FortiGate-7121F System Guide

FortiGate-7000F 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

November 8, 2023
FortiGate-7121F 7.0.13 System Guide
01-7013-669640-20231108

TABLE OF CONTENTS

Change log

Date	Change description
November 11, 2023	Added information about FortiGate 7121F hardware generation 1 and generation 2 see: • FortiGate 7121F series hardware generations on page 17. • FortiGate 7121F front panel on page 8. • Shipping components on page 15. • Optional accessories and replacement parts on page 16. • Physical description of the FortiGate 7121F chassis on page 16. • Power consumption for different FIM-7941F FortiGate 7121F configurations on page 20. • Power consumption for different FIM-7921F FortiGate 7121F configurations on page 22. • AC PSUs and supplying AC power to the chassis on page 23. • DC PSUs and supplying DC power to the chassis on page 25. • Crimping guidelines on page 27. • Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F on page 29. • Safety on page 73.
September 25, 2023	Corrections to the appearance of the FPM-7620F front panel.
November 2, 2022	Corrected the rating of the circuit breaker listed in DC PSUs and supplying DC power to the chassis on page 25. Added cable lengths to Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F on page 29.
October 3, 2022	Changes to Regulatory notices on page 75.
June 1, 2022	Page count fix and chassis label correction.
May 4, 2022	Added more information to Connecting the FortiGate 7121F chassis to ground on page 33. Added a missing item to the list in Shipping components on page 15.
April 19, 2022	New FIM-7941F content: • FIM-7941F interface module on page 10. • Power consumption for different FIM-7941F FortiGate 7121F configurations on page 20.
February 23, 2022	New DC content: • DC PSUs and supplying DC power to the chassis on page 25. • Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F on page 29.
October 7, 2021	Corrections to Shipping components on page 15. New section Installing AC PSUs on page 25.
August 4, 2021	New regulatory notice added to Regulatory notices on page 75.

Date	Change description
June 10, 2021	Changes to: • Installing firmware on individual FIMs or FPMs on page 52. • Upgrading the firmware on an individual FIM on page 53. • Upgrading the firmware on an individual FPM on page 54.
April 8, 2021	Removed information about the FPM-7620F console port, which is not supported.
March 30, 2021	Initial release.

FortiGate 7121F chassis

The FortiGate 7121F is a 16U 19-inch rackmount 12-slot chassis with a 1Tbps fabric backplane and 50Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication among chassis slots and the base backplane provides management and synchronization communication among the chassis slots.

