the *Network* tab to configure the network settings.
7. Click the *Business* tab to create business rules.
8. Click *OK*.

Creating new WAN settings

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

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 56.
4. Expand the *WAN* section, and click *+Create New*.
   The *WAN* dialog box is displayed.

Option	Description
Name	Type a name for the interface.
Port Type	Select the type of port.
Physical Port	Select the port number.
VLAN ID	Type an ID for the VLAN.
Enable	Toggle on to enable the interface. Toggle off to disable the interface.
ISP Link	Select an ISP link.
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: • *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.
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.
Mode	Select a mode.
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.

5. Complete the options, and click *OK*.
   The WAN settings are created.

Creating new LAN settings

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

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 56.
4. Expand the *LAN* section, and click +*Create New*.
   The *LAN* dialog box is displayed.

Option	Description
Name	Type a name for the interface.
Port Type	Select the type of port.
Physical Port	Select the port number.
Allow Overlap Between Devices	Toggle on to allow overlap between devices. Toggle off to disable this feature.
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.
VLAN ID	Available when *Allow Overlap Between Devices* is enabled.
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.

5. Complete the options, and click *OK*.
   The WAN settings are created.

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.

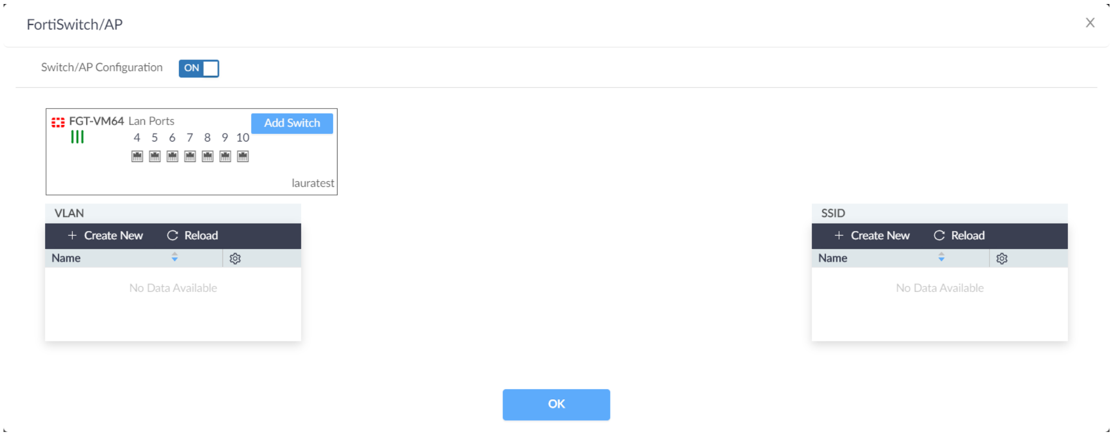
Do not connect FortiSwitch to the physical FortiGate port until the FortiSwitch profile is installed. See Install a profile on a device.

If FortiSwitch is already connected to FortiGate:

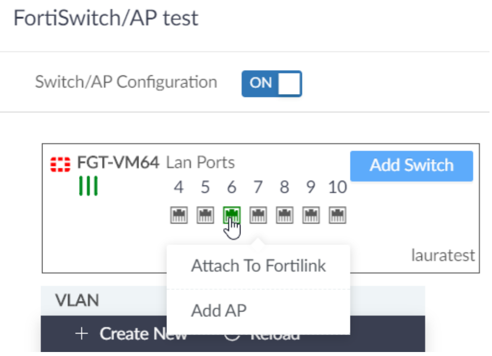
Configure and install the profile without FortiLink and FortiSwitch first. After the profile has successfully synchronized with FortiGate, add the FortiLink and FortSwitch configuration, and then install the profile again.

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 56.
   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*.

