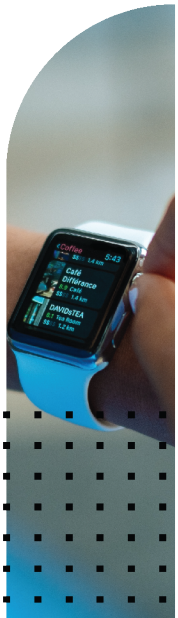
Large Campus Switching Deployment Guide

FortiSwitchOS 7.0.0



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

March 14, 2022
FortiSwitchOS 7.0.0 Large Campus Switching Deployment Guide
11-700-765827-20220314

TABLE OF CONTENTS

Change Log

Date	Change Description
February 8, 2022	Initial release
March 14, 2022	Updated the figure in the “Use case and topology” section.

Introduction

Executive summary

There are many ways to build redundancy and resiliency. In a switching network, you can accomplish this by adding redundant links and switches in the topologies. Using redundant and aggregate links, you can avoid a single link failure causing a network to go down.

A multichassis link aggregation group (MCLAG) provides node-level redundancy by grouping two FortiSwitch models together so that they appear as a single switch on the network. If either switch fails, the MCLAG continues to function without any interruption, increasing network resiliency and eliminating the delays associated with the Spanning Tree Protocol (STP).

This deployment guide shows how to use multiple tiers of MCLAGs to provide link and switch redundancy in a large campus.

Intended audience

This guide is intended for network and security architects and engineers who are interested in deploying Fortinet's FortiSwitch units in a new environment or in replacing their equipment in an existing environment. Readers are expected to have a firm understanding of networking and security concepts.

About this guide

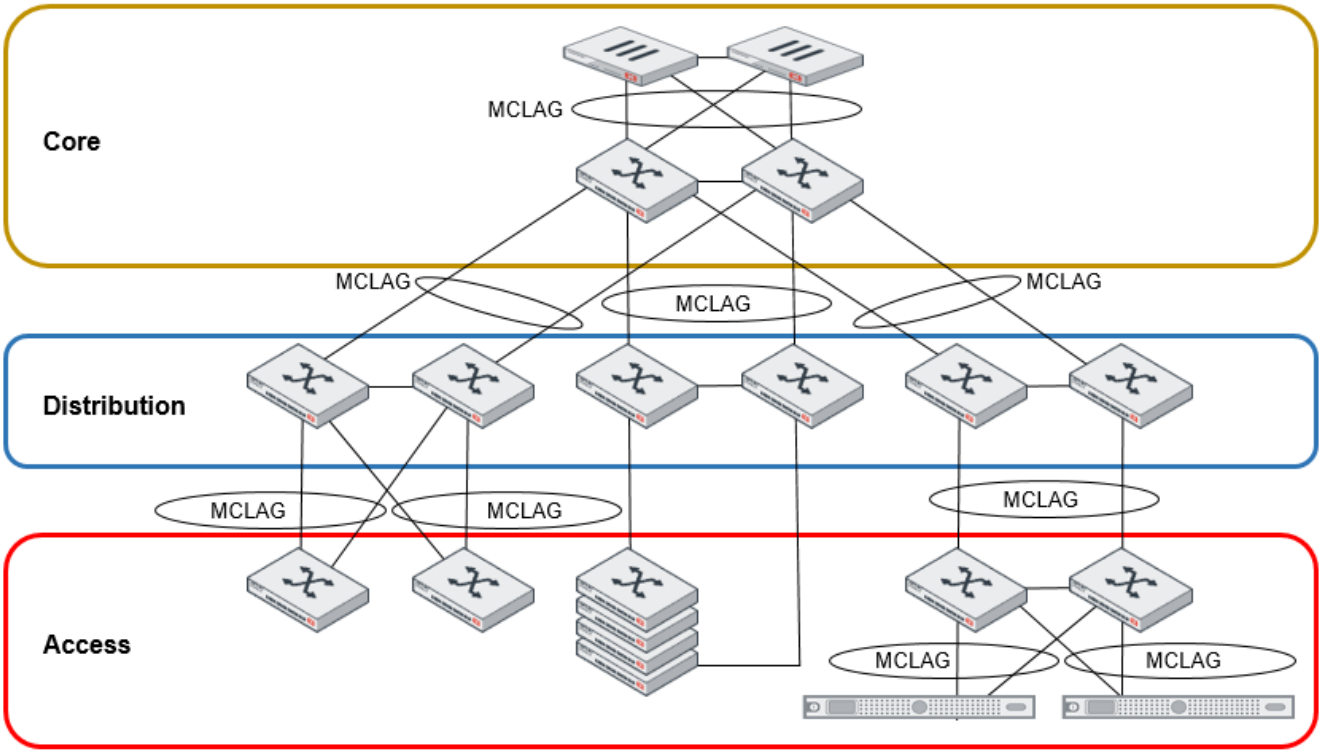
The deployment guide provides the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture and design outlined in this guide is suitable for them. It is advisable to review the administration guide if readers are still in the process of selecting the right architecture.