FortiGate 7121F front panel

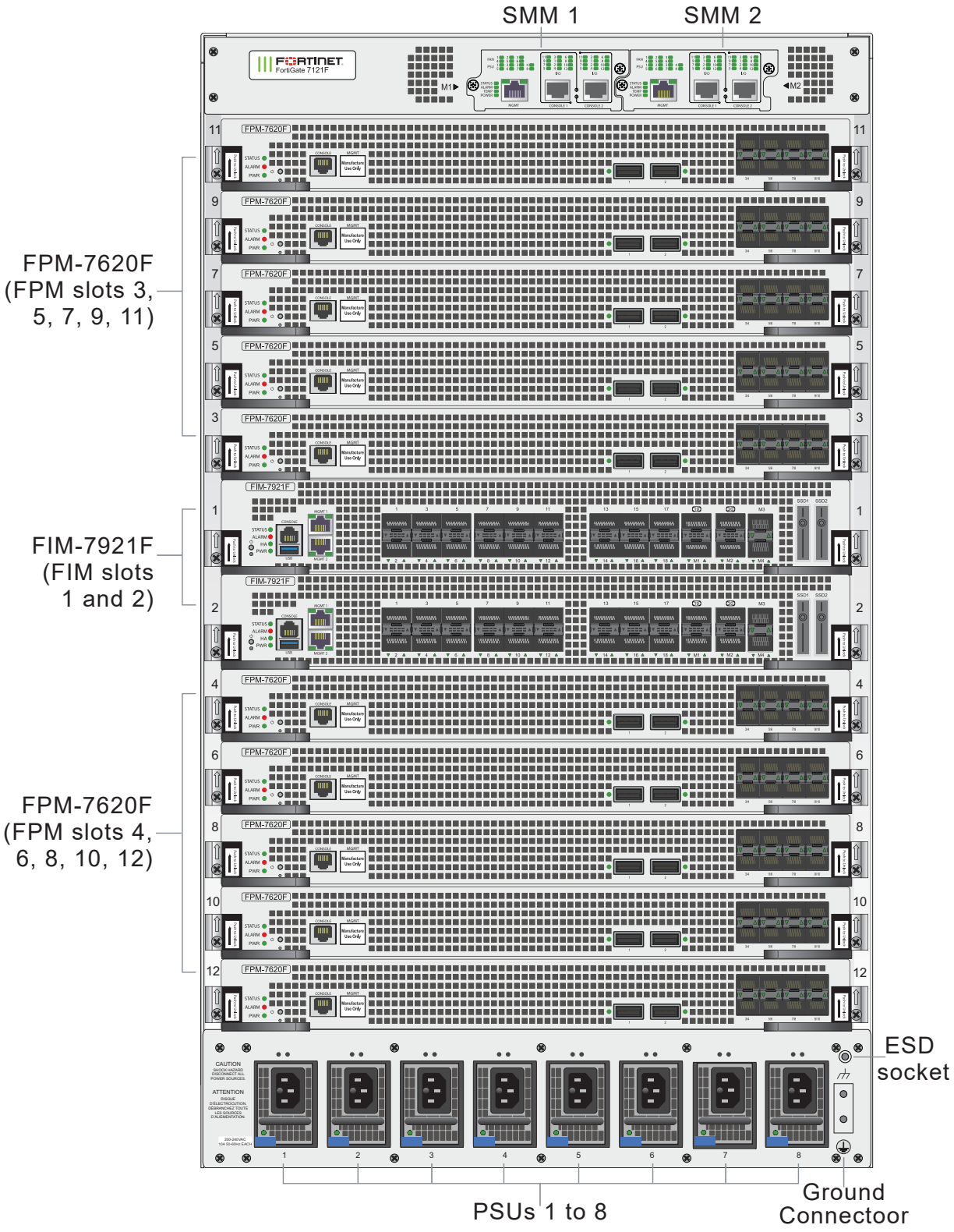
The FortiGate 7121F chassis is managed by two redundant System Management Modules (SMMs 1 and 2). Each SMM includes an ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. Chassis modules include two Fortinet Interface Modules (FIMs) in slots 1 and 2 and up to ten Fortinet Processor Modules (FPMs) in slots 3 to 12. The active SMM controls chassis cooling and power management and provides an interface for managing the FIMs and FPMs in the chassis.

Do not operate the FortiGate 7121F chassis with open slots on the front or back panel. For optimum cooling performance and safety, chassis front panel slots 1 and 2 must contain FIMs or FIM blank panels (also called dummy cards). Front panel slots 3 to 12 must contain FPMs or FPM blank panels. In addition, all cooling fan trays, power supplies or power supply slot covers must be installed while the chassis is operating. The FPM blank panels shipped with the chassis should be kept available in case an FPM is removed from the chassis. If an FIM or FPM fails and you don't have a replacement FIM or FPM or an available blank panel, you should keep the failed FIM or FPM in the chassis slot until you receive a replacement.

Power is provided to a generation 1 FortiGate 7121F chassis using eight hot swappable 200-240 VAC, 50-60 Hz 2000W AC or -48Vdc to -60Vdc 2000W power supply units (PSUs).

Power is provided to a generation 2 FortiGate 7121F chassis using eight hot swappable 200-240 VAC, 50-60 Hz 2500W AC or -48Vdc to -60Vdc 2500W power supply units (PSUs).

FortiGate 7121F generation 1 front panel, (showing AC PSUs, example module configuration)



FIM-7941F interface module

The FIM-7941F interface module is a hot swappable module that provides data, management, and session sync/heartbeat interfaces, base backplane switching, hardware acceleration, and fabric backplane session-aware load balancing for a FortiGate 7000F series chassis. The FIM-7941F includes an integrated switch fabric, five NP7 processors to load balance millions of data sessions over the FortiGate 7000F 400Gbps fabric backplane channel to FPM processor modules. The FIM-7941F also includes a 50Gbps base backplane channel for base backplane management communication with each FPM in the chassis, one 1Tbps fabric backplane channel for fabric backplane communication with the other FIM in the chassis, and a second 50Gbps base backplane channel for base backplane communication with the other FIM in the chassis. The FIM-7941F also includes two 4TByte SSD log disks in a RAID-1 configuration. The SSDs are accessible from the FIM-7941F front panel but should not be removed.