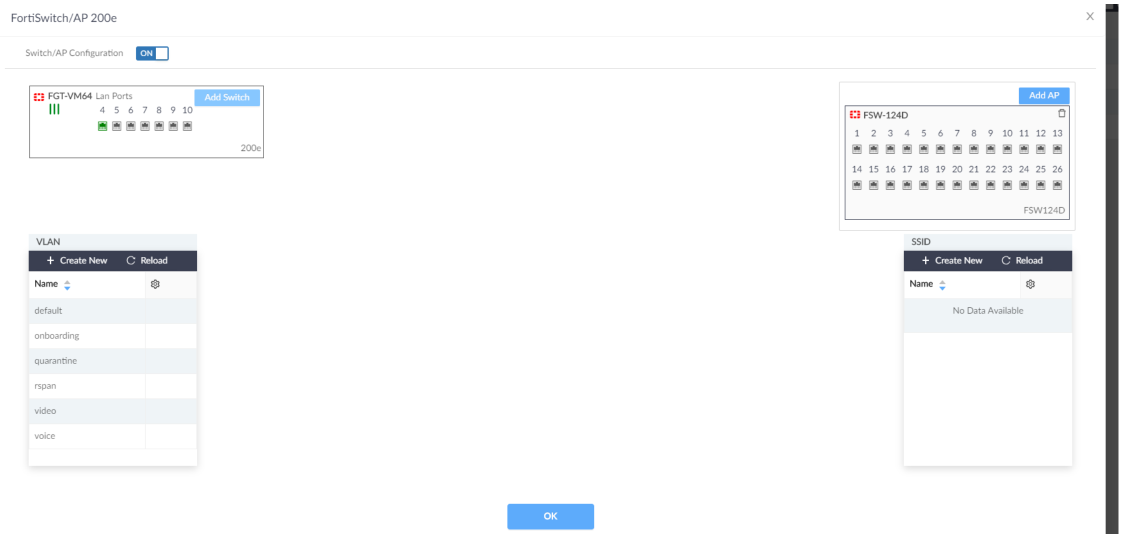


   The port is attached, and the VLAN settings are created.
5. Add a platform model.
   a. Click *Add Switch*.
   b. In the *Name* field, enter a name for the FortiSwitch.

c. From the *Platform* dropdown, select a FortiSwitch model.

d. Click *OK*.

The switch is added to the profile.



Switch/AP Configuration ON

Name
default
onboarding
quarantine
rspan
video
voice

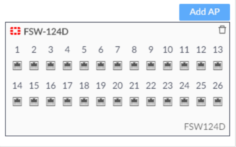
Name
No Data Available

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.



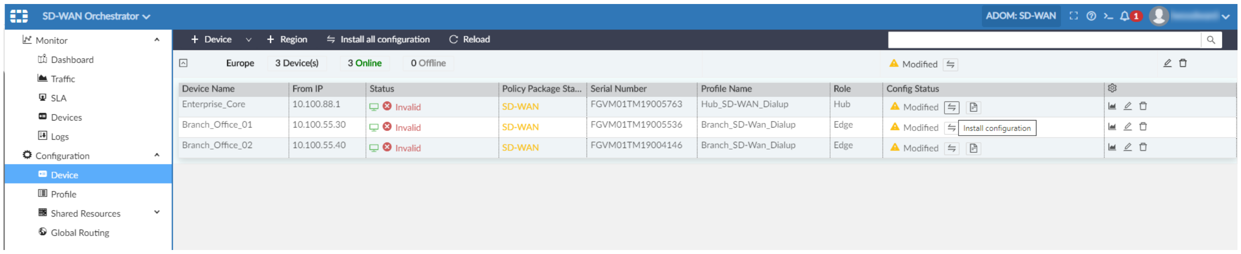
   The *More Configuration/ <port>* dialog box is displayed.

   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.
Lldp 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*.



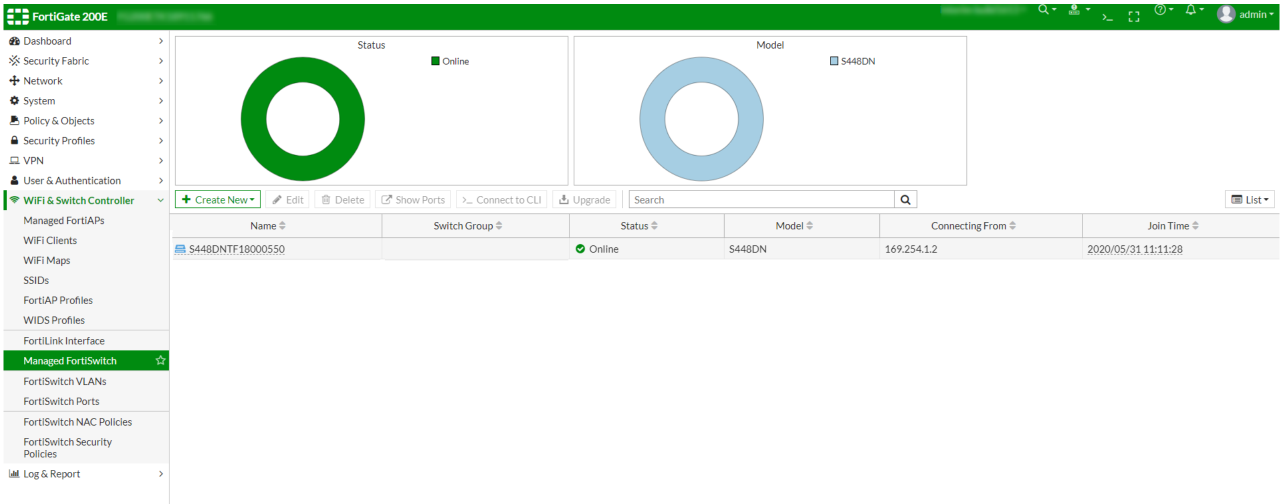
Device Name	From IP	Status	Policy Package Sta...	Serial Number	Profile Name	Role	Config Status
Enterprise_Core	10.100.88.1	Invalid	SD-WAN	FGVM01TM19005763	Hub_SD-WAN_Dialup	Hub	Modified
Branch_Office_01	10.100.55.30	Invalid	SD-WAN	FGVM01TM19005536	Branch_SD-Wan_Dialup	Edge	Modified
Branch_Office_02	10.100.55.40	Invalid	SD-WAN	FGVM01TM19004146	Branch_SD-Wan_Dialup	Edge	Modified

