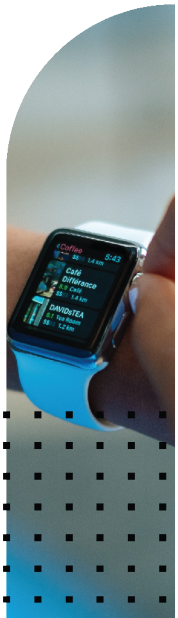
FortiGate 6000F Series System Guide

FortiGate 6000F Series



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

October 6, 2023
FortiGate 6000F Series 7.0.12 System Guide
01-7012-464766-20231006

TABLE OF CONTENTS

Change log

Date	Change description
October 6, 2023	Added information about the FortiGate 6001F, a new FortiGate 6000F series model that includes a total of ten FPCs, by default three of them are active. To increase throughput you can purchase perpetual or subscription licenses for each of the additional seven FPCs for a total of ten, see: • FortiGate 6000F series hardware description on page 7. • FortiGate 6001F model licensing on page 8. • FortiGate 6000F series schematic on page 14. • FortiGate 6000F series hardware generations on page 17.
March 28, 2023	Removed the Supported transceivers section. See the FortiGate 6000F datasheet or contact Fortinet for current information about supported transceivers.
August 17, 2022	Added information about what happens to the RAID configuration of a FortiGate 6301F or 6501F after installing firmware from the BIOS. See Installing firmware from the BIOS after a reboot on page 45.
December 22, 2021	Added links to information about grounding the FortiGate 6000F to AC and DC power sections.
July 15, 2021	Corrections and additions to Regulatory notices on page 51.
May 13, 2021	Added information about FortiGate 6000F DC models. • The DC models are listed here FortiGate 6000F series hardware description on page 7. • Details about DC power are here: DC PSUs and supplying DC power to a FortiGate 6000F on page 22.
January 21, 2021	Added information about FortiGate 6000F hardware generation 1 and generation 2, see FortiGate 6000F series hardware generations on page 17.
January 14, 2021	Updates and corrections to FortiGate 6000F AC power supply units (PSUs) on page 18. Removed DC power content that was added incorrectly.
December 23, 2020	The section FortiGate 6000F AC power supply units (PSUs) on page 18 has been updated for the FortiGate 6000F generation 2. The new section Connecting generation 1 or 2 FortiGate 6000F PSUs to low line AC power on page 20 describes FortiGate 6000F generation 1 AC PSUs.
September 2, 2020	More information about FPC failure with power loss added to FortiGate 6000F AC power supply units (PSUs) on page 18.
April 13, 2020	Updated Console port on page 12 and Shipping components on page 16 to include the USB to RJ-45 console cable. Other minor changes.
October 25, 2019	Misc. fixes.
October 18, 2019	Misc. fixes.

Date	Change description
October 11, 2019	New information added to: Console port on page 12 and FortiGate 6000F four post rack-mount installation on page 28. Corrections to FortiGate 6000F series back panel on page 14 and FortiGate 6000F AC power supply units (PSUs) on page 18.

FortiGate 6000F series hardware description

The FortiGate 6000F series is a collection of 3U 19-inch rackmount appliances that include twenty-four 1/10/25GigE SFP28 and four 40/100GigE QSFP28 data network interfaces, as well as NP6 and CP9 processors to deliver high IPS/threat prevention performance.

Currently, the following FortiGate 6000F series models are available:

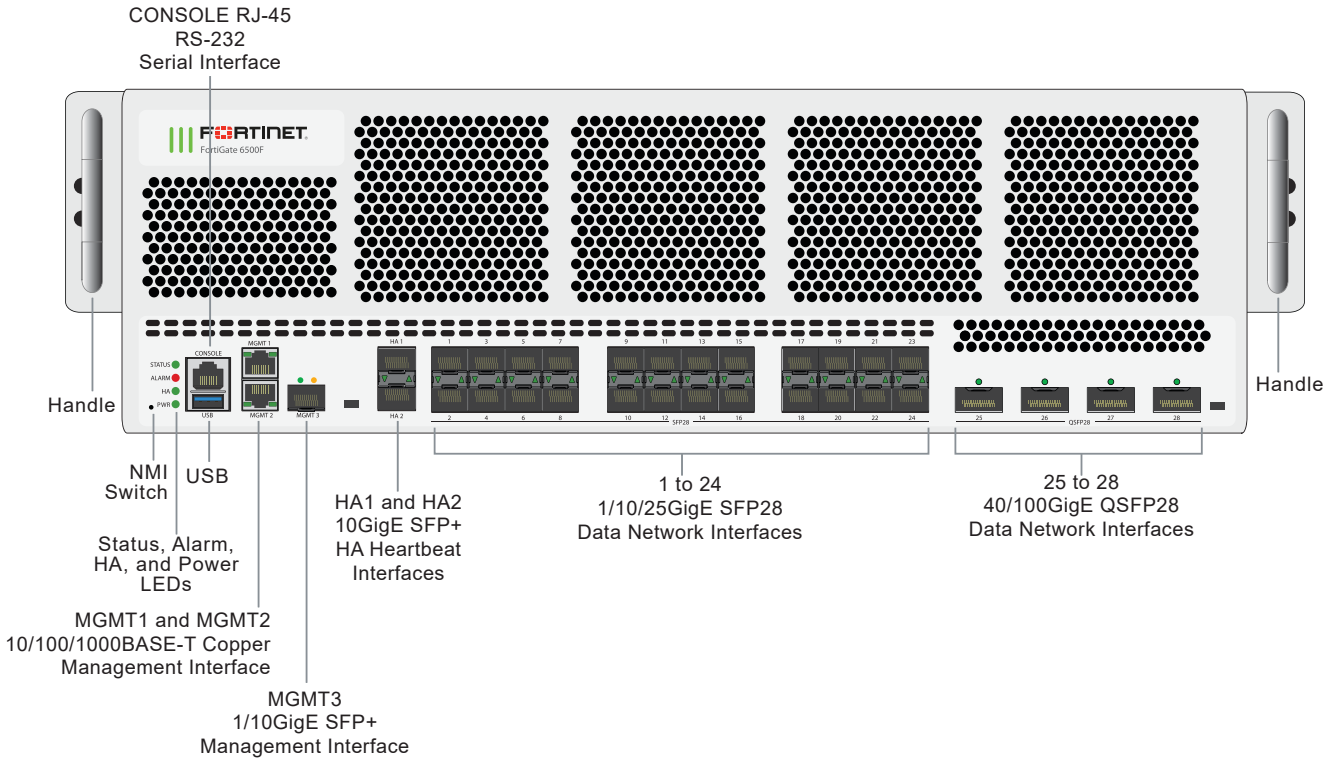
- FortiGate 6500F and FortiGate 6500F-DC
- FortiGate 6501F and FortiGate 6501F-DC
- FortiGate 6300F and FortiGate 6300F-DC
- FortiGate 6301F and FortiGate 6301F-DC
- FortiGate 6001F and FortiGate 6001F-DC

All FortiGate 6000F series models have the same front and back panel configuration including the same network interfaces. The differences are the processing capacity of the individual models. All FortiGate 6000F series models include a management board (MBD) and internal Fortinet Processor Cards (FPCs) that contain NP6 and CP9 security processors. The management board handles management tasks, separating management tasks from data processing tasks that are handled by the FPCs. The FortiGate 6000F series uses session-aware load balancing to distribute sessions to the FPCs. The FortiGate 6500F includes ten FPCs and the FortiGate 6300F includes six FPCs.

The FortiGate 6001F model includes a total of ten FPCs, by default three of them are active. To increase throughput you can purchase perpetual or subscription licenses for each of the additional seven FPCs for a total of ten.

Also the FortiGate 6501F, 6301F, and 6001F models include two internal 1 TByte log disks in a RAID-1 configuration.

FortiGate 6000F series front panel (FortiGate 6500F model shown)



FortiGate 6001F model licensing

The FortiGate 6001F model includes a total of ten FPCs, by default three of them are active. To increase throughput you can purchase perpetual or subscription licenses for each of the additional seven FPCs for a total of ten. You cannot mix perpetual and subscription licenses.

- A perpetual license provides permanent access to one or more additional FPCs.
- A subscription license provides access to one or more additional FPCs for the term of the subscription.

Perpetual or subscription licenses can be purchased from Fortinet. The package you get when you purchase the license includes instructions for obtaining a license key (if required) and activating the license on your FortiGate 6001F (if required).

Front panel interfaces

All FortiGate 6000F models have the following front panel interfaces:

- Twenty-four 1/10/25GigE SFP28 data network interfaces (1 to 24). The default speed of these interfaces is 10Gbps. These interfaces are divided into the following interface groups: 1 - 4, 5 - 8, 9 - 12, 13 - 16, 17 - 20, and 21 - 24.
- Four 40/100GigE QSFP28 data network interfaces (25 to 28). The default speed of these interfaces is 40Gbps.

- Two front panel 1/10GigE SFP+ HA interfaces (HA1 and HA2) used for heartbeat, session sync, and management communication between two and only two FortiGate 6000Fs in an HA cluster. The default speed of these interfaces is 10Gbps. Operating them at 1Gbps is not recommended. A FortiGate 6000F cluster consists of two (and only two) FortiGate 6000Fs of the same model. To set up HA, you can use a direct cable connection between the FortiGate 6000Fs HA1 interfaces and between their HA2 interfaces.
- Two 10/100/1000BASE-T out of band management Ethernet interfaces (MGMT1 and MGMT2).
- One front panel 1/10GigE SFP+ out of band management interface (MGMT3).
- One RJ-45 RS-232 serial console connection.
- One USB connector.

Interface groups and changing data interface speeds

Depending on the networks that you want to connect your FortiGate 6000F to, you may have to manually change the data interface speeds. The port1 to port24 data interfaces are divided into the following groups:

- port1 - port4
- port5 - port8
- port9 - port12
- port13 - port16
- port17 - port20
- port21 - port24

All of the interfaces in a group operate at the same speed. Changing the speed of an interface changes the speeds of all of the interfaces in that group. For example, if you change the speed of port18 from 10Gbps to 25Gbps the speeds of port17 to port20 are also changed to 25Gbps.

The port25 to port28 interfaces are not part of an interface group. You can set the speed of each of these interfaces independently of the other three.

Another example, the default speed of the port1 to port24 interfaces is 10Gbps. If you want to install 25GigE transceivers in port1 to port24 to convert these data interfaces to connect to 25Gbps networks, you can enter the following from the CLI:

```
config system interface
   edit port1
      set speed 25000full
   next
   edit port5
      set speed 25000full
   next
   edit port9
      set speed 25000full
   next
   edit port13
      set speed 25000full
   next
   edit port17
      set speed 25000full
   next
   edit port21
      set speed 25000full
   end
```

Front panel LEDs

LED	State	Description
STATUS	Off	The FortiGate 6000F is powered off.
	Green	The FortiGate 6000F is powered on and operating normally.
	Flashing Green	The FortiGate 6000F is starting up.
ALARM	Red	Major alarm. One or more analog sensors have surpassed a critical or non-recoverable (NR) threshold causing an alarm. When a critical threshold has been reached, it means that a condition has been detected that has surpassed an operating tolerance. For example, a temperature has increased above the allowed operating temperature range.
	Amber	Minor alarm. One or more analog sensors (excluding PSUs) has surpassed a major or critical (CR) threshold. Any sensor, including sensors on PSUs, has generated an alert. Sensor alert criteria is defined per sensor. For analog sensors, alerts usually mean passing an upper critical (UC) or lower critical (LC) threshold. For other sensors, an alert could mean a flag bit is indicating an anomaly.
	Off	No alarms
HA	Off	The FortiGate 6000F is operating in normal mode.
	Green	The FortiGate 6000F is operating in HA mode.
	Red	The FortiGate 6000F is operating in HA mode and the HA heartbeat cannot find the other FortiGate 6000F in the HA cluster.
PWR	Off	The FortiGate 6000F is powered off.
	Green	The FortiGate 6000F is powered on and operating normally.
1 to 24 Link/Activity	Green	This interface is connected at 25Gbps /10Gbps /1Gbps with the correct cable and the attached network device has power.
	Flashing Green	Network traffic on this interface.
	Off	No link is established.
25 to 28 Link/Activity	Green	This interface is connected at 100Gbps /40Gbps with the correct cable and the attached network device has power.
	Flashing Green	Network traffic on this interface.
	Off	No Link
MGMT1 MGMT2 Link/ Activity (Left	Green	This interface is connected at 1Gbps or 100Mbps with the correct cable and the attached network device has power.

LED	State	Description
LED)	Flashing Green	Network traffic on this interface.
	Off	No link is established.
MGMT1 MGMT2 Speed (Right LED)	Green	This interface is connected at 1Gbps.
	Amber	This interface is connected at 100Mbps
	Off	No link is established.
MGMT3 Link/ Activity (Left LED)	Green	This interface is connected at 10Gbps or 1Gbps with the correct cable and the attached network device has power.
	Flashing Green	Network activity at the interface.
	Off	No link is established.
MGMT3 (Right LED)	Not used.	
HA1 HA2 Link/Activity	Green	This interface is connected at 10Gbps or 1Gbps with the correct cable and the attached network device has power
	Flashing Green	Network activity at the interface.
	Off	No link is established.