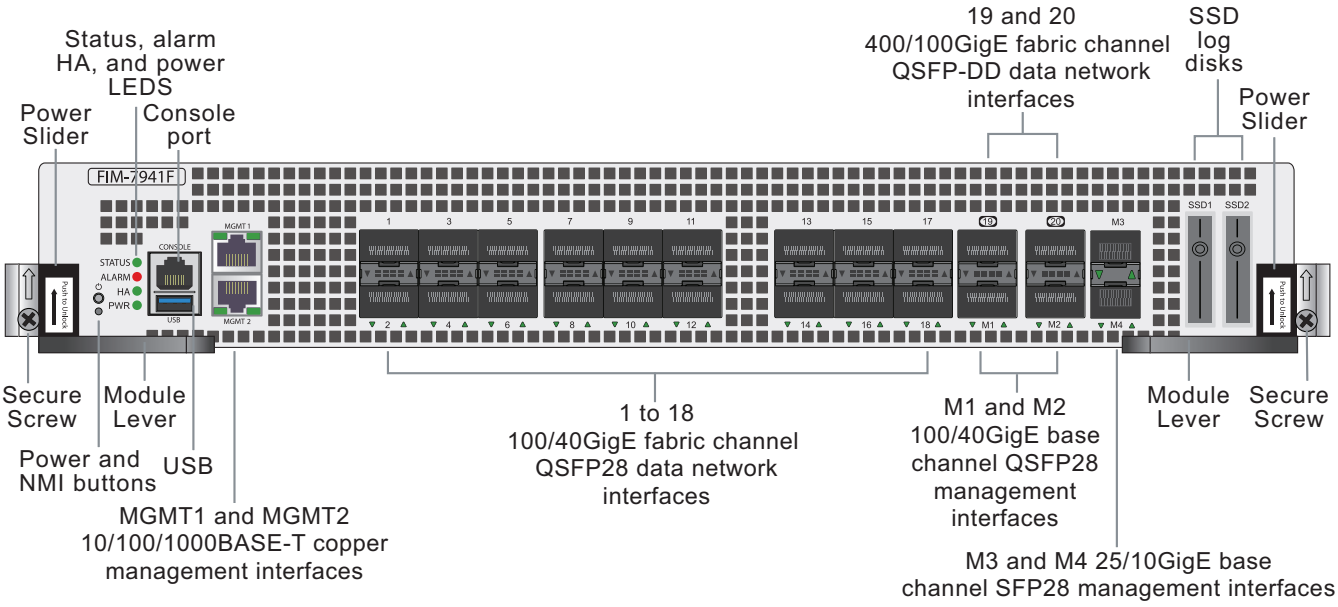
The FIM-7941F interface module is an update of the FIM-7921F interface module with the same architecture but a newer switch fabric that has a greater capacity and supports more advanced features. You cannot include a FIM-7941F and FIM-7921F in the same chassis. In an HA configuration, both chassis in the HA cluster must have the same FIMs.

The FIM-7941F can be installed in any FortiGate 7000F series chassis in chassis hub/switch slots 1 or 2. The FIM-7941F includes eighteen front panel 100GigE QSFP28 fabric channel data network interfaces (1 to 18) and two 400GigE QSFP-DD fabric channel data network interfaces (19 and 20). Interfaces 1 to 18 can be connected to 100Gbps data networks. Interfaces 19 and 20 can be connected to 400Gbps data networks. You can also change the interface type of interfaces 19 and 20 and change the speeds of all of the data interfaces. You can split interfaces 1 to 20, M1, and M2.

The FIM-7941F also includes two 100 GigE QSFP28 base channel management interfaces (M1 and M2) and two 25 GigE SPF28 base channel management interfaces (M3 and M4). The management interfaces can be used for HA heartbeat communication and session synchronization between two chassis in HA mode or for other management functions such as remote logging. You can also change the speeds of the management interfaces. You can also split the M1 and M2 interfaces.

The FIM-7941F includes a console port to provide console access to the FIM-7941F CLI.