   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.

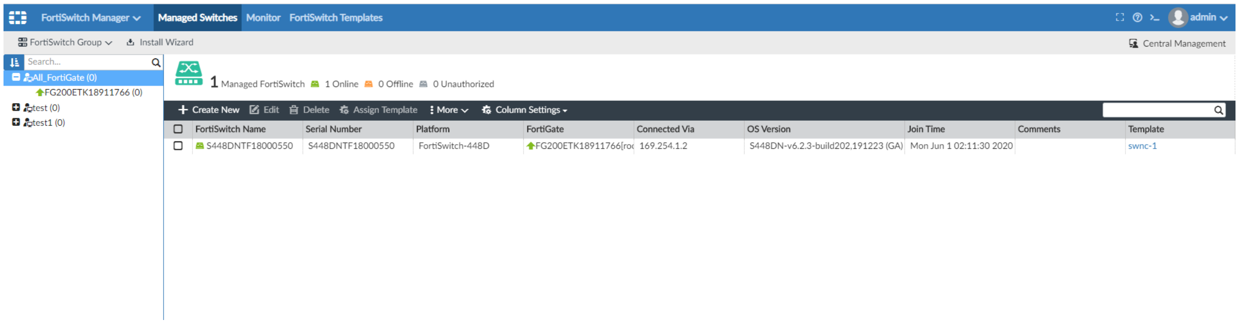
To verify the connection:

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



Name	Switch Group	Status	Model	Connecting From	Join Time
S448DNTF18000550		✓ Online	S448DN	169.254.1.2	2020/05/31 11:11:28

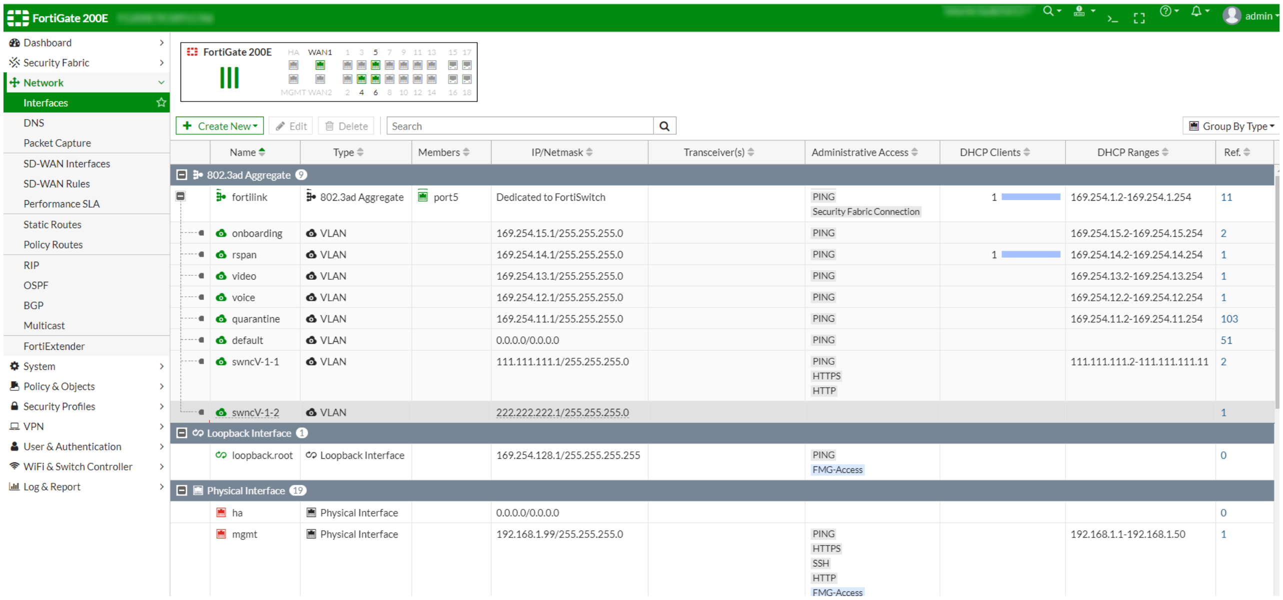
2. On FortiManager, go to *FortiSwitch Manager* > *Managed Switches* > *All_FortiGate* and select a device in the tree menu.
   Check the *FortiSwitch Name* column to verify the device is online.