Front panel connectors

You connect the FortiGate 6000F to your 25 Gbps or 10 Gbps networks using the 1 to 24 SFP28 front panel interfaces. You can also connect the FortiGate 6000F to your 100 Gbps or 40 Gbps networks using the 25 to 28 front panel QSFP28 interfaces. The front panel also includes 10 GigE SPF+ HA heartbeat interfaces (HA1 and HA2), two Ethernet 10/100/1000 copper management interfaces (MGMT1 and MGMT2), a 10 GigE SPF+ management interface (MGMT3), an RJ-45 RS-232 serial console port, and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

Connector	Type	Speed	Protocol	Description
1 to 24	SFP28	1/10/25Gbps	Ethernet	1/10/25GigE connection using SFP28 or SPF+ transceivers. For traffic interfaces.
25 to 28	QSFP28	40/100Gbps	Ethernet	40/100GigE connections using QSFP28 or QSFP+ transceivers. For traffic interfaces.

Connector	Type	Speed	Protocol	Description
MGMT1 MGMT2	RJ-45	10/100/1000Mbps	Ethernet	10/100/1000BASE-T copper connections for out of band management or system administration.
MGMT3	SFP+	1/10Gbps	Ethernet	1/10GigE connection using an SFP+ or SFP transceiver. For out of band management or system administration.
HA1 HA2	SFP+	1/10Gbps	Ethernet	1/10GigE connection using SFP+ or SFP transceivers. For HA heartbeat and synchronization. 1GigE not recommended.
CONSOLE	RJ-45	9600bps data bits: 8 parity: none stop bits: 1 flow control: none	RS-232	Serial interface for console access.
USB	USB 3.0 Type A		USB 3.0 USB 2.0	Standard USB connector.

Console port

You can use the USB to RJ-45 RS-232 Console port to connect to the FortiGate 6000F CLI with these settings:

Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None

From the Console port, you can connect to the management board (MBD) CLI of the FortiGate 6000F. You can also press Ctrl-T to switch between the management board CLI and the CLIs of each of the FPCs in your FortiGate 6000F (the new destination is displayed in the terminal window). The FortiGate 6500F has a management board and 10 FPCs; 11 consoles in total. The FortiGate 6300F has a management board and 6 FPCs; 7 consoles in total.

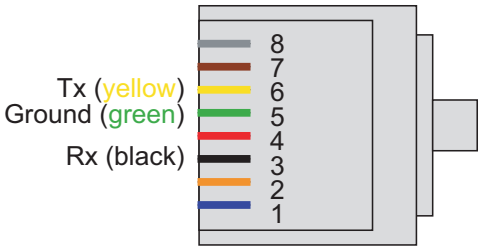
You should only make configuration changes on the management board CLI. You can cycle through individual FPC consoles to use `diagnose`, `get`, or `execute` commands to log into individual FPCs.

Once the console port is connected to the CLI that you want to use, press Enter to enable the CLI and log in. When your session is complete you can press Ctrl-T to connect to another CLI.

Your FortiGate 6000F package includes a USB to RJ-45 serial cable that you can use to connect a management PC USB port to the FortiGate 6000F console port.

Fortinet USB to RJ-45 serial cable RJ-45 pinout

RJ-45	Color	Function
5	Green	Ground
3	Black	Rx
6	Yellow	Tx



RJ-45

Connecting to the CLI of an individual FPC

Use the following steps to connect to the CLI of the FPC in slot 4: (FPC04)

1. Connect the console cable supplied with your FortiGate 6000F to the console port and to your PC USB port.
2. Start a terminal emulation program on the PC. Use these settings:
   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
3. Press Ctrl-T to enter console switch mode.
4. Repeat pressing Ctrl-T until you have connected to FPC04. Example prompt:
   `<Switching to Console: FPC04 (9600)>`
5. Login with an administrator name and password.
6. When your session is complete, enter the `exit` command to log out.

NMI switch and NMI reset commands

When working with Fortinet Support to troubleshoot problems with your FortiGate 6000F you can use the front panel non-maskable interrupt (NMI) switch to assist with troubleshooting. Pressing this switch causes the software to dump management board registers/backtraces to the console. After the data is dumped the management board reboots. While the management board is rebooting, traffic is temporarily blocked. The management board should restart normally and traffic can resume once the management board is up and running.

You can use the following command to dump registers/backtraces of one or more FPCs to the console. After the data is dumped, the FPCs reboot. While the FPCs are rebooting, traffic is distributed to the remaining FPCs. The FPCs should restart normally and traffic can resume once they are up and running.

```
execute load-balance slot nmi-reset <slot-number(s)>
```

Where `<slot-number(s)>` can be one or more FPC slot numbers or slot number ranges with no space and separated by commas. For example:

```
execute load-balance slot nmi-reset 1,3-4
```

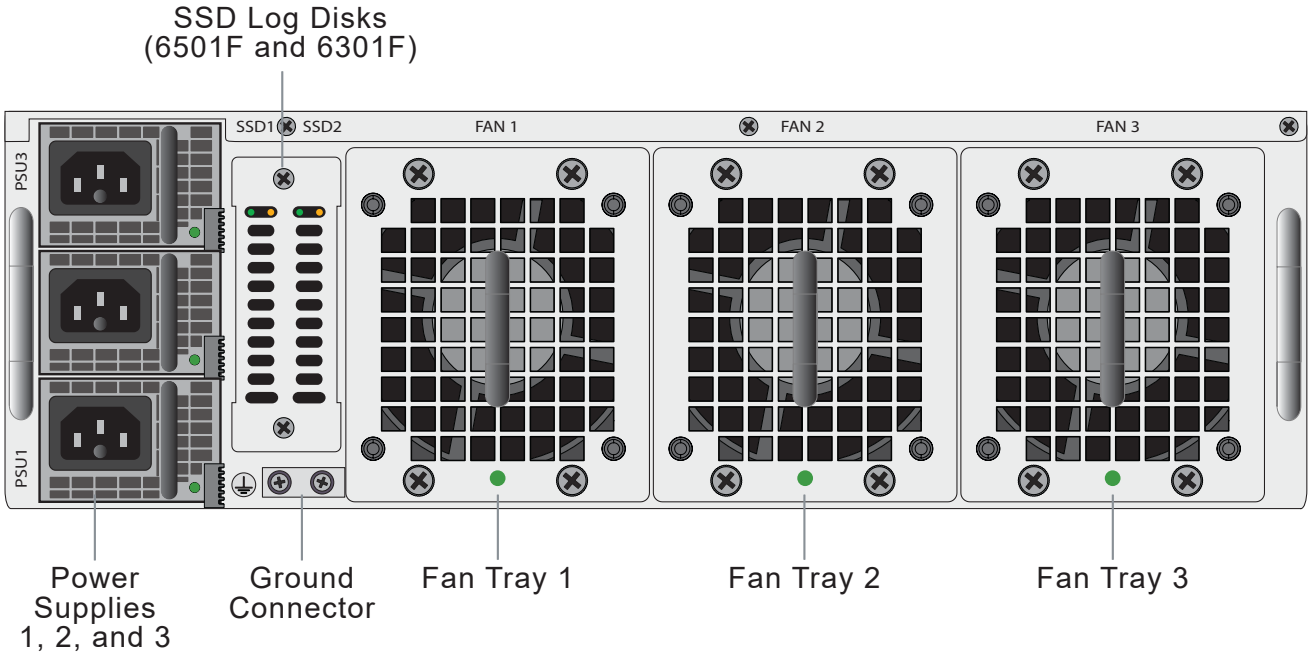
FortiGate 6000F series back panel

The FortiGate 6000F series back panel includes three hot swappable cooling fan trays and three hot swappable redundant AC power supply units (PSUs). For more information on power connections and redundant power, see FortiGate 6000F AC power supply units (PSUs) on page 18.

The FortiGate 6000F DC models include two hot swappable -48 to -60 VDC, 50A max DC PSUs. For DC power information, see DC PSUs and supplying DC power to a FortiGate 6000F on page 22.

The back panel also includes the FortiGate 6000F ground connector that must be connected to ground.

FortiGate 6000F back panel (FortiGate 6501F AC model shown)



FortiGate 6000F series schematic

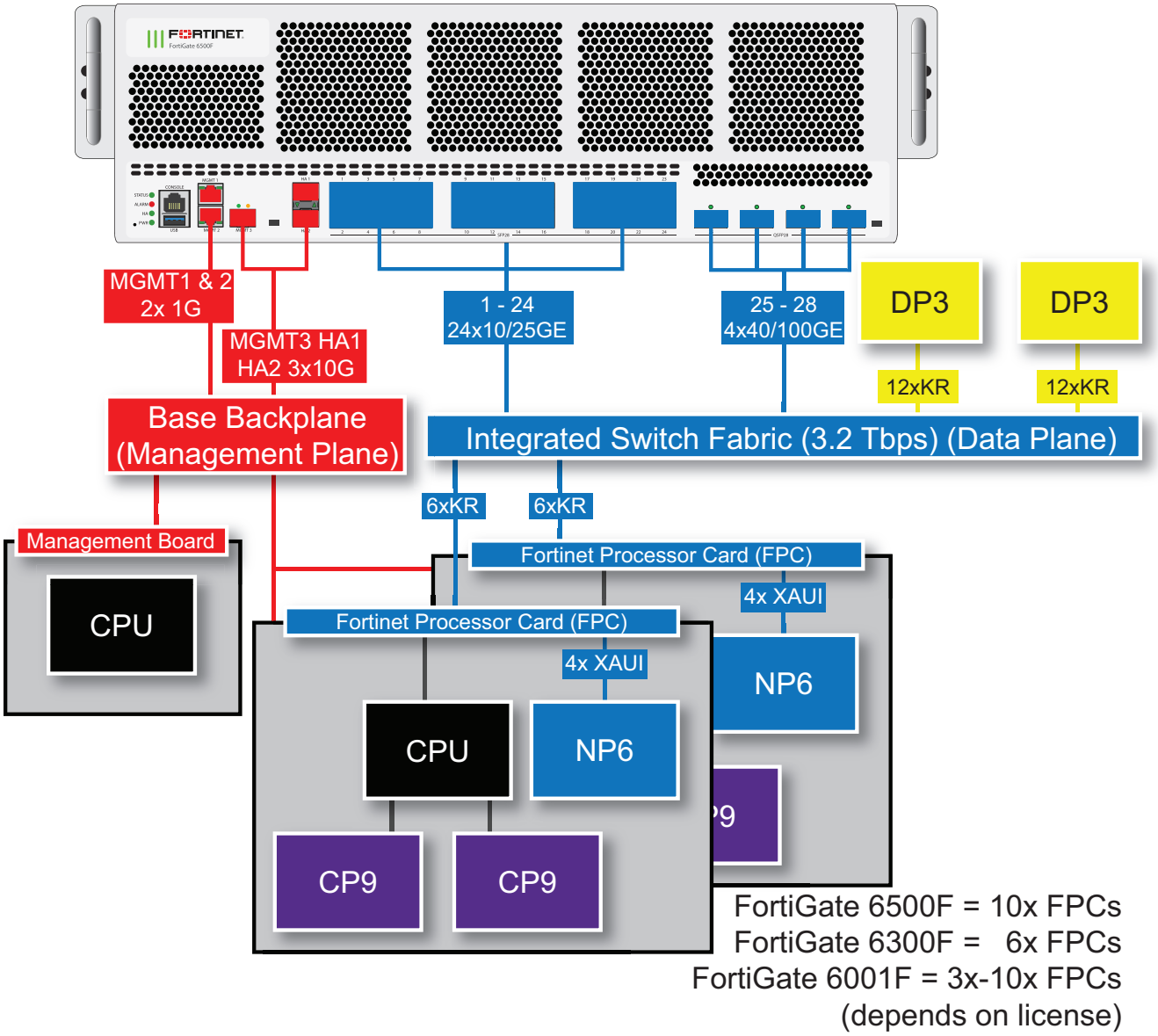
FortiGate 6000F hardware includes a data plane and a management plane. The data plane processes customer network data. The management plane handles management functions such as administrator logins, configuration and session synchronization, SNMP, and other monitoring, HA heartbeat communication, and remote and (if supported) local disk logging. Separating these two planes means that resources used for data processing are not compromised by management activities.

In the data plane, two DP3 load balancers use session-aware load balancing to distribute sessions from the front panel interfaces (port1 to 28) to Fortinet Processor Cards (FPCs). The DP3 processors communicate with the FPCs across the

3.2Tbps integrated switch fabric. Each FPC processes sessions load balanced to it. The FPCs send outgoing sessions back to the integrated switch fabric and then out the network interfaces to their destinations.

The NP6 processor in each FPC enhances network performance with fastpath acceleration that offloads communication sessions from the FPC CPU. The NP6 processor can also handle some CPU intensive tasks, like IPsec VPN encryption/decryption. The CP9 processors in each FPC accelerate many common resource intensive security related processes such as SSL VPN, Antivirus, Application Control, and IPS.

The management plane includes the management board, base backplane, management interfaces, and HA heartbeat interfaces. Configuration and session synchronization between FPCs in a FortiGate 6000F occurs over the base backplane. In an HA configuration, configuration and session synchronization between the FortiGate 6000Fs in the cluster takes place over the HA1 and HA2 interfaces. Administrator logins, SNMP monitoring, remote logging to one or more FortiAnalyzers or syslog servers, and other management functions use the MGMT1, MGMT2, and MGMT3 interfaces. You can use the 10Gbps MGMT3 interface for additional bandwidth that might be useful for high bandwidth activities such as remote logging.



