

Administration Guide

SD-WAN Orchestrator MEA 7.0.0.r3



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/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 24, 2021

SD-WAN Orchestrator MEA 7.0.0.r3 Administration Guide

02-700r3-715824-20210824

TABLE OF CONTENTS

Change Log	7
Introduction	8
Simplified SD-WAN deployment	8
SD-WAN Orchestrator MEA use cases	9
Key concepts	9
FortiGate devices	10
Regions and links	10
Normalized interfaces	12
Underlay and overlay links	12
Profiles	12
Configuration installation	12
Global routing	12
Global analysis and visibility	13
Device analysis and visibility	13
Business rules	13
High availability	13
How SD-WAN Orchestrator MEA works with FortiManager	13
Quick start	15
Enabling SD-WAN Orchestrator MEA	15
Planning your network	16
Creating shared resources	16
Creating profiles for all roles	16
Adding devices to FortiManager	17
Adding devices to SD-WAN Orchestrator MEA and installing configurations	17
Installing firewall policies	17
Monitoring devices and network traffic	18
Monitor	19
Monitor status	19
Dashboard	21
Viewing devices on the world map	22
Viewing device topology	22
Viewing shortcut overlays (ADVPN)	23
Viewing hub devices	23
Viewing regions	24
Traffic	26
Viewing global network traffic reports	26
Exporting global traffic reports	27
SLA	28
Devices	29
Viewing device overviews	29
Viewing device link reports	30
Viewing device traffic reports	31
Viewing device SLA	31

Viewing device local branches	32
Logs	32
Configuration	34
Device	34
Adding devices	35
Adding VDOMs	36
Adding devices in HA clusters	38
Adding model devices	38
Adding model devices in HA clusters	40
Adding regions	41
Adding unauthorized devices	43
Adding FortiExtenders to online devices	43
Adding devices with authorized FortiExtenders	45
Synchronizing with FortiManager	47
Installing configuration changes	48
Importing devices	48
Viewing configuration status	49
Overriding device settings	50
Adding static routes	51
Creating BGP neighbors	52
Adding IP pool to LAN port configuration	53
Executing WAN port speed tests	54
Updating regions	56
Deleting regions	56
Monitoring devices	56
Replacing FortiGate serial numbers	56
Profile	57
Creating profiles for hub devices	58
Creating profiles for edge devices	60
Creating profiles for VDOMs	60
Creating profiles with FortiExtender WAN ports	61
Creating profiles for HA devices	63
Adding physical interfaces for VDOMs	63
Creating new WAN settings	65
Creating new LAN settings	68
Attaching a FortiSwitch model to FortiGate	71
Adding a FortiAP model device	76
Creating new DMZ settings	81
Creating virtual wire pairs	83
Creating new BGP network	83
Creating new OSPF area	84
Creating business rules	85
Cloning profiles	87
Updating profiles	88
Deleting profiles	89
Profile options described	89
Shared resources	97
Intranet IP pool addresses	98

Address group change	98
Network	99
SLA	107
System	108
Health Threshold	111
Global routing	111
Maintenance	113
Upgrade	113
Configuration	113
Debug	114
More information	115
Appendix A - managed FortiGate CLI objects and attributes	116
extender-controller	117
config extender-controller dataplan	117
config extender-controller extender	117
firewall	118
config firewall address	118
config firewall addgrp	119
log	119
config log fortianalyzer setting	119
config log syslogd filter	120
config log syslogd setting	120
router	120
config router bgp	121
config router community-list	122
config router ospf	123
config router policy	125
config router prefix-list	125
config router route-map	126
config router static	126
system	126
config system admin	127
config system central-management	127
config system dhcp server	128
config system dns	129
config system email-server	129
config system fortiguard	129
config system global	130
config system ha	130
config system interface	130
config system ntp	131
config system sdwan	132
config system snmp community	134
config system snmp sysinfo	134
config system snmp user	135
config system settings	135
config system switch-interface	135

config system virtual-switch	136
vpn	136
config vpn ipsec phase1-interface	136
config vpn ipsec phase2-interface	137
wireless-controller	137
config wireless-controller vap	137
Appendix B - REST API	139
Setting up an API user	139
Logging in to the REST API	140

Change Log

Date	Change Description
2021-08-24	Initial release of 7.0.0.r3.

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 7.0.0.r3 requires FortiManager 7.0.0 or later, and you must be in a 6.4 ADOM or later 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 7.0.0.r3 Release Notes](#) on the [Docs Library](#). The release notes also identify any limitations of SD-WAN Orchestrator MEA.

This section contains the following topics:

- [Simplified SD-WAN deployment on page 8](#)
- [SD-WAN Orchestrator MEA use cases on page 9](#)
- [Key concepts](#)
- [How SD-WAN Orchestrator MEA works with FortiManager](#)

Simplified SD-WAN deployment

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

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

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

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

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

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

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

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

SD-WAN Orchestrator MEA use cases

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

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

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

	FortiManager SD-WAN	SD-WAN Orchestrator MEA
Strengths	<ul style="list-style-type: none"> • Full SD-WAN feature set • Scales to 10K plus sites • No additional license required 	<ul style="list-style-type: none"> • VPN overlay and routing automatically configured • Simplified provisioning workflow • Better SD-WAN charts and graphs
Limitations	<ul style="list-style-type: none"> • VPN and routing need separate configurations 	<ul style="list-style-type: none"> • Supports up to 1000 sites • Does not expose all configurations • Flexible per appliance license
Best suited to	<ul style="list-style-type: none"> • Large, complex SD-WAN deployments • Customers requiring advanced WAN remediation • NOC and SOC team collaboration • Large enterprise, MSSP, and carrier customers 	<ul style="list-style-type: none"> • Simple SD-WAN deployments • Customers looking for intelligent traffic steering • Mid-sized enterprise customers

Key concepts

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

- [FortiGate devices on page 10](#)
- [Regions and links on page 10](#)
- [Normalized interfaces on page 12](#)
- [Underlay and overlay links on page 12](#)

- [Profiles on page 12](#)
- [Configuration installation on page 12](#)
- [Global routing on page 12](#)
- [Global analysis and visibility on page 13](#)
- [Device analysis and visibility on page 13](#)
- [Business rules on page 13](#)
- [High availability on page 13](#)

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 13](#).

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 38](#) and [Importing devices on page 48](#).

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

Regions and links

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

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

Links between hub devices

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

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

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

Links between hub and edge devices in the same region

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

- Site-to-site VPN
- Dialup VPN
- Dialup full-mesh VPN

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

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

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

When overlay links between edge devices and the primary hub are down, links between the edge device and the secondary hub are used to forward traffic. However when a business rule has the *Dual Hub Load Mode* option set to *ACTIVE_ACTIVE*, the links between the edge device and the secondary hub might be used, even if the links between the edge device and the primary hub are up.

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

Edge device communication between regions

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

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

Normalized interfaces

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

- overlay_edge2hub
- overlay_hub2edge
- overlay_hub2hub
- underlay
- sdwan_loopback

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

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

Underlay and overlay links

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

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

You specify underlay and overlay links when you configure profiles.

Profiles

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

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



You can override profile settings for individual devices.

Configuration installation

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

Global routing

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

Global analysis and visibility

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

Device analysis and visibility

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

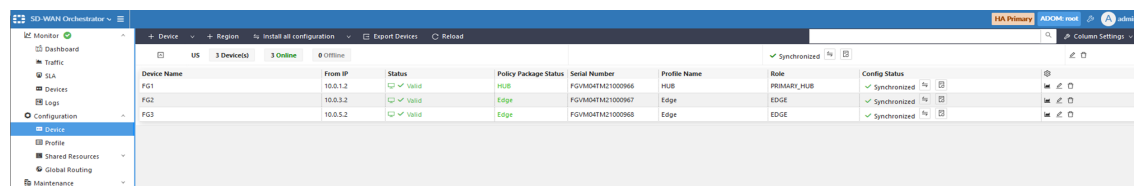
Business rules

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

High availability

SD-WAN Orchestrator MEA supports high availability (HA) to provide a solution for a key requirement of critical enterprise management and enhanced networking reliability. When two or more FortiManager units are configured in an HA cluster, and SD-WAN Orchestrator MEA is enabled on each FortiManager, and the versions of FortiManager and SD-WAN Orchestrator MEA are the same on the primary unit and secondary units, HA will negotiate successfully and synchronize configuration from primary to secondary.

The top-right corner of SD-WAN Orchestrator MEA banner displays *HA Primary* to identify the primary SD-WAN Orchestrator MEA, for example:



Device Name	From IP	Status	Policy Package Status	Serial Number	Profile Name	Role	Config Status
FG1	10.0.1.2	Valid	HUB	FGV8M4TAC1000966	HUB	PRIMARY_HUB	✓ Synchronized
FG2	10.0.3.2	Valid	Edge	FGV8M4TAC1000967	Edge	EDGE	✓ Synchronized
FG3	10.0.5.2	Valid	Edge	FGV8M4TAC1000968	Edge	EDGE	✓ Synchronized

How SD-WAN Orchestrator MEA works with FortiManager

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

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

1. SD-WAN Orchestrator MEA automatically generates CLI scripts of the configuration.
You can view the scripts in FortiManager on the *Device Manager > Scripts* pane.
2. SD-WAN Orchestrator MEA installs the CLI scripts to the *Device Manager* database in FortiManager.

3. FortiManager receives the CLI scripts, and FortiManager installs the configurations to the FortiGates. When the configuration is installed to FortiGates, the overlay and underlay links between all devices in the SD-WAN network are automatically created.

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

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

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

Quick start



SD-WAN Orchestrator MEA is a flexible application. Although you must add FortiGate devices to both SD-WAN Orchestrator MEA and FortiManager, you can add the devices using several different methods, depending on need. This section describes one method, which is to add the FortiGate device to FortiManager first, and then add the device to SD-WAN Orchestrator MEA second. See also [FortiGate devices on page 10](#).

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 15](#).
2. Plan your SD-WAN network. See [Planning your network on page 16](#).
3. Create shared resources. See [Creating shared resources on page 16](#).
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 17](#).
6. Add devices to SD-WAN Orchestrator MEA and install SD-WAN configurations. See [Adding devices to FortiManager on page 17](#).
7. Install firewall policies to FortiGate devices in SD-WAN networks. See [Installing firewall policies on page 17](#).
8. Monitor the SD-WAN network. See [Monitoring devices and network traffic on page 18](#).

Enabling SD-WAN Orchestrator MEA

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



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

To enable SD-WAN Orchestrator MEA:

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



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

Planning your network

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

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

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

Creating shared resources

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

- **Network resources**, such as DHCP servers, DHCP relays, DNS servers, intranet IP pools, SNMP hosts, and VPN address pools.
It is recommended to create intranet IP pools that SD-WAN Orchestrator MEA can use when it creates the SD-WAN network for selected devices.
ISP links are automatically created when a WAN port is enabled in a profile.
- **Service level agreements (SLA)**, such as quality levels and servers.
- **Servers**, such as NTP, FortiGuard, and email, that SD-WAN Orchestrator MEA can use.
- **Health threshold settings**

For more details, see [Shared resources on page 97](#).

Creating profiles for all roles

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

- Profile for primary hub devices and secondary hub devices - see [Creating profiles for hub devices on page 58](#)
- Profile for edge devices - see [Creating profiles for edge devices on page 60](#)

See also [Profile on page 57](#).

Adding devices to FortiManager

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

Adding devices to SD-WAN Orchestrator MEA and installing configurations

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

Following is a summary of the process:

1. Ensure that you have created profiles for hub and edge devices.
You should create a profile for the primary hub role and a profile for the edge role. If you are using secondary hub devices, ensure you have created a profile for the secondary hub role too.
2. Ensure that you have added FortiGate devices to FortiManager.
3. Add the FortiGate devices to SD-WAN Orchestrator MEA by adding a region.
When you add a region to SD-WAN Orchestrator MEA, you can specify a region name, and select the devices for hub and edge roles. You can also select profiles for each device in the region, and select an IPsec template for 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 13](#).
For more details about adding devices, see [Device on page 34](#).
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 19](#).

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 21](#), [Traffic on page 26](#) and [SLA on page 28](#).
- For device analysis and visibility, see [Devices on page 29](#).

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:

- [Monitor status on page 19](#)
- [Dashboard on page 21](#)
- [Traffic on page 26](#)
- [SLA on page 28](#)
- [Devices on page 29](#)
- [Logs on page 32](#)

Monitor status

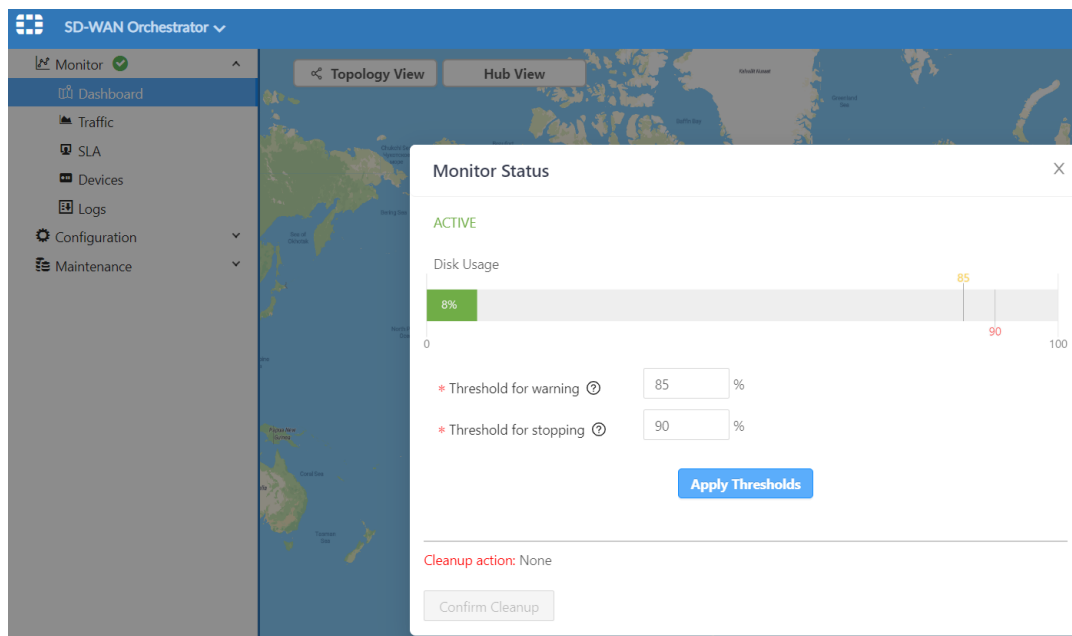
A status icon displays beside the *Monitor* tree menu to indicate one of the following monitoring statuses:

- Active (checkmark in green circle) - Monitoring is active and operating below the disk usage warning threshold. No cleanup is required.
- Warning (exclamation mark in yellow triangle) - Monitoring is active, but disk usage has passed the warning threshold. Click *Confirm Cleanup* to clear old monitoring data and reduce disk usage.
- Stopping (vertical lines in red circle) - Monitoring is stopped because disk usage has passed the stopping threshold. You must manually check disk usage.

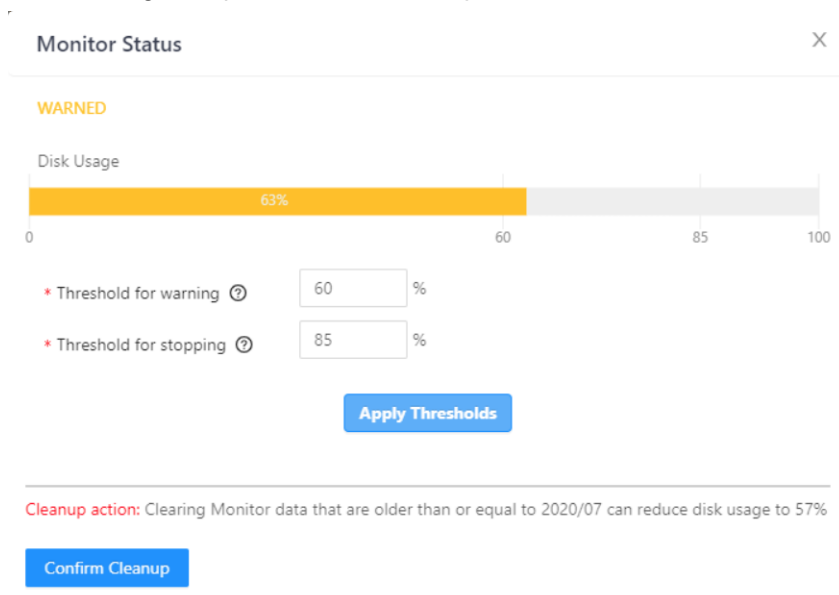
You can adjust the warning and stopping thresholds.

To view Monitor status details:

1. Go to *Monitor*, and click the status icon in the tree menu.
In the following example, the *Active* status is indicated by a checkmark in a green circle. Click the checkmark to display the *Monitor Status* dialog box.



The following example shows the *Warning* status.



The following example shows the *Stopping* status.

Monitor Status [X]

STOPPED

Disk Usage

0 60 85 100

99%

* Threshold for warning ⓘ 60 %

* Threshold for stopping ⓘ 85 %

Apply Thresholds

Cleanup action: Even if clearing all Monitor data, the disk usage will still be greater than the collector warning threshold. Please check the disk usage manually.

Confirm Cleanup

2. In the *Threshold for warning* and *Threshold for stopping* boxes, type new numbers, and click *Apply Thresholds* to change the warning and stopping thresholds.
3. When available, click *Confirm Cleanup* to clear old monitoring data and reduce disk usage.
4. Click *X* to close the dialog box.

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 22](#)
- [Viewing device topology on page 22](#)
- [Viewing shortcut overlays \(ADVPN\) on page 23](#)
- [Viewing hub devices on page 23](#)
- [Viewing regions on page 24](#)

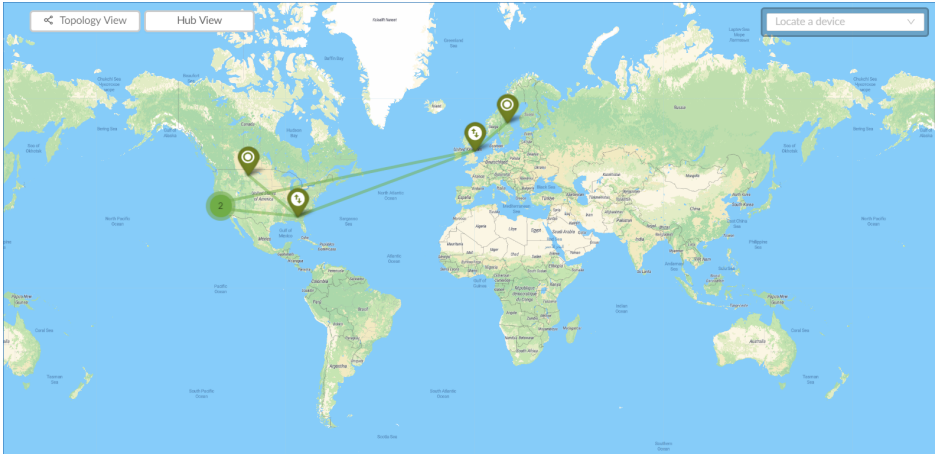


When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the maps. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

If you want to view details about individual devices in the SD-WAN network, see [Devices on page 29](#).

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.



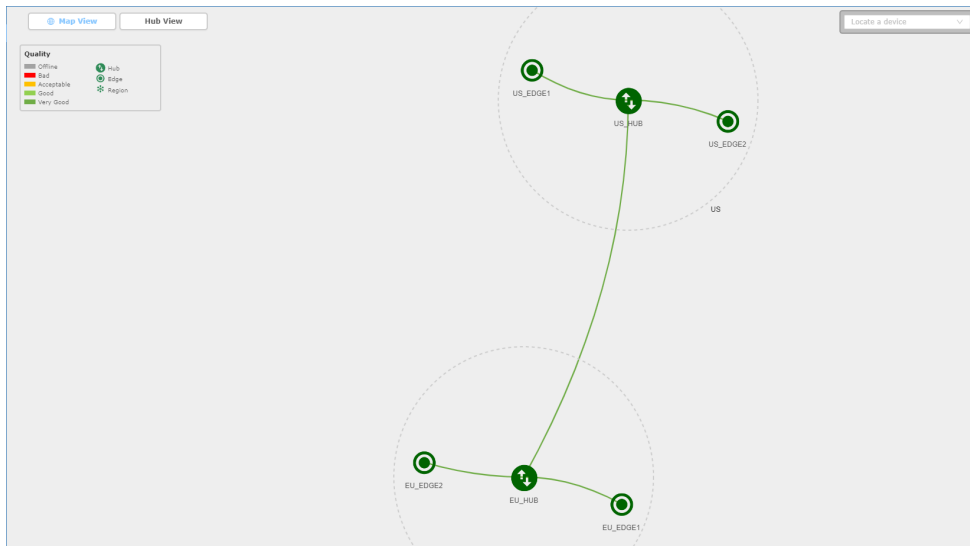
Viewing device topology

The *Topology View* displays all connected devices across the globe in the SD-WAN network, regardless of geographical distance. Any unknown peers are also displayed.

To view device topology:

1. Go to *Monitor > Dashboard*, and click *Topology View* at the top of the map.

The following example shows the topology view of two regions and two hubs. The color shows the quality, and the lines show the VPN tunnels between the devices. The width of the lines indicates the amount of traffic passing through the tunnel.



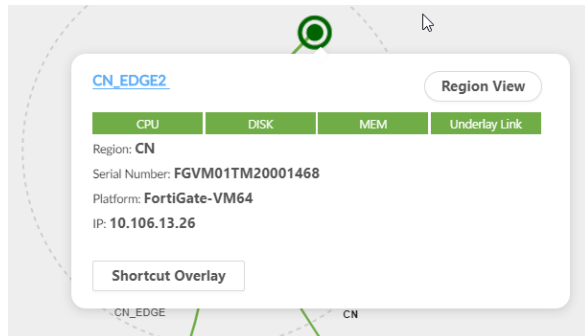
2. Click the lines to view link information, including the inbound and outbound bandwidth.