□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Join Time	Comments	Template
□	S448DNTF18000550	S448DNTF18000550	FortiSwitch-448D	FG200ETK18911766[ro	169.254.1.2	S448DN-v6.2.3-build202,191223 (GA)	Mon Jun 1 02:11:30 2020		swnc-1

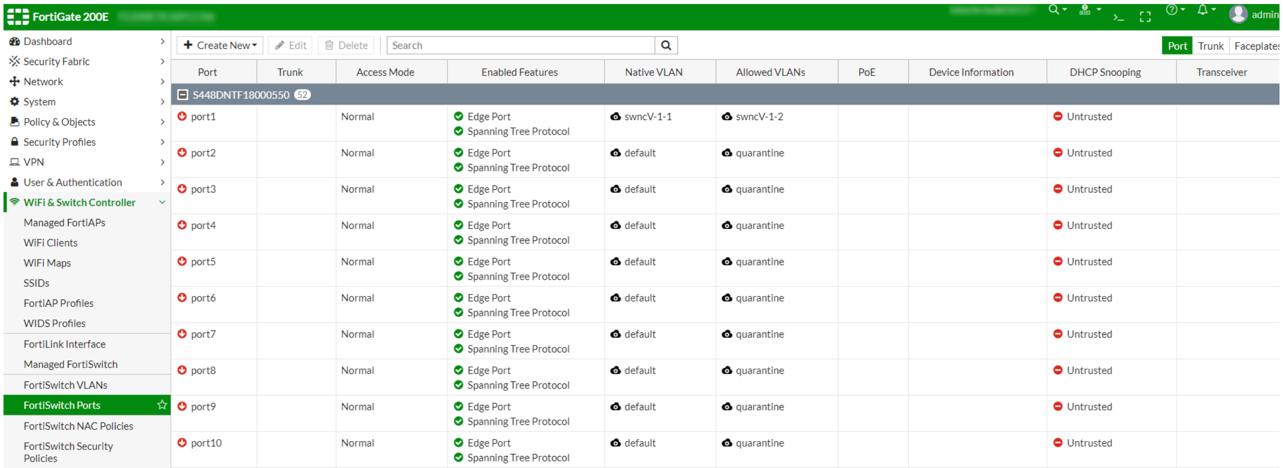
To verify the device received the configuration:

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.



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 9								
fortilink	802.3ad Aggregate	port5	Dedicated to FortiSwitch		PING Security Fabric Connection	1	169.254.1.2-169.254.1.254	11
onboarding	VLAN		169.254.15.1/255.255.255.0		PING		169.254.15.2-169.254.15.254	2
rspan	VLAN		169.254.14.1/255.255.255.0		PING	1	169.254.14.2-169.254.14.254	1
video	VLAN		169.254.13.1/255.255.255.0		PING		169.254.13.2-169.254.13.254	1
voice	VLAN		169.254.12.1/255.255.255.0		PING		169.254.12.2-169.254.12.254	1
quarantine	VLAN		169.254.11.1/255.255.255.0		PING		169.254.11.2-169.254.11.254	103
default	VLAN		0.0.0.0/0.0.0.0		PING			51
swncV-1-1	VLAN		111.111.111.1/255.255.255.0		PING HTTPS HTTP		111.111.111.2-111.111.111.11	2
swncV-1-2	VLAN		222.222.222.1/255.255.255.0					1
Loopback Interface 1								
loopback.root	Loopback Interface		169.254.128.1/255.255.255.255		PING FMG-Access			0
Physical Interface 19								
ha	Physical Interface		0.0.0.0/0.0.0.0					0
mgmt	Physical Interface		192.168.1.99/255.255.255.0		PING HTTPS SSH HTTP FMG-Access		192.168.1.1-192.168.1.50	1

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.



Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver
S448DNTF18000550 52									
port1		Normal	Edge Port Spanning Tree Protocol	swncV-1-1	swncV-1-2			Untrusted	
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port8		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port9		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	
port10		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted	

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.

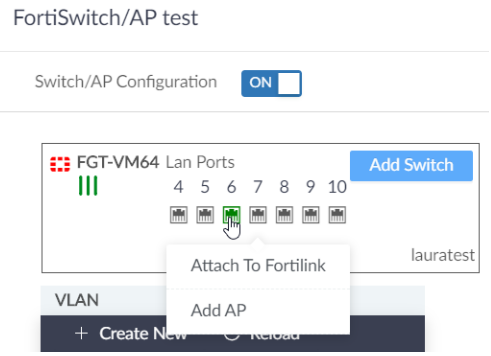
Requirements:

Connect the FortiAP LAN port to the target FortiGate port.

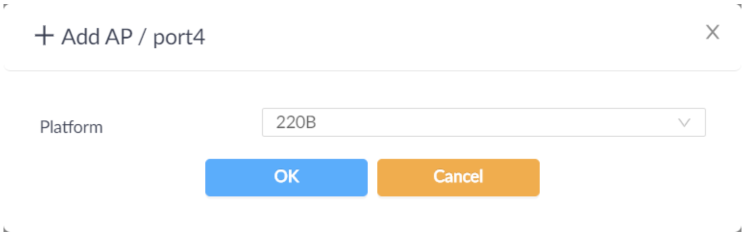
To add a model FortiAP to a FortiGate:

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

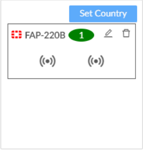
3. Display the FortiSwitch/AP settings.
   a. Click the *Network* tab.
   b. Expand the *LAN* section, and click *Switch/AP*.
      The *FortiSwitch/AP <Name>* dialog box is displayed.
4. Select a FortiGate port, and click *Add AP*.



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



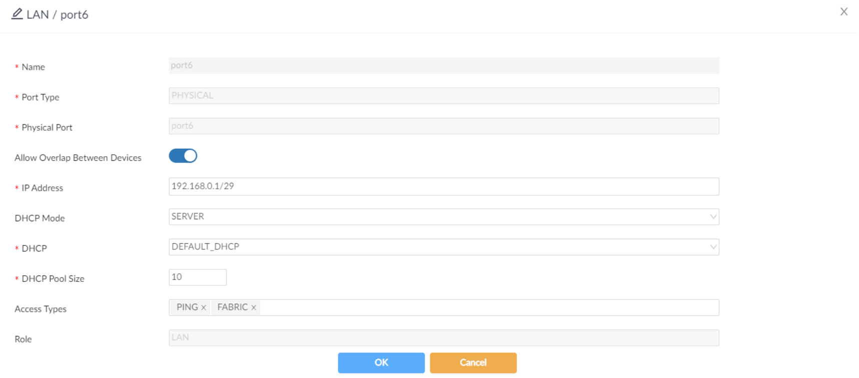
6. Click *OK*.
   The AP model is added to the profile.



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.

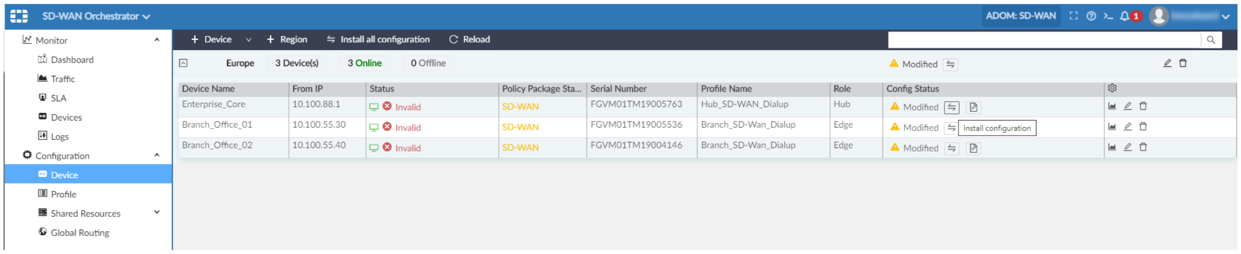
e. Configure the DHCP settings, and click *OK*



* Name	port6
* Port Type	PHYSICAL
* Physical Port	port6
Allow Overlap Between Devices	●
* IP Address	192.168.0.1/29
DHCP Mode	SERVER
* DHCP	DEFAULT_DHCP
* DHCP Pool Size	10
Access Types	PING × FABRIC ×
Role	LAN

f. Click OK again.