FortiGate 6000F series hardware information

This section introduces FortiGate 6000F series hardware components and accessories.

Shipping components

The FortiGate 6000F ships pre-assembled with the following components:

- The 3U FortiGate 6000F.
- The AC version of the FortiGate 6000F includes three AC Power Supply Units (PSUs) installed in the back panel.
- The DC version of the FortiGate 6000F includes two DC PSUs installed in the back panel.
- The AC version of the FortiGate 6000F includes three power cords with C15 power connectors.
- The DC version of the FortiGate 6000F includes two custom DC power cables that include a two prong connector with a release tab on one end and double hole lug plates on the other end.
- Three cooling fan trays installed in the back panel.
- One set of two sliding rails for 4-post rack mounting.
- Six rubber feet.
- One USB to RJ-45 RS-232 console cable.
- One RJ-45 Ethernet cable.
- Two FG-TRAN-SFP+SR transceivers.

Optional accessories and replacement parts

The following optional accessories can be ordered separately:

SKU	Description
FG-6000F-FAN	FortiGate 6000F fan tray.
SP-FG4000F-PS	2000W AC PSU when connected to high line AC power (200VAC or higher). 1500W AC if connected to low-line AC (120VAC or below).
SP-FG4000F-DC-PS	2000W DC PSU.
FG-7040E-PS-AC	1500W AC PSU. (FortiGate 6000F Generation 1)

You can also order the following:

- Transceivers

Physical description of the FortiGate 6000F

The FortiGate 6000F is a 3U appliance that can be installed in a standard 19-inch rack. The following table describes the physical characteristics of the FortiGate 6000F chassis.

Form factor	3RU

Dimensions (H x W x D)	5.20 x 17.20 x 26.18 in (132 x 437 x 665 mm)
Rack mount type	Sliding rail
FortiGate 6300F and 6301F weight	67.68 lbs 30.7 kg
FortiGate 6500F and 6501F weight	78.26 lbs 35.5 kg
FortiGate 6001F weight	78.26 lbs 35.5 kg
Operating temperature	32 to 104°F (0 to 40°C)
Storage temperature	-31 to 158°F (-35 to 70°C)
Relative humidity	20% to 90% non-condensing
Average noise level	57.43 dbA
Input voltage range	100 to 240 VAC (50 to 60 Hz)
Supplied power supply units (PSUs)	3xSP-FG4000F-PS (2+1 redundancy) or 2xSP-FG4000F-DC-PS (1+1 redundancy)
Max power consumption	1568W
Average power consumption	1328W
Max current (AC)	30A@100VAC, 20A@240VAC
Heat dissipation	5350 BTU/hr
Joules/hr	5645 KJ/hr

FortiGate 6000F series hardware generations

Two generations of FortiGate 6000F series hardware are now available. Both generations support the same software features. Generation 2 has two hardware improvements:

- The FPCs include more memory.
- When connected to high-line AC power, generation 2 FortiGate 6000F series models provide 1+1 PSU redundancy. When connected to high-line AC power, each PSU provides 2000W, which is enough power to run the entire system including all FPCs.

For more information on FortiGate 6000F series generation 1 and generation 2, including supported firmware versions and how to determine the generation of your FortiGate 6000F series hardware, see the Fortinet Community article: Technical Tip: Information on FortiGate 6000F series Gen1 and Gen2.

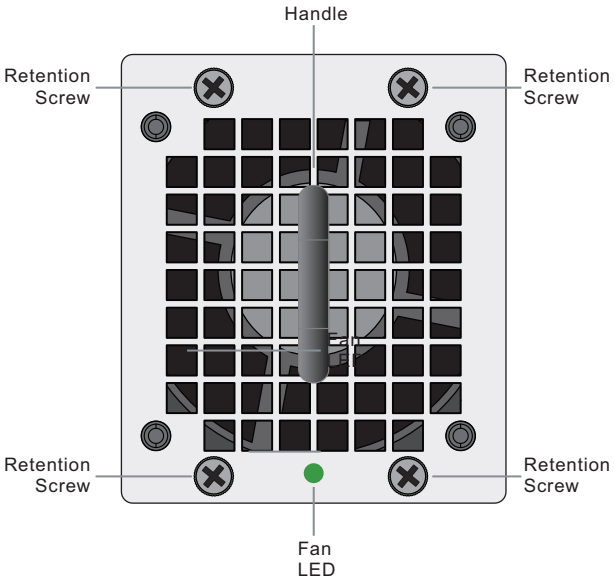
For more information on generation 1 and generation 2 AC PSUs, see FortiGate 6000F AC power supply units (PSUs) on page 18.

The FortiGate 6001F is a generation 2 appliance.

Cooling fan trays

The FortiGate 6000F contains three hot swappable cooling fan trays installed in the back of the appliance. When the fan LED is green the fan tray is operating normally. If a fan tray LED turns red or goes off the fan tray should be replaced.

Cooling Fan Tray



Fan trays are hot swappable. You can replace a failed fan tray while the FortiGate 6000F is operating. To replace a fan tray, unscrew the four retention screws and use the handle to pull the fan tray out of the chassis. Install the new fan tray by sliding it into place. As you slide the new fan into place it will power up. Tighten the retention screws.

The other fan trays will continue to operate and cool the chassis as a fan tray is being removed and replaced. However an open fan tray slot will result in less air flow through the appliance so do not delay installing the replacement fan tray.

The FortiGate 6000F monitors the internal temperature of the appliance and adjusts the operating speed of the cooling fans as required. When the device is first powered on all cooling fans run at full speed. Once the system is up and running, the fan speeds are reduced to maintain an optimum temperature in the appliance.

During normal operation, all fan trays are active. If cooling requirements increase, the fan speed will increase.

FortiGate 6000F AC power supply units (PSUs)

The FortiGate 6000F back panel includes three hot swappable redundant AC PSUs (PSU1, PSU2, and PSU3). Two generations of FortiGate 6000F models have been released. Generation 1 and generation 2 have different AC PSUs:

- Generation 2 FortiGate 6000F PSUs can be connected to high-line AC power (200VAC or higher) and each PSU provides 2000W AC. A generation 2 FortiGate 6000F with two high line power feeds connected to PSU1 and PSU2 is a fully 1+1 redundant solution because a single PSU can fully power a FortiGate 6000F.
- Generation 1 FortiGate 6000F PSUs can be connected to low line AC power (120VAC or below) and each PSU provides 1500W AC. Requires at least 2 PSUs to be connected to power. Connecting a third PSU provides 2+1

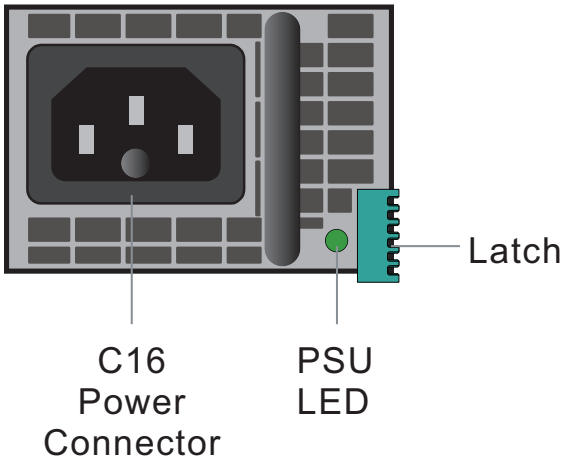
redundancy. If only one PSU is operating, some FPCs will be shut down and performance will be reduced.

- You can also connect generation 2 FortiGate 6000F PSUs to low-line AC power (120VAC or below) and each PSU provides 1500W AC. Requires at least 2 PSUs to be connected to power. Connecting a third PSU provides 2+1 redundancy. If only one PSU is operating, some FPCs will be shut down and performance will be reduced.

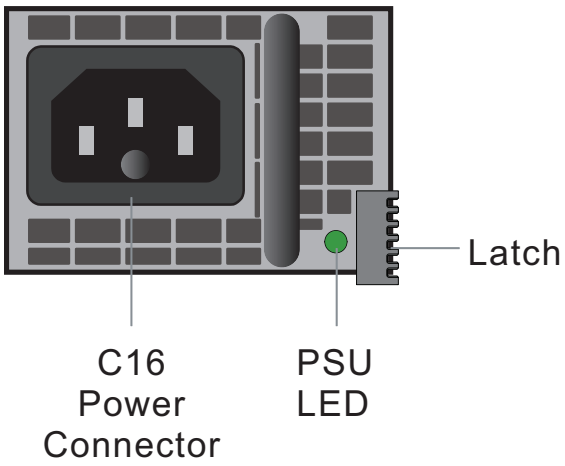
Use a supplied C15 power cable to connect power to each PSU C16 power connector. C15/C16 power connectors are used for high temperature environments and are rated up to 120°C.

For more information on FortiGate 6000F generation 1 and generation 2, including supported firmware versions and how to determine the generation of your FortiGate 6000F hardware, see the Fortinet Knowledge base article: Technical Tip: Information on FortiGate 6000F series Gen1 and Gen2.

Generation 1 AC PSU showing C16 power connector



Generation 2 AC PSU showing C16 power connector



Individual AC PSUs do not have to be connected to ground. Instead you can use the information in Connecting the FortiGate 6000F to ground on page 25 to connect the FortiGate 6000F to ground.

Connecting generation 2 FortiGate 6000F PSUs to high line AC power

If you connect a generation 2 FortiGate 6000F to high-line AC power, each PSU provides 2000W AC, which is all the power required by the FortiGate 6000F. Only two PSUs (PSU1 and PSU2) each connected to separate power feeds, are required for full 1+1 power redundancy. PSU3 may also be connected if you have three separate power feeds and provides 1+1+1 redundancy. To maintain redundancy, you should replace any failed PSUs.

See FortiGate 6000F series back panel on page 14 for locations of the PSUs.

Recommended fully redundant configuration when connected to high-line AC power:

- Two FortiGate 6000Fs in a High Availability (HA) configuration connected to two power feeds.
- On both FortiGate 6000Fs, connect PSU1 and PSU2 to different power feeds.

Connecting generation 1 or 2 FortiGate 6000F PSUs to low line AC power

If you connect a generation 1 FortiGate 6000F or a generation 2 FortiGate 6000F PSU to low line AC power, each PSU provides 1500W AC and at least two PSUs (PSU1 and PSU2) must be connected to power. PSU3 is a backup PSU and provides 2+1 redundancy. All PSUs should be connected to AC power.

See FortiGate 6000F series back panel on page 14 for locations of the PSUs.

Recommended FortiGate 6000F low line AC power fully redundant configuration:

- Two FortiGate 6000Fs (Unit 1 and Unit 2) in a High Availability (HA) configuration with two power feeds (Feed A and Feed B).
- Connect PSU1 and PSU2 of Unit 1 to Feed A. Connect PSU3 of Unit 1 to Feed B.
- Connect PSU1 and PSU2 of Unit 2 to Feed B. Connect PSU3 of Unit 2 to Feed A.

For normal operation of a FortiGate 6000F connected to low line AC power, at least 2 PSUs must be operating and connected to power. If two PSUs fail and only one PSU is operating, the FortiGate 6000F will continue to operate but only four FPCs will be running, the remaining FPCs are shut down. This means the performance of the FortiGate 6000F is reduced until at least two PSUs are connected.

If only one PSU is operating, the FortiGate 6000F shuts down the FPCs starting with the FPC with the highest slot number, until only four FPCs are running. Usually this results in the FPCs in slots 1 to 4 running if there is only one PSU connected.

If one of the FPCs in slot 1 to 4 has previously shut down, the FortiGate 6000F keeps the four operational FPCs in the lowest slot numbers running. For example, if the FPC in slot 2 has previously shut down, if only one PSU is operating, the FPCs in slots 1, 3, 4, and 5 continue running.

The FortiGate 6000F also keeps the primary FPC running. Usually the FPC in slot 1 is the primary FPC, so if only one PSU is operating, the FPCs in slots 1 to 4 continue running. However, if the FPC in another slot has become the primary FPC, then this FPC as well as the three remaining FPCs with the lowest slot numbers will continue running. For example, if the FPC in slot 6 has become the primary FPC, then when only one PSU is operating, the FPCs in slots 1, 2, 3, and 6 continue running.

AC PSU LED states

The PSU LED indicates whether the PSU is operating correctly and connected to power.

State	Description
Off	AC power not connected. If this LED is not lit, check to make sure the PSU is connected to a power feed. If the power feed is good then the PSU has failed and should be replaced.
Flashing green	The PSU is in standby mode, not supplying power to the chassis.
Green	Normal Operation with AC power connected.
Amber	Fault condition (PSU shuts down). This can occur if power input or output is out of the normal operating range, temperature is out of the normal range, or one or more fans are not operating. This may be caused by a problem with the PSU. This could also be caused by conditions external to the PSU, for example, if there is a problem with the power supplied to the PSU or if the PSU has gotten too hot because of insufficient ventilation.
Flashing amber	Warning that power input or output, temperature, or fan operation is close to being outside of the normal operating range. This may be caused by a problem with the PSU. This could also be caused by conditions external to the PSU, for example, if there is a problem with the power supplied to the PSU or if the PSU has gotten too hot because of insufficient ventilation.