Viewing shortcut overlays (ADVPN)

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

To view shortcut overlays (ADVPN):

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



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

Viewing hub devices

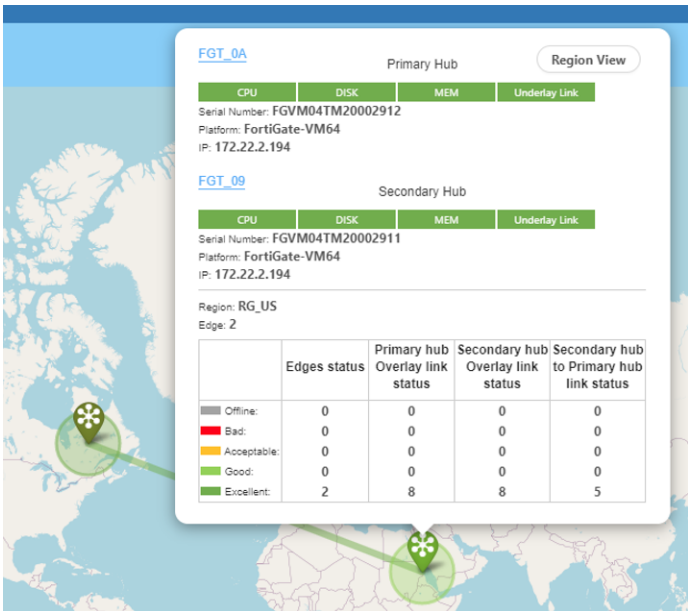
You can view all hub devices across the globe in the SD-WAN network on the *Hub View* pane.



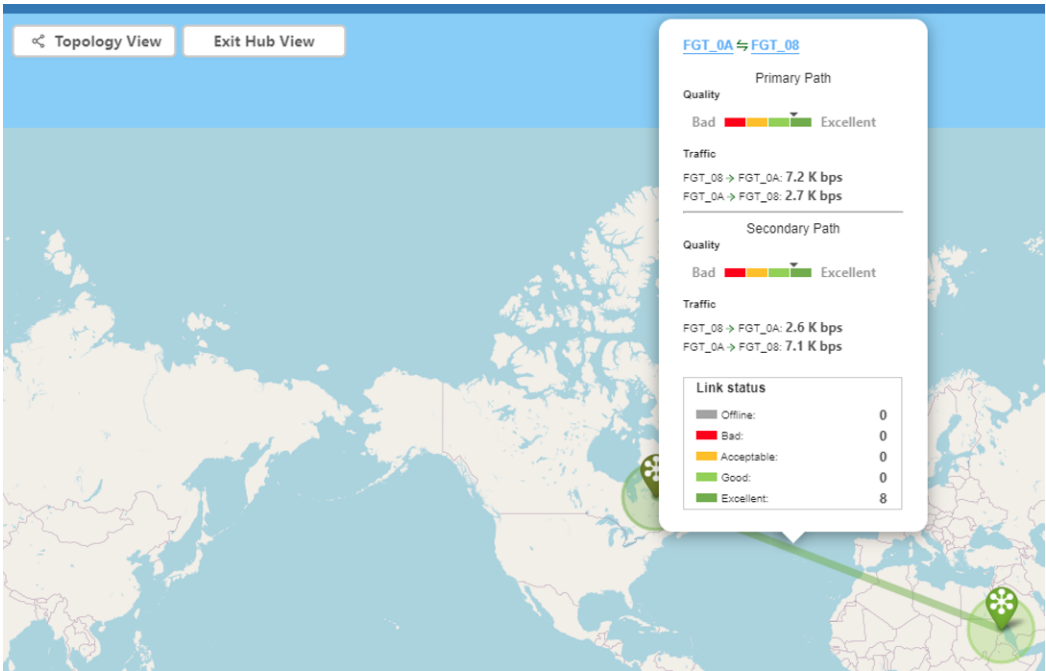
When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the map. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

To view hub devices:

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



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



Viewing regions

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

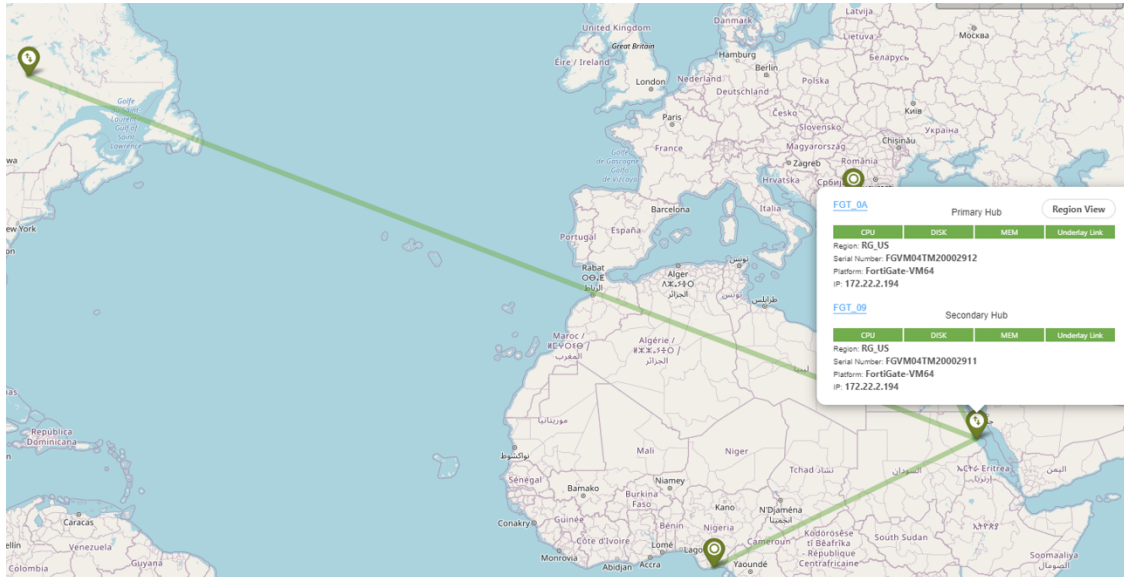


When you have both a primary hub and a secondary hub in a region, only one hub icon displays on the map. When you access details about the hub icon on a map, you can view information about both the primary and secondary hubs.

To view regions:

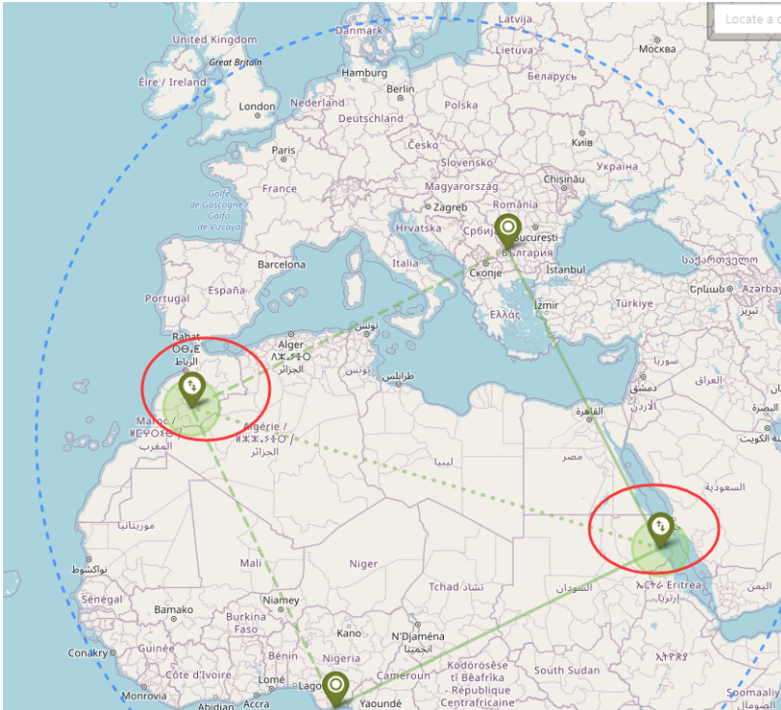
1. Go to *Monitor > Dashboard*, and click *Hub View*.
2. Click a hub to view status information.

Status information is displayed, and the dialog box includes a *Region View* button.



3. In the dialog box, click *Region View*.

Details about the region are displayed. In the following example, the region includes both a primary hub and a secondary hub.



Traffic

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

This section includes the following topics:

- [Viewing global network traffic reports on page 26](#)
- [Exporting global traffic reports on page 27](#)

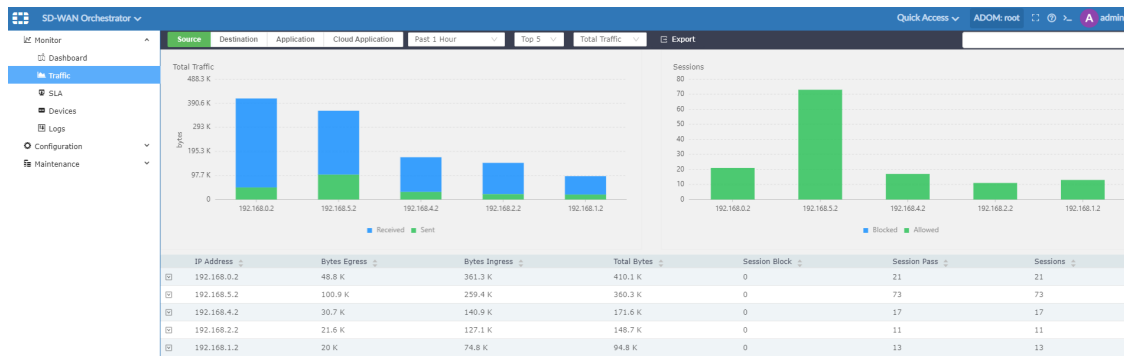
Viewing global network traffic reports

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 27](#).

To view network traffic reports:

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



Report

Description

Source

The statistics generated in the report are based on the source IP of the traffic. The report contains two statistical charts (*Total Traffic* and *Sessions*), 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:

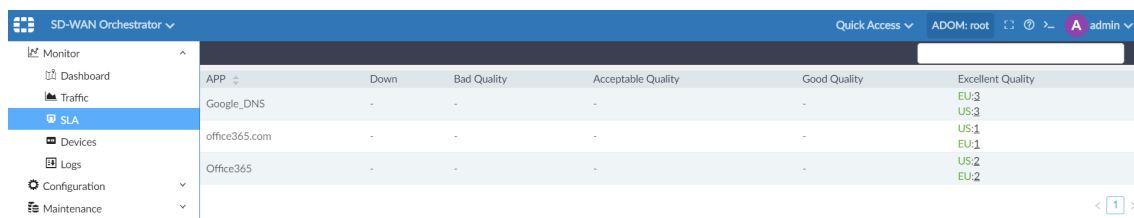
1. Go to *Monitor > Traffic*.
2. Display the desired traffic report. See [Viewing global network traffic reports on page 26](#).
3. In the toolbar, click *Export*.
A PDF of the traffic report is exported to your computer.

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*.

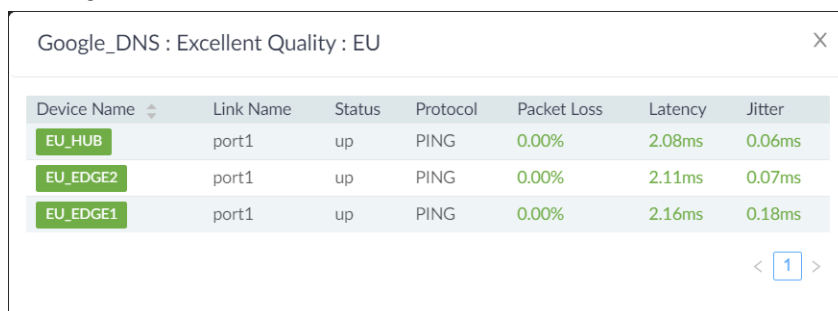


APP	Down	Bad Quality	Acceptable Quality	Good Quality	Excellent Quality
Google_DNS	-	-	-	-	EU:3 US:3
office365.com	-	-	-	-	US:1 EU:1
Office365	-	-	-	-	US:2 EU:2

The following table identifies the SLA criteria for each rating.

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

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



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 29](#)
- [Viewing device link reports on page 30](#)
- [Viewing device traffic reports on page 31](#)
- [Viewing device SLA on page 31](#)
- [Viewing device local branches on page 32](#)

If you want to view information about all devices in the SD-WAN network, see [Dashboard on page 21](#).

Viewing device overviews

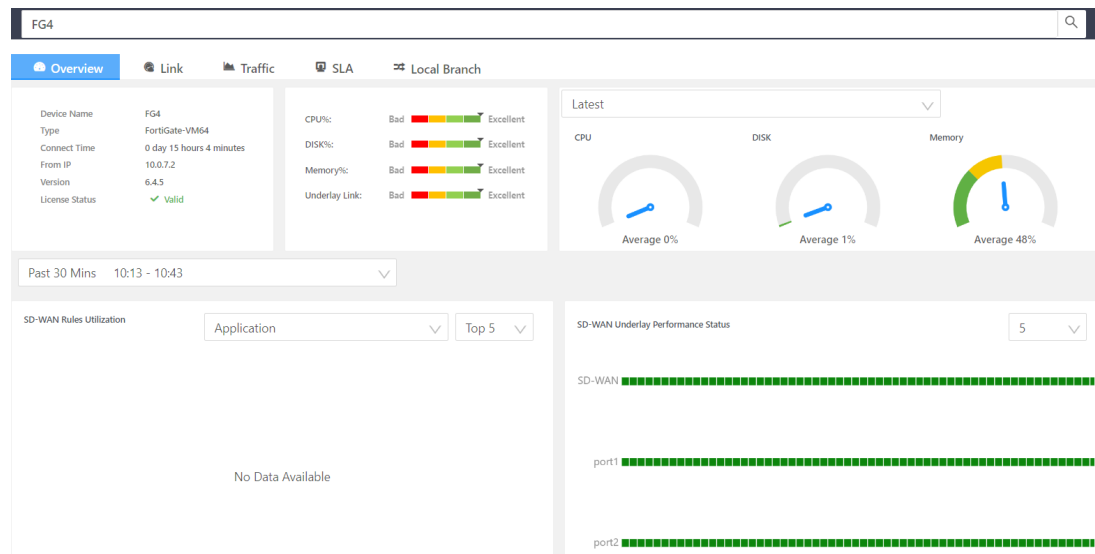
You can use the *Devices > Overview* tab to monitor SD-WAN rules utilization, performance status, disk utilization, traffic, and more for each device in the SD-WAN network.

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

To view device overviews:

1. Go to *Monitor > Devices > Overview*.

You can switch between devices by using the dropdown menu in the toolbar at the top of the page.



2. Hover over each chart to display additional detail.
3. You can also filter data in some charts by selecting a filter from the dropdown menu.

Viewing device link reports

The *Devices > Link* tab contains information about the following links: underlay, static overlay, shortcut overlay, and external VPN gateway overlay.

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	
Underlay	<p>The <i>Underlay</i> pane includes the following views:</p> <ul style="list-style-type: none"> • Traffic: Contains reports about the total inbound and outbound throughput, and session ramp-up of the SD-WAN underlay links. The table features information about the device's status, inbound/outbound bytes, and session of the underlay link. • Quality: Contains reports about performance status, packet loss, jitter, and latency for the device overlay links.
Static Overlay	<p>The <i>Static Overlay</i> pane is the default view of the <i>Link</i> page and includes the views:</p> <ul style="list-style-type: none"> • Quality: Contains reports of quality evaluation, jitter, latency, and packet loss in the device overlay links. • Traffic: Contains reports about the total inbound/outbound throughput and session.
Shortcut Overlay	<p>Available when ADVPN is enabled on devices, and shortcut links are established.</p> <p>The charts monitor the total inbound and outbound throughput of the shortcut overlay links.</p> <p>The table features information about peer devices, inbound/outbound bytes, and bandwidth.</p> <p>You can also view unknown peer devices and unknown peer ports.</p> <p>At the bottom of the pane is a table of additional information, such as <i>Name</i>, <i>Peer Device</i>, <i>Status</i>, <i>Quality</i>, and so on.</p>
External VPN Gateway Overlay	<p>Available when external VPN gateways are enabled on devices, and links are established.</p>

2. Set one or more of the following filters to change the view.
Not all filters are available on all tabs.

Filter	
Time	From the time dropdown menu, select a time range.
Underlay Name Filter	Click the <i>Underlay Name Filter</i> box to select an underlay port.
Peer Device Filter	Click the <i>Peer Device Filter</i> box to select one of the following filters:

Filter	
	<ul style="list-style-type: none"> • <i>All hubs</i> • <i>All edges</i> <p>Alternately, you can select one or more of the individual devices displayed in the filter list.</p>
Status Filter	Click the <i>Status Filter</i> box to select <i>Up</i> or <i>Down</i> status.
Quality Filter	<p>Click the <i>Quality</i> box to select one of the following filters:</p> <ul style="list-style-type: none"> • <i>Disconnected</i> • <i>Bad</i> • <i>Acceptable</i> • <i>Good</i> • <i>Excellent</i>

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 26](#).

To view device traffic reports:

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

Viewing device SLA

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

To view device SLA:

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

FGVM04TM21000968						
Overview Link Traffic SLA Local Branch						
Past 10 Mins 10:57 - 11:07						
Name	Detect Server	Protocol	Packet Loss	Latency	Jitter	
<input checked="" type="checkbox"/> Google_DNS	8.8.8.8	PING	port1: 0.00% port2: 0.00%	port1: 2.41ms port2: 2.30ms	port1: 0.11ms port2: 0.11ms	

Viewing device local branches

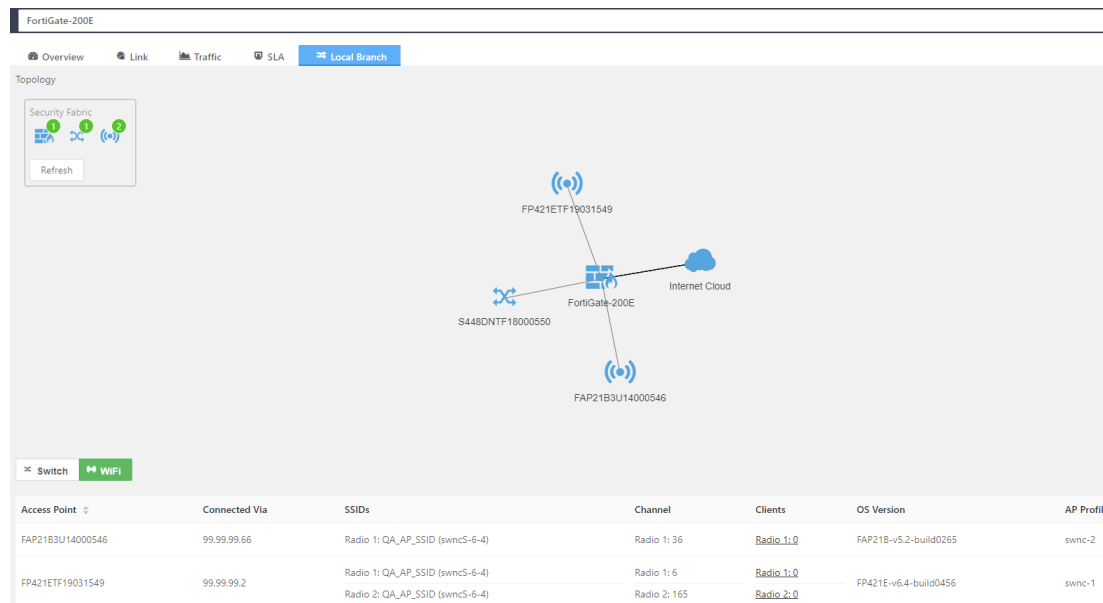
The *Devices > Local Branch* tab displays topology and statistics for connected FortiSwitch and FortiAP devices.

To view device local branches:

1. Go to *Monitor > Devices > Local Branch*.

The *Local Branch* tab displays the topology for the selected device.

You can switch between devices by using the dropdown menu in the toolbar at the top of the page.



2. In the *Security Fabric* box, hover the mouse over the *FortiGate*, *FortiSwitch*, and *FortiAP* icons to display information about connected devices.
3. At the bottom of the page, click the *Switch* tab to display information about connected FortiSwitch devices.
4. At the bottom of the page, click the *WiFi* button to display connected FortiAP devices.

Logs



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

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. You can filter the logs, and download a zip file of filtered logs.

To view and filter logs:

1. Go to *Monitor > Logs*.
2. For each log entry, click *Detail* to view more details.
3. Filter logs by setting the following options:

Start	Click the <i>Start</i> box to select a start date.
End	Click the <i>End</i> box to select an end date.
Type	Click the <i>Type</i> box to select one or more log types.
Subtype	Click the <i>Subtype</i> box to display the log types, and then expand each log type to select one or more subtypes.
Device	Click the <i>Device</i> box to select a device.

Selected filters are applied immediately.

4. Remove filters:
 - Click the *x* above a selected filter to remove it.
 - Hover over each option with selected filters, and click the *x* in the top-right corner to remove all filters for the option.
5. Click *Download* to download a zip file of log information.
Inside the zip file is a .csv file of log information.

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 34](#)
- [Profile on page 57](#)
- [Shared resources on page 97](#)
- [Global routing on page 111](#)

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 57](#).