This deployment guide presents one of many possible ways to deploy the solution. It might omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product administration guides, Knowledge Base articles, cookbooks, release notes, and other documents where appropriate.

Design overview

Use case and topology

The following figure shows the reference architecture:



Design concept and considerations

In the core level of the reference architecture, two FortiGate units form a high availability (HA) cluster. They manage a pair of FortiSwitch units that form an MCLAG peer group. The core-level switches interconnect to the FortiGate units and provide aggregate distribution ports. The FortiGate units function as the next-generation firewall and the Security Fabric controller; they also connect to the wide-area network (WAN). In the deployment example, the core level is the main building communications room.

The distribution level of the reference architecture is composed of multiple pairs of FortiSwitch units that form the MCLAG peer groups. The distribution-level switches interconnect to the core-level switches and aggregate multiple access switches. In the deployment example, the distribution level is the building communications room.

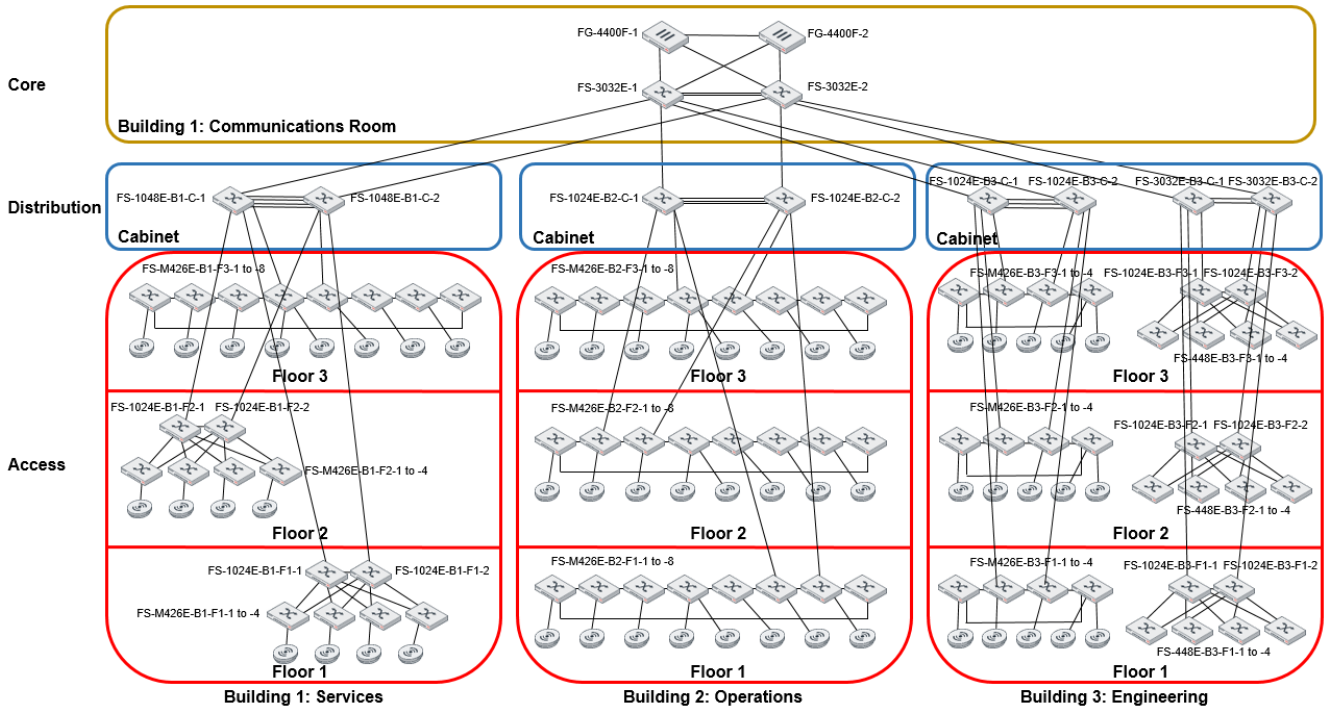
The access level of the reference architecture consists of the following:

- Multiple pairs of FortiSwitch units forming the MCLAG peer groups
- Multiple dual-homed access switches
- Multiple access switches in a ring topology

The access-level switches interconnect endpoints to the network and enforce security at the access ports. In the deployment example, the access level is one floor of each building.