Connecting FortiGate 6000F PSUs to AC power

Use the following steps to connect a FortiGate 6000F PSU to AC power after connecting the chassis to ground.

1. Use the supplied C15 Power cables to connect each PSU C16 power connector to a separate surge protected power supply.

   You can install power cord clamps into the back of the chassis beside each PSU. Install the clamps by inserting them into the holes adjacent each supply at the back of the chassis. Use the clamps to secure the AC power cords so they are not accidentally disconnected.
2. As the FortiGate 6000F powers up, the status LED flashes green.

   Once the FortiGate 6000F has started up and is operating correctly, the front and back panel LEDs should indicate normal operation (see Confirming startup status on page 36).

Individual AC PSUs do not have to be connected to ground. Instead you can use the information in Connecting the FortiGate 6000F to ground on page 25 to connect the FortiGate 6000F to ground.

Hot swapping an AC PSU

Follow these steps to safely hot swap an AC PSU.

You can hot swap a PSU without affecting performance or interrupting traffic as long as one PSU remains connected to power at all times.

1. Attach an ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Turn off the power being supplied to the PSU and disconnect the power cord.
3. Press the latch towards the handle until the PSU is detached then pull it out of the FortiGate 6000F.
4. Insert a replacement PSU into the FortiGate 6000F and slide it in until it locks into place.
5. Use a supplied C15 power cable to connect power to the PSU C16 power connector.
6. Turn on power to the PSU.
7. Verify that the PSU status LED is solid green meaning that the PSU is powered up and operating normally.

DC PSUs and supplying DC power to a FortiGate 6000F

The DC version of the FortiGate 6000F includes two hot swappable -48 to -60 VDC, 50A max DC PSUs. Each PSU has an internal 60A/170VDC fast blow fuse on the DC line input.

Only one PSU must be connected to power. The second PSU is a backup PSU that provides 1+1 redundancy. See FortiGate 6000F series back panel on page 14 for locations of the PSUs. The diagram shows three AC PSUs, the DC version replaces the AC PSUs with two DC PSUs in slots PSU1 and PSU2. PSU3 is covered by a metal panel.

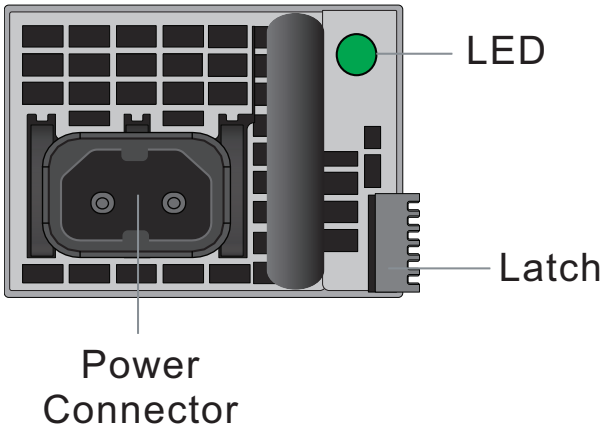
Recommended fully redundant configuration:

- Two FortiGate 6000Fs in a High Availability (HA) configuration with two power feeds (A and B). FortiGate 6000F supports HA with two and only two FortiGate 6000Fs.
- On both FortiGate 6000Fs, connect each PSU to a different power feed.

For normal operation of a single FortiGate 6000F, only one DC PSU must be operating and connected to power. If only one DC PSU is operating, all components and all FPCs continue to operate normally. However, to maintain redundancy, you should replace a failed DC PSU.

Each DC PSU is designed to be installed in a Telecom data center or similar location that has available -48VDC power fed from a listed 50A circuit breaker. To improve redundancy you can connect each PSU to a separate power circuit.

DC PSU



Individual DC PSUs do not have to be connected to ground. Instead you can use the information in Connecting the FortiGate 6000F to ground on page 25 to connect the FortiGate 6000F to ground.

Fortinet supplies custom DC power cables that connect to the two-prong power connector on each DC PSU. The connector clicks into a release tab that secures the cable into place. DC terminal rings on the supplied cable must be securely and safely fastened to the your data center power supply terminals. The supplied DC power cables are intended to be used only for in-rack wiring, must be routed away from sharp edges, and must be adequately fixed to prevent excessive strain on the wires and terminals.

DC PSU Power ratings

Max Inrush Current	50A
Max Inrush Current Duration	200ms
Normal Input Voltage	-48VDC to -60VDC
Maximum Input Voltage	-40.8VDC to -72VDC
Input Current	Average: 12.5A@48V for each PSU, Max: 50A

DC PSU LED States

State	Description
Off	DC power not connected.
Flashing green	The PSU is in standby mode, not supplying power to the chassis.
Green	Normal operation with DC power connected.
Amber	Fault condition (PSU shuts down). This can occur if power input or output is out of the normal operating range, temperature is out of the normal range, or one or more fans are not operating. This may be caused by a problem with the PSU. This could also be caused by conditions external to the PSU, for example, if there is a problem with the power supplied to the PSU or if the PSU has gotten too hot because of insufficient ventilation.
Flashing amber	Warning that power input or output, temperature, or fan operation is close to being outside of the normal operating range. This may be caused by a problem with the PSU. This could also be caused by conditions external to the PSU, for example, if there is a problem with the power supplied to the PSU or if the PSU has gotten too hot because of insufficient ventilation.

Crimping guidelines

The DC power cord is a two prong connector with a release tab on one end and double hole lug plates on the other end. The DC power source must have a 1/4" (0.64cm) stud to secure the lugs . The distance between the studs should be 5/8"

(1.59cm). The DC power source terminals should allow at least support 50A. If the DC power source does not meet these requirements the cord must be cut and re-crimped to match the DC terminals.

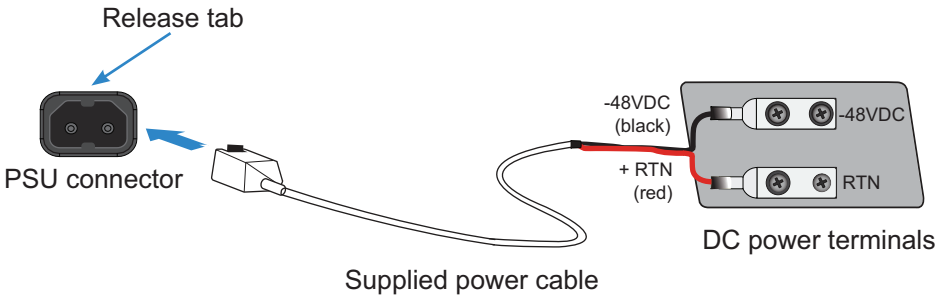
Do not crimp energized wires.

Follow these crimping guidelines:

- Strip the insulation from cable. Be careful not to nick cable strands which may later result in stands breaking.
- Cable end should be clean: wire brush or clean with emery cloth if necessary. Insert cable into connector until it stops. The insertion length must approximate the stripped length of cable.
- Insert connector in die and compress between the markings beginning near the tongue of the connector. Using the wrong installing die may result in a defective connection.
- After crimping, remove all sharp edges, flash, or burrs.

Connecting a FortiGate 6000F DC PSU to DC power

The following procedure describes how to connect a FortiGate 6000F DC PSU to DC power. Repeat this procedure to connect each PSU.



You need the following equipment to connect the FortiGate 6000F DC PSUs to DC power:

- An electrostatic discharge (ESD) preventive wrist strap with connection cord.
- One of the supplied DC power cables, that include a two prong connector with a release tab on one end and black and red double hole lug plates on the other end. Black for -48V and red for RTN.

Individual DC PSUs do not have to be connected to ground. Instead you can use the information in Connecting the FortiGate 6000F to ground on page 25 to connect the FortiGate 6000F to ground.

To connect a DC PSU to DC power

1. Attach the ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Make sure that the PSU and power cords are not energized.
3. Connect the black -48V power wire to your -48V DC power source using the ring terminal.
4. Connect the red RTN power wire from to your RTN connector using the ring terminal.
5. Plug the power cable into the FortiGate 6000F PSU connector.
   Slide the connector in until the release tab clicks, locking the cable in place.

6. Make sure the power wires are secured using tie wraps if required.
7. If required, label the black wire -48V.
8. If required, label the red wire RTN.
9. Turn on power to the PSU.
10. Verify that the PSU status LED is solid green meaning that the PSU is powered up and operating normally.

Hot Swapping a DC PSU

Follow these steps to safely hot swap a DC PSU.

You can hot swap a PSU without powering down the FortiGate 6000F as long as one PSU continues to be connected to power and operating normally.

1. Attach an ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the chassis or frame.
2. Turn off the power being supplied to the DC PSU to be hot swapped.
3. Disconnect the power cable from the FortiGate 6000F DC PSU by pressing the release tab and unplugging the cable.
4. To remove the PSU, press the latch towards the handle until the PSU is detached then pull it out of the chassis.
5. Insert a replacement PSU into the chassis and slide it in until it locks into place.
6. Plug power cord into the FortiGate 6000F PSU connector.
   Slide the connector in until the release tab clicks, locking the cable in place.
7. Turn on power to the PSU.
8. Verify that the PSU status LED is solid green meaning that the PSU is powered up and operating normally.

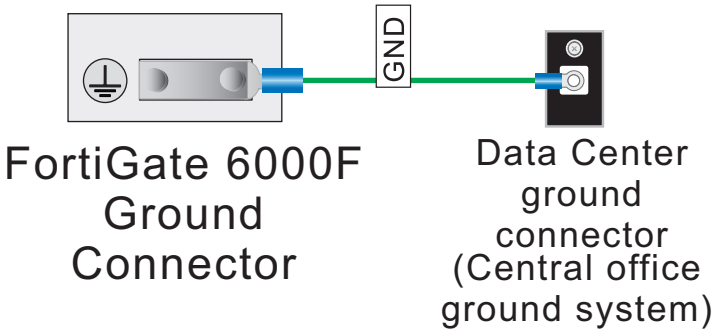
Connecting the FortiGate 6000F to ground

The FortiGate 6000F appliance includes a ground terminal on the FortiGate 6000F back panel. The ground terminal provides two connectors to be used with a double-holed lug such as Thomas & Betts PN 54850BE. This connector must be connected to a local ground connection.

You need the following equipment to connect the FortiGate 6000F to ground:

- An electrostatic discharge (ESD) preventive wrist strap with connection cord.
- One green 6 AWG stranded wire with listed closed loop double-hole lug suitable for minimum 6 AWG copper wire, such as Thomas & Betts PN 54850BE.

To connect the FortiGate 6000F chassis to ground



1. Attach the ESD wrist strap to your wrist and to an ESD socket or to a bare metal surface on the FortiGate 6000F.
2. Make sure that the FortiGate 6000F and ground wire are not energized.
3. Connect the green ground wire from the local ground to the ground connector on the FortiGate 6000F.
4. Secure the ground wire to the FortiGate 6000F.
5. Optionally label the wire GND.

FortiGate 6000F hardware assembly and rack mounting

The FortiGate 6000F appliance can be mounted in a standard 19-inch rack and requires 3U of vertical space in the rack. The FortiGate 6000F can also be surface mounted.

Cautions and warnings

FortiGate 6000Fs must be protected from static discharge and physical shock. Only handle or work with FortiGate 6000Fs at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate 6000Fs.

If you install the FortiGate 6000F appliance in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Make sure the operating ambient temperature does not exceed the manufacturer's maximum rated ambient temperature.

To avoid personal injury or damage to the FortiGate 6000F appliance, it is recommended that two or more people install the FortiGate 6000F into the rack.

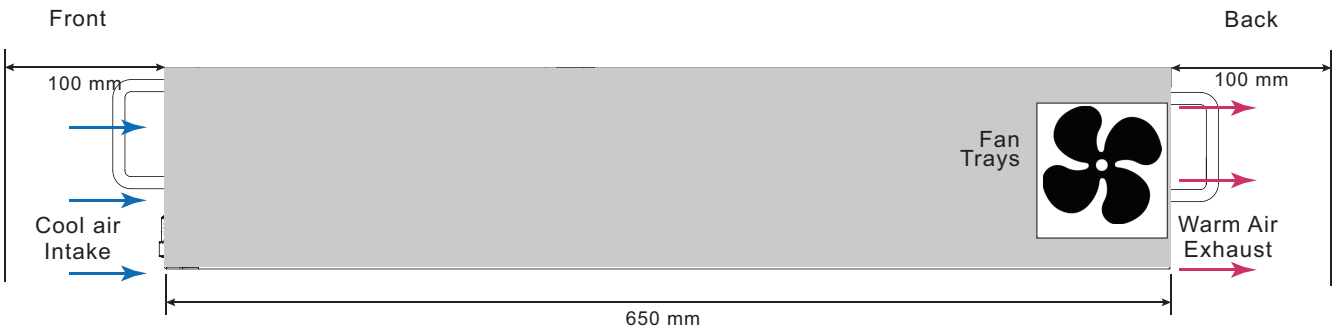
Do not place heavy objects on the appliance.

Ensure there is enough room around the appliance to allow for sufficient air flow.