This section contains the following topics:

- [Adding devices on page 35](#)
- [Adding devices in HA clusters on page 38](#)
- [Adding model devices on page 38](#)
- [Adding model devices in HA clusters on page 40](#)
- [Adding regions on page 41](#)
- [Adding unauthorized devices on page 43](#)
- [Adding devices with authorized FortiExtenders on page 45](#)
- [Synchronizing with FortiManager on page 47](#)
- [Installing configuration changes on page 48](#)
- [Importing devices on page 48](#)
- [Viewing configuration status on page 49](#)
- [Overriding device settings on page 50](#)
- [Adding static routes on page 51](#)
- [Creating BGP neighbors on page 52](#)
- [Adding IP pool to LAN port configuration on page 53](#)
- [Executing WAN port speed tests on page 54](#)
- [Updating regions on page 56](#)
- [Deleting regions on page 56](#)
- [Monitoring devices on page 56](#)
- [Replacing FortiGate serial numbers on page 56](#)

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 57](#).
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 <i>Create</i> 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: <ul style="list-style-type: none"> <i>NONE</i>: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. <i>RETRIEVE_CONFIG</i>: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. <i>SYNC_CONFIG</i>: 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 <i>Create Region</i> to create a new region.
Password	The <i>Password</i> option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from: <ul style="list-style-type: none"> 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 VDOMs

You can use VDOMs for primary or secondary hub devices as well as edge devices.

Before using this method to add VDOMs to SD-WAN Orchestrator MEA, you must:

- Create VDOMs on the FortiGate device
This method adds the VDOM to SD-WAN Orchestrator MEA, so you must create the VDOM first.
- Configure interfaces for the VDOM by using FortiManager
This method retrieves interfaces for the VDOM from FortiManager, so you must configure them first.

After you add the VDOM to SD-WAN Orchestrator MEA and retrieve VDOM interfaces, overrides are automatically enabled in the assigned profile for WAN and LAN settings.

To add a VDOM:

1. Ensure that you have created a profile for a VDOM. See [Creating profiles for VDOMs on page 60](#).
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:
The following table identifies settings that are specific to adding a VDOM. You can set the remaining settings as desired.

Option	Description
Device Name	Select the device VDOM.
Profile Name	Select a profile that is configured for VDOMs.

5. Click *OK*.
The VDOM is added to the device list.
6. For the VDOM in the device list, click the *Update* button.
The settings for the VDOM open for editing, and the *General* tab is displayed.

The screenshot shows the 'Device / FG4 (FG-traffic)' configuration window with the 'General' tab selected. The settings are as follows:

Field	Value
Device Name	FG4 (FG-traffic)
Host Name	FGVM-1234567890
Profile Name	test-vdom(SECONDARY_HUB)
First Online Action	SYNC_CONFIG
Running On Cloud	OFF
Serial Number	FGVM-1234567890
Type	FortiGate-VM64
Region	test
Password	No Cha... (Please Enter Passw...)

Buttons: OK, Cancel

7. Go to the *Network* tab, and click *Retrieve VDOM Interfaces*.

The screenshot shows the 'Device / FG4 (FG-traffic)' configuration window with the 'Network' tab selected. The 'Retrieve VDOM Interfaces' button is highlighted. Below it is a list of network interfaces:

- > WAN
- > LAN
- > DMZ
- > Static Routing
- > BGP
- > OSPF
- > DNS Server
- > SNMP
- > HA Interfaces

Buttons: OK, Cancel

A warning message is displayed.

● If the interfaces of this device are different from current profile, the corresponding settings will be overridden. Are you sure?

No Yes



8. Click **Yes** to proceed.
Interfaces are retrieved, and the *Override* option is automatically toggled on for LAN and WAN ports in the associated profile.
9. On the *Success* message dialog box, click the X to close it.

Adding devices in HA clusters

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



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

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

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



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

To add devices in HA clusters:

1. Ensure you have created profiles for devices in HA clusters. See [Creating profiles for HA devices on page 63](#).
2. Perform a factory reset on the FortiGates in the HA cluster.
3. Add the managed devices to SD-WAN Orchestrator MEA. See [Adding devices on page 35](#).

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 57](#).
2. Go to *Configuration > Device*.

3. In the *Device* menu, select **+ Model Device**.

The **+ Model Device** dialog box opens.

4. Configure the following settings:

Option	Description
Serial Number	Enter the serial number for the device.
Device Name	Enter a name for the device.
Host Name	Enter the host name.
Type	The model is displayed after you enter the device serial number.
Profile Name	Select a profile from the dropdown, or click <i>Create</i> to create a new profile.
Region	Select a region from the dropdown, or click <i>Create Region</i> to create a new region.
First Online Action	Specify how to manage device configuration when the device comes online for the first time. Choose from: <ul style="list-style-type: none"> • NONE: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • RETRIEVE_CONFIG: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • SYNC_CONFIG: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Assign Policy Package	Available when <i>First Online Action</i> is set to SYNC_CONFIG . Select a FortiManager policy package to install when the device first comes online.
HA Mode	Select STANDALONE to disable HA mode. Select AP to enable active-passive HA mode.
Enforce Firmware Version	(Optional) Select the required FortiOS version for the device when it comes online.
Password	The <i>Password</i> option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from: <ul style="list-style-type: none"> • 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 in HA clusters

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

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

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

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

To add model devices to HA clusters:

1. Ensure that you have created profiles for HA devices. See [Creating profiles for HA devices on page 63](#).
2. Go to *Configuration > Device*.
3. In the *Device* menu, select *+ Model Device*.
The *+ Model Device* dialog box opens.
4. Configure the following settings for the primary device and cluster:

Option	Description
Serial Number	Enter the serial number for the primary device in the HA cluster.
Device Name	Enter a name for the primary device.
Host Name	Not available when <i>HA Mode</i> is set to <i>AP</i> .
Type	The model is displayed after you enter the device serial number.
Profile Name	Select a profile for HA devices from the dropdown, or click <i>Create</i> to create a new profile.
Region	Select a region from the dropdown, or click <i>Create Region</i> to create a new region.
First Online Action	Specify how to manage device configuration when the device comes online for the first time. Choose from: <ul style="list-style-type: none"> • <i>NONE</i>: Select to disable automatic configuration action. Instead you can manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA. • <i>RETRIEVE_CONFIG</i>: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings. • <i>SYNC_CONFIG</i>: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.
Enforce Firmware Version	(Optional) Select the required FortiOS version for the device when it comes online.
Password	The <i>Password</i> option is displayed after the device serial number is added and recognized. Specify how to handle the device password. Choose from:

Option	Description
	<ul style="list-style-type: none"> No change: Keep the original password of the newly added device. Manual: Specify the password of the device. Auto: Generate a random password for the device automatically. Click the eye icon to view the password.
HA Mode	Select <i>STANDALONE</i> to disable HA mode. Select <i>AP</i> to enable active-passive HA mode.
Cluster Name	Available when <i>HA Mode</i> is set to <i>AP</i> . Type a name for the HA cluster. Minimum length is 1 character, and maximum length is 21 characters. The #,(,) characters are not supported.
HA Password	(Optional) Available when <i>HA Mode</i> is set to <i>AP</i> . Specify a password for the HA cluster. Maximum length is 128 characters.
Priority	Type a high number between 0-255 to set the priority for the primary HA member.
HA Secondaries	Available when <i>HA Mode</i> is set to <i>AP</i> . Click <i>Add</i> to add a secondary model device to the HA cluster by serial number. In the <i>SerialNumber #1</i> box, type the serial number for the FortiGate device in the HA cluster. It should be the same type of serial number as the primary FortiGate in the HA cluster. In the <i>Priority</i> box, type the priority restriction for the device in the HA cluster. Type a number between 0 and 255.

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

Adding regions

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

When you create a region, you select the devices, assign the profiles of configuration settings, assign an IPsec template for the region, and install configurations to all devices in the region. See also [Creating custom IPsec templates on page 106](#).

To add a region:

1. Ensure that you have created profiles for hub and edge devices. See [Profile on page 57](#).
2. Go to *Configuration > Device*.

3. In the toolbar, click + *Region*.
The + *Region* dialog box is displayed.

4. In the *Name* field, type a name for the region.
5. Add one or more hub devices:
 - a. In the *Hub* table, click *Select*.
The *Select Device* dialog box is displayed.
 - b. Select one or more devices from the list, and click *OK*.
The selected devices display in the *Hub* table.
 - c. In the *Hub* table, select a device, and click *Assign Profile*.
The *Select Profile* dialog box displays.
 - d. From the list, select a profile, and click *OK*.
The selected profile is assigned to the device.
 - e. In the *Hub* table, select a device, and click *First Online Action*.
The *Set First Online Action* dialog box is displayed.
The first online action is specified in the assigned profile, but you can use this option to override the profile setting for the selected device.
 - f. Select an action, and click *OK*.
The selected action is displayed for the device in the *Hub* table.
6. Add one or more edge devices:
 - a. In the *Edges* table, click *Select*.
The *Select Device* dialog box is displayed.
 - b. Select one or more devices from the list, and click *OK*.
The selected devices display in the *Edges* table.
 - c. In the *Edges* table, select a device, and click *Assign Profile*.
The *Select Profile* dialog box displays.
 - d. From the list, select a profile, and click *OK*.
The selected profile is assigned to the device.
 - e. In the *Edges* table, select a device, and click *First Online Action*.
The *Set First Online Action* dialog box is displayed.
The first online action is specified in the assigned profile, but you can use this option to override the profile setting for the selected device.

- f. Select an action, and click *OK*.

The selected action is displayed for the device in the *Edges* table.

7. (Optional) In the *Description* field, enter a description of the region.
8. In the *IPsec Template Within Region* list, select an IPsec template for the region.
9. Click *OK*.

The region is created. 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 <number>*.
The *Add Unauthorized Devices* dialog box opens.
3. Configure the following settings:

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

4. Click *OK*.

Adding FortiExtenders to online devices

You can use FortiExtender as a WAN port. This topic describes how to add a FortiExtender to a device managed by SD-WAN Orchestrator MEA.

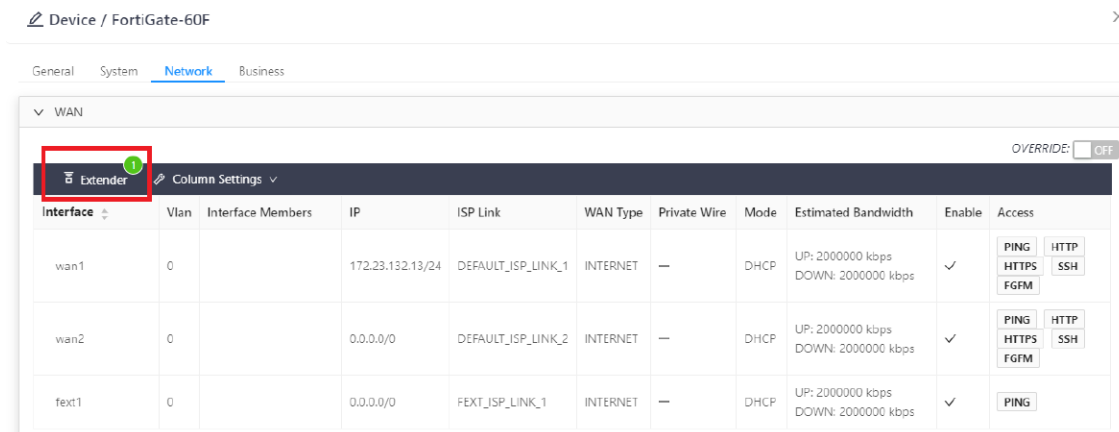
After you add FortiExtender settings to the profile, you can add FortiExtender to the device. SD-WAN Orchestrator MEA detects the FortiExtender, and you can authorize FortiExtender.

To add FortiExtenders to online devices:

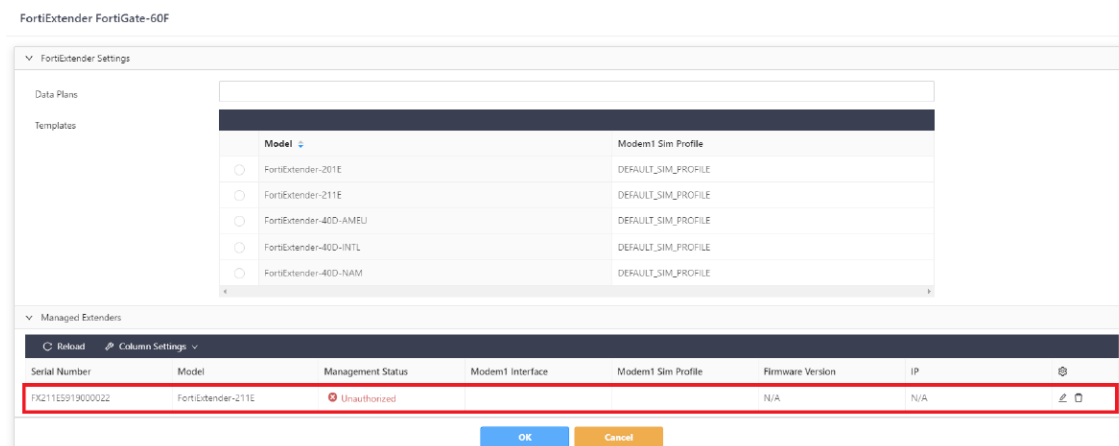
1. Ensure that you have created a profile with a FortiExtender WAN port configured. See [Creating profiles with FortiExtender WAN ports on page 61](#).
2. Attach FortiExtender to the managed device.
FortiExtender is detected.

3. Authorize FortiExtender for the WAN port by overriding the profile settings for the device:

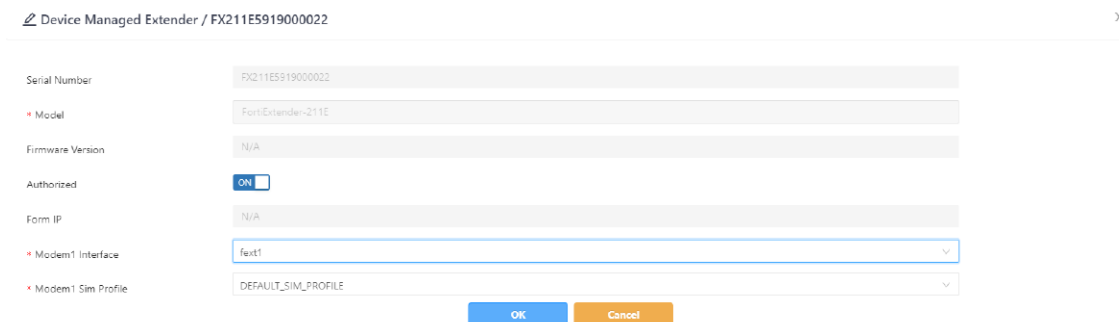
- Go to *Configuration > Device*.
- Double-click the device to open the profile for editing.
The *General* tab is displayed.
- Go to the *Network* tab.
An unauthorized FortiExtender has been detected.



- Click *Extender*.
The *FortiExtender* dialog box is displayed.



- Under *Managed Extenders*, click the *Update* button for the unauthorized device.
The *Device Managed Extender* dialog box is displayed.
- Toggle *Authorized* to on, and click *OK*.



The FortiExtender is authorized, and the *Device Managed Extender* dialog box is closed.

- g. Click **OK**.

The *FortiExtender* dialog box is closed.

- h. Click **OK**.

The profile override changes are saved.

4. Install the SD-WAN Orchestrator MEA profile changes to the device with authorized FortiExtender. See [Installing configuration changes on page 48](#).

Adding devices with authorized FortiExtenders

You can use FortiExtender as a WAN port. This topic describes how to add a device with an authorized FortiExtender to SD-WAN Orchestrator MEA.

After you create a profile with FortiExtender configured as a WAN port, you can add the device with authorized FortiExtender to SD-WAN Orchestrator MEA.

When you add the device to SD-WAN Orchestrator MEA, select the profile and enable the configuration to be retrieved. Wait for the configuration to be retrieved from the device. After the configuration is retrieved, FortiExtender is bound to the port and displays as authorized in the WAN settings.

To add devices with authorized FortiExtenders:

1. Ensure that you have created a profile with a FortiExtender WAN port configured. See [Creating profiles with FortiExtender WAN ports on page 61](#).

When creating profiles for managed devices with authorized FortiExtenders, ensure that you use the same settings for FortiExtender in the SD-WAN Orchestrator MEA profile that you used in FortiOS because the profile will be applied to all authorized FortiExtenders.

2. Add the device with authorized FortiExtender to SD-WAN Orchestrator MEA:

- a. Go to *Configuration > Device*.

- b. In the toolbar, click **+ Device**.

The *Device* dialog box opens.

- c. On the *General* tab, configure the following settings:

The following table identifies settings that are specific to adding FortiExtender as a WAN port. You can set the remaining settings as desired.

Option	Description
Device Name	Select a model that supports FortiExtender, such as FortiWiFi-40F-3G4G.
Profile Name	Select a profile that is configured to use FortiExtender as a WAN port.
First Online Action	Select <i>RETRIEVE_CONFIG</i> .

- d. Click **OK**.

Wait for the configuration to be retrieved from the device.

3. Go to *Monitor > Logs* to view progress about the process.

In time you should see a log subtype of *device_online* for the device and *retrieve_config*.

After the configuration is retrieved, the FortiExtender displays as authorized in SD-WAN Orchestrator MEA.

4. Check that FortiExtender is authorized for the WAN port.
 - a. For the device, click the *Update* button to open the settings.
The *General* tab is displayed.

Device / FortiWiFi-40F-3G4G

General System Network Business

* Device Name: FortiWiFi-40F-3G4G

Host Name: FortiWiFi-40F-3G4G

* Profile Name: 40F(PRIMARY_HUB)

* First Online Action: RETRIEVE_CONFIG

* Serial Number: FW40

* Type: FortiWiFi-40F-3G4G

* Region: Extender

Running On Cloud: ☐ Off

OK Cancel

- b. Go to the *Network* tab, and expand the *WAN* section.
FortiExtender displays in the interface list.

Device / FortiWiFi-40F-3G4G

General System **Network** Business

WAN

OVERWRITE: ☐ ON

+ Create New Reload Extender Column Settings

Interface	Vlan	Interface Members	IP	ISP Link	WAN Type	Private Wire	Mode	Estimated Bandwidth	Enable	Access
wan	0		0.0.0.0/0	DEFAULT_JSP_LINK_1	INTERNET	—	DHCP	UP: 2000000 kbps DOWN: 2000000 kbps	<input checked="" type="checkbox"/>	PING HTTPS FGFM SSH
wwan	0		0.0.0.0/0	DEFAULT_JSP_LTE_1	LTE	—	DHCP	UP: 2000000 kbps DOWN: 2000000 kbps	<input checked="" type="checkbox"/>	PING HTTPS FGFM SSH
fext-wan	0		72.250.81.1/30	FEXT_JSP_LINK_1	INTERNET	—	DHCP	UP: 2000000 kbps DOWN: 2000000 kbps	<input checked="" type="checkbox"/>	PING FGFM

1 WAN

- c. In the toolbar, click *Extender*.
The *FortiExtender Settings* dialog box is displayed.
 - d. Expand the *Managed Extenders* section, and ensure that FortiExtender is authorized.

FortiExtender FortiWiFi-40F-3G4G

FortiExtender Settings

Data Plans

Templates

Model	Modem1 Sim Profile
<input type="radio"/> FortiExtender-201E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-211E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-40D-AMEU	DEFAULT_SIM_PROFILE

Managed Extenders

Reload Column Settings

Serial Number	Model	Management Status	Modem1 Interface	Modem1 Sim Profile	Firmware Version	IP
FX201E5920005497	FortiExtender-201E	✓ Authorized	fext-wan	DEFAULT_SIM_PROFILE	FXT201E-v4.2.2-build302	192.168.1.1

OK Cancel

- e. For the authorized FortiExtender, click the *Update* button.
The *Device Managed Extender* dialog box is displayed, and the *Modem 1 Interface* box displays the WAN port name.
- f. Click *Cancel* to close the *Device Managed Extender* dialog box.
- g. Click *Cancel* to close the *FortiExtender Settings* dialog box.
- h. Click *Cancel* to close the *Device* dialog box.
FortiExtender is authorized as a WAN port.
5. Install the SD-WAN Orchestrator MEA profile changes to the device with authorized FortiExtender. See [Installing configuration changes on page 48](#).

Synchronizing with FortiManager

You can use the *Sync to FortiManager* option to send configuration scripts from SD-WAN Orchestrator MEA to FortiManager for additional configuration before installation on FortiGate devices. After the configuration scripts are synchronized to FortiManager, the *Config Status* of the device in SD-WAN Orchestrator MEA changes to *Synchronized_to_FortiManager*.

After FortiManager receives the scripts, you can use FortiManager to add additional configuration information, and then install the configuration changes to FortiGate devices. SD-WAN Orchestrator MEA periodically polls FortiGate devices for configuration information.

After changes from FortiManager are successfully installed on FortiGate devices, the *Config Status* of the devices in SD-WAN Orchestrator MEA changes to *Synchronized*.

This workflow is useful for a zero-touch provisioning (ZTP). You can use both SD-WAN Orchestrator MEA and FortiManager to provide configuration information, and the configuration is installed to FortiGate devices when they are online.

To synchronize with FortiManager:

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

Goal	Method
Send all configuration changes for all regions and devices to FortiManager.	In the toolbar, from the <i>Install all configuration</i> menu, select <i>Sync to FortiManager</i> .
Send all configuration changes for all devices in a region to FortiManager.	For a region name, click the <i>Sync region configuration to FortiManager</i> button.
Send configuration changes to FortiManager for a device.	For a device, click the <i>Sync to FortiManager</i> button.

3. View synchronization details for a device:
 - a. When the *Config Status* column displays *Synchronized_to_FortiManager* for a device, click the *Show Sync Details* button.
The *Config to be Synchronized to Device* dialog box is displayed.
 - b. At the bottom of the pane, click the *Copy Message* button to copy the details.
 - c. At the bottom of the pane, click *Close* to close the dialog box.

4. Go to FortiManager and continue making configuration changes.
5. In FortiManager, install the configuration to FortiGates.