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



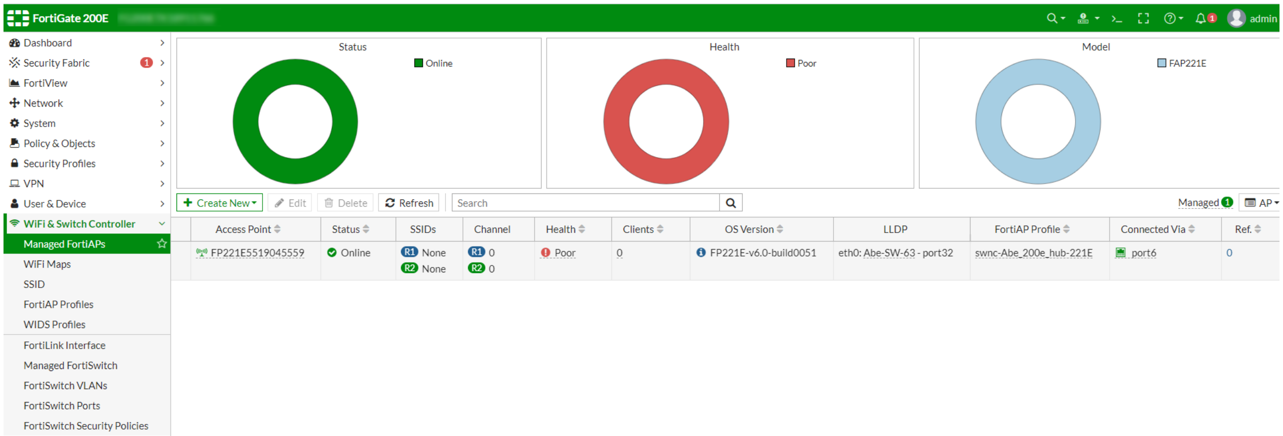
Device Name	From IP	Status	Policy Package Sta...	Serial Number	Profile Name	Role	Config Status
Enterprise_Core	10.100.88.1	Invalid	SD-WAN	FGVM01TM19005763	Hub_SD-WAN_Dialup	Hub	Modified
Branch_Office_01	10.100.55.30	Invalid	SD-WAN	FGVM01TM19005536	Branch_SD-Wan_Dialup	Edge	Modified
Branch_Office_02	10.100.55.40	Invalid	SD-WAN	FGVM01TM19004146	Branch_SD-Wan_Dialup	Edge	Modified

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.

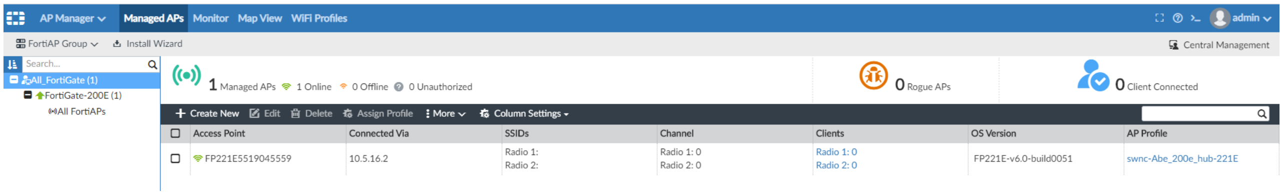


Access Point	Status	SSIDs	Channel	Health	Clients	OS Version	LLDP	FortiAP Profile	Connected Via	Ref.
FP221E5519045559	Online	R1 None R2 None	R1 0 R2 0	Poor	0	FP221E-v6.0-build0051	eth0: Abe-SW-63 - port32	swnc-Abe_200e_hub-221E	port6	0

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.



☐	Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
☐	FP221E5519045559	10.5.16.2	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	FP221E-v6.0-build0051	swnc-Abe_200e_hub-221E

To add an SSID profile to a ports AP profile:

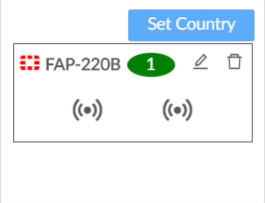
1. In the SSID table, create a new profile or select a profile to update.
   The *+SSID* dialog box is displayed.
2. Configure the SSID settings, and click *OK*.

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*.