FIM-7941F front panel



FIM-7921F interface module

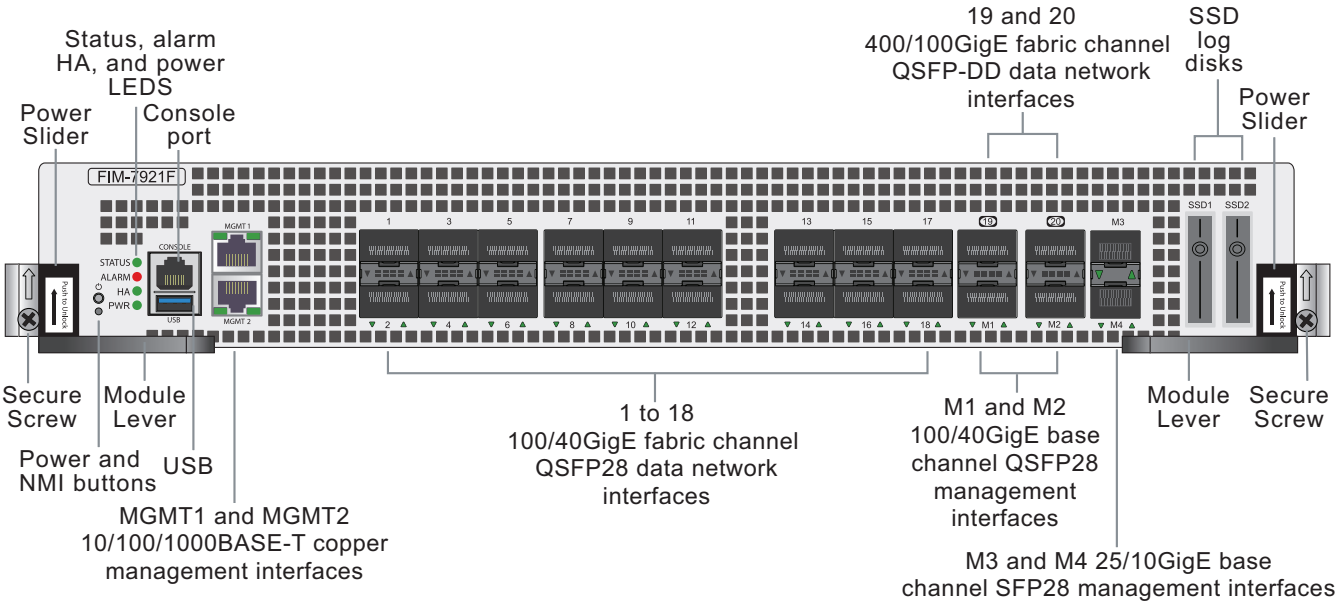
The FIM-7921F interface module is a hot swappable module that provides data, management, and session sync/heartbeat interfaces, base backplane switching, hardware acceleration, and fabric backplane session-aware load balancing for a FortiGate 7000F series chassis. The FIM-7921F includes an integrated switch fabric, five NP7 processors to load balance millions of data sessions over the FortiGate 7000F 400Gbps fabric backplane channel to FPM processor modules. The FIM-7921F also includes a 50Gbps base backplane channel for base backplane management communication with each FPM in the chassis, one 1Tbps fabric backplane channel for fabric backplane communication with the other FIM in the chassis, and a second 50Gbps base backplane channel for base backplane communication with the other FIM in the chassis. The FIM-7921F also includes two 4TByte SSD log disks in a RAID-1 configuration. The SSDs are accessible from the FIM-7921F front panel but should not be removed.

The FIM-7921F can be installed in any FortiGate 7000F series chassis in chassis hub/switch slots 1 or 2. The FIM-7921F includes eighteen front panel 100GigE QSFP28 fabric channel data network interfaces (1 to 18) and two 400GigE QSFP-DD fabric channel data network interfaces (19 and 20). Interfaces 1 to 18 can be connected to 100Gbps data networks. Interfaces 19 and 20 can be connected to 400Gbps data networks. You can also change the interface type of interfaces 19 and 20 and change the speeds of all of the data interfaces. You can also split interfaces 1 to 8, 19, and 20.

The FIM-7921F also includes two 100 GigE QSFP28 base channel management interfaces (M1 and M2) and two 25 GigE SPF28 base channel management interfaces (M3 and M4). The management interfaces can be used for HA heartbeat communication and session synchronization between two chassis in HA mode or for other management functions such as remote logging. You can also change the speeds of the management interfaces. You can also split the M1 and M2 interfaces.

The FIM-7921F includes a console port to provide console access to the FIM-7921F CLI.