When the configuration installation is complete, and SD-WAN Orchestrator MEA receives confirmation that the configuration is successfully installed, the *Config Status* column displays *Synchronized* in SD-WAN Orchestrator MEA.

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 <i>Install all configuration</i> .
Install all configuration changes for all devices in a region.	For a region name, click the <i>Install Region Configuration</i> button.
Install configuration changes to a device.	For a device, click the <i>Install Configuration</i> 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: <ul style="list-style-type: none"> <i>NONE</i>: Select to disable automatic configuration action. Instead you can

manually initiate configuration installation after adding the device to SD-WAN Orchestrator MEA.

- **RETRIEVE_CONFIG**: Select to import some of the configuration settings from the device when the device comes online for the first time. Settings such as host name, WAN port, WAN port IP, LAN/DMZ port, and static route are imported. WAN and LAN settings from the imported configuration automatically override the assigned WAN and LAN settings from the SD-WAN Orchestrator MEA profile. You should use the profile to assign additional settings.
- **SYNC_CONFIG**: Select to install the SD-WAN Orchestrator MEA configuration associated with the profile when the device comes online for the first time.

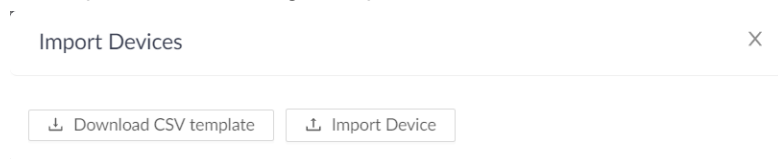
Host Name

Specify the host name for the FortiGate.

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

To import a device:

1. Ensure that you have created profiles for hub and edge devices. See [Profile on page 57](#).
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.

Status	Description
Modified	The configuration in SD-WAN Orchestrator MEA differs from the configuration installed on the device.
Synchronizing	The configuration scripts are either being sent to FortiManager or are being installed to the device.
Synchronized to FortiManager	The configuration scripts have been sent to FortiManager, but the configuration is not yet installed to the device. See also Synchronizing with FortiManager on page 47 .

Status	Description
Synchronized	The configuration is successfully installed to the device.

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 51](#)
- [Creating BGP neighbors on page 52](#)
- [Creating business rules on page 85](#)
- [Adding IP pool to LAN port configuration on page 53](#)
- [Executing WAN port speed tests on page 54](#)

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.

The screenshot shows the 'Device / FGVMSLT20002454' configuration dialog box. The 'General' tab is selected, displaying various configuration fields. The 'Device Name' is 'FGVM', 'Host Name' is 'FGVMSLT20002454', 'Profile Name' is 'Primary-hub-italy(PRIMARY_HUB)', and 'First Online Action' is 'RETRIEVE_CONFIG'. The 'Running On Cloud' checkbox is 'OFF'. The 'Serial Number' is 'FGVM', 'Type' is 'FortiGate-VM64', and 'Region' is 'Italy'. The 'Password' field is set to 'No Cha...'. The dialog box has 'OK' and 'Cancel' buttons at the bottom.

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

The screenshot shows the 'Device /' configuration window with the 'System' tab selected. The 'NTP Setting' section is expanded, showing options to 'Synchronize with NTP Server' (toggled ON), 'Server Type' (set to FORTIGUARD), and 'Interval' (60 minutes). There are expandable sections for 'FortiGuard Setting', 'Email Setting', 'Log Setting', and 'Misc Setting'. An 'OVERRIDE' button is visible in the top right corner. At the bottom are 'OK' and 'Cancel' buttons.

- Expand the setting that you want to override, such as *NTP Setting*, and toggle on the *Override* button. A confirmation dialog box displays.
- Click *OK* to confirm the desire to enable an override, and select the settings you want to override.
- Click *OK* to save the changes.
- Install the configuration changes. See [Installing configuration changes on page 48](#).

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.

You can establish an IPsec tunnel with an external VPN gateway that is not managed by SD-WAN Orchestrator MEA. See also [Creating external VPN gateways on page 105](#).

You can also use the router prefix-list configuration to inject routes learned through OSPF/BGP to global routing. In the *Static Routing* dialog box, toggle *Inject to SDWAN Route* to *On* to enable this feature.

To add static routes:

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

The screenshot shows the 'Device /' configuration window with the 'General' tab selected. Fields include 'Device Name' (FGVM), 'Host Name' (FGVMSLT20002454), 'Serial Number' (FGVM), 'Type' (FortiGate-VM64), 'Profile Name' (Primary-hub-italy(PRIMARY_HUB)), 'Region' (Italy), 'First Online Action' (RETRIEVE_CONFIG), and 'Running On Cloud' (OFF). There is a 'Password' field with a dropdown set to 'No Cha...' and a warning icon. At the bottom are 'OK' and 'Cancel' buttons.

- Click the *Network* tab, and expand the *Static Routing* section.

- Click **Create New**.
A + **Static Routing** dialog box displays.

+ Static Routing

* Destination: 172.22.15.0/24

* Blackhole: ☐ OFF

* Interface:

Gateway: 172.22.15.3

Inject to SDWAN Route: ☐ OFF

Distance: 10

Priority: 0

Description: description

OK **Cancel**

- Configure the options, and click **OK**.
The static route is created.
- Click **OK** to save the changes.
- Install the configuration changes. See [Installing configuration changes on page 48](#).

Creating BGP neighbors

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

To create BGP neighbors:

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

Device / FGVM: FortiGate-VM64

General System Network Business

* Device Name: FGVM: FortiGate-VM64

Host Name: FGVM:SLTM20002454

* Profile Name: Primary-hub-italy(PRIMARY_HUB)

* First Online Action: RETRIEVE_CONFIG

Running On Cloud: ☐

* Serial Number: FGVM:SLTM20002454

* Type: FortiGate-VM64

* Region: Italy

Password: No Cha... Please Enter Passw...

OK **Cancel**

- Click the **Network** tab, and expand the **BGP** section.
- Under Neighbors, click **Create New**.
A + **BGP Neighbor** dialog box displays.

+ BGP Neighbor

* Neighbor: 172.22.15.3

* Remote As: 6

Auto Inject: ☒ ON

Set Next Hop Self: ☐ OFF

Set Link Down Failover: ☐ OFF

Set EBGP Enforce Multihop: ☐ OFF

Set Soft Reconfiguration: ☐ OFF

* Advertisement Interval: 30

OK Cancel

6. Configure the options, and click **OK**.
The BGP neighbor is added.
7. Click **OK** to save the changes.
8. Install the configuration changes. See [Installing configuration changes on page 48](#).

Adding IP pool to LAN port configuration

To add IP pool to LAN port configuration:

1. Go to *Configuration > Device*.
2. Expand the region.
The devices in the region are displayed.
3. Double-click the device to open it for editing.
The *Device / <name>* dialog box is displayed.
4. Click the *Network* tab, and expand the *LAN* section.
5. Toggle *Override* to *ON*.
6. Double-click an interface to open it for editing.
The *LAN / <interface name>* dialog box displays.

7. Create an IP pool:

- a. Beside *IP Address*, click *Create IP Pool*.

The *IP Pool* dialog box is displayed.

- b. In the *Name* box, type a name for the IP pool.
- c. In the *Pool* box, type an IP address range.
- d. Click *OK* to save the changes.

The IP pool is created. You can also view the IP pool by going to *Configuration > Shared Resources > Network > Intranet IP Pool*.

8. In the *IP Address* box, type the IP address range for the IP pool to select it.
9. Click *OK* to save the device override changes.
10. Install the configuration changes. See [Installing configuration changes on page 48](#).

Executing WAN port speed tests

You can execute a WAN port speed test. After the speed test, you can click *Apply Results to Estimated Bandwidth* button to copy the results to *Estimated Upstream Bandwidth* and *Estimated Downstream Bandwidth*. If you want to apply this configuration, click *OK*, and manually synchronize the device.

You can also schedule a recurring speed test using one of the default schedules. You can also create custom schedules. See [Creating custom speed test schedules on page 110](#).

To execute an interface speed test:

1. Go to *Configuration > Device*.
2. Expand the region.
The devices in the region are displayed.
3. Double-click the device to open it for editing.
The *Device / <name>* dialog box is displayed.
4. Click the *Network* tab, and expand the *WAN* section.
5. Toggle *Override* to *ON*.
6. Double-click an interface to open it for editing.
The *WAN / <interface name>* dialog box displays.
7. Click *Execute Speed Test*.
The speed test begins, and the results are displayed.

The screenshot shows a dialog box for speed test results. At the top, it displays 'Measure Upstream' as 18,154 kbps, 'Measure Downstream' as 293,532 kbps, and 'Measure Time' as 2021-08-24 16:34:26. Below these values are two buttons: 'Execute Speed Test' and 'Apply Results To Estimated Bandwidth'. A green progress bar with a checkmark is visible. Below the progress bar is a section titled '> Schedule Recurring Speed Test'. Under this section, there are two toggle switches: 'Auto Apply Speed Test Result' (OFF) and 'First Online Speed Test' (OFF). Below these are two input fields: 'Access Types' (containing PING X, HTTP X, HTTPS X, SSH X, FGFM X) and 'Role' (containing WAN). At the bottom are 'OK' and 'Cancel' buttons.

8. (Optional) Click *Apply Results to Estimated Bandwidth*.
The *Estimated Upstream Bandwidth* and *Estimated Downstream Bandwidth* options are updated.
9. (Optional) Schedule a recurring speed test:
 - a. Expand *Schedule Recurring Speed Test*, and toggle *Enable Schedule Speed Test* to *ON*.
The schedule options are displayed.

The screenshot shows the 'Schedule Recurring Speed Test' dialog box. It has a title bar with a dropdown arrow. Inside, there are several settings: 'Enable Schedule Speed Test' (ON), '* Schedule' (default-darrp-optimize), 'Update Inbandwidth' (ON), 'Update Outbandwidth' (ON), 'Update Inbandwidth Maximum' (2000000 Kbps), 'Update Inbandwidth Minimum' (2000000 Kbps), 'Update Outbandwidth Maximum' (2000000 Kbps), and 'Update Outbandwidth Minimum' (2000000 Kbps). At the bottom, there are two toggle switches: 'Auto Apply Speed Test Result' (ON) and 'First Online Speed Test' (OFF).

- b. In the *Schedule* list, select a schedule.
- c. Determine whether to use the test results to update the incoming bandwidth and the outgoing bandwidth.
- d. Specify minimum and maximum bandwidths amounts.

- e. Specify whether to automatically apply the test results.
- f. Click *OK* to save the speed test settings for the WAN port.
- 10. Click *OK* to save the profile override settings the device.
- 11. Install the configuration changes. See [Installing configuration changes on page 48](#).

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.
The *Region / <name>* dialog box is displayed.
3. Edit the settings, and click *OK*.
The configuration changes are saved to the region.
4. Install the configuration changes to devices. See [Installing configuration changes on page 48](#).

Deleting regions

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

To delete a region:

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

Monitoring devices

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

To monitor a device:

1. Go to *Configuration > Device*.
2. Expand the region to view details about each device.
When the device is part of an HA cluster, an HA icon displays in the *Status* column. You can hover over the icon to view details about the HA cluster.
3. Click the *monitor* button beside the device you want to monitor.
The *Devices > Overview* tab is displayed. For more information, see [Viewing device overviews on page 29](#).

Replacing FortiGate serial numbers

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

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

To replace FortiGate serial numbers:

1. In SD-WAN Orchestrator MEA, go to *Configuration > Device*, and ensure that the *Config Status* for the device is *Synched*.
2. Turn off the FortiGate device that you want to replace.
3. Edit the serial number in SD-WAN Orchestrator MEA
 - a. Go to *Configuration > Device*, and double-click the device to open it for editing.
 - b. Beside the *Serial Number* box, click the *Pencil* icon.
The *Serial Number* box becomes editable.
 - c. In the *Serial Number* box, type the new serial number, and click *Confirm*.
 - d. Click *OK*.
The serial number is updated.
4. In FortiManager, download a configuration revision for the FortiGate device you are replacing.
 - a. Go to *Device Manager > Device & Groups*, and select the device group.
The devices in the group display in the left tree menu and in the content pane.
 - b. Double-click a device.
The *System > Dashboard > Summary* is displayed in the content pane.
 - c. In the *Configuration and Installation* widget, click the *Revision History* button.
The *Configuration Revision History* dialog box is displayed.
 - d. Select the revision, and select *Download Revision* from the *More* menu.
 - e. Select the *Regular Download*, and click *OK*.
The configuration is downloaded to your computer.
5. Open the downloaded configuration file in a text editor, and remove the FortiManager IP address from the `central-management` configuration section.
The change ensures that the new FortiGate device isn't registered as a new device.
6. Turn on the new FortiGate.
7. Go to FortiOS, and restore the configuration.
8. Go to FortiManager, and replace the serial number by using the following CLI.

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



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

Profile

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

This section contains the following topics:

- [Creating profiles for hub devices on page 58](#)
- [Creating profiles for edge devices on page 60](#)
- [Creating profiles for VDOMs on page 60](#)
- [Creating profiles with FortiExtender WAN ports on page 61](#)
- [Creating profiles for HA devices on page 63](#)
- [Creating new WAN settings on page 65](#)
- [Creating new LAN settings on page 68](#)
- [Attaching a FortiSwitch model to FortiGate on page 71](#)
- [Adding a FortiAP model device on page 76](#)
- [Creating new DMZ settings on page 81](#)
- [Creating virtual wire pairs on page 83](#)
- [Creating business rules on page 85](#)
- [Cloning profiles on page 87](#)
- [Updating profiles on page 88](#)
- [Deleting profiles on page 89](#)
- [Profile options described on page 89](#)

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 97](#).

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

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

To create profiles for hub devices:

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

The following table identifies settings that are specific to configuring a hub device. You can set the remaining settings as desired.

Option	Description
Device Role	Select <i>PRIMARY_HUB</i> to create a profile for primary hubs. Select <i>SECONDARY_HUB</i> to create a profile for secondary hubs.
VPN Mode with Edge	Select one of the following options to connect the hub device with edge devices: <ul style="list-style-type: none">• Select <i>DIAL_UP</i> to create one-to-one overlay links between the hub device and its edge devices. When you select <i>DIAL_UP</i>, you can enable ADVPN on the <i>Network</i> tab in the <i>WAN</i> settings.• Select <i>DIAL_UP_FULL_MESH</i> to create full-mesh overlay links on WAN ports between hub devices and edge devices in the same region.• Select <i>SITE_TO_SITE</i> to create full-mesh overlay links between the hub device and its edge devices in the same region.

Option	Description
VDOM Mode	Toggle on to create a profile for a FortiGate VDOM. Toggle off to disable this feature.
Max Edge Count	Available when <i>VPN Mode with Edge</i> is set to <i>DIAL_UP</i> . 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.

4. Click **OK**. The profile is created, and the *System* tab opens.

5. Configure the *System* settings.

For a description of the options on the *System* tab, see [Profile options described on page 89](#).

6. Click the *Network* tab to configure the network settings.

If you're using primary and secondary hubs in a region, you can optionally configure LAN port communication between the hubs. The LAN port communication is used in addition to the default full-mesh overlay link communication between the hubs.

a. On the *Network* tab, expand the *LAN* section.

b. Either click *Create New*, or double-click an interface to open it for updating.

The LAN options are displayed.

The screenshot shows a configuration window for a LAN interface. On the left, there is a list of settings with red asterisks indicating required fields. On the right, there are corresponding input fields or dropdown menus. The settings and their values are: Name (text field with hint 'Start with 'a-z' or 'A-Z' followed with 'a-z' or 'A-Z' or '0-9' or '_' or '-''), Port Type (VLAN), Physical Port (text field), VLAN Id (1), Connect to Peer Hub (OFF), Allow Overlap Between Devices (OFF), Advertise Via BGP (ON), IP Auto Assign (ON), IP Pool (text field), Subnet Mask Length (24), DHCP Mode (NONE), DHCP Pool Size (10), and Access Types (text field). At the bottom, there are two buttons: OK (blue) and Cancel (orange).

c. Toggle *Connect to Peer Hub* to **ON**.

You must enable this option in the profile for the primary hub and the profile for the secondary hub.

d. For primary hub devices, toggle *Allow Overlap Between Devices* to **ON**.

In the *IP Address* box, type the IP address for the primary hub, and in the *Peer Hub's IP Address* box, type the IP address for the secondary hub.

This option is not available for secondary hubs.

e. Set the remaining options as desired, and click **OK** to save the WAN configuration.

For a description of the options on the *Network* tab, see [Profile options described on page 89](#).

7. Click the *Business* tab to create business rules.
For a description of the options on the *Business* tab, see [Profile options described on page 89](#).
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 97](#).

To create profiles:

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

The following table identifies settings that are specific to configuring an edge device. You can set the remaining settings as desired.

Option	Description
Device Role	Select <i>Edge</i> 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: <ul style="list-style-type: none"> • Select <i>DIAL_UP</i> to create one-to-one overlay links between the hub device and its edge devices. When you select <i>DIAL_UP</i>, you can enable ADVPN on the <i>Network</i> tab in the <i>WAN</i> settings. • Select <i>DIAL_UP_FULL_MESH</i> to create full-mesh overlay links on WAN ports between hub devices and edge devices in the same region. • Select <i>SITE_TO_SITE</i> to create full-mesh overlay links between the hub device and its edge devices in the same region.
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.

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 89](#).
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 VDOMs

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 97](#).

You can configure a VDOM as a primary or secondary hub device as well as an edge device.

To create profiles for VDOMs:

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

The following table identifies settings that are specific to configuring a FortiGate VDOM. You can set the remaining settings as desired.

Option	Description
VDOM Mode	Toggle on to create a profile for a FortiGate VDOM.
Running on Cloud	Toggle off to disable this feature.

4. Click **OK**. The profile is created, and the *System* tab opens.
5. Configure the *System* settings.
For a description of the options on the *System* tab, see [Profile options described on page 89](#).
6. Configure the *Network* settings.
You can add physical interfaces for the VDOM to the profile. See [Adding physical interfaces for VDOMs on page 63](#).
Alternately, you can retrieve the VDOM interfaces when you add the VDOM to SD-WAN Orchestrator MEA. It is recommended to retrieve VDOM interfaces. See [Adding VDOMs on page 36](#).
For a description of the options on the *Network* tab, see [Profile options described on page 89](#).
7. Click the *Business* tab to create business rules.
For a description of the options on the *Business* tab, see [Profile options described on page 89](#).
8. Click **OK**.

Creating profiles with FortiExtender WAN ports

You can use a FortiExtender as a WAN port for FortiGates.

Before configuring the WAN port, configure shared resources for FortiExtender for selection in the profile. For example, you can configure a profile for the data plan. For SIM cards, you can use the default profiles for SIM cards, or you can create a custom SIM card profile. For information about creating the shared resources, see [Creating extender resources on page 104](#).



When creating profiles for managed devices with authorized FortiExtenders, ensure that you use the same settings for FortiExtender in the SD-WAN Orchestrator MEA profile that you used in FortiOS because the profile will be applied to all authorized FortiExtenders.

To create profiles with FortiExtender WAN ports:

1. Go to *Configuration > Profile*.
2. In the toolbar, click **+Create New**.
The settings on the *General* tab are displayed.
3. Complete the settings on the *General* tab, and click **OK**:
 - a. In the *Platform* box, select a device that supports FortiExtender, such as *FortiWiFi-40F-3G4G*.
 - b. Set the remaining options as desired.
The profile is created, and the *System* tab opens.

4. Click the *Network* tab, and add a WAN interface for FortiExtender:

- Under WAN, click *Create New*.
The *WAN* dialog box is displayed.
- In the *Name* box, type a name for the interface.
- In the *Port Type* box, select *EXTENDER*.
- In the *ISP Link* box, select the default *FEXT_ISP_Link_1*.
- Set the remaining options as desired, and click *OK*.

FortiExtender is added as a WAN port.

5. Define the FortiExtender data plan and SIM card settings:

- In the *WAN* section, and click *Extender*.
The *FortiExtender <profile name>* dialog box is displayed.

FortiExtender

Data Plans

Templates

Model	Modem1 Sim Profile
<input type="radio"/> FortiExtender-201E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-211E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-40D-AMEU	DEFAULT_SIM_PROFILE

OK Cancel

- In the *Data Plans* box, select a data plan.
- Beside *Templates*, select the FortiExtender model.
The *Update* button is displayed.

FortiExtender

Data Plans

best-data-plan

Templates

Update

Model	Modem1 Sim Profile
<input checked="" type="radio"/> FortiExtender-201E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-211E	DEFAULT_SIM_PROFILE
<input type="radio"/> FortiExtender-40D-AMEU	DEFAULT_SIM_PROFILE

OK Cancel

- Click the *Update* button to select a different SIM profile for the selected FortiExtender model, and click *OK*.
The SIM profile is updated.
- Click *OK*.

A data plan profile and SIM card profile are defined for the FortiExtender model.

6. Set options on the other tabs as needed.

For a description of the options on each tab, see [Profile options described on page 89](#).

7. Click *OK*.

The profile is updated with the specified configuration.

8. Add FortiExtender to SD-WAN Orchestrator MEA by using one of the following methods:

- [Adding FortiExtenders to online devices on page 43](#)
- [Adding devices with authorized FortiExtenders on page 45](#)

Creating profiles for HA devices

Before you create a profile, you should create all of the needed shared resources, so you can select them in the profile. See [Shared resources on page 97](#).

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

To create profiles for HA devices:

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

The screenshot shows the 'Profile /' configuration window with the 'Network' tab selected. The 'HA Interfaces' section is expanded, showing 'Monitor Interfaces' with a dropdown menu set to 'port1 x' and 'Heartbeat Interfaces' with a dropdown menu set to 'port10 x'. At the bottom of the window are 'OK' and 'Cancel' buttons.