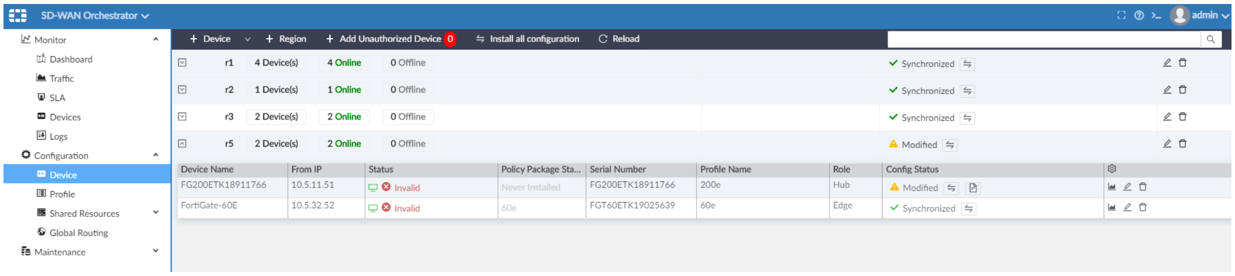
The *AP<Name>* dialog box is displayed.

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*.



r1	4 Device(s)	4 Online	0 Offline	✓ Synchronized
r2	1 Device(s)	1 Online	0 Offline	✓ Synchronized
r3	2 Device(s)	2 Online	0 Offline	✓ Synchronized
r5	2 Device(s)	2 Online	0 Offline	⚠ Modified

Device Name	From IP	Status	Policy Package Sta...	Serial Number	Profile Name	Role	Config Status
FG200ETK18911766	10.5.11.51	✕ Invalid	Never Installed	FG200ETK18911766	200e	Hub	⚠ Modified
FortiGate-60E	10.5.32.52	✕ Invalid	60e	FGT60ETK19025639	60e	Edge	✓ Synchronized

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 56.
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.
Physical Port	Select the port number.
VLAN ID	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.

Creating business rules

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

To create a business rule:

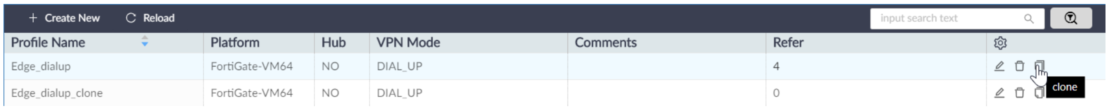
1. Go to *Configuration > Profile*.
   The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
   The *Profile <name>* dialog box is displayed.
3. Click the *Business* tab.
   The *Business* pane is displayed.
4. Click +*Create New*.
   The *Business Rule* dialog box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

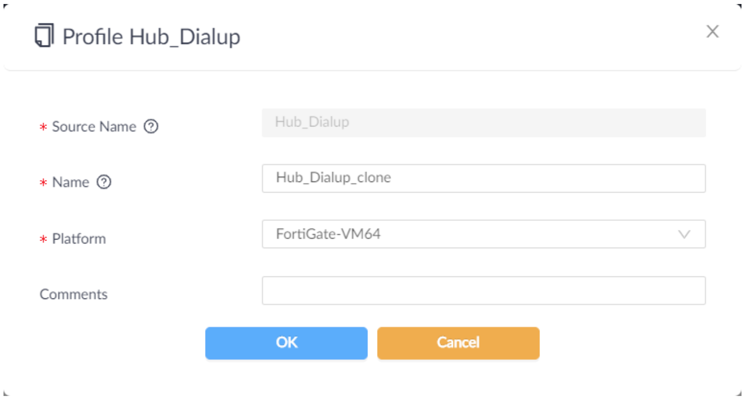
To clone profiles:

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



Profile Name	Platform	Hub	VPN Mode	Comments	Refer
Edge_dialup	FortiGate-VM64	NO	DIAL_UP		4
Edge_dialup_clone	FortiGate-VM64	NO	DIAL_UP		0

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



* Source Name: Hub_Dialup

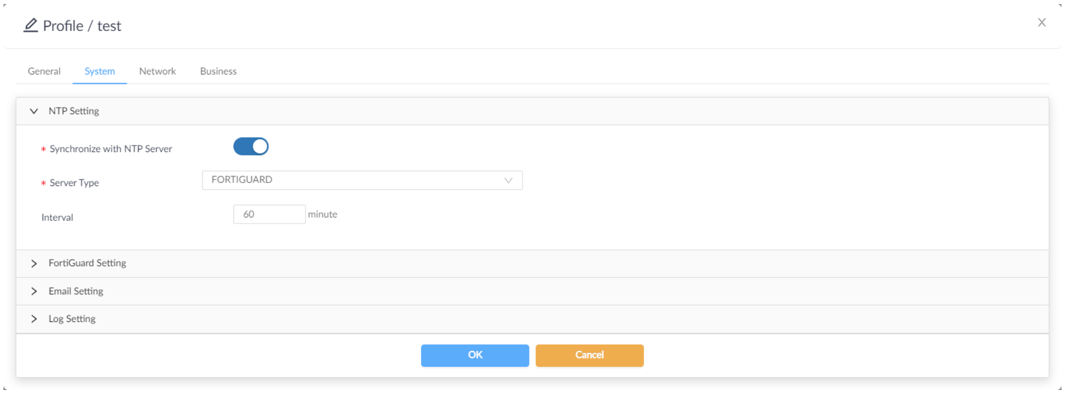
* Name: Hub_Dialup_clone

* Platform: FortiGate-VM64

Comments:

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.