FIM-7921F front panel



FPM-7620F processor module

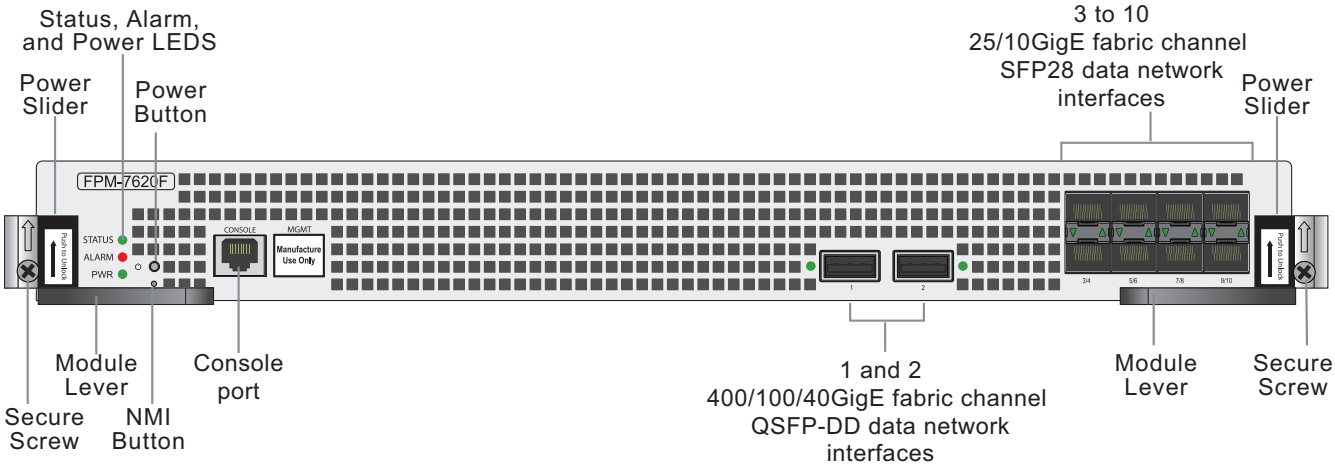
The FPM-7620F processor module is a high-performance worker module that processes sessions load balanced to it by FIMs over the chassis fabric backplane. The FPM-7620F includes two 400Gbps data connections to the FIMs over the chassis fabric backplane and two 50Gbps management connections to the FIMs over base backplane. FPM-7620Fs are installed in chassis slots 3 and up.

The FPM-7620F also includes two front panel 400GigE QSFP-DD fabric channel data interfaces (1 and 2) and eight 10/25GigE SFP28 fabric channel data interfaces (3 to 10). Interfaces 1 and 2 can be connected to 400Gbps data networks. Interfaces 3 to 10 can be connected to 25Gbps data networks. You an also change the speeds of the front panel data interfaces.

FPM fabric channel data interfaces increase the number of data interfaces supported by FortiGate 7000F. Data traffic received by these interfaces is sent over the fabric backplane to the FIM NP7 processors to be load balanced back to the FPMs.

The FPM-7620F processes sessions using a dual CPU configuration, accelerates network traffic processing with two NP7 processors and accelerates content processing with eight CP9 processors. The NP7 network processors are connected by the FIM switch fabric so all supported traffic types can be fast path accelerated by the NP7 processors.