For a description of the options on the *Network* tab, see [HA Interfaces on page 96](#).

7. Configure the options on the *System* and *Business* tabs as desired.
For a description of the options on the *System* and *Business* tabs, see [Profile options described on page 89](#).
8. Click *OK*.

Adding physical interfaces for VDOMs

When creating a profile for VDOMs, you can add physical interfaces to the profile and configure them. The settings in the profile can be used for all VDOMs.

Instead of adding physical interfaces to the profile for all VDOMs, you can retrieve interfaces for the VDOM when you add it to SD-WAN Orchestrator MEA. See [Adding VDOMs on page 36](#).

To add physical interfaces:

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.

The screenshot shows the 'Profile / test-vdom' dialog box with the 'General' tab selected. The fields are as follows:

Field	Value
Name	test-vdom
Platform	FortiGate-VM64
Device Role	SECONDARY_HUB
VPN Mode with Edge	DIAL_UP
Vdom Mode	ON
Max Edge Count	500
Port Number	10
Running On Cloud	OFF
Comments	

Buttons: OK, Cancel

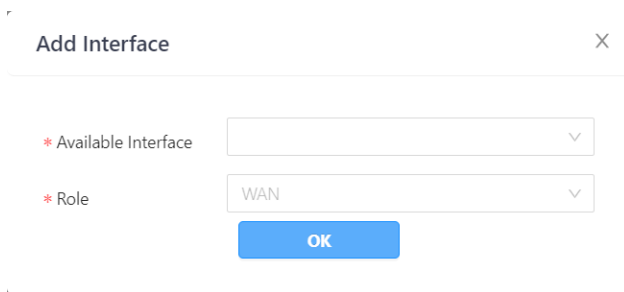
3. Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).

The screenshot shows the 'Profile / test-vdom' dialog box with the 'Network' tab selected. The 'Add Physical Interface' button is highlighted. Below it is a list of expandable sections:

- > WAN
- > LAN
- > DMZ
- > MGMT
- > BGP
- > OSPF
- > DNS Server
- > SNMP
- > HA Interfaces

Buttons: OK, Cancel

4. Add physical interfaces to the profile:
 - a. Click *Add Physical Interface*.
The *Add Interface* dialog box is displayed.



The 'Add Interface' dialog box contains two dropdown menus. The first is labeled '* Available Interface' and is currently empty. The second is labeled '* Role' and has 'WAN' selected. Below the dropdowns is a blue 'OK' button. There is a close 'X' button in the top right corner of the dialog.

- b. Complete the options, and click **OK**.

Option	Description
Available Interface	Select an interface.
Role	Specify a role for the interface. Choose from the following: <ul style="list-style-type: none"> • WAN • LAN • DMZ

- c. When you are finished adding physical interfaces, close the dialog box.

The added interfaces display in the section for the role. For example, if you added a physical interface for a role of WAN, the interface displays in the WAN table.

5. Click **OK**.

The profile is saved.

Creating new WAN settings

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

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

To create new WAN settings:

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

Profile / edge

General
System
Network
Business

* Name
edge

* Platform
FortiGate-VM64

* Device Role
EDGE

VPN Mode with Edge
DIAL_UP

Vdom Mode
OFF

* Port Number
10

Running On Cloud
OFF

Comments

OK Cancel

3. Click the *Network* tab.

The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).

4. Expand the *WAN* section, and click *+Create New*.

The WAN dialog box is displayed.

+ WAN

* Name
Start with 'a-z' or 'A-Z' followed with 'a-z' or 'A-Z' or '0-9' or '_' or '-'

* Port Type
VLAN

* Physical Port

* VLAN Id
1

Enable SDWAN
ON

* ISP Link

* VPN Connect to Hub ISP Link

ADVPN
OFF

* Mode
STATIC

* Estimated Upstream Bandwidth
2000000 Kbps

* Estimated Downstream Bandwidth
2000000 Kbps

Access Types

OK Cancel

5. In the *Name* box, type a name for the WAN settings.

6. In the *Port Type* box, select the port, and complete the options.

Port Type	Description
VLAN	Select to configure a virtual interface.
Aggregate	Select to configure an aggregate virtual interface.

Port Type	Description
Hard_Switch	<p>Select to configure a hardware switch. A hardware switch is a virtual switch interface that groups different ports together. FortiGate uses the group of ports as a single interface.</p> <p>Supported FortiGate models have a default hardware switch called either <i>internal</i> or <i>lan</i>. The hardware switch is supported by the chipset at the hardware level. For example, the FortiGate 60E/61E series supports hardware switches.</p>
Soft_Switch	<p>Select to configure a software switch. A software switch is a virtual switch interface that is implemented at the software or firmware level and not at the hardware level. FortiGate uses the group of ports as a single interface.</p>
Extender	<p>Select to configure FortiExtender as a WAN port. See also Creating profiles with FortiExtender WAN ports on page 61.</p>

7. Complete the remaining options, and click OK.

Option	Description
Physical Port	<p>Available when <i>Port Type</i> set to <i>VLAN</i>.</p> <p>Select the port number.</p> <p>Displays <i>wwan</i> for FortiGate 40F-3G4G models with enabled WWAN ports.</p>
VLAN ID	<p>Available when <i>Port Type</i> is set to <i>VLAN</i>.</p> <p>Type an ID for the VLAN.</p>
Enable SDWAN	<p>Toggle on to enable the interface. Toggle off to disable the interface.</p>
Interface Status	<p>Available when <i>Enable SDWAN</i> is toggled <i>OFF</i>.</p> <p>Overlay links are not initiated on a WAN port with the following settings:</p> <ul style="list-style-type: none"> • <i>Enable SDWAN</i> is toggled <i>OFF</i>. • <i>Interface Status</i> is set to <i>UP</i>. • <i>Mode</i> is set to <i>STATIC</i>. <p>However, overlay links can be established on VLAN ports that are based on the physical WAN port.</p>
ISP Link	<p>Available for edge devices when <i>VPN Mode with Hub</i> is set to <i>SITE_TO_SITE</i> on the <i>General</i> tab.</p>
VPN Connect to Hub ISP Link	<p>Available for edge devices when <i>VPN Mode with Hub</i> is set to <i>SITE_TO_SITE</i> on the <i>General</i> tab.</p> <p>When configuring WWAN interfaces, select an LTE type of ISP link, such as <i>DEFAULT_ISP_LTE_1</i>. Any other setting will disable the wwan feature.</p>
ADVPN	<p>Available for edge devices when <i>VPN Mode with Hub</i> is set to <i>DIAL_UP</i> on the <i>General</i> tab.</p> <p>On hub devices, select one of the following options:</p> <ul style="list-style-type: none"> • <i>NONE</i> - ADVPN is disabled. Edge devices from the same region will communicate with each other by forwarding packets through their region's hub.

Option	Description
	<ul style="list-style-type: none"> INSIDE_REGION - Shortcut tunnels are triggered by traffic and established only inside a region. <p>On edge devices, toggle <i>ADVPN</i> on to enable ADVPN. Toggle off to disable ADVPN.</p>
Connected External VPN Gateway	Select an external VPN Gateway. See also Creating external VPN gateways on page 105 .
Mode	Select a mode.
DNS Server Override	Toggle <i>On</i> to enable DNS server override.
Use VIP for VPN Connection	<p>Toggle <i>On</i> to enable VIP mapping for the WAN port.</p> <p>This feature allows overlay tunnels to be established when FortiGate devices are deployed on Cloud platforms, such as AWS, Azure, and on. It also helps establish overlay links between devices when both devices are behind a NAT gateway.</p>
VIP Address	<p>Available when <i>Use VIP for VPN Connection</i> is on.</p> <p>Type the VIP address for the device. When enabled, tunnels are established with the VIP address instead of the intranet IP address.</p> <p>If the FortiGate is deployed on a Cloud platform, contact the Cloud operator to obtain the public IP address .</p>
Estimated Upstream Bandwidth	Leave the default value, or specify an estimated value.
Estimated Downstream Bandwidth	Leave the default value, or specify an estimated value.
Schedule Recurring Speed Test	Expand to display the <i>Enable Schedule Speed Test</i> option. See also Executing WAN port speed tests on page 54 .
Enable Schedule Speed Test	Toggle <i>On</i> to display the schedule options for the speed test.
Schedule	<p>Available when <i>Enable Schedule Speed Test</i> is toggled <i>On</i>.</p> <p>From the list select a schedule for the speed test. See also Creating custom speed test schedules on page 110.</p>
Auto Apply Speed Test Result	Toggle <i>On</i> to automatically apply speed test results to the <i>Estimated Upstream Bandwidth</i> and <i>Estimated Downstream Bandwidth</i> options.
First Online Speed Test	Toggle <i>On</i> to run the speed test when the device first comes online.
Access Types	Select one or more types of access.

The WAN settings are created.

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

Creating new LAN settings

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

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

To create new LAN settings:

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

The screenshot shows the 'Profile / edge' dialog box with the 'General' tab selected. The fields are as follows:

- Name:** edge
- Platform:** FortiGate-VM64
- Device Role:** EDGE
- VPN Mode with Edge:** DIAL_UP
- Vdom Mode:** OFF
- Port Number:** 10
- Running On Cloud:** OFF
- Comments:** (empty text area)

At the bottom are 'OK' and 'Cancel' buttons.

3. Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).
4. Expand the *LAN* section, and click *+Create New*.
The *LAN* dialog box is displayed.

The screenshot shows the 'LAN' dialog box with the following fields:

- Name:** (placeholder: Start with 'a-z' or 'A-Z' followed with 'a-z' or 'A-Z' or '0-9' or '.' or '-')
- Port Type:** VLAN
- Physical Port:** (empty dropdown)
- VLAN Id:** 1
- Connect to Peer Hub:** OFF
- Allow Overlap Between Devices:** OFF
- Advertise Via BGP:** ON
- IP Auto Assign:** ON
- IP Pool:** (empty dropdown)
- Subnet Mask Length:** 24
- DHCP Mode:** NONE
- DHCP Pool Size:** 10
- Access Types:** (empty text area)

At the bottom are 'OK' and 'Cancel' buttons.

5. In the *Name* box, type a name for the LAN settings.
6. In the *Port Type* box, select the port.

Port Type	Description
VLAN	Select to configure a virtual interface.
WiFi_SSID	Select to configure a wireless network interface (SSID).
Aggregate	Select to configure an aggregate virtual interface.
Hard_Switch	<p>Select to configure a hardware switch. A hardware switch is a virtual switch interface that groups different ports together. FortiGate uses the group of ports as a single interface.</p> <p>Supported FortiGate models have a default hardware switch called either <i>internal</i> or <i>lan</i>. The hardware switch is supported by the chipset at the hardware level. For example, the FortiGate 60E/61E series supports hardware switches.</p>
Soft_Switch	Select to configure a software switch. A software switch is a virtual switch interface that is implemented at the software or firmware level and not at the hardware level. FortiGate uses the group of ports as a single interface.

7. Complete the remaining options, and click *OK*.

Option	Description
Connect to Peer Hub	<p>Available when configuring profiles for primary or secondary hubs.</p> <p>Toggle on to configure LAN communication between a primary hub and a secondary hub in a region. You must enable this option in the profile for the primary hub and the profile for the secondary hub to enable communication for the interface.</p>
Allow Overlap Between Devices	<p>For edge devices, toggle on to allow overlap between devices. Toggle off to disable this feature.</p> <p>For primary hub devices, toggle on to configure the local address and peer hub address for the LAN port to communicate between the primary and secondary hubs.</p> <p>For secondary hubs, this feature is disabled and cannot be enabled.</p>
Advertise via BGP	<p>Toggle <i>ON</i> to advertise the subnets of LAN interfaces that are not allowed overlap to other devices via BGP.</p> <p>For LAN on a secondary hub with the <i>Share Primary Hub Subnet</i> toggled <i>ON</i>, the <i>Allow Overlap Between Devices</i> option is toggled <i>ON</i> and hidden. You can choose whether to advertise subnets via BGP.</p> <p>Toggle <i>OFF</i> to disable advertisement of subnets via BGP.</p>
IP Address	Available when <i>Allow Overlap Between Devices</i> is enabled.
Peer Hub's IP Address	Available when <i>Allow Overlap Between Devices</i> is enabled.
IP Auto Assign	<p>Available when <i>Allow Overlap Between Devices</i> is disabled.</p> <p>Toggle on to automatically assign IP addresses. Toggle off to disable this feature.</p>

Option	Description
IP Pool	Available when <i>IP Auto Assign</i> is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator MEA to automatically assign.
Subnet Mask Length	Available when <i>IP Auto Assign</i> is enabled. Specify the length of the subnet mask.
DHCP Mode	Specify whether to use DHCP for automatic IP assignment. Select one of the following options: <ul style="list-style-type: none"> • <i>None</i> - DHCP is not used. • <i>Server</i> - Enable DHCP server. • <i>Relay</i> - Enable DHCP relay agent.
Access Types	Select the types of access to allow on the interface.
Interface Members	Available when <i>Port Type</i> is set to <i>Hard_Switch</i> or <i>Soft_Switch</i> . Select the ports to include in the interface group.

The LAN settings are saved.

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

Attaching a FortiSwitch model to FortiGate

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



Do not connect FortiSwitch to the physical FortiGate port until the FortiSwitch profile is installed. See [Install a profile on a device](#).

If FortiSwitch is already connected to FortiGate:

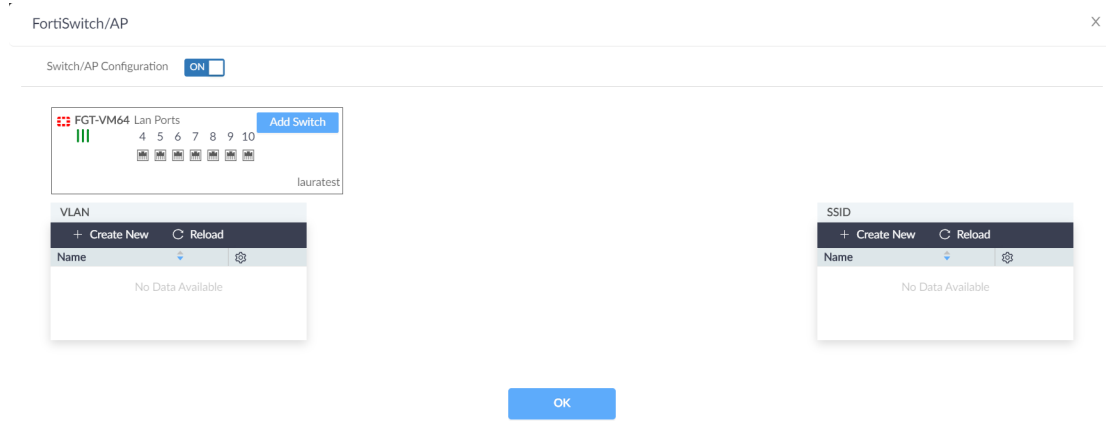
Configure and install the profile without FortiLink and FortiSwitch first. After the profile has successfully synchronized with FortiGate, add the FortiLink and FortiSwitch configuration, and then install the profile again.

To attach a FortiGate port to a FortiSwitch:

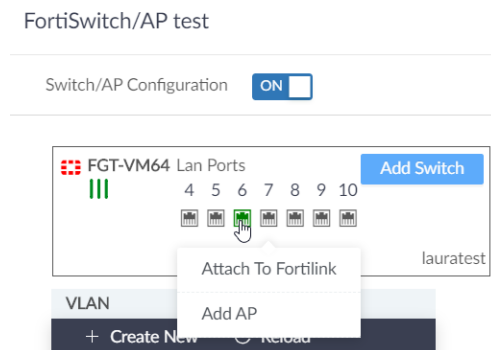
1. Go to *Configuration > Profile*.
The list of profiles is displayed.
2. Create a new profile, or open a profile for updating.
The *Profile / <Name>* dialog box is displayed.
3. Display the Switch/AP settings.
 - a. Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).
 - b. Expand the *LAN* section, and toggle *Switch/AP Configuration* to *ON*.
The *Switch/AP* button is displayed.

c. Click *Switch/AP*.

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



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

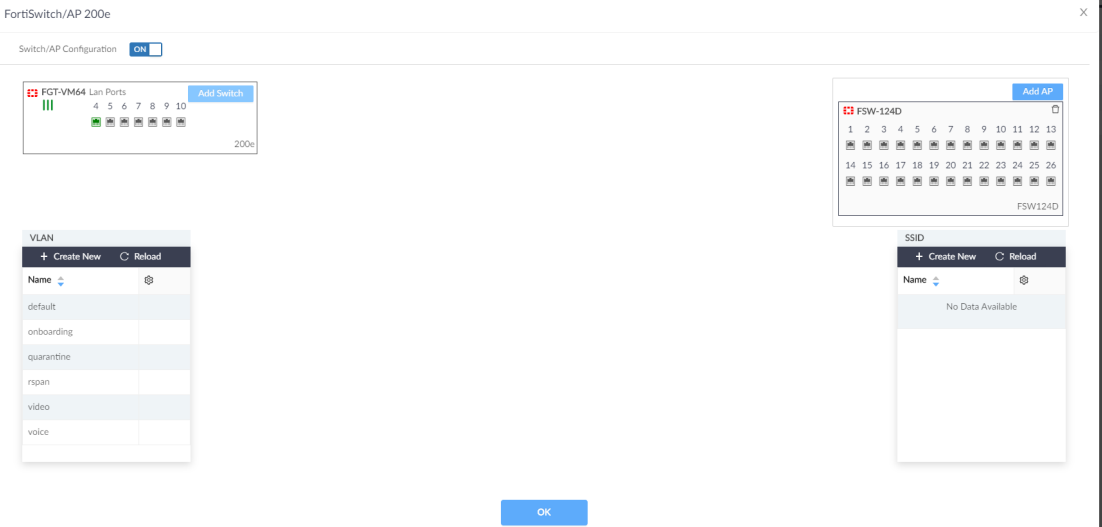


The port is attached, and the VLAN settings are created.

5. Add a platform model.

- a. Click *Add Switch*.
- b. In the *Name* field, enter a name for the FortiSwitch.
- c. From the *Platform* dropdown, select a FortiSwitch model.
- d. Click *OK*.

The switch is added to the profile.



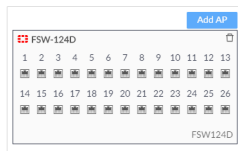
To assign a VLAN to ports in a switch template:

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

Option	Description
Name	Type a name for the interface.
Allow Overlap Between Devices	Toggle on to allow overlap between devices. Toggle off to disable this feature.
VLAN Id	Enter a unique VLAN ID.
IP Auto Assign	Available when <i>Allow Overlap Between Devices</i> is disabled. Toggle on to automatically assign IP addresses. Toggle off to disable this feature.
IP Pool	Available when <i>IP Auto Assign</i> is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator to automatically assign.
Subnet Mask Length	Available when <i>IP Auto Assign</i> is enabled.
DHCP Mode	Specify whether to use DHCP for automatic IP assignment. Select one of the following options: <ul style="list-style-type: none"> • <i>None</i> - DHCP is not used. • <i>Server</i> - Enable DHCP server. • <i>Relay</i> - Enable DHCP relay agent.
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.



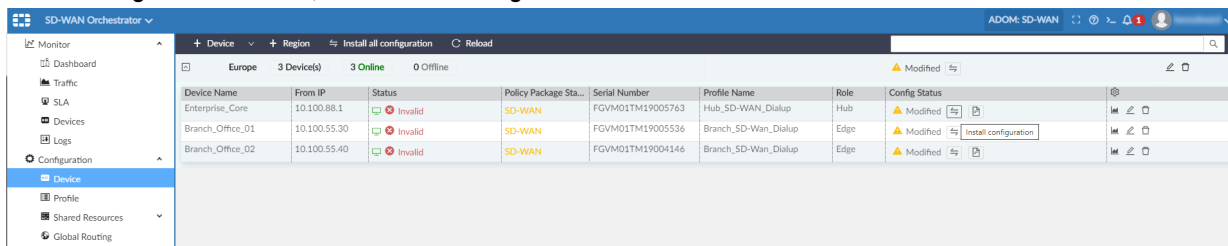
The *More Configuration/ <port>* dialog box is displayed.

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 <i>default</i> or <i>default-auto-isl</i> .
Loop Guard	Toggle on to enable Loop Guard for the port. Loop Guard cannot be applied to ports that are in trunks.
Port Security-policy	Select a port security policy from the dropdown.
Stp State	Toggle on to enable this feature.
stp Root-gaurd	Toggle on to enable STP Root Guard for the port.
Edge Port	Right-click to enable or disable Edge Port for the port.
stp bpdu-guard	Toggle on to enable STP BPDU Guard for the port.

To install a profile on a device:

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



Wait for the status to change to *Synchronized*.

- 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:

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

The screenshot shows the FortiGate 200E web interface. The left sidebar has 'WiFi & Switch Controller' expanded, with 'Managed FortiSwitch' selected. The main content area shows a 'Status' widget with a green circle and 'Online' text, and a 'Model' widget with a blue circle and 'S448DN' text. Below these is a table of managed FortiSwitches.

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

- On FortiManager, go to *FortiSwitch Manager > Device & Groups*, and select a device in the tree menu.
Check the *FortiSwitch Name* column to verify the device is online.