Deployment overview

The deployment example uses the large-campus reference architecture. There are three buildings with three floors in each building.



Building 1

The Services department is in Building 1

The Communications room of Building 1 has the two FortiGate units in an HA cluster. There is a full-mesh configuration of the two FortiGate units and the two FortiSwitch units. The links are 100G.

The Building 1 cabinet contains the MCLAG peer group with four 10G inter-chassis links (ICLs). There are 100G uplinks to the core level, 10G downlinks to the Floor 3, and 40G downlinks to Floors 1 and 2. There are additional 10G ports for severs or more switches.

Floors 1 and 2 each use an MCLAG peer group for critical infrastructure, including the wireless network, and use 40G uplinks. The switches are dual-homed for redundancy and to increase the bandwidth. There are additional 10G ports for severs or more switches. Additional 1G and 2.5G ports can be used for endpoints, video, and so on.

Floor 3 contains eight switches in a ring topology, which provide the switch infrastructure for the wireless network. The switches use 10G uplinks. Additional 1G and 2.5G ports can be used for endpoints, video, and so on.

Building 2

The Operations department is in Building 2.

The Building 2 cabinet contains the MCLAG peer group with three 10G ICLs. There are 100G uplinks to the core level and 10G downlinks to Floors 1, 2, and 3. There are additional 10G ports for severs or more switches.

Floors 1, 2, and 3 each contain eight switches in a ring topology, which provides the switch infrastructure for the wireless network. The switches use 10G uplinks. Additional 1G and 2.5G ports can be used for endpoints, video, and so on.

Building 3

The Engineering department is in Building 3.

The Building 3 cabinet contains two MCLAG peer groups:

- One MCLAG peer group has three 10G ICLs. There are 100G uplinks to the core level and 10G downlinks to Floors 1, 2, and 3. There are additional 10G ports for severs or more switches.
- The other MCLAG peer group provides critical infrastructure and has three 100G ICLs and 100G downlinks to Floors 1, 2, and 3.

Floors 1, 2, and 3 each contain four switches in a ring topology, which provides the switch infrastructure for the wireless network. The switches use 10G uplinks. Additional 1G and 2.5G ports can be used for endpoints, video, and so on.

On each floor, an MCLAG peer group provides critical infrastructure with 100G uplinks and 10G downlinks. There are additional 10G ports for severs or more switches. Additional 1G and 2.5G ports can be used for the engineering environment.

The access ports in the large-campus example are distributed as follows:

Speed of access ports	Number of access ports
1G	1,408
2.5G	416
10G	318
100G/40G	100
Total	**2,242**

Additional capacity is available if more switches are added on each floor. For example, for 10,000 1G access ports, add twenty 48-port switches per floor.

Deployment plan

1. Configure the core level.
2. Configure the distribution level.
3. Configure the access level.
   a. For the MCLAG peer groups (Building 1, Floors 1 and 2, and Building 3, Floors 1, 2, and 3), configure each MCLAG peer group before you configure the other switches to be dual-homed.
   b. For the switches in the ring topologies, connect the FortiSwitch units with uplinks to the distribution level, wait until the switches are managed, and then connect the rest of the FortiSwitch units.

Deployment procedures

Use the following procedure to deploy the entire topology from the FortiGate switch controller without the need for direct console access to the FortiSwitch units.

NOTE:

- Fortinet recommends using at least two links for ICL redundancy.
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- In this topology, you must use the `auto-isl-port-group` setting as described in the following configuration example. This setting instructs the switches to group ports from MCLAG peers together into one MCLAG when the inter-switch link (ISL) is formed.
- The `auto-isl-port-group` setting must be done directly on the FortiSwitch unit.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