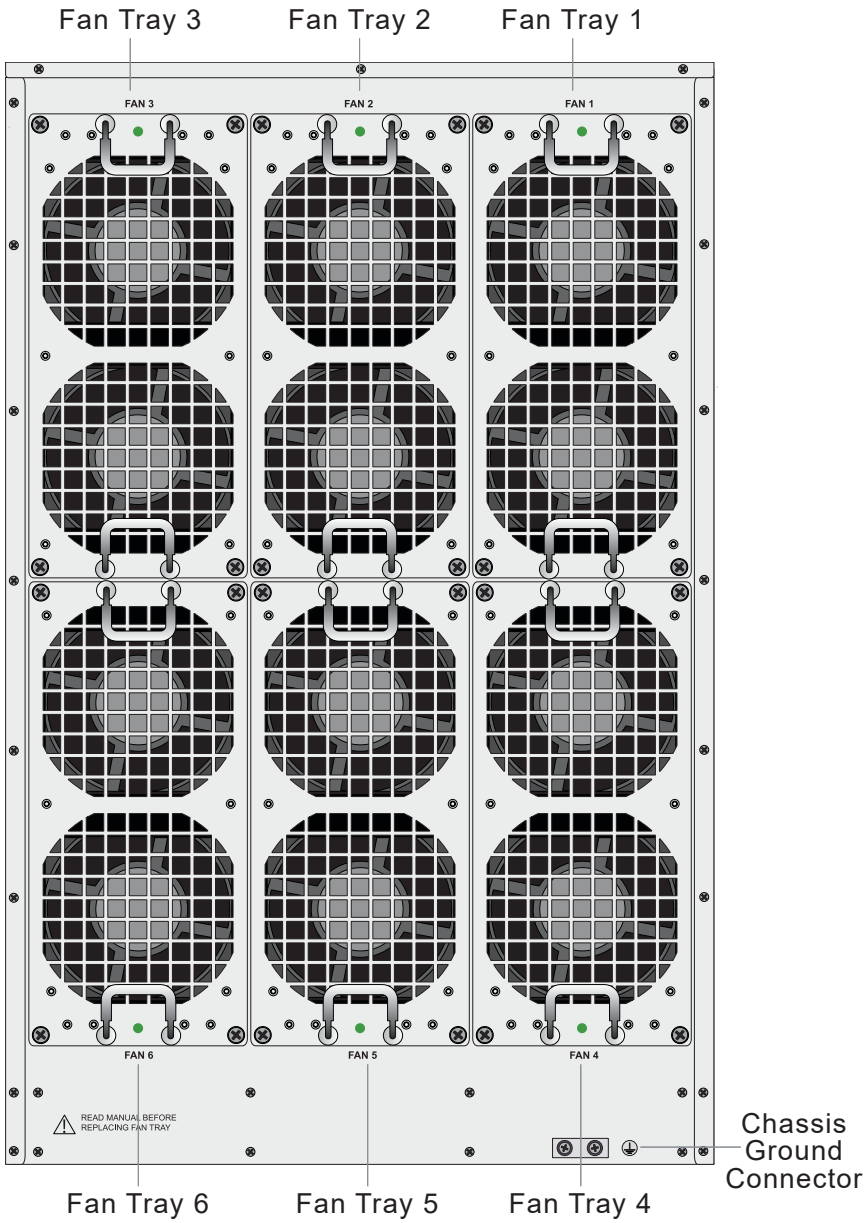
FPM-7620F front panel



FortiGate 7121F back panel

The FortiGate 7121F back panel provides access to six hot swappable cooling fan trays and the chassis ground connector that must be connected to ground.