To verify the device received the configuration:

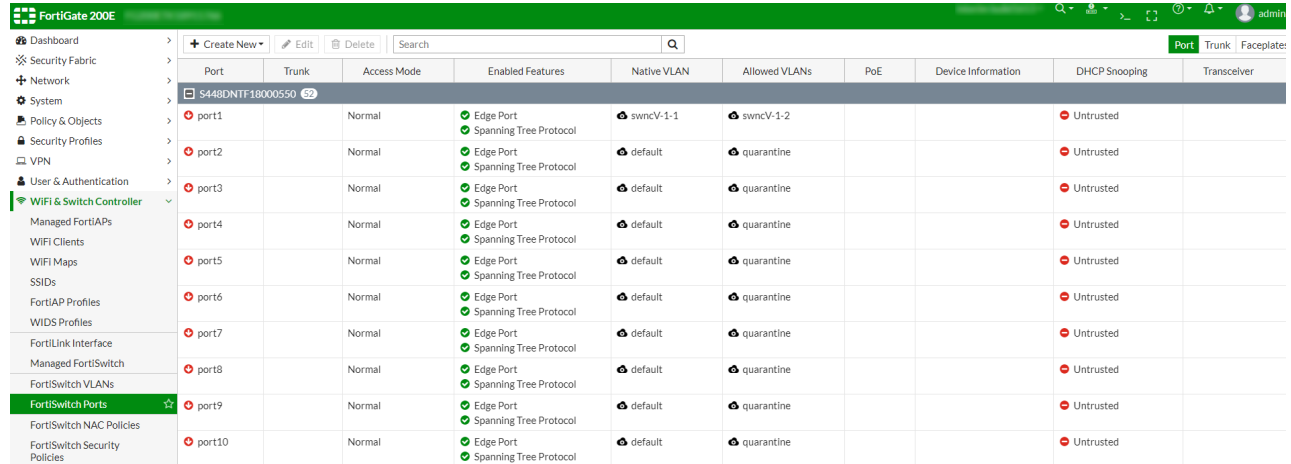
- On FortiGate go to *Network > Interfaces*, and expand the interface in the table.
In the *Name* column check that the target interface is set as *fortilink* member.
In the *Type* column check that then VLANs in the controller profile are displayed.

The screenshot shows the FortiGate 200E web interface with 'Network > Interfaces' selected. A table lists the configured interfaces. The 'fortilink' interface is highlighted, showing it is a '802.3ad Aggregate' type with 'port5' as a member. Below it, a list of VLANs is shown, each associated with a specific IP address and administrative access.

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
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 SSH HTTP		111.111.111.2-111.111.111.11	2
swncv-1-2	VLAN		222.222.222.1/255.255.255.0					1
loopback-root	Loopback Interface		169.254.128.1/255.255.255.255		PING FMG-Access			0
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		Normal	Edge Port Spanning Tree Protocol	swncV-1-1	swncV-1-2			Untrusted	
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine			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.

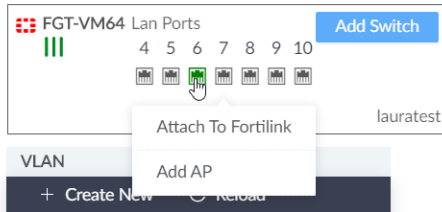
To add a model FortiAP to a FortiGate:

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 toggle *Switch/AP Configuration* to *ON*.
The *Switch/AP* button is displayed.
 - c. Click *Switch/AP*.
The *FortiSwitch/AP <Name>* dialog box is displayed.

4. Select a FortiGate port, and click *Add AP*.

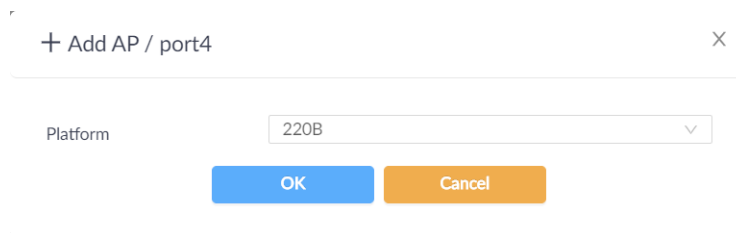
FortiSwitch/AP test

Switch/AP Configuration



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**

LAN / port6

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 x FABRIC x

Role: LAN

OK Cancel

- f. Click OK again.

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

SD-WAN Orchestrator

ADOM: SD-WAN

Device Region Install all configuration Reload

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.

FortiGate 200E

Dashboard Security Fabric FortiView Network System Policy & Objects Security Profiles VPN User & Device

WiFi & Switch Controller

Managed FortiAPs

Access Point	Status	SSIDs	Channel	Health	Clients	OS Version	LLDP	FortiAP Profile	Connected Via	Ref.
FP221E5519045559	Online	None	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 > Device & Groups*.

Check the *Access Point* column to verify the device is online.

Check the *AP Profile* column to verify the correct profile was deployed.

To add an SSID profile to a ports AP profile:

- In the SSID table, create a new profile or select a profile to update.
The +SSID dialog box is displayed.

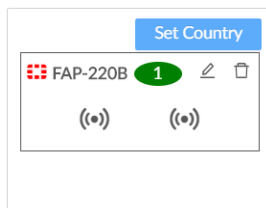
2. Configure the SSID settings, and click *OK*.

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: <ul style="list-style-type: none"> • <i>Open</i> • <i>WPA2_PERSONAL</i> • <i>WPA3_SAE</i> • <i>WPA3_SAE_TRANSITION</i>
Pre-shared Key	Enter the pre-shared key for the SSID. This option is only available when the security mode includes <i>WPA2_PERSONAL</i> and <i>WPA3_SAE_TRANSITION</i> .
SAE Password	Enter the password for the SSID. This option is only available when the security mode includes <i>WPA3_SAE</i> and <i>WPA3_SAE_TRANSITION</i> .
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 <i>Allow Overlap Between Devices</i> is disabled. Toggle on to automatically assign IP addresses. Toggle off to disable this feature.
IP Pool	Available when <i>IP Auto Assign</i> is enabled. Specify a pool of IP addresses to be used for SD-WAN Orchestrator to automatically assign.
Subnet Mask Length	Available when <i>IP Auto Assign</i> is enabled. Specify the length of the subnet mask.
DHCP Mode	Specify whether to use DHCP for automatic IP assignment. Select one of the following options: <ul style="list-style-type: none"> • <i>None</i> - DHCP is not used. • <i>Server</i> - Enable DHCP server.

Option	Description
	<ul style="list-style-type: none"> <i>Relay</i> - Enable DHCP relay agent.
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: <ul style="list-style-type: none"> <i>HTTPS</i> <i>SSH</i> <i>SNMP</i>
Login Password Change	Choose from: <ul style="list-style-type: none"> <i>LEAVE_UNCHANGED</i> <i>SET</i> <i>SET_EMPTY</i>
Mode	Choose from: <ul style="list-style-type: none"> <i>DISABLED</i> <i>AP</i> <i>MONITOR</i>
Wids Profile	Choose from: <ul style="list-style-type: none"> <i>default</i> <i>default-wids-apscan-enabled</i>
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.
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-	Select to enable the short guard interval.

Option	Description
interval	
Auto TX Power Control	Enable automatic adjustment of transmit power.
TX Power (%)	If <i>Auto TX Power Control</i> is disabled, enter the TX power in the form of the percentage of the total available power. If <i>Auto TX Power Control</i> is enabled, enter the <i>TX Power Low (dBm)</i> and <i>TX Power High (dBm)</i> 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.

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

- 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:

- Go to *Configuration > Profile*.
The list of profiles is displayed.
- Create a new profile, or open a profile for updating.
The *Profile <name>* dialog box is displayed.
- Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).
- Expand the *DMZ* section, and click *+Create New*.
The *DMZ* dialog box is displayed.

Option	Description
Name	Type a name for the interface.
Port Type	Select the type of port. Choose from <i>VLAN</i> or <i>AGGREGATE</i> .

Option	Description
Physical Port	Available when <i>Port Type</i> is set to <i>VLAN</i> . Select the port number.
VLAN ID	Available when <i>Port Type</i> is set to <i>VLAN</i> . Type an ID for the VLAN.
Allow Overlap Between Devices	Toggle on to allow overlap between devices and specify the IP address of the other device.
Advertise via BGP	Toggle <i>ON</i> to advertise the subnets of DMZ interfaces that are not allowed overlap to other devices via BGP. Toggle <i>OFF</i> to disable advertisement of subnets via BGP.
IP Address	Available when <i>Allow Overlap Between Devices</i> is toggled on. Type the IP address of the device that can be overlapped.
IP Auto Assign	Available when <i>Allow Overlap Between Devices</i> is toggled off. Toggle on to allow automatic IP assignment from a pool of IP addresses.
IP Pool	Available when <i>IP Auto Assign</i> is toggled on. Select the pool of IP addresses to use for automatic assignment. If you have not yet created a pool of IP addresses, you can create one. In the dropdown list, click <i>Create</i> . See also Creating intranet IP pools on page 101 .
Subnet Mask Length	Type the prefix of the IP address or subnet mask.
DHCP Mode	Specify whether to use DHCP for automatic IP assignment. Select one of the following options: <ul style="list-style-type: none"> <i>None</i> - DHCP is not used. <i>Server</i> - Enable DHCP server. <i>Relay</i> - Enable DHCP relay agent.
DHCP	When <i>DHCP Mode</i> is set to <i>Server</i> , select a server from shared resources. See Creating DHCP servers on page 100 . When <i>DHCP Mode</i> is set to <i>Relay</i> , select a relay agent from shared resources. See Creating DHCP relay agents on page 100 .
DHCP Pool Auto Assign	Available when <i>DHCP Mode</i> is set to <i>Server</i> . Toggle on to enable and specify the pool size.
Access Types	Select the types of access to allow on the interface.

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

Creating virtual wire pairs

When creating a profile, you can also create a virtual wire pair. A virtual wire pair consists of two interfaces that do not have IP addressing and are treated like a transparent-mode VDOM.

You can create a virtual wire pair for FortiGate VMs and hardware.

To create a virtual wire pair:

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 92](#).
4. Expand the *Virtual Wire Pair* section, and click *+Create New*.
The *Virtual Wire Pair* dialog box is displayed.

Option	Description
Name	Type a name for the virtual wire pair.
Interface Members	Select two interface members for the virtual wire pair. A virtual wire pair must have exactly two interface members.
Wildcard VLAN	Toggle <i>ON</i> to enable wildcard VLAN. Toggle <i>OFF</i> to disable this feature.
VLAN Filter	Available when <i>Wildcard VLAN</i> is toggled <i>ON</i> . Click <i>Add</i> to create a VLAN filter.

5. Complete the options, and click *OK*.
The virtual wire pair is created.
6. Go to FortiManager, and configure a virtual wire pair policy.

Creating new BGP network

When creating a profile, you can also create a new port subnet for BGP.

To create new BPG network 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 92](#).
4. Expand the *BGP* section, and click *+Create New*.
The *BGP Network* dialog box is displayed.

Option	Description
Type	Displays <i>Port Subnet</i> .
Physical Port	Select the port for the subnet.

- Complete the options, and click **OK**.
The port subnet for BGP is created.

Creating new OSPF area

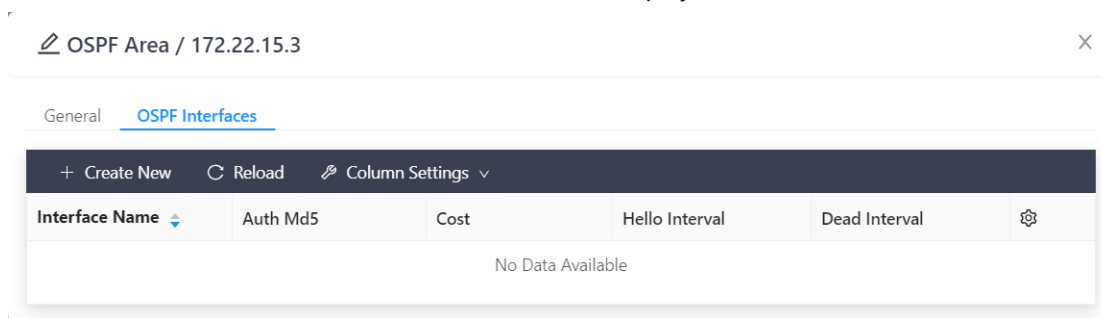
When creating a profile, you can also create a new OSPF area and add interface members.

To create new OSPF area:

- Go to *Configuration > Profile*.
The list of profiles is displayed.
- Create a new profile, or open a profile for updating.
The *Profile <name>* dialog box is displayed.
- Click the *Network* tab.
The *Network* pane is displayed. For a description of the options, see [Network tab on page 92](#).
- Expand the *OSPF* section, and click **+Create New**.
The *OSPF Area* dialog box is displayed.
- Complete the options, and click **OK**.

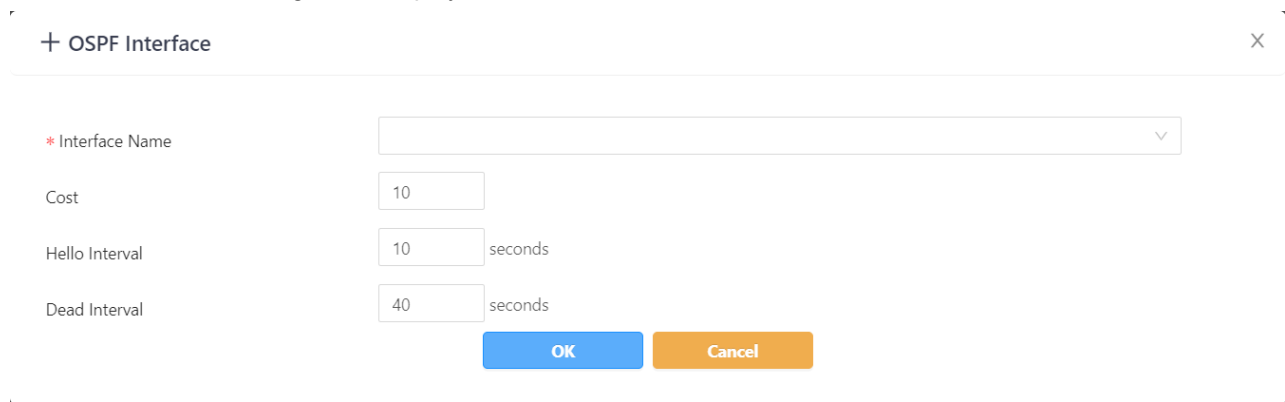
Option	Description
Area	Type the IP address for the OSPF area.
Type	Select the type of area. Choose from the following: <ul style="list-style-type: none"> Regular Stub NSSA
Authentication	Choose whether to enable authentication. Choose from the following: <ul style="list-style-type: none"> None MD5 Text

The OSPF area is created, and *OSPF Interfaces* tab is displayed.



6. Click *Create New*.

The *OSPF Interface* dialog box is displayed.

**7. Configure the options, and click *OK*.**

The interface is defined for OSPF.

8. Close the dialog box.

The OSPF area is displayed with the defined interfaces.

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.

+ Business Rule
X

* Name ⓘ Allowed characters: a-z A-Z 0-9 _ -

Criteria

* Source Address

Users

User Groups

Destination Type ADDRESS

* Dest Address

* Service

* Enable ON

Link Policy

* Group Type UNDERLAY

* Path MULTIPLE_PATH

* Load Policy LOW_COST

* SLA Quality Level LOW

* SLA Server Type AUTOMATIC

OK Cancel

5. Complete the options, and click OK.

Option	Description
Name	Type a name for the business rule.
Criteria	
Source Address	Select the source address or address group.
Users	Select or create users.
User Groups	Select or create user groups
Destination Type	Select the type of destination for the traffic.
Dest Address	Select or create the destination address or address group.
Service	Select or create the Internet service.
Enable	Toggle <i>ON</i> to enable the rule, and Toggle <i>OFF</i> to disable the rule.
Link Policy	
Group Type	For hub devices, choose from <i>UNDERLAY</i> , <i>EXTERNAL_VPN_GATEWAY</i> , or <i>OVERLAY</i> . For edge devices, choose from <i>UNDERLAY</i> , <i>OVERLAY</i> , <i>ALL</i> , or <i>EXTERNAL_VPN_GATEWAY</i> .
Path	When <i>Group Type</i> is set to <i>OVERLAY</i> , displays the path. When <i>Group Type</i> is set to <i>UNDERLAY</i> , choose from <i>SINGLE_PATH</i> , <i>MULTIPLE_PATH</i> , or <i>ALL_PUBLIC_LINE</i> .
Gateway Path	When <i>Group Type</i> is set to <i>EXTERNAL_VPN_GATEWAY</i> , select the gateway path.
Load Policy	When <i>Group Type</i> is set to <i>Overlay</i> , choose from <i>LOW_COST</i> , <i>HIGH_QUALITY</i> , or <i>HIGH_THROUGHPUT</i> .

Option	Description
	When <i>Group Type</i> is set to <i>Underlay</i> for hub devices, choose from <i>LOW_COST</i> , <i>HIGH_QUALITY</i> , <i>HIGH_THROUGHPUT</i> , or <i>MANUAL</i> .
SLA Quality Level	Displays the minimum quality level.
Dual Hub Load Mode	<p>Available for dual hubs when <i>Group Type</i> is set to <i>OVERLAY</i>. Choose from <i>ACTIVE_PASSIVE</i> or <i>ACTIVE_ACTIVE</i>.</p> <p>When you choose <i>ACTIVE_PASSIVE</i>, the business rule is split and deployed to FortiGate as two rules:</p> <ul style="list-style-type: none"> One rule is for the primary hub, and includes all overlay links to the primary hub as priority members. The other rule is for secondary hub, and includes all overlay links to the secondary hub as priority members. <p>When you choose <i>ACTIVE_ACTIVE</i>, a business rule is deployed to FortiGate as one rule. The priority members include all overlay links between the edge and both hubs.</p>
SLA Server Type	When <i>Group Type</i> is set to <i>Overlay</i> , select the type of SLA server.
SLA Server	Select the SLA server.
Backhaul to Group	When <i>Group Type</i> is set to <i>Overlay</i> for hub devices, choose the backhaul route to the group.

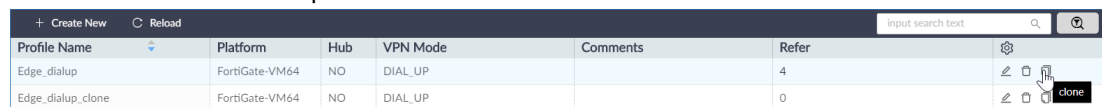
The business rule is created.

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.



+ Create New ○ Reload		Input search text				
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	clone

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

Profile Hub_Dialup

* Source Name ? Hub_Dialup

* Name ? Hub_Dialup_clone

* Platform FortiGate-VM64

Comments

OK Cancel

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.

Profile / test

General **System** Network Business

▼ NTP Setting

* Synchronize with NTP Server ☒

* Server Type FORTIGUARD

Interval 60 minute

> FortiGuard Setting

> Email Setting

> Log Setting

OK Cancel

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.

+ Create New ○ Reload							Input search text		
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				update

The *Profile <name>* dialog box opens.

3. Edit the settings, and click **OK**.
4. Install profile changes. See [Installing configuration changes on page 48](#).

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 89](#)
- [System tab on page 90](#)
- [Network tab on page 92](#)
- [Business tab on page 97](#)

General tab

The *General* tab contains the following sections:

Option	Description
Name	Type a name for the profile. You can use lowercase and uppercase letters, numbers 0 to 9, underscores, and dashes.
Platform	Select a platform for the profile settings.
Device Role	Select <i>PRIMARY_HUB</i> to create a profile for primary hubs. Select <i>SECONDARY_HUB</i> to create a profile for secondary hubs. Select <i>EDGE</i> to create a profile for edge devices.
VPN Mode with Edge	Select one of the following options to connect the hub device with edge devices: <ul style="list-style-type: none"> • Select <i>DIAL_UP</i> to create one-to-one overlay links between the hub device and its edge devices. When you select <i>DIAL_UP</i>, you can enable ADVPN on the <i>Network</i> tab in the <i>WAN</i> settings. • Select <i>DIAL_UP_FULL_MESH</i> to create full-mesh overlay links on WAN ports between hub devices and edge devices in the same region. • Select <i>SITE_TO_SITE</i> to create full-mesh overlay links between the hub

Option	Description
	device and its edge devices in the same region.
VDOM Mode	Toggle on to create a profile for a FortiGate VDOM. Toggle off to disable this feature.
Max Edge Count	Available when <i>Device Role</i> set to <i>Primary_Hub</i> or <i>Secondary_Hub</i> and <i>VPN Mode with Edge</i> is set to <i>DIAL_UP</i> or <i>DIAL_UP_FULL_MESH</i> . 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.
Running on Cloud	Toggle on to support FortiGate Cloud. Toggle off to disable this feature.
Comments	(Optional) Type a comment about the profile.

System tab

The *System* tab contains the following sections:

- [NTP on page 90](#)
- [FortiGuard on page 90](#)
- [Email on page 91](#)
- [Log on page 91](#)
- [Misc Setting on page 92](#)

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: <ul style="list-style-type: none"> • <i>FortiGuard</i> • <i>Specify</i> When you select <i>Specify</i> , you must also select an NTP server.
NTP Servers	Available when <i>Server Type</i> is set to <i>Specify</i> . 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
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: <ul style="list-style-type: none"> • <i>This FortiManager or managed FortiAnalyzer</i>: 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. • <i>Specify IP Address</i>: 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
	<ul style="list-style-type: none">• UDP• Legacy reliable• Reliable
Port	Specify which port to use. See the SD-WAN Orchestrator MEA GUI tooltip (?) for port suggestions.
Minimum Log Level	Specify the minimum level of logs to include.
Format	Specify the log format.

Misc Setting

Expand *Misc Setting* to view the following options:

Option	Description
Admin HTTPS Port	Specify the HTTPS port to use for admin access.

Network tab

The *Network* tab contains the following sections:

- [Physical Interface on page 92](#)
- [WAN on page 93](#)
- [LAN on page 93](#)
- [DMZ on page 94](#)
- [Virtual Wire Pair on page 94](#)
- [BGP on page 95](#)
- [OSPF on page 95](#)
- [DNS Server on page 96](#)
- [SNMP on page 96](#)
- [HA Interfaces on page 96](#)

Physical Interface

On the *General* tab when *VDOM mode* is toggled on, the *Add Physical Interface* button is available on the *Network* tab. In other words, it is available when configuring a profile for VDOM mode.