Cooling air flow and required minimum air flow clearance

When installing the FortiGate 6000F, make sure there is enough clearance for effective cooling air flow**.** The following diagram shows the cooling air flow through the FortiGate 6000F and the location of fan trays. Make sure the cooling air intake and warm air exhaust openings are not blocked by cables or rack construction because this could result in cooling performance reduction and possible overheating and component damage.

FortiGate 6000F cooling air flow and minimum air flow clearance (appliance side view)



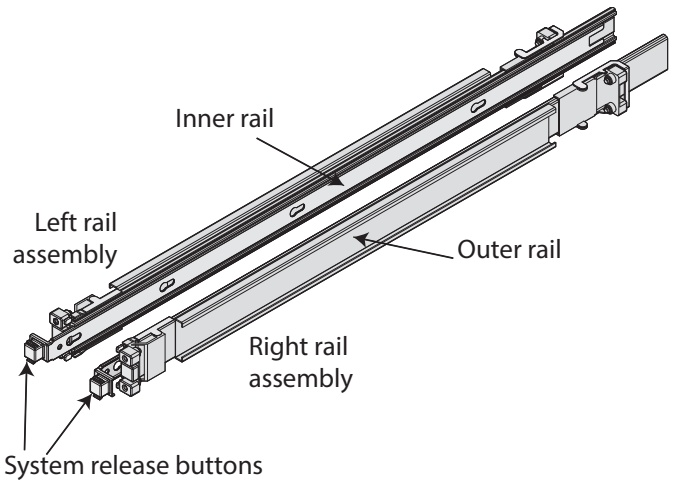
All cool air enters the appliance through the front panel and all warm air exhausts out the back. For optimal cooling allow 100 mm of clearance at the front and back of the chassis. This results in a total footprint of 850 mm from front to back. Side clearance is not required.

FortiGate 6000F four post rack-mount installation

This section describes how to use the sliding rails included with your FortiGate 6000F package to install the FortiGate 6000F in a 4-post rack.

The FortiGate 6000F is shipped with a left and a right rail assembly. Each rail assembly includes an inner rail, a middle rail, and an outer rail. The inner rail attaches to the side of the FortiGate 6000F. The middle rail remains attached to the outer rail which attaches to the rack. The middle rail is used to guide the inner rail into the outer rail.

Sliding rails



When mounted on the rails and fully slid into the rack, the FortiGate 6000F locks into place. You can press the system release buttons that project out of the front of the rack to unlock the rails and slide the FortiGate 6000F out.

No tools are required to install the rails and the FortiGate 6000F. Once the FortiGate 6000F is slid into the rack you can use a screw driver to install four rack screws to secure the FortiGate 6000F in the rack.

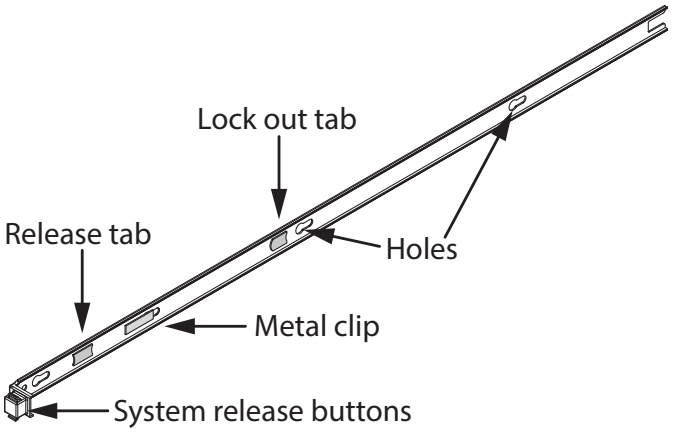
Installation steps

There are three steps to use the sliding rails to install the FortiGate 6000F in a four-post the rack:

1. Attach the right and left inner rails to the right and left sides of the FortiGate 6000F.
2. Attach the right and left outer rails to the right and left rack posts.
3. Slide the FortiGate 6000F into the rack.

As a supplement to the instructions below, you can view the following video:
https://video.fortinet.com/latest/rack-mount-sliding-rail-installation

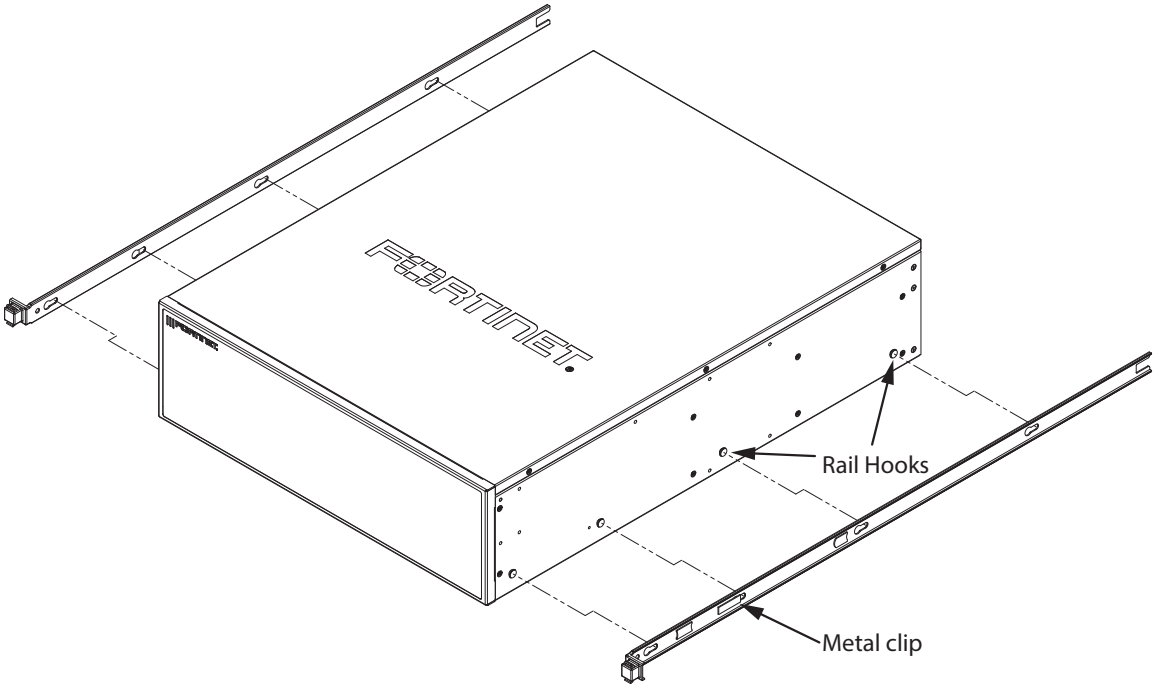
Tabs, holes, and clips on the right inner rail



Attaching the inner rails to the FortiGate 6000F

Use the following steps to install the right inner rail and then repeat them for the left inner rail.

1. Remove the FortiGate 6000F from its packaging and place it on a flat surface.
   For example, on a lifting device in front of the rack that it will be installed into.
2. Remove the right rail assembly from the packaging, and begin sliding the right inner rail out of it.
3. Unlock the right inner rail release tab to release the inner rail and slide it completely out of its rail assembly.
4. Locate the four rail hooks on the right side of the FortiGate 6000F and the corresponding holes on the inner rail.



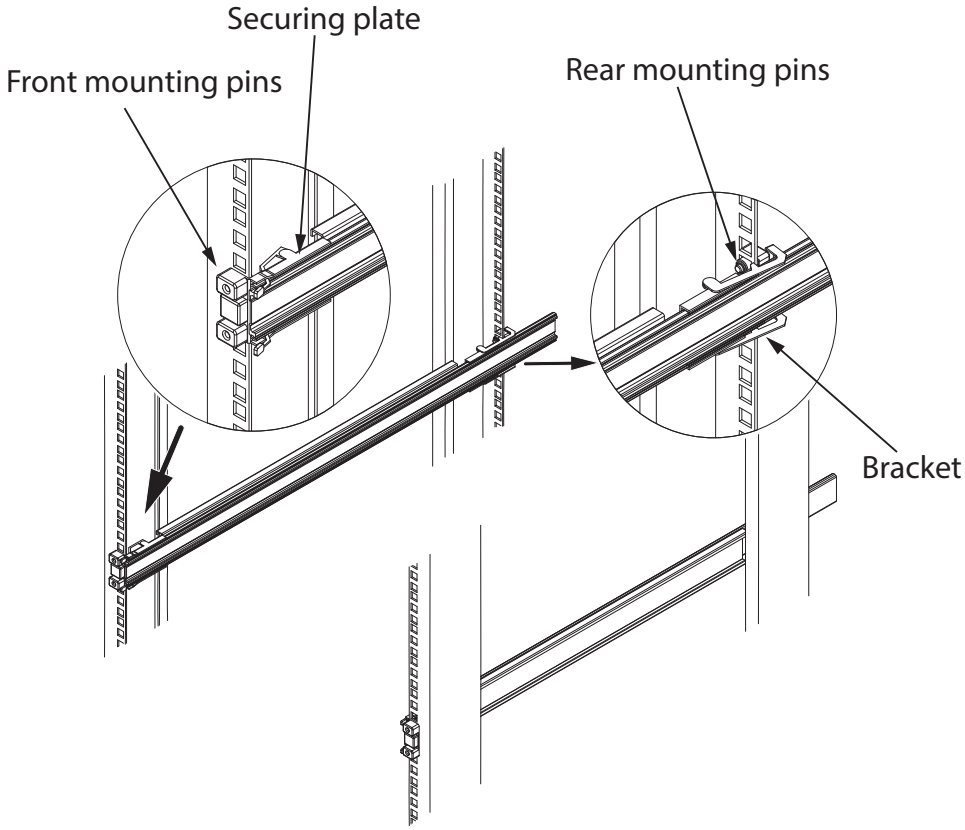
5. Align the holes with the hooks and press the hooks into the holes to attach the right inner rail to the right side of the FortiGate 6000F.

6. Slide the inner rail towards the front of the FortiGate 6000F until the inner rail metal clip clicks, locking the rail onto the side of the FortiGate 6000F.
7. Repeat these steps to attach the left inner rail to the left side of the FortiGate 6000F.

Attaching the outer rails to the rack

The ends of outer rails wrap around the inside edge of the rack posts and the mounting pins click into place.

1. Align the front of right outer rail with the right front post of the rack.
2. Push the front mounting pins into the rack post holes.
3. Pull the securing plate over the rack post and close it to lock the pins in place.
4. Pull out the bracket on the back of the right outer rail to adjust its position until it matches up with the back post of the rack.
5. Verify that the rail is level, then push the rear mounting pins into the rack post holes.
6. Repeat these steps for the left outer rail. Make sure it is installed at the same height as the right outer rail.