FortiGate 7121F back panel

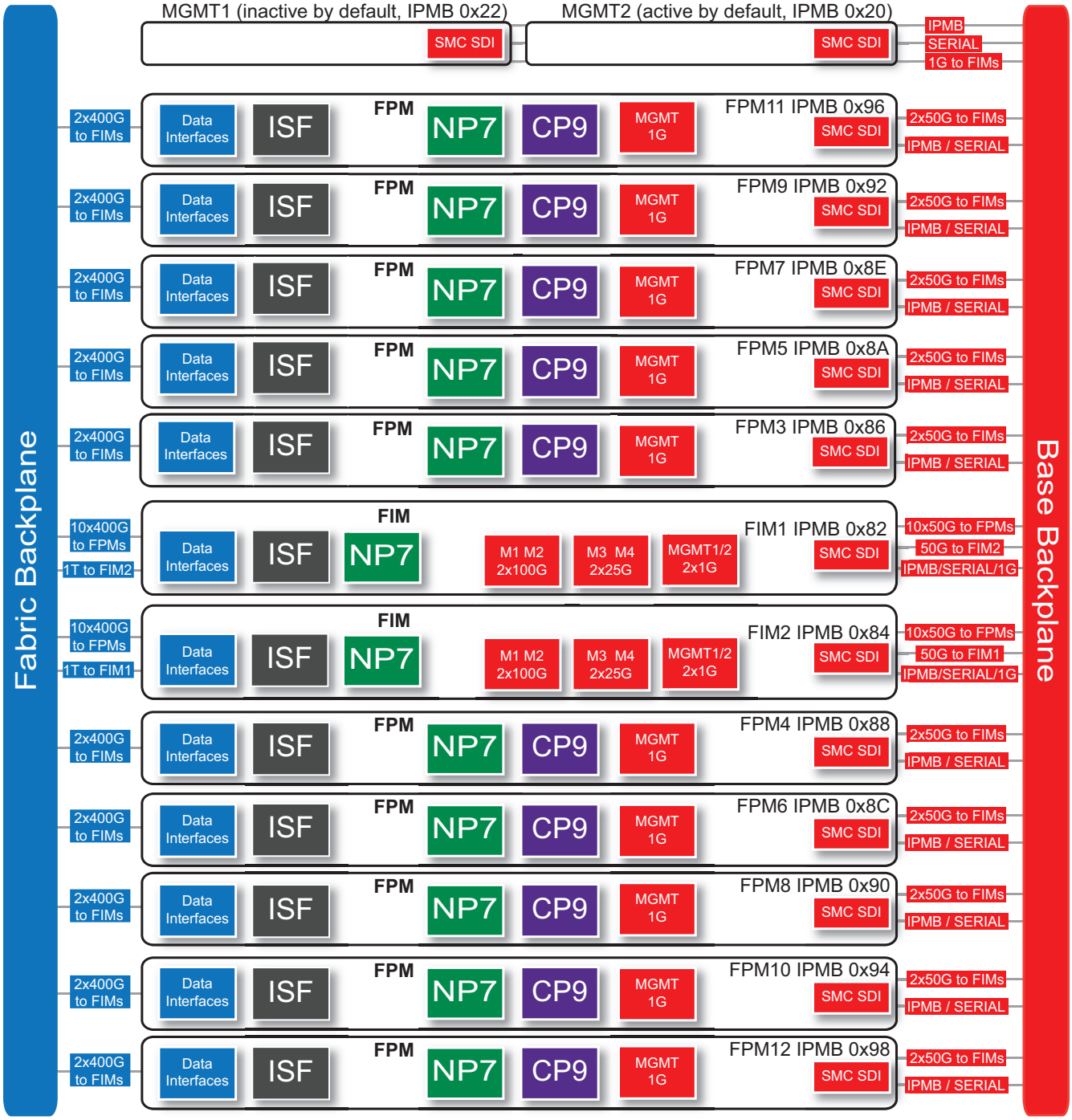


Registering your FortiGate 7121F

FortiGate 7000F series products are registered according to the chassis serial number. You need to register your chassis to receive Fortinet customer services such as product updates and customer support. You must also register your product for FortiGuard services. Register your product by visiting https://support.fortinet.com. To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased.

FortiGate-7121F chassis schematic

The FortiGate 7121F chassis schematic shows the communication channels between chassis components including the SMMs (MGMT1 and MGMT2), the FIMs (FIM1 and FIM2), and the FPMs (FPM3 to FPM12).



By default, MGMT2 is the active SMM and MGMT1 is inactive or passive. The active SMM always has the Intelligent Platform Management Bus (IPMB) address 0x20 and the passive SMM always has the IPMB address 0x22. Active and

passive refers to the SMM that is controlling the chassis. The MGMT interfaces and console ports on both SMMs are always available.

Each FIM and FPM and the SMMs have a Shelf Management Controller (SMC). These SMCs support IPMB communication between the active SMM and the FIMs and FPMs and other chassis components for storing and sharing sensor data that the SMM uses to control chassis cooling and power distribution. The FortiGate 7121F also includes serial communications to allow console access from the SMM to all FIMs and FPMs.

The base backplane includes 1Gbps ethernet management connections between the SMMs and the FIMs. The base backplane also supports 50Gbps Ethernet communication for management and heartbeat communication between FIMs and FPMs.

FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIM interface modules in slots 1 and 2. FIM data interfaces connect the chassis to data networks. NP7 processors in the FIMs use session-aware load balancing (SLBC) to distribute data sessions over the FIM Integrated Switch Fabric (ISF) to the 10x400Gbps connections over the fabric backplane to the FPMs. Data communication between FIM1 and FIM2 occurs over a 1TB fabric connection.

The FIM 1Gbps MGMT1 and MGMT2 interfaces are used for Ethernet management access to chassis components. The 2x100Gbps M1 and M2 interfaces are used for HA heartbeat communication between chassis. The 2x25Gbps M3 and M4 interfaces are used for remote logging or other management functions.

FPM3 to FPM12 (IPMB addresses 0x86 to 0x98) are the FPM processor modules in slots 3 to 12. These worker modules process sessions distributed to them over the fabric backplane by the NP7 processors in the FIMs. FPMs include NP7 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing. FPMs also include data interfaces that increase the number of data interfaces supported by the FortiGate 7121F. Data sessions received by the FPM data interfaces are sent over the fabric backplane to the FIM NP7 processors to be load balanced back to the FPMs using SLBC.

The FPM 1Gbps MGMT interfaces are used for Ethernet management access to chassis components.

Chassis hardware information

This section introduces FortiGate 7121F hardware components and accessories including power requirements and FIMs and FPMs that can be installed in the chassis.

Shipping components

The FortiGate 7121F chassis ships pre-assembled with the following components:

- The 16U FortiGate 7121F chassis.
- Two FIMs.
- Up to ten FPMs.
- Two System Management Modules (SMMs) in the front of the chassis. (SMMs are not field replacable. If a SMM fails, you must RMA the chassis. The chassis will continue to operate with one or no operating SMMs.)
- Eight 2000W Power Supply Units (PSUs) (generation 1).
- Eight 2500W Power Supply Units (PSUs) (generation 2).
- Six cooling fan trays installed in the back of the chassis.
- Eight FPM blank panels installed in chassis slots 5 to 12. The FPM blank panels are part of the chassis package and all blank panels should be kept available in case an FPM needs to be removed from the chassis. You can purchase additional FPM blank panels.