Click *Add Physical Interface* to add one or more physical interfaces for the role of WAN, LAN, or DMZ. See [Adding physical interfaces for VDOMs on page 63](#).



Instead of adding physical interfaces for use by VDOMs, you can retrieve interfaces when you add a VDOM to SD-WAN Orchestrator MEA. See [Adding VDOMs on page 36](#).

WAN

Expand *WAN* to view the following options:

Option	Description
Create New	Click <i>Create New</i> to define a new WAN interface. You can define the port type as <i>VLAN</i> , <i>Aggregate</i> , <i>Hard_Switch</i> , <i>Soft_Switch</i> , and <i>Extender</i> . When the port type is <i>AGGREGATE</i> , you must save the WAN configuration, and then open it for editing to add interface members. See also Creating new WAN settings on page 65 .
Extender	Available when <i>Running on Cloud</i> is toggled off on the <i>General</i> tab of the profile. Click <i>Extender</i> to configure FortiExtender as a WAN port for FortiGate. See also Creating profiles with FortiExtender WAN ports on page 61 .
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
Interface Members	Displays the interface members for an aggregate interface.
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 <i>Update</i> icon to edit the settings.

LAN

Expand *LAN* to view the following options:

Option	Description
Create New	Click <i>Create New</i> to define a new LAN interface. You can define the port type as <i>VLAN</i> , <i>WiFi_SSID</i> , <i>Aggregate</i> , <i>Hard_Switch</i> , and <i>Soft_Switch</i> . When the port type is <i>AGGREGATE</i> , you must save the LAN configuration, and then open it for editing to add interface members. See also Creating new LAN settings on page 68 .
Switch/AP Configuration	Toggle on to enable configuration of managed FortiSwitch and FortiAP devices, and display the <i>Switch/AP</i> button.

Option	Description
	Toggle off to disable configuration of managed FortiSwitch and FortiAP devices. If you toggle this feature off after configuring switch and AP devices, the configuration is reset for all managed switch and AP devices.
Switch/AP	Available when <i>Switch/AP Configuration</i> is toggled on. Click <i>Switch/AP</i> to define settings for FortiSwitch and FortiAP devices. See also Attaching a FortiSwitch model to FortiGate on page 71 and Adding a FortiAP model device on page 76 .
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
Interface Members	Displays the interface members for an aggregate interface.
Subnet Type	Displays the type of subnet.
IP Address	Displays the IP address.
DHCP Server/Relay	Displays the DHCP mode
DHCP Pool Size	Displays the DHCP pool size.
Access	Displays the types of access to allowed for the interface.
Update	Click the <i>Update</i> icon to edit the settings.

DMZ

Expand *DMZ* to view the following options:

Option	Description
Create New	Click <i>Create New</i> to define a new DMZ interface. You can define the port type as <i>VLAN</i> or <i>AGGREGATE</i> . When the port type is <i>AGGREGATE</i> , you must save the DMZ configuration, and then open it for editing to add interface members. See also Creating new DMZ settings on page 81 .
Interface	Displays the interface name.
Vlan	Displays whether VLAN is used.
Interface Members	Displays the interface members for an aggregate interface.
Enable	Indicates whether the interface is enabled.
Access	Displays the types of access to allowed for the interface.
Update	Click the <i>Update</i> icon to edit the settings.

Virtual Wire Pair

Expand *Virtual Wire Pair* to view the following options:

Option	Description
Create New	Click <i>Create New</i> to define a virtual wire pair. See also Creating virtual wire pairs on page 83 .
Interface Members	Select two interface members for the virtual wire pair. A virtual wire pair must have exactly two interface members.
Wildcard VLAN	Toggle <i>ON</i> to enable wildcard VLAN. Toggle <i>OFF</i> to disable this feature.
VLAN Filter	Available when <i>Wildcard VLAN</i> is toggled <i>ON</i> . Click <i>Add</i> to create a VLAN filter.

MGMT

Expand *MGMT* to view the following options:

Option	Description
Interface	Displays the management interface.

BGP

Expand *BGP* to view the following options:

Option	Description
Router ID	Displays <i>Auto Assign</i> to indicate that the router ID will be automatically assigned.
Redistribute OSPF	Toggle on to enable redistribution of routing table learned by OSPF to other devices controlled by SD-WAN Orchestrator MEA through BGP, or to devices not controlled by SD-WAN Orchestrator MEA, such as Cisco routers. Toggle off to disable.
Create New	Click <i>Create New</i> to define a new BGP network. See also Creating new BGP network on page 83 .
Type	Displays <i>Port Subnet</i> .
Subnet	Displays the physical port name.

OSPF

Expand *OSPF* to view the following options:

Option	Description
Settings	The <i>Settings</i> section displays the OSPF settings.
Router ID	Displays <i>Auto Assign</i> .
Inject Default Route	Select from the following options:

Option	Description
	<ul style="list-style-type: none"> • Always • Enable • Disable
Redistribute	The <i>Settings > Redistribute</i> section lets you enable redistribution of routes between devices managed by SD-WAN Orchestrator MEA and devices that are not managed by SD-WAN Orchestrator MEA.
Redistribute Connected	Toggle on to enable redistribution of connected routes.
Redistribute Static	Toggle on to enable redistribution of static routes.
Redistribute BGP	Toggle on to enable redistribution of routing table learned by BGP to other devices controlled by SD-WAN Orchestrator MEA through OSPF, or to devices not controlled by SD-WAN Orchestrator MEA, such as Cisco routers.
Areas	The <i>Areas</i> section lets you define OSPF areas.
Create New	Click <i>Create New</i> to define a new OSPF area. See Creating new OSPF area on page 84 .

DNS Server

Expand *DNS Server* to view the following options:

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

SNMP

Expand *SNMP* to view the following options:

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

HA Interfaces

Expand *HA Interfaces* to view the following options:

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

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

Business tab

The *Business* tab contains the following options:

Option	Description
Create New	Click <i>Create New</i> to create a new business rule. See Creating business rules on page 85 .
Name	Displays the name of the business rule.
Source	Displays the traffic source.
Destination	Displays the destination for the traffic.
Service	Displays the Internet service.
Policy	Displays the policy for the business rule.
Group Type	Displays the group type for the business rule.
Path	Displays the path for the traffic.
SLA Quality Level	Displays the minimum quality level.
SLA Server	Displays the SLA server.
Enable	Displays whether the business rule is enabled.
Edit	Click to edit the business rule.
Delete	Click to delete the business rule.
Move up	Click to move the business rule up the priority list.
Move down	Click to move the business rule down the priority list.
Clone	Click to clone the business rule to create a new business rule, and then edit the business rule.

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



Starting with SD-WAN Orchestrator MEA 6.4.1.r6, all user specified, custom IP addresses in the LAN/DMZ interface must also be in an intranet IP pool address. See [Address group change on page 98](#).

To view intranet IP pool addresses:

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

Address group change

Starting with SD-WAN Orchestrator MEA 6.4.1.r6, all user specified, custom IP addresses in the LAN/DMZ interface must also be in an intranet IP pool. As a result, the *GROUP.CUSTOM_groupname* address group is no longer needed.

All subnets of LAN/DMZ must be included in a blackhole static route, and the subnet of the blackhole must not equal any subnet of LAN/DMZ. If the subnet of the blackhole equals any subnet of LAN/DMZ, the route of that interface becomes invalid. All user specified, custom IP addresses must be included in an intranet IP pool. See [Creating intranet IP pools on page 101](#).

Address groups in SD-WAN Orchestrator MEA 6.4.1.r5 and earlier

In SD-WAN Orchestrator MEA 6.4.1.r5 and earlier, you could create an address group named *GROUP.CUSTOM_groupname* for each region to contain user specified, custom IP addresses. A custom IP address is an address specified by the user in the LAN/DMZ interface. The IP address is not allocated by SD-WAN Orchestrator MEA. The custom IP address must NOT be in an IP pool, or a conflict occurs.

GROUP_ALL contains all regions' *GROUP.CUSTOM_groupname* address group and all address groups for IP pools, because all addresses allocated from IP pool are included in IP pool address group. As a result, *GROUP_ALL* contains all addresses.

It is not recommended to use *GROUP.CUSTOM_groupname* address group in business rules and in FortiManager policy packages, because it only contains part of the addresses of the corresponding region. It contains only user specified custom addresses of that region, and doesn't contain the addresses allocated from IP pool.

Example

For example, we have a region named Seattle, and an intranet IP pool named *pool1* with a subnet 192.168.0.0/16, a user specified custom address 172.1.1.0/24 for port4 in device with ID 1, and an address 192.168.1.0/24 for port5.

SD-WAN Orchestrator MEA 6.4.1.r5 and earlier handles the scenario as follows:

- *GROUP_ALL* includes address group *GROUP.CUSTOM_Seattle*, *POOL_pool1* two address groups.
- *GROUP.CUSTOM_Seattle* contains *DEVICE_1_port4* (with address 172.1.1.0/24).
- *POOL_pool1* contains *POOL_192.168.0.0_16* (with address 192.168.0.0/16).
- The address *port5* doesn't need to merge in *GROUP_ALL* as an item, because it is included in *POOL_192.168.0.0_16*.

GROUP_Seattle for region Seattle is also created, and this group contains address group *DEVICE_1*, which includes *DEVICE_1_port4* (with address 172.1.1.0/24) and *DEVICE_1_port5* (with address 192.168.1.0/24).

GROUP.CUSTOM_Seattle is not recommended for use in business rules and in FortiManager policy packages; *GROUP_Seattle* is recommended instead.

SD-WAN Orchestrator MEA 6.4.1.r6 and later handles the scenario as follows:

- User must create an intranet IP pool for port4, for example, an intranet IP pool named *pool2* with a subnet 172.1.0.0/23.

As a result, *GROUP_ALL* contains *POOL_pool1* and *POOL_pool2*.

POOL_pool1 contains *POOL_192.168.0.0_16* (with address 192.168.0.0/16).

POOL_pool2 contains *POOL_172.1.0.0_23* (with address 172.1.0.0/23).

The *GROUP.CUSTOM_Seattle* is not need any more, because 172.1.1.0/24 is included in *GROUP_ALL* already.

The old *GROUP_Seattle* and its members are not changed, and you can use the group in business rules and FortiManager policy packages as before.

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 100](#)
- [Creating DHCP relay agents on page 100](#)
- [Creating DNS servers on page 101](#)
- [Creating intranet IP pools on page 101](#)
- [Creating SNMP hosts on page 102](#)
- [Changing network settings on page 102](#)
- [Creating ISP links on page 103](#)
- [Creating extender resources on page 104](#)
- [Creating MD5 keys for OSPF on page 104](#)
- [Creating external VPN gateways on page 105](#)
- [Creating custom IPsec templates on page 106](#)

Creating DHCP servers

To create DHCP servers:

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

Option	Description
Name	Enter a name for the DHCP server.
Lease Time (in Seconds)	Toggle on to specify how long in seconds the DHCP lease time should remain active before it expires. Toggle off to disable lease time.
TFTP Server	Specify the IP address for the Trivial File Transfer Protocol (TFTP) server if used.
DNS Server Res Type	Specify the DNS service to use. Choose from: <ul style="list-style-type: none"> • Default - IP address of the interface that the DHCP server is added to becomes the client's DNS server IP address. • Local - Clients are assigned to FortiGate's configured DNS servers. • Specify - Specify up to three DNS servers.
DNS Server1	Available when <i>DNS Server Res Type</i> is set to <i>Specify</i> . Type the IP address for the DNS server.

4. Beside *Additional DHCP* options, click *Create*.
The *DHCP Option* dialog box is displayed.
5. In the *Code* box, select the code for the type of DHCP server.
For example, code *6* is for a *Domain server*.
6. In the *Type* box, select one of the following options:
7. In the *Value* box, type a value for the type.
8. Click *OK*.
The DHCP option is created and displayed.
9. Click *OK*.
The DHCP server is created.

Creating DHCP relay agents

To create DHCP relay agents:

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 relay agent configuration.
Primary Relay IP	Enter IP address for the primary relay agent.
Secondary Relay IP	Enter IP address for the secondary relay agent.

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:

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

4. Click *OK*.
The DNS server is created.

Creating intranet IP pools

A blackhole static route is added to FortiGates for all intranet IP pools to avoid intranet prefixes being resolved in underlay WAN ports in BGP. All LAN port IP subnets should be contained in one IP pool, and the LAN port subnet must be smaller than IP Pool subnet.

If a LAN port is configured with a custom subnet that is not automatically assigned, ensure that you create or modify an IP pool to include the LAN custom subnet.

See also [Address group change on page 98](#).

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.

Option	Description
Pool	Enter the IP address for the pool.

Creating SNMP hosts

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

To create SNMP hosts:

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

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

Changing network settings

In the network settings, you can change VPN address pool, loopback address pool, and enable anti-theft protection. You can also select an IPsec template to define the IPsec tunnel configuration between hubs in different regions.

To change network settings:

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

Option	Description
VPN Address Pool	Enter the IP address for the VPN address pool.
Loopback Address Pool	Enter the IP address for the loopback address pool.

Option	Description
Auth After Location Change	Toggle <i>On</i> to enable anti-theft protection. When a device is disconnected from the SD-WAN network and reappears in a different geographic location or in a different network topology, access to the overlay is blocked, and information is displayed about the device location change. Administrators can choose whether manually approve access to the network. Toggle <i>Off</i> to disable anti-theft protection.
BGP Community Prefix (First 8 bits)	Displays the prefix number for BGP communities.
IPsec Configuration Between Hubs cross Region	Select an IPsec template to define the configuration between hubs in different regions.

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	<p>From the dropdown, select one of the following options:</p> <ul style="list-style-type: none"> • <i>Internet</i>: An Internet ISP link with a public IP can both initiate or respond IPsec negotiation with peer devices. • <i>MPLS</i>: If a WAN port is set as <i>MPLS</i> link type with <i>Private Wire</i> on, it can only establish IPsec tunnels with other devices' WAN ports that are also configured as <i>MPLS</i>. • <i>LTE</i>: Usually used when local WAN port is behind NAT or without a public IP address. If a WAN port is set as <i>LTE</i>, it can only be IPsec initiator but not responder.
Cost	<p>From the dropdown, select <i>Low</i>, <i>Medium</i>, or <i>High</i>.</p> <ul style="list-style-type: none"> • <i>High</i> sets cost to 3. • <i>Medium</i> sets cost to 2. • <i>Low</i> sets cost to 1. <p>For example, if the Load Policy is <i>LOW_COST</i>, FortiGates usually choose links with lower cost first. As a result, the interface with the lowest assigned cost of 1 is selected.</p>
Public IP	Toggle <i>On</i> if the IP is public.

Creating extender resources

When you create a profile to configure FortiExtender as a WAN port for FortiGates, you can select a SIM card profile and a data plan profile from the pool of shared resources.

This section describes how to create the following shared resources to select in profiles:

- [Creating SIM card profiles on page 104](#)
- [Creating data plan profiles on page 104](#)

Creating SIM card profiles

This section describes how to create profiles for extender SIM cards that you can select when you create profiles that configure FortiExtender as a WAN port for FortiGates.

To create SIM card profiles:

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

Creating data plan profiles

This section describes how to create profiles for extender data plans that you can select when you create profiles that configure FortiExtender as a WAN port for FortiGates.

To create data plan profiles:

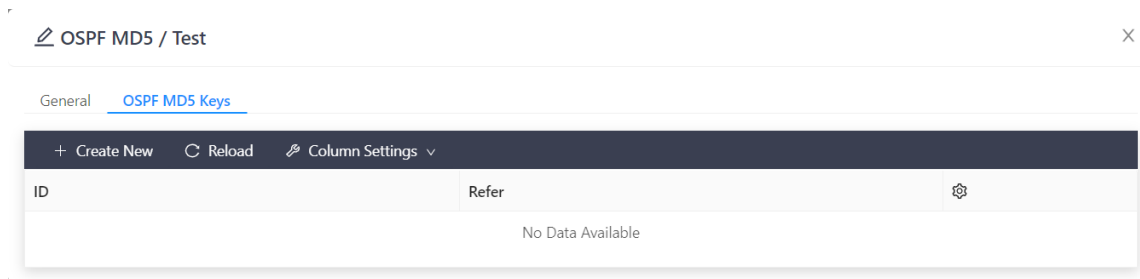
1. Go to *Configuration > Shared Resources > Network > Extender Resources > Data Plan*.
2. In the toolbar, click *+Create New*.
The *Data Plan* dialog box is displayed.
3. Configure the settings, and click *OK*.

Creating MD5 keys for OSPF

You can create profiles of MD5 authentication keys to use for the Open Shortest Path First (OSPF) protocol.

To create profiles of MD5 keys for OSPF:

1. Go to *Configuration > Shared Resources > Network > OSPF MD5*.
2. Create a profile:
 - a. In the toolbar, click *+Create New*.
The *OSPF MD5* dialog box is displayed.
 - b. In the *Name* box, type a name, and click *OK*.
The profile is created, and the *OSPF MD5 Keys* tab is displayed.



3. Create MD5 keys for the profile:

- a. Click *Create New*.
The *OSPF MD5 Key* dialog box is displayed.
- b. In the *ID* box, type an ID number for the key.
- c. In the *Key* box, type the MD5 key.
- d. Click *OK*.
The key is created.
- e. (Optional) Click *Create New* to create additional keys for the profile, or close the dialog box.

Creating external VPN gateways

SD-WAN Orchestrator MEA supports establishing IPsec tunnels with external VPN gateways. External VPN gateways can be any generic IPsec gateways that are not managed by SD-WAN Orchestrator MEA. This is useful for creating IPsec VPN connections to third-party devices.

To create external VPN gateways:

1. Go to *Configuration > Shared Resources > Network > External VPN Gateway*.
2. In the toolbar, click *+Create New*.
The *+External VPN Gateway* dialog box is displayed.

+

External VPN Gateway

X

* Name ⓘ

Test

* Type ⓘ

SITE_TO_SITE

IKE Settings

* IPsec Template

Default_IPSEC_Template

* Authentication

PRE_SHARED_KEY

* Pre-Shared Key

.....

Gateway Settings

* Remote Gateway ⓘ

STATIC_IP_ADDRESS

* IP Address

172.22.15.3

Tunnel Interface Local IP Address ⓘ

172.22.15.3

Health-Check Settings

* Enable Health-Check Settings

OFF

BGP Settings

- Complete the options, and click OK.
The external VPN gateway is created.

Creating custom IPsec templates

You can create a custom IPsec template and apply it to a region. IPsec templates settings are used when FortiGate devices negotiate IPsec tunnels (overlay links) with other devices.

When you add a region, you can choose one of the default templates. Alternately, you can create custom IPsec templates, and select them in regions. See also [Adding regions on page 41](#).

You can also create IPsec templates to define the IPsec tunnel configuration between hubs in different regions. See [Changing network settings on page 102](#).

To create custom IPsec templates:

- Go to *Configuration > Shared Resources > Network > IPsec Template*.
- In the toolbar, click *+Create New*.
The *+IPsec Template* dialog box is displayed.

+ IPsec Template
X

* Name ⓘ
 Allowed characters: a-z A-Z 0-9 _ - ⓘ

IKE Settings

* Version

IKE Security (Phase 1) Properties

* Encryption

* Authentication

* DH Group

* Key Lifetime

* Dead Peer Detection

* NAT Traversal

* Keep Alive Frequency

- Complete the options, and click **OK**.
The IPsec template is created.

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 107](#)
- [Adding SLA servers on page 108](#)

Adding SLA quality levels

To add SLA quality levels:

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

Option	Description
Name	Enter a name for the quality level.

Option	Description
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 (<i>Ping</i> or <i>HTTP</i>).
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 108](#)
- [Adding FortiGuard servers on page 109](#)
- [Adding email servers on page 109](#)
- [Creating custom speed test schedules on page 110](#)

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.

Option	Description
Address Type	From the dropdown, select <i>IP</i> or <i>FQDN</i> .
Address	Enter the server's IP address or host name.
NTP v3	Toggle <i>On</i> to enable NTP v3.
Authentication	Toggle <i>On</i> to enable authentication.
Key	Available when <i>Authentication</i> is enabled.
Key ID	Available when <i>Authentication</i> 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 <i>Update</i> or <i>Rating</i> .
Address Type	From the dropdown, select <i>IP4</i> , <i>IP6</i> , or <i>FQDN</i> .
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 <i>IPv4</i> or <i>FQDN</i> .
Address	Enter the email server's IP address or host name.
Authentication	Toggle <i>On</i> to enable authentication, then enter the <i>Username</i> and <i>Password</i> .

Option	Description
Username	Available when <i>Authentication</i> is enabled.
Password	Available when <i>Authentication</i> is enabled.
Port	Enter the port number.
Reply To	Enter the email address users can reply to.
Security	From the dropdown, select <i>None</i> , <i>STARTTLS</i> , or <i>SMTPS</i> .
SSL Version	From the dropdown, select the SSL version.
Validate Server	Toggle <i>On</i> to enable validation.

Creating custom speed test schedules

SD-WAN Orchestrator MEA supports WAN port speed tests. The following default schedules are available:

- always
- default-darrp-optimize
- none

You cannot delete the default schedules, but you can create custom schedules for WAN speed tests. See also [Executing WAN port speed tests on page 54](#).

To create custom speed test schedules:

1. Go to *Configuration > Shared Resources > System > Schedule*.
2. In the toolbar, click *Create New*.

The *Schedule* dialog box is displayed.

The screenshot shows a 'Schedule' dialog box with the following fields and controls:

- Name:** A text input field with a red asterisk and a help icon. The placeholder text is 'Allowed characters: a-z A-Z 0-9 _ -'.
- Start Time:** A time selection field showing '00:00' with a clock icon.
- End Time:** A time selection field showing '00:00' with a clock icon.
- Day:** A text input field with a calendar icon.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

- Configure the options, and click **OK**.