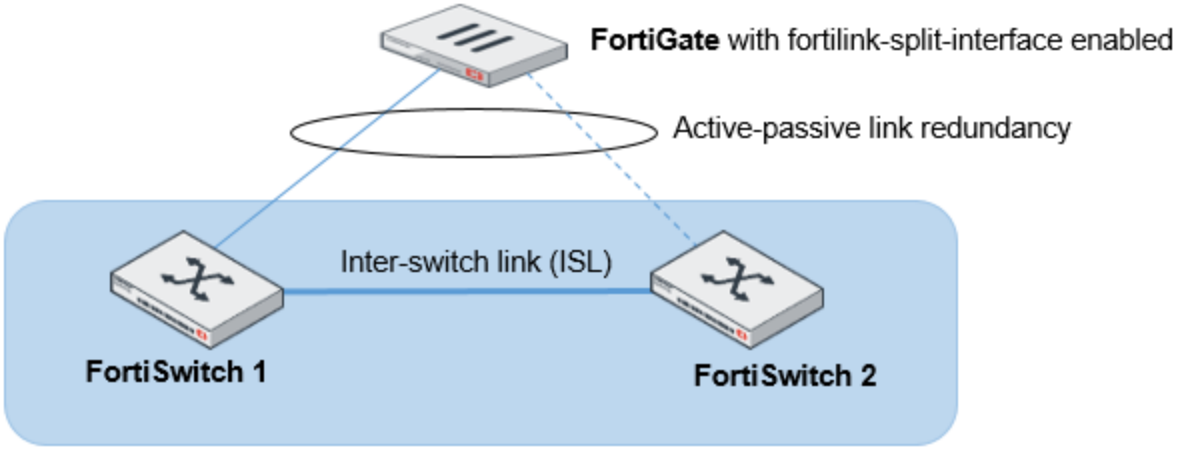
- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.

To create a three-tier FortiLink MCLAG topology, use FortiOS 6.2.3 GA or later and FortiSwitchOS 6.2.3 GA or later.

Configure the core-level (tier-1) MCLAG

Wire the two core-level FortiSwitch units to the FortiGate units. You can use the FortiLink split interface to connect the FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units. When the FortiLink split interface is enabled, only one link remains active.

In this topology, the FortiLink split interface connects a FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units. The aggregate interface of the FortiGate unit for this configuration contains at least one physical port connected to each FortiSwitch unit.



NOTE:

- Make sure that the split interface is enabled.
- This procedure also applies to a FortiGate unit in HA mode.
- More links can be added between the FortiGate unit and FortiSwitch unit.

Use the FortiGate CLI to change the FortiSwitch units' configuration without losing their management from the FortiGate unit. You do not need to change anything on the individual FortiSwitch units. The MCLAG-ICL can also be enabled on the FortiSwitch unit directly using console cables or management ports.

1. Using the FortiGate CLI, assign the LLDP profile `default-auto-mclag-icl` to the ports that should form the MCLAG ICL in FortiSwitch unit 1. For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

2. Repeat step 1 for FortiSwitch unit 2. The port numbers can be different.
3. Disable the split interface in the FortiLink interface. For example:

```
config system interface
   edit <aggregate_name>
      set fortilink-split-interface disable
   next
end
```

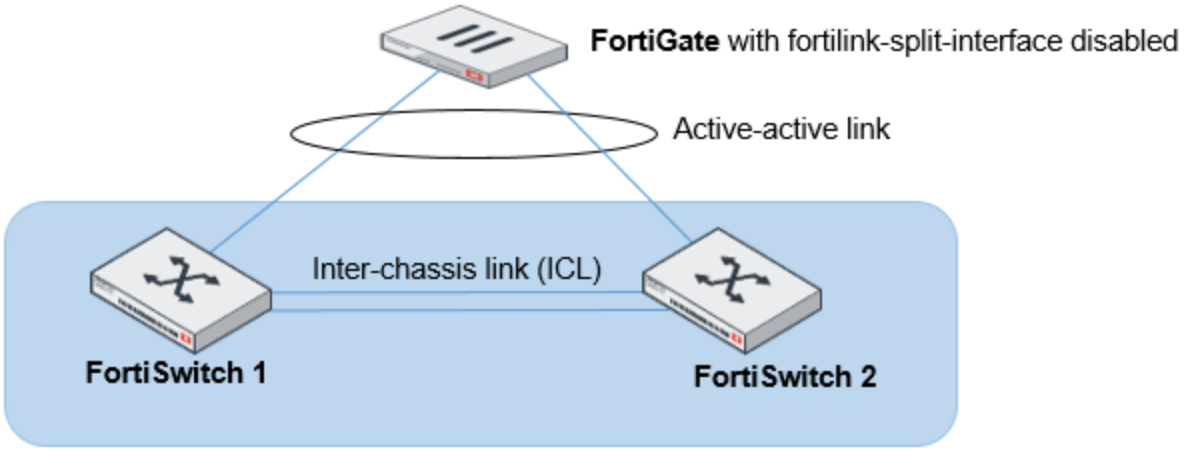
4. From the FortiGate unit, enable the LACP active mode if not already set:

```
   config system interface
      edit <aggregate_name>
         set lacp-mode active
      next
   end
```

   NOTE: If you are using FortiOS 6.2 or earlier, use the `set lacp-mode static` command instead.