* Synchronize with NTP Server: on

* Server Type: FORTIGUARD

Interval: 60 minute

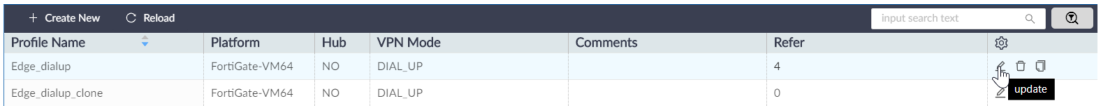
4. Set the options on the *System*, *Network*, and *Business* tabs, and click *OK*.

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.



Profile Name	Platform	Hub	VPN Mode	Comments	Refer
Edge_dialup	FortiGate-VM64	NO	DIAL_UP		4
Edge_dialup_clone	FortiGate-VM64	NO	DIAL_UP		0

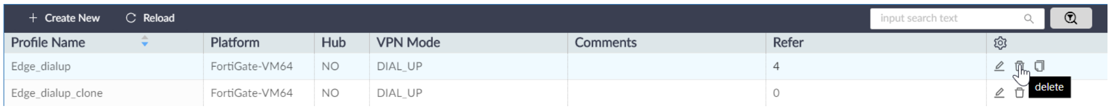
   The *Profile <name>* dialog box opens.
3. Edit the settings, and click *OK*.
4. Install profile changes. See Installing configuration changes on page 31.

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.



Profile Name	Platform	Hub	VPN Mode	Comments	Refer
Edge_dialup	FortiGate-VM64	NO	DIAL_UP		4
Edge_dialup_clone	FortiGate-VM64	NO	DIAL_UP		0

   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 53
- System tab on page 54
- Network tab on page 56
- Business tab on page 58

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.
Hub	Toggle on to designate the device as a hub. Toggle off to designate the device as an edge.
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 54
- FortiGuard on page 54
- Email on page 55
- Log on page 55

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

WAN

Expand *WAN* to view the following options:

Option	Description
Create New	Click *Create New* to define a new WAN interface.
Interface	Displays the interface name.
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.
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 interface members.

Option	Description
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.
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
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 DMZ 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.
Hosts	

Business tab

The *Business* tab contains the following options:

Option	Description
Create New	Click *Create New* to create a new business rule.
Name	Displays the name of the business rule.
Valid	Displays whether the rule is valid. A checkmark indicates a valid rule.
Source Address	Displays the source address or address group.
Destination Type	Displays the type of destination for the traffic.
Service	Displays the Internet service.
Group Type	For hub devices, choose from UNDERLAY or OVERLAY. For edge devices, choose from UNDERLAY, OVERLAY, or ALL.
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.
Path	When *Group Type* is set to *Overlay*, displays the path.
SLA Server Type	When *Group Type* is set to *Overlay*, select the type of SLA server.
Backhaul to Group	When *Group Type* is set to *Overlay* for hub devices, choose the backhaul route to the group.
SLA Quality Level	Displays the minimum quality level.

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 59
- Creating DHCP relays on page 60
- Creating DNS servers on page 60
- Creating intranet IP pools on page 60
- Creating SNMP hosts on page 61
- Changing VPN address pools on page 61
- Creating ISP links on page 61

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.
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 VPN address pools

To change the VPN address pools:

1. Go to *Configuration* > *Shared Resources* > *Network* > *Network Settings*.
   The VPN address pool information is displayed.
2. Configure the settings, and click *OK*.

Option	Description
VPN Addr Pool	Enter the IP address for the address pool.
Loopback Address Pool	Enter the IP address for the loopback address pool.
Auth After Location Change	Toggle *On* to authorize the address change.

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 62
- Adding SLA servers on page 63

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 63
- Adding FortiGuard servers on page 64
- Adding email servers on page 64

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 66.
- Back up and restore configurations for SD-WAN Orchestrator MEA. See Configuration on page 66.
- Export a zip file of debug information for SD-WAN Orchestrator MEA. See Debug on page 67.

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.