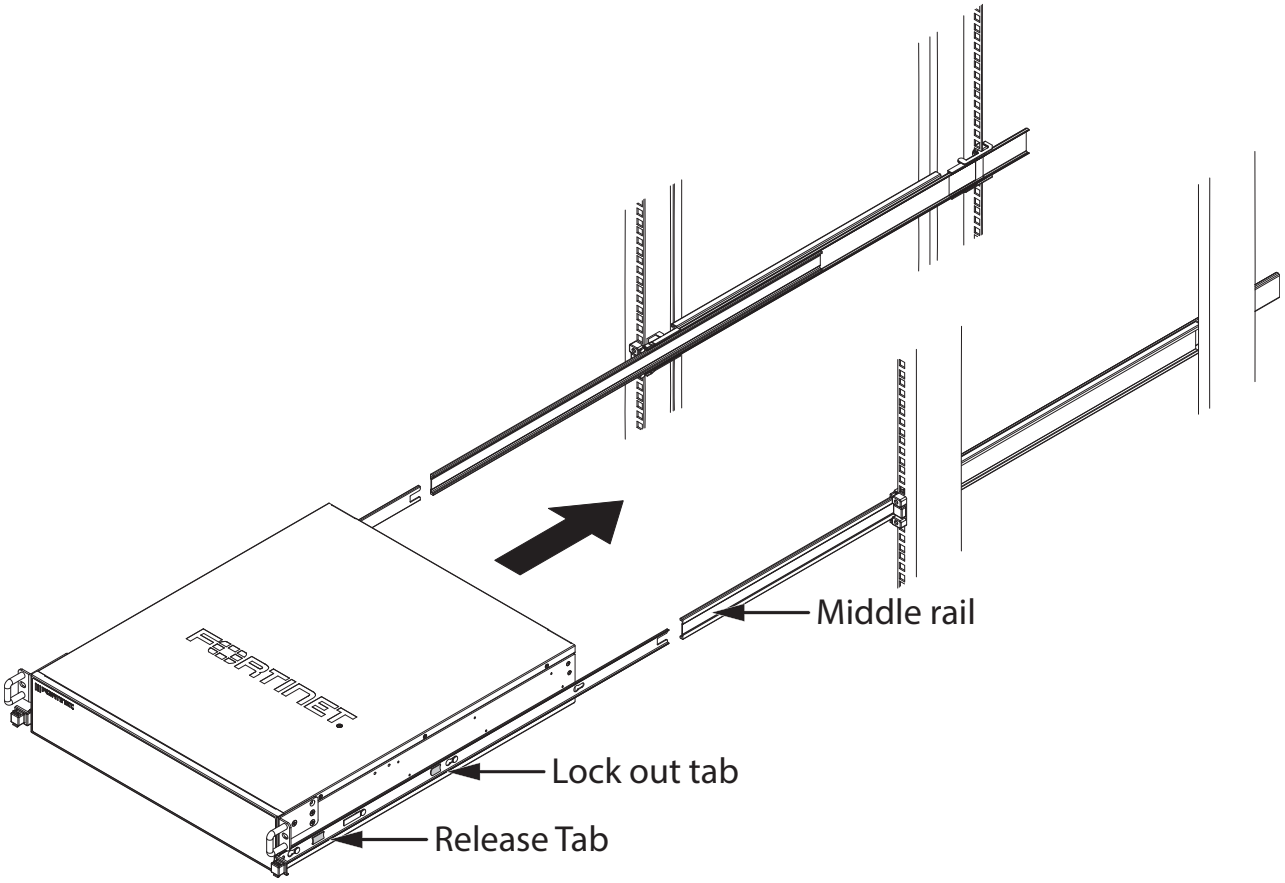


Sliding the FortiGate 6000F into the rack

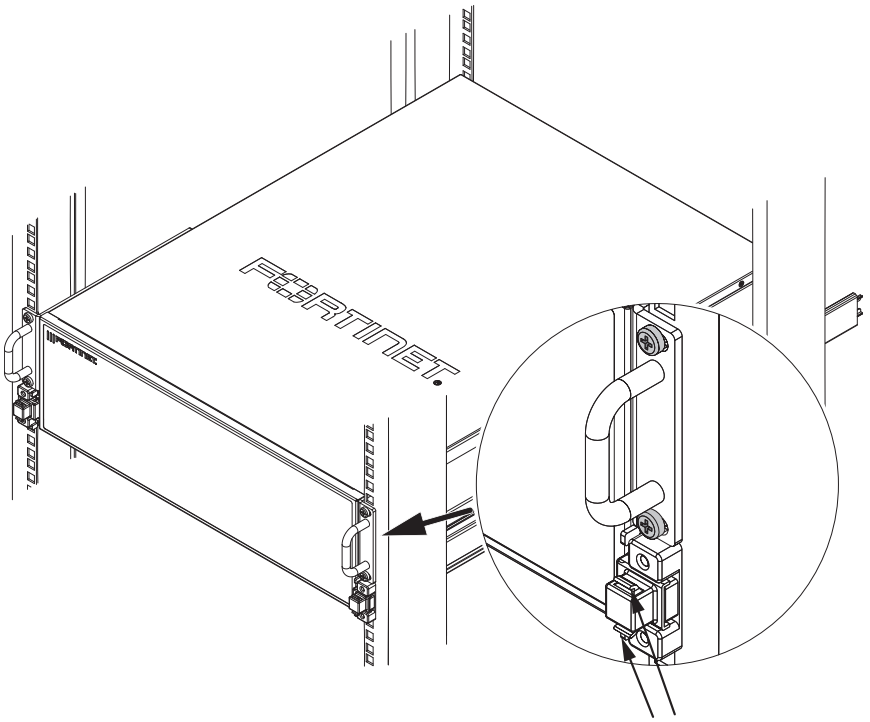
Now that the inner and outer rails are attached, you can slide the FortiGate 6000F into the rack by matching the inner rails with the outer rails.

1. Verify that the inner rail holes are properly connected to the FortiGate 6000F hooks and locked into place.
2. Verify that the outer rails are level, both at the same height, and securely attached to the rack.
3. Pull the middle rails out from the front of the outer rails until they lock into place.

4. Use a lifting device to raise the FortiGate 6000F to allow you to align the inner rails with the middle rails.



5. Slide the inner rails into the middle rails until the lock out tabs on the inner rails click into the front of the middle rails. Keep the rails aligned and apply even pressure to both sides of the FortiGate 6000F while doing this.
6. Slide the release tabs forward on both inner rails at the same time.
7. Push the FortiGate 6000F all the way into the rack until the system release buttons click into the locked position on the front of the rack.
8. Use a screw driver to install four rack screws into the handle brackets on the front of the FortiGate 6000F to secure it in the rack.



Removing the FortiGate 6000F from a four-post rack

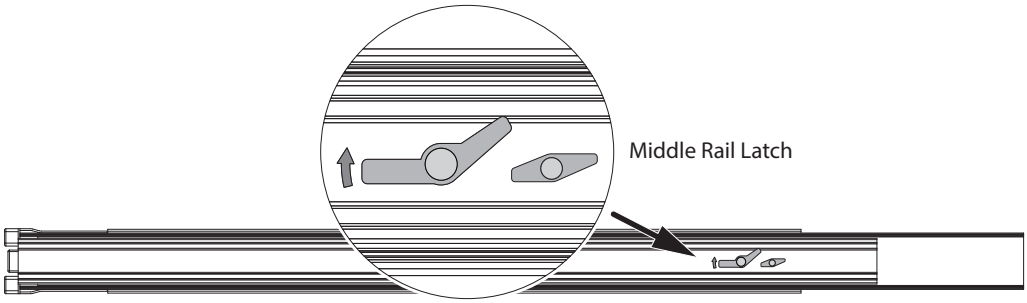
Make sure that a lifting device is available to slide the FortiGate 6000F on to when removing it from the rack. You will need a screwdriver to remove the four rack screws.

The rack must be stable before sliding the FortiGate 6000F out. Failure to stabilize the rack may cause it to tip over.

Do not pick up the FortiGate 6000F by the front handles. They are designed to pull the FortiGate 6000F from the rack on the rails.

1. Power down the FortiGate 6000F and remove all cables connected to it.
2. Remove the four rack screws to allow the FortiGate 6000F to slide out of the rack.
3. Squeeze the system release buttons on the front of both inner rails at the same time to release the FortiGate 6000F.
4. Use the front handles to pull the FortiGate 6000F out of the rack until the rails lock in their fully extended position.
5. Raise the lifting device under the FortiGate 6000F.
6. Slide the system lock out tabs forward on both inner rails, and slowly slide the FortiGate 6000F away from the rack and onto the lifting device.

   Apply even pressure to both sides of the FortiGate 6000F while doing this. As you slide the FortiGate 6000F out, the inner rails will slide out of the middle rails.
7. Push the middle rail latch counter clockwise, and slide the middle rails back into the outer rails.



8. Push the metal clip on each inner rail toward the front of the FortiGate 6000F to release the inner rails from the hooks on the side of the FortiGate 6000F and remove the inner rails.

Surface-mount installation

1. Make sure that the surface onto which the FortiGate 6000F is to be installed is clean, level, and stable and that there is at least 100 mm of front and back clearance to allow for adequate cooling air flow.
2. Attach the six provided rubber feet to the bottom of the FortiGate 6000F.
3. Place the FortiGate 6000F in the designated location.
4. Verify that the spacing around the FortiGate 6000F conforms to requirements and that the FortiGate 6000F is level.

Installing QSFP28, SFP28, SFP+, and SFP transceivers

You must install QSFP28 or QSFP+ transceivers into the 25 to 28 interfaces before connecting them to 100Gbps or 40Gbps networks.

You must install SFP28, SFP+, or SPF transceivers into the 1 to 24 interfaces before connecting them to 25Gbps, 10Gbps. or Gigabit networks.

You may need to manually change interface speeds as described in Interface groups and changing data interface speeds on page 9.

You must install the following types of SFP+ or SFP transceivers into the MGMT3, HA1, and HA2 interfaces before connecting them to 10Gbps or Gigabit networks.

- 10GBASE-SR SFP+ (10Gbps)
- 10GBASE-LR SFP+ (10Gbps)
- 1000BASE SFP (1Gbps)

The HA1 and HA2 interfaces are used for heartbeat, session sync, and management communication between two and only two FortiGate 6000Fs in HA mode. This communication requires SFP+ 10 Gbps connections. Using to SFP 1 Gbps connections is not recommended.

To install transceivers

To complete this procedure, you need:

- A FortiGate 6000F
- Transceivers to install
- An electrostatic discharge (ESD) preventive wrist strap with connection cord

FortiGate 6000Fs must be protected from static discharge and physical shock. Only handle or work with FortiGate 6000Fs at a static-free workstation. Always wear a grounded electrostatic discharge (ESD) preventive wrist strap when handling FortiGate 6000Fs.

Handling the transceivers by holding the release latch can damage the connector. Do not force transceivers into their cage slots. If the transceiver does not easily slide in and click into place, it may not be aligned correctly. If this happens, remove the transceiver, realign it and slide it in again.

1. Attach the ESD wrist strap to your wrist and to an available ESD socket or wrist strap terminal.
2. Remove the caps from the cage sockets on the FortiGate 6000F front panel.
3. Hold the sides of the transceiver and slide it into the cage socket until it clicks into place.

Getting started with FortiGate 6000F series

This section is a quick start guide to connecting and configuring a FortiGate 6000F for your network.

Before using this chapter, your FortiGate 6000F should be mounted and connected to your grounding and power system. In addition, your FortiGate 6000Fs should be powered up and the front and back panel LEDs should indicate normal operation.

When your FortiGate 6000F is operating normally, the front panel LEDs should appear as follows.

LED	State
Status	Green
Alarm	Off
HA	Off
Power	Green
Connected network interfaces	Solid or flashing green.

During normal operation, the back panel PSU and fan try LEDs should all be solid green. This indicates that each component has power and is operating normally.

Once the system has initialized, you have a few options for connecting to the FortiGate 6000F GUI or CLI:

- Log in to the management board GUI by connecting MGMT1 or MGMT2 to your network and browsing to https://192.168.1.99 or https://192.168.2.99.
- Log in to the management board CLI by connecting MGMT1 or MGMT2 to your network and using an SSH client to connect to 192.168.1.99 or 182.168.2.99.
- Log in to the management board CLI by connecting to the RJ-45 RS-232 CONSOLE port with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate 6000F ships with the following factory default configuration.

Option	Default Configuration
Administrator Account User Name	admin

Password	(none) For security reasons you should add a password to the admin account before connecting the FortiGate 6000F to your network.
	From the GUI, access the Global GUI and go to **System > Administrators**, edit the **admin** account, and select **Change Password**.
	From the CLI:
	`config global`
	`  config system admin`
	`  edit admin`
	`  set password <new-password>`
	`  end`

Option	Default Configuration
MGMT1 IP/Netmask	192.168.1.99/24
MGMT2 IP/Netmask	192.168.2.99/24

All configuration changes must be made from the management board GUI or CLI and not from individual FPCs.

All other management communication (for example, SNMP queries, remote logging, and so on) use the MGMT1 or MGMT2 interfaces and are handled by the management board.

Confirming startup status

Before verifying normal operation and making configuration changes and so on you should wait until the FortiGate 6000F is completely started up and synchronized. This can take a few minutes.

The FortiGate 6000F uses the Fortinet Security Fabric for communication and synchronization between the management board and the FPCs and for normal GUI operation. By default, the Security Fabric is enabled and must remain enabled for normal operation.

You can also view the **Sensor Information** dashboard widget to confirm that the system temperatures are normal and that all power supplies and fans are operating normally.

From the CLI you can use the `diagnose sys confsync status | grep in_sy` command to view the synchronization status of the management board and FPCs. If all of the FPCs are synchronized, each output line should include `in_sync=1`. If a line ends with `in_sync=0`, that FPC is not synchronized. The following example just shows a few output lines:

```
diagnose sys confsync status | grep in_sy
FPC6KF3E17900200, Secondary, uptime=5385.45, priority=119, slot_id=2:1, idx=2, flag=0x4, in_sync=1
F6KF313E17900031, Secondary, uptime=5484.74, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900032, Primary, uptime=5488.57, priority=1, slot_id=2:0, idx=1, flag=0x10, in_sync=1
FPC6KF3E17900201, Secondary, uptime=5388.78, priority=120, slot_id=2:2, idx=2, flag=0x4, in_sync=1
F6KF313E17900031, Secondary, uptime=5484.74, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
...
```

Default VDOM configuration and configuring the management interfaces

By default, when you first start up a FortiGate 6000F it is operating in Multi VDOM mode. The default Multi VDOM configuration includes the **root** VDOM and a management VDOM named **mgmt-vdom**. The mgmt1, mgmt2, mgmt3, ha1, and ha2 interfaces are in mgmt-vdom and all of the data interfaces are in the root VDOM.

You cannot delete or rename mgmt-vdom. You also cannot remove interfaces from it or add interfaces to it. You can however, configure other settings such as routing required for management communication, interface IP addresses, and so on. You can also add VLANs to the interfaces in mgmt-vdom and create a LAG that includes the mgmt1 and mgmt2 interfaces.

You can use the root VDOM for data traffic and you can also add more VDOMs for data traffic as required, depending on your Multi VDOM license.

Changing data interface network settings

To change the IP address of any FortiGate 6000F data interface:

- From the GUI access the Global GUI and go to **Network > Interfaces**. Edit any interface to change its IP address and other settings.
- From the CLI:

```
config system interface
   edit <interface-name>
   set ip <ip-address> <netmask>
end
```

Resetting to factory defaults

At any time during the configuration process, if you run into problems, you can reset the FortiGate 6000F to factory defaults and start over. From the primary FIM CLI enter:

```
config global
   execute factoryreset
```

Restarting the FortiGate 6000F

To restart the FortiGate 6000F, connect to the management board CLI and enter the `execute reboot` command. After you enter this command, the management board and all of the FPCs restart.

To restart an individual FPC, log in to the CLI of that FPC and run the `execute reboot` command.