5. Check that the LAG is working correctly. For example:

```
diagnose netlink aggregate name <aggregate_name>
```



If you disable the MCLAG ICL (with the `set mclag-icl disable` command), you need to enable `fortilink-split-interface`.

Configure the distribution-level (tier-2) MCLAGs

1. Connect *only* the distribution-level (tier-2) MCLAG FortiSwitch units (FS-1048E-B1-C-1 and FS-1048-B1-C-2) to the core FortiSwitch units (FS-3032E-1 and FS-3032E-2). Wait until they are discovered and authorized (if automatic authorization is disabled, you must authorize the switches manually).
2. Using the FortiGate CLI, assign the LLDP profile `default-auto-mclag-icl` to the ports that will form the MCLAG ICL in the tier-2 MCLAG switches FS-1048E-B1-C-1 and FS-1048-B1-C-2. For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

3. On both core-level switches, FS-3032E-1 and FS-3032E-2, add an `auto-isl-port-group` for the distribution-level (tier-2) MCLAG peer group in building 1 (FS-1048E-B1-C-1 and FS-1048-B1-C-2).

   To the Building 1 cabinet:

```
config switch auto-isl-port-group
   edit tier2-B1-C1
      set members port1
   next
end
```

This configuration is done directly in the FortiSwitch CLI, which can be accessed using the *Connect to CLI* option on the FortiGate *Managed FortiSwitches* page (or by binding a custom script using custom commands on the FortiGate unit. See Executing custom FortiSwitch scripts.

4. Repeat steps 1, 2, and 3 for the other MCLAG peer groups in the Building 2 cabinet and Building 3 cabinet.

Configure the access-level (tier-3) MCLAGs

1. Wire the access-level (tier-3) MCLAG switches from Building 1 floor 1(FS-1024E-B1-F1-1 and FS-1024E-B1-F1-2). Wait until they are discovered and authorized (if automatic authorization is disabled, you must authorize the switches manually).
2. Using the FortiGate CLI, assign the LLDP profile `default-auto-mclag-icl` to the ports that will form the ICL in the access-level (tier-3) MCLAG peers switches from Building 1 floor 1 (FS-1024E-B1-F1-1 and FS-1024E-B1-F1-2). For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

3. On both distribution-level switches in the Building 1 cabinet (FS-1048E-B1-C-1 and FS-1048-B1-C-2), add an `auto-isl-port-group` for the access-level (tier-3) MCLAG peer group from Building 1 floor 1.

```
config switch auto-isl-port-group
   edit to_B1-F2
      set member <port_name>
   next
   edit to_B1-F1
      set member <port_name>
   next
end
```

This configuration is done directly in the FortiSwitch CLI (or by binding a custom script using custom commands on the FortiGate unit. See Executing custom FortiSwitch scripts.

4. Repeat steps 1, 2, and 3 for the other access-level (tier-3) MCLAG peer groups in building 1 and then in the floors in buildings 2 and 3.
5. Connect the access switches to the access-level MCLAG peer groups in the floors of each building, and the inter-switch links are formed automatically. Wait until they are discovered and authorized (authorization must be done manually if auto-authorization is disabled).
6. For the switches in the ring topologies, connect the FortiSwitch units with uplinks to the distribution level, wait until the switches are managed, and then connect the rest of the FortiSwitch units.
7. All FortiSwitch units are now authorized; therefore, the complete FortiSwitch topology is fully managed on the FortiGate unit. The deployment is completed, and the administrator can now configure the FortiSwitch VLANs and assign them to the access ports or configure 802.1x security, network access control (NAC), and dynamic port policies for dynamic VLAN assignment.

Appendix A: Products used in this guide

The following product models and firmware were used in the large-campus example:

Product	Model	Firmware
FortiGate	FG-4400F	7.0
FortiSwitch	FS-3032E	7.0
FortiSwitch	FS-1048E	7.0
FortiSwitch	FS-1024E	7.0
FortiSwitch	FS-M426E	7.0
FortiSwitch	FS-448E	7.0
FortiAP	FAP-431F	7.0

Appendix B: Documentation references

For more information, use the following resources:

- Product administration guides
  - FortiGate Administration Guide
  - Managed FortiSwitch Administration Guide
  - FortiWiFi and FortiAP Configuration Guide
- Solution hub
  - Secure Access

www.fortinet.com