Option	Description
Name	Enter a name for the speed test schedule.
Start Time	Click the box to select the hour and minutes, and then click OK . The test start time is defined.
End Time	Click the box to select the hour and minutes, and then click OK . The test end time is defined.
Day	Click the box to one or more days on which to run the test.

The schedule is saved.

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:

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

Global routing

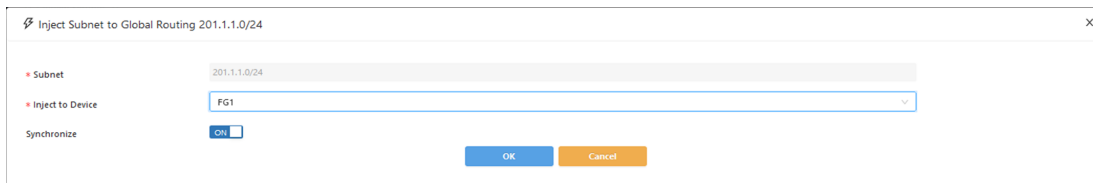
You can view the subnet, next hop, and type information for global routing. You can also use the router prefix-list configuration to manually inject routes learned through OSPF/BGP to global routing.

To view global routing:

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

Subnet	Next Hop	Address Group Injected
100.1.1.0/24	FG1:direct connected port4(SAN_DIRECT_CONNECT)	GROUP_ALL_GROUP-SDWAN_ALL_GROUP-US_DEVICE_1
200.1.1.0/24	FG1:static route ET_IPN: port2_Port2_to_FG4_FortiG2(S2M1C)	GROUP_ALL_GROUP-SDWAN_ALL_GROUP-US_DEVICE_1
201.1.1.0/24	FG1:ET4 via 4.0.0.0(BGP)	GROUP_ALL_GROUP-SDWAN_ALL_GROUP-US_DEVICE_1

- (Optional) Inject the subnet to global routing.
 - For the subnet, click the *Inject Subnet* button.
The *Inject Subnet to Global Routing <subnet>* dialog box is displayed.



The screenshot shows a configuration window titled "Inject Subnet to Global Routing 201.1.1.0/24". It contains three sections: "Subnet" with a text field containing "201.1.1.0/24", "Inject to Device" with a dropdown menu showing "FG1", and "Synchronize" with a toggle switch set to "ON". At the bottom right are "OK" and "Cancel" buttons.

- b. In the *Inject to Device* list, select the device.
- c. Ensure *Synchronize* is toggled *ON*.
- d. Click *OK*.

Maintenance



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

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 113](#).
- Back up and restore configurations for SD-WAN Orchestrator MEA. See [Configuration on page 113](#).
- Export a zip file of debug information for SD-WAN Orchestrator MEA. See [Debug on page 114](#).

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](#).

Appendix A - managed FortiGate CLI objects and attributes

SD-WAN Orchestrator MEA can create and manage some, but not all FortiGate CLI objects and attributes. SD-WAN Orchestrator MEA uses two methods to manage objects. Some objects are managed by the first method, and some objects are managed by the second method. SD-WAN Orchestrator MEA uses the following methods to manage FortiOS CLI objects:

1. Manage partial objects for a FortiOS command and use an ID, name, or description to indicate when an object is managed by SD-WAN Orchestrator MEA
For example, with the `config router static` command, SD-WAN Orchestrator MEA only manages ID range 1,000,000 to 1,100,000. If you create a static route with ID = 100 on FortiGate or FortiManager, SD-WAN Orchestrator MEA does not touch the static route.
2. Manage all objects for a FortiOS command
When this method is used, it affects some objects created by FortiOS or FortiManager. When you create a FortiGate object by using FortiOS or FortiManager, the object is removed by SD-WAN Orchestrator MEA when the *Install configuration* option is executed.
For example, if you use FortiOS or FortiManager to create an SD-WAN health-check server with name XXX by using the `config system sdwan -> config health-check` command, SD-WAN Orchestrator MEA removes the health-check server with name XXX when you execute the *Install configuration* option.

SD-WAN Orchestrator MEA uses the following methods to manage different attributes of FortiOS CLI objects:

1. For attributes managed by SD-WAN Orchestrator MEA, you can use FortiOS or FortiManager to change the attribute, but SD-WAN Orchestrator MEA overwrites the change.
For example, SD-WAN Orchestrator MEA was used to configure a static route:

```
Config router static
edit 1000001
set dst 10.248.0.0 255.252.0.0
set comment "SDWAN.Orchestrator.created.automatically."
set blackhole enable
next
end
```

SD-WAN Orchestrator MEA manages following static route attributes: device, distance, priority, gateway, dst, virtual-wan-link, sdwan, comment, blackhole, status

If you change the static route by using FortiOS to:

```
Config router static
edit 1000001
set dst 10.248.0.0 255.252.0.0
set comment "SDWAN.Orchestrator.created.automatically."
set blackhole disable
next
end
```

SD-WAN Orchestrator MEA overwrites the change made by FortiOS and sets `blackhole` back to `enable`.

2. For attributes not managed by SD-WAN Orchestrator MEA, you can change the attributes using any method you like, and SD-WAN Orchestrator MEA does not change the attribute.
3. Some attributes are initiated by SD-WAN Orchestrator MEA, but not managed by SD-WAN Orchestrator MEA. In this case, SD-WAN Orchestrator MEA sets the attribute when it creates the object, but you can change the attribute using any method you like, and SD-WAN Orchestrator MEA will not overwrite your changes.

SD-WAN Orchestrator MEA manages the following FortiGate CLI objects and attributes:

- [extender-controller on page 117](#)
- [firewall on page 118](#)
- [log on page 119](#)
- [router on page 120](#)
- [system on page 126](#)
- [vpn on page 136](#)
- [wireless-controller on page 137](#)

For information about all FortiOS configuration commands, see the [FortiOS 7.0 CLI Reference](#).

extender-controller

This section includes information about the following commands:

- [config extender-controller dataplan on page 117](#)
- [config extender-controller extender on page 117](#)

config extender-controller dataplan

FortiExtender dataplan configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ modem-id, type, carrier, slot, iccid, auth-type, username, password, PDN, preferred-  
  subnet, APN,private-network, capacity, monthly-fee, billing-date, overage, signal-  
  threshold, signal-period ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config extender-controller extender

Extender controller configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ id, authorized ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config modem

Configuration options for modem <number>.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[ifname, default-sim, gps, sim1-pin, sim2-pin, sim1-pin-code, sim2-pin-code, preferred-carrier]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config auto-switch

FortiExtender auto switch configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[disconnect, disconnect-threshold, disconnect-period, signal, dataplan, switch-back, switch-back-time, switch-back-timer]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

firewall

This section includes information about the following commands:

- [config firewall address on page 118](#)
- [config firewall addrgrp on page 119](#)

config firewall address

Configure IPv4 addresses.

ID generated by SD-WAN Orchestrator MEA:

Prefix: `DEVICE_`

Attributes managed by SD-WAN Orchestrator MEA:

[`subnet`, `fqdn`, `wildcard-fqdn`, `start-ip`, `end-ip`, `country`, `type`, `comment`, `interface`]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config firewall addrgrp

Configure IPv4 address groups.

ID generated by SD-WAN Orchestrator MEA:

Prefix: `DEVICE_` or `GROUP_`

Attributes managed by SD-WAN Orchestrator MEA:

[`member`, `comment`]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

log

This section includes information about the following commands:

- [config log fortianalyzer setting on page 119](#)
- [config log syslogd filter on page 120](#)
- [config log syslogd setting on page 120](#)

config log fortianalyzer setting

Global FortiAnalyzer settings.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[`status`, `server`, `upload-option`, `enc-algorithm`, `reliable`, `certificate-verification`]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config log syslogd filter

Filters for remote system server.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[severity]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config log syslogd setting

Global settings for remote syslog server.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[status, server, mode, port, facility, format, enc-algorithm, ssl-min-proto-version,
certificate]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

router

This section includes information about the following commands:

- [config router bgp on page 121](#)
- [config router community-list on page 122](#)
- [config router ospf on page 123](#)
- [config router policy on page 125](#)
- [config router prefix-list on page 125](#)

- [config router route-map on page 126](#)
- [config router static on page 126](#)

config router bgp

Configure BGP.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ as, router-id, ibgp-multipath, ebgp-multipath, additional-path, additional-path-select, recursive-next-hop ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config network

BGP network table.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ prefix, route-map ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config neighbor

BGP neighbor table.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ remote-as, advertisement-interval, link-down-failover, additional-path, adv-additional-path, attribute-unchanged, ebgp-enforce-multihop, route-map-in, route-map-out, next-hop-self, route-reflector-client, soft-reconfiguration, description ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config neighbor-group

BGP neighbor range table.

ID generated by SD-WAN Orchestrator MEA:

Prefix: SWNC-

Attributes managed by SD-WAN Orchestrator MEA:

```
[ remote-as, link-down-failover, additional-path, adv-additional-path, route-reflector-client, route-map-in, route-map-out, next-hop-self, description ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config redistribute ospf

BGP neighbor range table.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ status, route-map ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config router community-list

Configure community lists.

ID generated by SD-WAN Orchestrator MEA:

Prefix: SWNC-

Attributes managed by SD-WAN Orchestrator MEA:

```
[ rule ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config router ospf

Configure OSPF.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ router-id, default-information-originate ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config area

Configure OSPF area.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ type, authentication ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config ospf-interface

OSPF interface configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ interface, cost, hello-Interval, dead-Interval, authentication, authentication-key, md5-  
  keys ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config network

OSPF network configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[prefix, area]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config redistribute bgp

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[status, metric]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config redistribute connected

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[status, metric]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config redistribute static

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[status, metric]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config router policy

Configure IPv4 routing policies.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 60000 to 61000.

Attributes managed by SD-WAN Orchestrator MEA:

[action, output-device, input-device, gateway, dstaddr, dst, comment]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config router prefix-list

Configure community lists.

ID generated by SD-WAN Orchestrator MEA:

Prefix: SWNC-

Attributes managed by SD-WAN Orchestrator MEA:

[rule]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config router route-map

Configure route maps.

ID generated by SD-WAN Orchestrator MEA:

Prefix: SWNC-

Attributes managed by SD-WAN Orchestrator MEA:

```
[ rule ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config router static

Configure IPv4 static routing tables.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1,000,000 to 1,100,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ device, distance, priority, gateway, dst, virtual-wan-link, sdwan, comment, blackhole,
  status ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

system

This section includes information about the following commands:

- [config system admin on page 127](#)
- [config system central-management on page 127](#)
- [config system dhcp server on page 128](#)
- [config system dns on page 129](#)
- [config system email-server on page 129](#)
- [config system fortiguard on page 129](#)
- [config system global on page 130](#)
- [config system ha on page 130](#)
- [config system interface on page 130](#)
- [config system ntp on page 131](#)

- [config system sdwan on page 132](#)
- [config system settings on page 135](#)
- [config system snmp community on page 134](#)
- [config system snmp sysinfo on page 134](#)
- [config system snmp user on page 135](#)
- [config system switch-interface on page 135](#)
- [config system virtual-switch on page 136](#)

config system admin

Configure admin users.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[password]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config system central-management

Configure central management.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[include-default-servers]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config server-list

Additional servers that the FortiGate can use for updates (for AV, IPS, updates) and ratings (for web filter and antispam ratings) servers.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1,000,000 to 1,100,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ server-type, addr-type, server-address, server-address6, fqdn ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config system dhcp server

Configure DHCP servers.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ interface, domain, tftp-server, netmask, default-gateway, dns-service, timezone-option,
  ntp-service, vci-match, vci-string, lease-time, dns-server1, dns-server2, dns-server3,
  dns-server4 ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config ip-range

DHCP IP range configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ start-ip, end-ip ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config options

DHCP options.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[code, type, value, ip]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config system dns

Configure DNS.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[primary, secondary]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[server, authenticate, username, password, port, reply-to, security, ssl-min-protocol-version, validate-server]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config system fortiguard

Configure FortiGuard services.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[antispam-force-off, webfilter-force-off]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config system global

Configure global attributes.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[hostname, switch-controller, fortiextender, admin-https-redirect, admin-sport]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config system ha

Configure HA.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[group-name, mode, hbdev, override, monitor]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

[N/A]

config system interface

Configure interfaces.

ID generated by SD-WAN Orchestrator MEA:

No IDs generated, except for VLANs and SSIDs:

- For managed VLANs, add a comment `SDWAN.Orchestrator.created.` to interface.
- All SSIDs are managed by SD-WAN Orchestrator MEA.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ interface, dhcp-relay-service, vlanid, type, mode, dhcp-relay-ip, username, password,
  disc-retry-timeout, dns-server-override, ip, vdom, fortilink, member, allowaccess,
  status, role, estimated-downstream-bandwidth, estimated-upstream-bandwidth, preserve-
  session-route, auto-auth-extension-device, security-mode, device-identification,
  switch-controller-access-vlan, switch-controller-feature, description ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

tunnel interface: config system interface

Configure tunnel interface type.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1 to 10,000,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ remote-ip, description, alias ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config system ntp

Configure system NTP information.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ ntpsync, type, syncinterval ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config ntpserver

Configure the FortiGate to connect to any available third-party NTP server.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1,000,000 to 1,100,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ server, ntpv3, authentication, key, key-id ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config system sdwan

Configure redundant Internet connections with multiple outbound links and health-check profiles.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ status, load-balance-mode, fail-detect ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config health-check

SD-WAN status checking or health checking. Identify a server on the Internet and determine how SD-WAN verifies that the FortiGate can communicate with it.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ addr-mode, server, protocol, interval, failtime, recoverytime, update-static-route, members, sla, sla-fail-log-period, sla-pass-log-period, port ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config members

FortiGate interfaces added to the SD-WAN.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ interface, gateway, priority, status, comment, cost ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config service

Create SD-WAN rules (also called services) to control how sessions are distributed to interfaces in the SD-WAN.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ name, addr-mode, mode, protocol, dst, src, internet-service, internet-service-id,
  internet-service-name, sla, health-check, priority-members, start-port, end-port,
  status, users, groups, internet-service-group, internet-service-custom, internet-
  service-custom-group, internet-service-app-ctrl, internet-service-app-ctrl-group,
  link-cost-factor, packet-loss-weight, latency-weight, jitter-weight, route-tag ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config zone

Configure SD-WAN zones.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config system snmp community

SNMP community configuration.

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1,000,000 to 1,100,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ name, status, query-v1-status, query-v1-port, query-v2c-status, query-v2c-port, trap-v1-status, trap-v1-lport, trap-v1-rport, trap-v2c-status, trap-v2c-lport, trap-v2c-rport ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ events ]
```

config hosts

Configure IPv4 SNMP managers (hosts).

ID generated by SD-WAN Orchestrator MEA:

SD-WAN Orchestrator MEA managed ID range 1,000,000 to 1,100,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ host-type, ip ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ N/A ]
```

config system snmp sysinfo

SNMP system info configuration.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ status, trap-high-cpu-threshold, trap-low-memory-threshold, trap-log-full-threshold ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ description, contact-info, location ]
```

config system snmp user

SNMP user configuration.

ID generated by SD-WAN Orchestrator MEA:

Prefix: SWNC-

Attributes managed by SD-WAN Orchestrator MEA:

```
[ status, queries, query-port, trap-status, trap-lport, trap-rport, notify-hosts, security-level, auth-proto, auth-pwd, priv-proto, priv-pwd ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ events ]
```

config system settings

Configure VDOM settings.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ ecmp-max-paths ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ vdom, member ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config system virtual-switch

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ physical-switch ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

config port

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ speed, status ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

vpn

This section includes information about the following commands:

- [config vpn ipsec phase1-interface on page 136](#)
- [config vpn ipsec phase2-interface on page 137](#)

config vpn ipsec phase1-interface

Configure VPN remote gateway.

ID generated by SD-WAN Orchestrator MEA:

- Change the IPsec tunnel name on edge devices.
- The general rule is <port_name> + <hub_role_indicator> + <peer_port_name>
- For keeping the length of the tunnel name within 15 characters, the components of the general rule are simplified as follows:
 - If the port is a physical interface, we will compose the `port_name` with the first letter and the number of interface name. For example, if the interface is `port1`, `port_name` should be `p1`.

- If the port is a VLAN interface, we will compose the `port_name` with the abbreviated physical port name and VLAN ID. For example, if the VLAN interface is configured on port2, and the VLAN ID is 1500, the `port_name` is `p2v1500`.
- If the port is an aggregate interface, we will compose the `port_name` with the prefix `a_` and the last three letters of interface name. For example, if the interface is `agg_test`, the `port_name` is `a_est`.
- If the hub is a primary hub, `hub_role_indicator` is H1. If the hub is secondary hub, `hub_rule_indicator` is H2.
- If the length of new tunnel name exceeds 15 characters, the previous numerical tunnel name is used, which is the method used in SD-WAN Orchestrator MEA 7.0.0.r1 and earlier.
- The previous numerical tunnel name will be recorded in the comment of the phase1/phase2 configuration.
- If the IPsec tunnel name is numerical, it starts from 1,000,000.

Attributes managed by SD-WAN Orchestrator MEA:

```
[ type, interface, psksecret, remote-gw, peertype, localid, peerid, comments, auto-  
discovery-sender, auto-discovery-forwarder, auto-discovery-receiver, net-device, add-  
route, tunnel-search, exchange-interface-ip, ike-version, network-overlay, network-id  
]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ dhgrp, dpd, keylife, proposal, idle-timeout ]
```

config vpn ipsec phase2-interface

Configure VPN remote gateway.

ID generated by SD-WAN Orchestrator MEA:

The ID for IPsec phase2 is the same as IPsec phase1. See [config vpn ipsec phase1-interface on page 136](#).

Attributes managed by SD-WAN Orchestrator MEA:

```
[ phaselname, auto-negotiate, comments ]
```

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

```
[ proposal, dhgrp ]
```

wireless-controller

This section includes information about the following commands:

- [config wireless-controller vap on page 137](#)

config wireless-controller vap

Configure Virtual Access Points (VAPs).

ID generated by SD-WAN Orchestrator MEA:

No ID generated. SD-WAN Orchestrator MEA manages all objects.

Attributes managed by SD-WAN Orchestrator MEA:

[ssid]

Attributes initialized but not managed by SD-WAN Orchestrator MEA:

N/A

Appendix B - REST API

SD-WAN Orchestrator MEA supports a REST API. Before using the REST API, you must set up an API user in FortiManager to use with the API. This section includes the following topics:

- [Setting up an API user on page 139](#)
- [Logging in to the REST API on page 140](#)

Setting up an API user

In FortiManager, set up an API user by creating an administrator profile and an administrator account that uses the profile. Then you can use the administrator account with the SD-WAN Orchestrator MEA REST API.

To create an administrator profile:

1. In FortiManager, go to *System Settings > Admin > Profile*, and click *Create New*.

Name	Type
Restricted_User	System Admin
Standard_User	System Admin
Super_User	System Admin
Package_User	System Admin
No_Permission_User	System Admin

New Profile

Profile Name:

Description:

Type: ☒ System Admin ☐ Restricted Admin

Read-Write Read-Only None

System Settings ☐ ☐ ☒

Administrative Domain ☐ ☐ ☒

FortiGuard Center ☐ ☐ ☒

License Management ☐ ☐ ☒

Firmware Management ☐ ☐ ☒

Settings ☐ ☐ ☒

Device Manager ☐ ☐ ☒

Add/Delete/Edit Devices/Groups ☐ ☐ ☒

Retrieve Configuration from Devices ☐ ☐ ☒

Revert Configuration from Revision History ☐ ☐ ☒

OK Cancel

2. In the *Name* box, type a name for the profile.
3. Beside type, select *System Admin*.
4. For *Extension Access*, select *Read-Write*.
5. Set the remaining options as desired.
6. Click *OK* to save the profile.

To create an administrator account:

1. In FortiManager, go to *System Settings > Admin > Administrators*, and click *Create New*.
2. In the *User Name* box, type a name for the user.
3. Beside *Admin Profile*, select the profile you created.
4. Beside *Administrative Domain*, configure what ADOMs the administrator needs to access.

5. For *JSON API Access*, select *Read-Write*.

The screenshot shows the 'Create New Administrator' window in FortiManager. The left sidebar has 'Administrators' selected. The main area shows a table of existing administrators: 'admin' (LOCAL), 'apiuser' (LOCAL), and 'lwoodward' (LOCAL). The 'apiuser' entry is selected. On the right, the 'Create New Administrator' form is displayed with the following settings:

- User Name:
- Avatar: +Add Photo -Remove Photo
- Description:
- Admin Type:
- New Password:
- Confirm Password:
- Admin Profile:
- Administrative Domain: All ADOMs except specified ones Specify
- Policy Package Access: Specify
- JSON API Access:
- Theme Mode: Use Own Theme
- Trusted Hosts: ☐
- Meta Fields:
- Advanced Options:

At the bottom right are 'OK' and 'Cancel' buttons.

6. Set the remaining options as desired.

7. Click **OK** to save the administrator account.

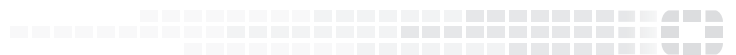
Logging in to the REST API

After you create an administrator account in FortiManager to use for the SD-WAN Orchestrator MEA REST API, you are ready to use the API.

To log in to the SD-WAN Orchestrator MEA REST API:

1. Use the JSON RPC standard and the username and password for the administrative account you created to log in to the FortiManager API.
If authentication succeeds, cookies are returned.
2. Send POST requests to `https://<fmg_ip>/fortiwan/jsonrpc` with FortiManager cookies.
The request format is similar to FortiManager JSON API, which is based on the JSON RPC standard.

For an introduction to FortiManager JSON API, see the Fortinet Developer Network site at <https://fndn.fortinet.net/>. A login is required.



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.