Changing the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F log disk and RAID configuration

The FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F include two internal 1-TByte log disks. By default the disks are in a RAID-1 configuration. In the RAID-1 configuration you can use the disks for disk logging only. You can use the `execute disk raid` command to disable RAID and use one of the disks for disk logging and the other for other purposes such as disk caching. You can also change the RAID level to RAID-0. Changing the RAID configuration deletes all data from the disks and can disrupt disk logging so a best practice is set the RAID configuration when initially setting up the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F.

From the CLI you can use the following command to show disk status:

```
execute disk list
```

Use the following command to disable RAID:

```
execute disk raid disable
```

RAID is disabled, the disks are separated and formatted.

Use the following command to change the RAID level to RAID-0:

```
execute disk raid rebuild-level 0
```

The disks are formatted for RAID-0.

Use the following command to rebuild the current RAID partition:

```
execute disk raid rebuild
```

The RAID is rebuilt at the current RAID level.

Use the following command to show RAID status. The following command output shows the disks configured for RAID-1.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1: OK Used 953GB
Disk 2: OK Used 953GB
```

Managing individual FortiGate 6000F management boards and FPCs

You can manage individual FPCs using special management port numbers, FPC consoles, or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate 6000F in an HA configuration.

Special management port numbers

You may want to connect to individual FPCs to view status information or perform a maintenance task, such as installing firmware or performing a restart. You can connect to the GUI or CLI of individual FPCs (or the management board) using the MGMT1 interface IP address with a special port number.

You can use the `config load-balance setting slbc-mgmt-intf` command to change the management interface used. The default is `mgmt1` and it can be changed to `mgmt2`, or `mgmt3`.

To enable using the special management port numbers to connect to individual FPCs, set `slbc-mgmt-intf` to an interface that is connected to a network, has a valid IP address, and has management or administrative access enabled. To block access to the special management port numbers you can set `slbc-mgmt-intf` to an interface that is not connected to a network, does not have a valid IP address, or has management or administrative access disabled.

For example, if the MGMT1 interface IP address is 192.168.1.99 you can connect to the GUI of the first FPC (the FPC in slot 1) by browsing to :

`https://192.168.1.99:44301`

The special port number (in this case, 44301) is a combination of the service port (for HTTPS, the service port is 443) and the FPC slot number (in this example, 01).

You can view the special HTTPS management port number for and log in to the GUI of an FPC from the Configuration Sync Monitor.

The following table lists the special ports you can use to connect to individual FPCs or the management board using common management protocols. The FortiGate 6300F and 6301F have 7 slots (0 to 6) and the FortiGate 6500F and 6501F have 11 slots (0 to 10). Slot 0 is the management board (MBD) slot. Slots 1 to 10 are FPC slots.

You can't change the special management port numbers. Changing configurable management port numbers, for example the HTTPS management port number (which you might change to support SSL VPN), does not affect the special management port numbers.

FortiGate 6000F special management port numbers

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8000	44300	2300	2200	16100
Slot 1 (FPC01)	8001	44301	2301	2201	16101
Slot 2 (FPC02)	8002	44302	2302	2202	16102
Slot 3 (FPC03)	8003	44303	2303	2203	16103
Slot 4 (FPC04)	8004	44304	2304	2204	16104
Slot 5 (FPC05)	8005	44305	2305	2205	16105
Slot 6 (FPC06)	8006	44306	2306	2206	16106
Slot 7 (FPC07)	8007	44307	2307	2207	16107
Slot 8 (FPC08)	8008	44308	2308	2208	16108
Slot 9 (FPC09)	8009	44309	2309	2209	16109
Slot 10 (FPC10)	8010	44310	2310	2210	16110

For example, to connect to the CLI of the FPC in slot 3 using SSH, you would connect to ssh://192.168.1.99:2203.

To verify which slot you have logged into, the GUI header banner and the CLI prompt shows the current hostname. The System Information dashboard widget also shows the host name and serial number. The CLI prompt also shows slot address in the format `<hostname> [<slot address>] #`.

Logging in to different FPCs allows you to use the FortiView or Monitor GUI pages to view the activity on that FPC. You can also restart the FPC from its GUI or CLI. Even though you can log in to different FPCs, you can only make configuration changes from the management board.

HA mode special management port numbers

In an HA configuration consisting of two FortiGate 6000Fs in an HA cluster, you can connect to individual FPCs or to the management board in chassis 1 (chassis ID = 1) using the same special port numbers as for a standalone FortiGate 6000F.

You use different special port numbers to connect to individual FPCs or the management board in the FortiGate 6000F with chassis ID 2 (chassis ID = 2).

FortiGate 6000F special management port numbers (chassis ID = 2)

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8020	44320	2320	2220	16120
Slot 1 (FPC01)	8021	44321	2321	2221	16121
Slot 2 (FPC02)	8022	44322	2322	2222	16122

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 3 (FPC03)	8023	44323	2323	2223	16123
Slot 4 (FPC04)	8024	44324	2324	2224	16124
Slot 5 (FPC05)	8025	44325	2325	2225	16125
Slot 6 (FPC06)	8026	44326	2326	2226	16126
Slot 7 (FPC07)	8027	44327	2327	2227	16127
Slot 8 (FPC08)	8028	44328	2328	2228	16128
Slot 9 (FPC09)	8029	44329	2329	2229	16129
Slot 10 (FPC10)	8030	44330	2330	2230	16130

Connecting to individual FPC consoles

From the management board CLI, you can use the `execute system console-server` command to access individual FPC consoles. Console access can be useful for troubleshooting. For example, if an FPC does not boot properly, you can use console access to view the state of the FPC and enter commands to fix the problem or restart the FPC.

From the console, you can also perform BIOS-related operations, such as rebooting the FPC, interrupting the boot process, and installing new firmware.

For example, from the management board CLI, use the following command to log in to the console of the FPC in slot 3:

```
execute system console-server connect 3
```

Authenticate to log in to the console and use CLI commands to view information, make changes, or restart the FPC. When you are done, use **Ctrl-X** to exit from the console back to the management board CLI. Using **Ctrl-X** may not work if you are accessing the CLI console from the GUI. Instead you may need to log out of the GUI and then log in again.

Also, from the management board CLI you can use the `execute system console-server showline` command to list any active console server sessions. Only one console session can be active for each FPC, so before you connect to an FPC console, you can use the following command to verify whether or not there is an active console session. The following command output shows an active console session with the FPC in slot 4:

```
execute system console-server showline
MB console line connected - 1
Telnet-to-console line connected - 4
```

To clear an active console session, use the `execute system console-server clearline` command. For example, to clear an active console session with the FPC in slot 4, enter:

```
execute system console-server clearline 4
```

In an HA configuration, the `execute system console-server` commands only allow access to FPCs in the FortiGate 6000F that you are logged into. You can't use this command to access FPCs in the other FortiGate 6000F in an HA cluster

Connecting to individual FPC CLIs

From the management board CLI you can use the following command to log into the CLI of individual FPCs:

```
execute load-balance slot manage <slot-number>
```

Where:

<slot> is the slot number of the component that you want to log in to. The management board is in slot 0 and the FPC slot numbers start at 1.

When connected to the CLI of a FPC, you can view information about the status or configuration of the FPC, restart the FPC, or perform other operations. You should not change the configuration of individual FPCs because this can cause configuration synchronization errors.

Performing other operations on individual FPCs

You can use the following commands to restart, power off, power on, or perform an NMI reset on individual FPCs while logged into the management board CLI:

```
execute load-balance slot {nmi-reset | power-off | power on | reboot | set-primary-worker}
     <slots>
```

Where <slots> can be one or more slot numbers or slot number ranges separated by commas. Do not include spaces.

For example, to shut down the FPCs in slots 2, and 4 to 6 enter:

```
execute load-balance slot power-off 2,4-6
```

Firmware upgrades

In addition to introducing the basics of upgrading FortiGate 6000F firmware, this section describes how to:

- Upgrade the firmware running on individual FPCs.
- Upgrade the management board firmware from the BIOS and reset the configuration of all of the FPCs.

Firmware upgrade basics

The management board and the FPCs in your FortiGate 6000F system run the same firmware image. You upgrade the firmware from the management board GUI or CLI just as you would any FortiGate product.

You can perform a graceful firmware upgrade of an FGCP cluster by setting `upgrade-mode` to `uninterruptible` and enabling `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Upgrading the firmware of a standalone FortiGate 6000F, or FortiGate 6000F HA cluster with `upgrade-mode` set to `simultaneous` interrupts traffic because the firmware running on the management board and all of the FPCs upgrades in one step. These firmware upgrades should be done during a quiet time because traffic will be interrupted during the upgrade process.

A firmware upgrade takes a few minutes, depending on the number of FPCs in your FortiGate 6000F system. Some firmware upgrades may take longer depending on factors such as the size of the configuration and whether an upgrade of the DP3 processor is included.

Before beginning a firmware upgrade, Fortinet recommends that you perform the following tasks:

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path, as documented in the release notes.
- Back up your FortiGate 6000F configuration.

To make sure a FortiGate 6000F firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the management board and the FPCs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the following Fortinet community article:

Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Fortinet recommends that you review the services provided by your FortiGate 6000F before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

Installing firmware on an individual FPC

You may want to install firmware on an individual FPC to resolve a software-related problem with the FPC or if the FPC is not running the same firmware version as the management board. The following procedure describes how to transfer a new firmware image file to the FortiGate 6000F internal TFTP server and then install the firmware on an FPC.

1. Copy the firmware image file to a TFTP server, FTP server, or USB key.
2. To upload the firmware image file onto the FortiGate 6000F internal TFTP server, from the management board CLI, enter one of the following commands.
   - To upload the firmware image file from an FTP server:
     ```
     execute upload image ftp <image-file-and-path> <comment> <ftp-server-address>
          <username> <password>
     ```
   - To upload the firmware image file from a TFTP server:
     ```
     execute upload image tftp <image-file> <comment> <tftp-server-address>
     ```
   - To upload the firmware image file from a USB key:
     ```
     execute upload image usb <image-file-and-path> <comment>
     ```
3. Enter the following command to install the firmware image file on to an FPC:
   ```
   execute load-balance update image <slot-number>
   ```
   where `<slot-number>` is the FPC slot number.

   This command uploads the firmware image to the FPC and the FPC restarts. When the FPC starts up, the configuration is reset to factory default settings and then synchronized by the management board. The FPC restarts again, rejoins the cluster, and is ready to process traffic.
4. To verify that the configuration of the FPC has been synchronized, enter the `diagnose sys confsync status | grep in_sy` command. The command output below shows an example of the synchronization status of some of the FPCs in an HA cluster of two FortiGate 6301F devices. The field `in_sync=1` indicates that the configuration of the FPC is synchronized.

   ```
   FPC6KFT018901327, Secondary, uptime=615368.33, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
   FPC6KFT018901372, Secondary, uptime=615319.63, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
   FPC6KFT018901346, Secondary, uptime=423.91, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=1
   ```

   FPCs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FPC that is not synchronized, log into the CLI of the FPC and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support at https://support.fortinet.com.

The example output also shows that the uptime of the FPC in slot 3 is lower than the uptime of the other FPCs, indicating that the FPC in slot 3 has recently restarted.

If you enter the `diagnose sys confsync status | grep in_sy` command before an FPC has completely restarted, it will not appear in the output. Also, the Configuration Sync Monitor will temporarily show that it is not synchronized.

Installing firmware from the BIOS after a reboot

A common method for resetting the configuration of a FortiGate involves installing firmware by restarting the FortiGate, interrupting the boot process, and using BIOS prompts to download a firmware image from a TFTP server. This process is also considered the best way to reset the configuration of your FortiGate.

Installing or upgrading FortiGate 6000F firmware from the BIOS after a reboot installs firmware on and resets the configuration of the management board only. FPCs will continue to operate with their current configuration and firmware build. The FortiGate-6000 system does not synchronize firmware upgrades that are performed from the BIOS. After you install firmware on the management board from the BIOS after a reboot, you must synchronize the new firmware build and configuration to the FPCs.

Installing or upgrading FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F firmware from the BIOS after a reboot disables the log disk RAID configuration. You must rebuild the RAID configuration for normal log disk operation. If the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F is part of an FGCP HA cluster, both FortiGates in the cluster must have the same log disk RAID configuration. See Changing the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F log disk and RAID configuration on page 37.

Use the following steps to upload firmware from a TFTP server to the management board. This procedure involves creating a connection between the TFTP server and one of the MGMT interfaces.

This procedure also involves connecting to the management board CLI using the FortiGate 6000F console port, rebooting the management board, interrupting the boot from the console session, and following BIOS prompts to install the firmware. During this procedure, the FortiGate 6000F will not be able to process traffic.

1. Set up a TFTP server and copy the firmware file to the TFTP server default folder.
2. Set up your network to allow traffic between the TFTP server and one of the management interfaces, (for example, MGMT1).
3. Using the console cable supplied with your FortiGate 6000F, connect the console port on the FortiGate to a USB port on your management computer.
4. Start a terminal emulation program on the management computer. Use these settings:
   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
5. Log in to the management board CLI.
6. To restart the management board, enter the `execute reboot` command.
7. When the management board starts up, follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
8. To set up the TFTP configuration, press C.
9. Use the BIOS menu to set the following.Change settings only if required.

   `[P]: Set image download port`: MGMT1 (the connected MGMT interface)

   `[D]: Set DHCP mode`: Disabled

`[I]: Set local IP address`: The IP address of the MGMT interface that you want to use to connect to the TFTP server. This address can be the same as the FortiGate 6000F management IP address and cannot conflict with other addresses on your network.

`[S]: Set local Subnet Mask`: Set as required for your network.

`[G]: Set local gateway`: Set as required for your network.

`[V]: Local VLAN ID`: Should be set to `<none>`. (use -1 to set the Local VLAN ID to `<none>`.)

`[T]: Set remote TFTP server IP address`: The IP address of the TFTP server.

`[F]: Set firmware image file name`: The name of the firmware image file that you want to install.

10. To quit this menu, press Q.
11. To review the configuration, press R.
    To make corrections, press C and make the changes as required. When the configuration is correct, proceed to the next step.
12. To start the TFTP transfer, press T.
    The management board downloads the firmware image from the TFTP server and installs it on the management board. The management board then restarts with its configuration reset to factory defaults.
13. Once the management board restarts, verify that the correct firmware is installed.
    You can do this from the management board GUI dashboard or from the CLI using the `get system status` command.

If you are installing firmware on a FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F, the log disk RAID configuration will be disabled once the management board restarts. You must rebuild the RAID configuration for normal log disk operation. If the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F is part of an FGCP HA cluster, both FortiGates in the cluster must have the same log disk RAID configuration. See Changing the FortiGate 6001F, FortiGate 6501F, or FortiGate 6301F log disk and RAID configuration on page 37.

14. Continue by Synchronizing the FPCs with the management board on page 46.

Synchronizing the FPCs with the management board

After you install firmware on the management board from the BIOS after a reboot, the firmware version and configuration of the management board will most likely not be synchronized with the FPCs. You can verify this from the management board CLI using the `diagnose sys confsync status | grep in_sy` command. The `in_sync=0` entries in the following example output for a FortiGate 6301F show that the management board (serial number ending in 143) is not synchronized with the FPCs.

```
diagnose sys confsync status | grep in_sy
FPC6KFT018901327, Secondary, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901372, Secondary, uptime=58.48, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901346, Secondary, uptime=58.44, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901574, Secondary, uptime=58.43, priority=22, slot_id=1:4, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901345, Secondary, uptime=57.40, priority=23, slot_id=1:5, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901556, Secondary, uptime=58.43, priority=24, slot_id=1:6, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
```

```
F6KF31T018900143, Primary, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901327, Secondary, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
FPC6KFT018901345, Secondary, uptime=57.40, priority=23, slot_id=1:5, idx=2, flag=0x4, in_sync=0
FPC6KFT018901346, Secondary, uptime=58.44, priority=21, slot_id=1:3, idx=3, flag=0x4, in_sync=0
FPC6KFT018901372, Secondary, uptime=58.48, priority=20, slot_id=1:2, idx=4, flag=0x4, in_sync=0
FPC6KFT018901556, Secondary, uptime=58.43, priority=24, slot_id=1:6, idx=5, flag=0x4, in_sync=0
FPC6KFT018901574, Secondary, uptime=58.43, priority=22, slot_id=1:4, idx=6, flag=0x4, in_sync=0
```

You can also verify the synchronization status from the management board Configuration Sync Monitor.

To re-synchronize the FortiGate 6000F, which has the effect of resetting all of the FPCs, re-install firmware on the management board.

You can also manually install firmware on each FPC from the BIOS after a reboot. This multi-step manual process is just as effective as installing the firmware for a second time on the management board to trigger synchronization to the FPCs, but takes much longer.

1. Log in to the management board GUI.
2. Install a firmware build on the management board from the GUI or CLI. The firmware build you install on the management board can either be the same firmware build or a different one.

   Installing firmware synchronizes the firmware build and configuration from the management board to the FPCs.
3. Check the synchronization status from the Configuration Sync Monitor or using the `diagnose sys confsync status | grep in_sy` command. The following example FortiGate 6301F output shows that the management board is synchronized with all of the FPCs because each line includes `in_sync=1`.

   ```
   diagnose sys confsync status | grep in_sy
   FPC6KFT018901327, Secondary, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901372, Secondary, uptime=3774.26, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901346, Secondary, uptime=3774.68, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901574, Secondary, uptime=3774.19, priority=22, slot_id=1:4, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901345, Secondary, uptime=3773.59, priority=23, slot_id=1:5, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901556, Secondary, uptime=3774.82, priority=24, slot_id=1:6, idx=1, flag=0x4, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   F6KF31T018900143, Primary, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
   FPC6KFT018901327, Secondary, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x24, in_sync=1
   FPC6KFT018901345, Secondary, uptime=3773.59, priority=23, slot_id=1:5, idx=2, flag=0x24, in_sync=1
   FPC6KFT018901346, Secondary, uptime=3774.68, priority=21, slot_id=1:3, idx=3, flag=0x24, in_sync=1
   FPC6KFT018901372, Secondary, uptime=3774.26, priority=20, slot_id=1:2, idx=4, flag=0x24, in_sync=1
   FPC6KFT018901556, Secondary, uptime=3774.82, priority=24, slot_id=1:6, idx=5, flag=0x24, in_sync=1
   FPC6KFT018901574, Secondary, uptime=3774.19, priority=22, slot_id=1:4, idx=6, flag=0x24, in_sync=1
   ```

Cautions and warnings

Environmental specifications

Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

Instructions de montage en rack - Les instructions de montage en rack suivantes ou similaires sont incluses avec les instructions d'installation:

Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Température ambiante élevée - S'il est installé dans un rack fermé ou à unités multiples, la température ambiante de fonctionnement de l'environnement du rack peut être supérieure à la température ambiante de la pièce. Par conséquent, il est important d'installer le matériel dans un environnement respectant la température ambiante maximale (Tma) stipulée par le fabricant.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Ventilation réduite - Installation de l'équipement dans un rack doit être telle que la quantité de flux d'air nécessaire au bon fonctionnement de l'équipement n'est pas compromise.

Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Chargement Mécanique - Montage de l'équipement dans le rack doit être telle qu'une situation dangereuse n'est pas lié à un chargement mécanique inégal.

Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Surtension - Il convient de prendre l'ensemble des précautions nécessaires lors du branchement de l'équipement au circuit d'alimentation et être particulièrement attentif aux effets de la suralimentation sur le dispositif assurant une protection contre les courts-circuits et le câblage. Ainsi, il est recommandé de tenir compte du numéro d'identification de l'équipement.

Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Fiabilité de la mise à la terre - Fiabilité de la mise à la terre de l'équipement monté en rack doit être maintenue. Une attention particulière devrait être accordée aux connexions d'alimentation autres que les connexions directes au circuit de dérivation (par exemple de l'utilisation de bandes de puissance).

Blade Carriers, Cards and Modems must be Listed Accessories or Switch, Processor, Carrier and similar blades or cards should be UL Listed or Equivalent.

Serveur-blades, cartes et modems doivent être des accessoires listés ou commutateurs, processeurs, serveurs et similaire blades ou cartes doivent être listé UL ou équivalent.

Refer to specific Product Model Data Sheet for Environmental Specifications (Operating Temperature, Storage Temperature, Humidity, and Altitude).

Référez à la Fiche Technique de ce produit pour les caractéristiques environnementales (Température de fonctionnement, température de stockage, humidité et l'altitude).

Safety

Moving parts - Hazardous moving parts. Keep away from moving fan blades.

Pièces mobiles - Pièces mobiles dangereuses. Se tenir éloigné des lames mobiles du ventilateur.

Warning: Equipment intended for installation in Restricted Access Location.

Avertissement: Le matériel est conçu pour être installé dans un endroit où l'accès est restreint.

Warning: A readily accessible disconnect device shall be incorporated in the building installation wiring.

Avertissement: Un dispositif de déconnexion facilement accessible doit être incorporé dans l'installation électrique du bâtiment.

Battery - Risk of explosion if the battery is replaced by an incorrect type. Do not dispose of batteries in a fire. They may explode. Dispose of used batteries according to your local regulations. IMPORTANT: Switzerland: Annex 4.10 of SR814.013 applies to batteries.

Batterie - Risque d'explosion si la batterie est remplacée par un type incorrect. Ne jetez pas les batteries au feu. Ils peuvent exploser. Jetez les piles usagées conformément aux réglementations locales. IMPORTANT: Suisse: l'annexe 4.10 de SR814.013 s'appliquent aux batteries.

警告

本電池如果更換不正確會有爆炸的危險

請依製造商說明書處理用過之電池

CAUTION:

There is a danger of explosion if a battery is incorrect replaced. Replace only with the same or equivalent type. Dispose batteries of according to the manufacturer's instructions. Disposing a battery into fire, a hot oven, mechanically crushing, or cutting it can result in an explosion. Leaving a battery in an extremely hot environment can result in leakage of flammable liquid, gas, or an explosion. If a battery is subjected to extremely low air pressure, it may result in leakage of flammable liquid, gas, or an explosion.

WARNUNG:

Lithium-Batterie Achtung: Explosionsgefahr bei fehlerhafter Batteriewechsel. Ersetzen Sie nur den gleichen oder gleichwertigen Typ. Batterien gemäß den Anweisungen des Herstellers entsorgen.

Beseitigung einer BATTERIE in Feuer oder einen heißen Ofen oder mechanisches Zerkleinern oder Schneiden einer BATTERIE, die zu einer EXPLOSION führen kann.

Verlassen einer BATTERIE in einer extrem hohen Umgebungstemperatur, die zu einer EXPLOSION oder zum Austreten von brennbarer Flüssigkeit oder Gas führen kann.

Eine BATTERIE, die einem extrem niedrigen Luftdruck ausgesetzt ist, der zu einer EXPLOSION oder zum Austreten von brennbarer Flüssigkeit oder Gas führen kann.

CAUTION: Shock Hazard. Disconnect all power sources.

ATTENTION: Risque d'électrocution. Débranchez toutes les sources d'alimentation.

Grounding - To prevent damage to your equipment, connections that enter from outside the building should pass through a lightning / surge protector, and be properly grounded. Use an electrostatic discharge workstation (ESD) and/or wear an anti-static wrist strap while you work. In addition to the grounding terminal of the plug, on the back panel, there is another, separate terminal for earthing.

Mise à la terre - Pour éviter d'endommager votre matériel, assurez-vous que les branchements qui entrent à partir de l'extérieur du bâtiment passent par un parafoudre / parasurtenseur et sont correctement mis à la terre. Utilisez un poste de travail de décharge électrostatique (ESD) et / ou portez un bracelet anti-statique lorsque vous travaillez. Ce produit possède une borne de mise à la terre qui est prévu à l'arrière du produit, à ceci s'ajoute la mise à la terre de la prise.

This product has a separate protective earthing terminal provided on the back of the product in addition to the grounding terminal of the attachment plug. This separate protective earthing terminal must be permanently connected to earth with a green with yellow stripe conductor minimum size # 6 AWG and the connection is to be installed by a qualified service personnel.

Ce produit a une borne de mise à la terre séparé sur le dos de l'appareil, en plus de la borne de mise à la terre de la fiche de raccordement. Cette borne de mise à la terre séparée doit être connecté en permanence à la terre avec un conducteur vert avec la taille bande jaune de minimum # 6 AWG et la connexion doit être installé par un personnel qualifié.

Caution: Slide/rail mounted equipment is not to be used as a shelf or a work space.

Attention: Un équipement monté sur bâti ne doit pas être utilisé sur une étagère ou dans un espace de travail.

Fiber optic transceiver must be rated 3.3V, 22mA max, Laser Class 1, UL certified component.

Le transceiver optique doit avoir les valeurs nominales de 3.3 V, maximum 22 mA, Laser Class 1, homologué UL

Regulatory notices

Federal Communication Commission (FCC) – USA

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received; including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

WARNING: Any changes or modifications to this product not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Equipment Standard for Digital Equipment (ICES) – Canada

CAN ICES-003 (A) / NMB-003 (A)

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Cet appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicte par le ministère des Communications du Canada.

European Conformity (CE) - EU

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Voluntary Control Council for Interference (VCCI) – Japan

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Product Safety Electrical Appliance & Material (PSE) – Japan

日本では電気用品安全法(PSE)の規定により、同梱している電源コードは本製品の専用電源コードとして利用し、他の製品に使用しないでください。

Bureau of Standards Metrology and Inspection (BSMI) – Taiwan

The presence conditions of the restricted substance (BSMI RoHS table) are available at the link below:

限用物質含有情況表 (RoHS Table) 請到以下 網址下載:

https://www.fortinet.com/bsmi

警告: 為避免電磁干擾, 本產品不應安裝或使用於住宅環境。

英屬蓋曼群島商防特網股份有限公司台灣分公司

地址:台北市內湖區行愛路176號2樓

電話:(02) 27961666

China

警告:在居住环境中, 运行此设备可能会造成无线电干扰。

Agência Nacional de Telecomunicações (ANATEL) – Brazil

Este produto não é apropriado para uso em ambientes domésticos, pois poderá causar interferências eletromagnéticas que obrigam o usuário a tomar medidas necessárias para minimizar estas interferências.”

Para maiores informações, consulte o site da ANATEL www.anatel.gov.br.

Korea Certification (KC) – Korea

A급 기기 (업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기를 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.