- Eight power cords with C15 power connectors.
- Eight power cord management clamps.
- One set of 4-post rack mounting components.
- One set of 2-post rack mounting components.
- Twenty-four M4x8 flat-head screws.
- Two M4x6 pan-head screws.
- Four M5x10 pan-head screws with double-washers.
- Eight rubber feet.
- Two USB to RJ-45 RS-232 console cables.
- One RJ-45 Ethernet cable.

Optional accessories and replacement parts

The following optional accessories can be ordered separately:

SKU	Description
FG-7121F-FAN	FortiGate-7121F fan tray.
FG-7121F-PS-2KAC	2000W AC power supply units (PSUs) for the generation 1 FortiGate-7121F.
FG-7121F-PS-25KAC	2500W AC power supply units (PSUs) for the generation 2 FortiGate-7121F.
FG-7121F	Generation 1 FortiGate-7121F chassis including 2x SMM, 6x fan trays, and 8x ACPSUs.
FG-7121F-DC	Generation 1 FortiGate-7121F chassis including 2x SMM, 6x fan trays, and 8x DC PSUs.
FG-7121F-GEN2	Generation 2 FortiGate-7121F chassis including 2x SMM, 6x fan trays, and 8x ACPSUs.
FG-7121F-DC-GEN2	Generation 2 FortiGate-7121F chassis including 2x SMM, 6x fan trays, and 8x DC PSUs.

- Additional FIMs and FPMs.FG-7121F-CH
- FIM and FPM blank panels to be installed in empty chassis slots.
- Transceivers.
- Cable bracket kit for data cable management.
- Front air filter kit.
- Additional AC PSUs.
- Additional DC PSUs.
- Additional FAN trays.

Physical description of the FortiGate 7121F chassis

The FortiGate 7121F chassis is a 16U chassis that can be installed in a standard 19-inch rack. The following table describes the physical characteristics of the FortiGate 7121F chassis.

Dimensions (H x W x D)	28.63 x 17.33 x 26.6 in (727.2 x 440 x 675.5 mm)
Chassis weight completely assembled with FIMs and FPMs installed	447.36 lbs (203.1 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
AC Input Voltage Range	200 to 240 VAC (50 to 60 Hz)
Supplied Power Supply Units (PSUs)	8
Power supplied by each AC PSU (generation 1)	2000W
Power supplied by each DC PSU (generation 1)	2000W
Power supplied by each AC PSU (generation 2)	2500W
Power supplied by each DC PSU (generation 2)	2500W
Max Power Consumption	9754W
Average Power Consumption	8296W
Max Current (generation 1)	8 x 10A
Max Current (generation 2)	8 x 16A
Heat Dissipation	35114KJ/h (33261BTU/h)

FortiGate 7121F series hardware generations

Two generations of FortiGate 7121F series are now available. Both generations support the same software features. Generation 2 has the following hardware improvements:

- The generation 2 FortiGate 7121F ships with eight 2500W AC or DC PSUs. The generation 1 FortiGate 7121F ships with eight 2000W AC or DC PSUs.
- Because the generation 2 PSUs can supply enough power for 4 x 4 redundancy, the DC combiner is not required for the generation 2 FortiGate 7121F.
- In a generation 2 FortiGate 7121F, you can include a FIM-7921F and a FIM-7941F in the same chassis.

For more information on generation 1 and generation 2 AC PSUs, see AC PSUs and supplying AC power to the chassis on page 23 and DC PSUs and supplying DC power to the chassis on page 25.

Cooling fans, cooling air flow, and minimum clearance

The FortiGate 7121F chassis contains six hot swappable cooling fan trays installed in the back of the chassis. Each fan tray includes two fans that operate together. When the fan tray LED is green, both fans are operating normally. If the LED turns red or goes off, one or both of the fans is not working and the fan tray should be replaced.

During normal chassis operation, all six fan trays are active and the fan speed is controlled by the active SMM. If a single fan tray fails, the SMM sends a warning message and the SMM front panel fan LEDs indicate that a fan tray has failed. The SMM maintains sufficient cooling by running the still operating fans at full speed to make up the airflow loss caused by the failed fan tray. The failed fan tray should be replaced as soon as possible.

If a second fan tray fails, the chassis can continue to operate but the chassis may experience high temperature warnings. Maintaining a lower ambient temperature can reduce the chance of overheating.

Fan trays are hot swappable. You can replace a failed fan tray while the chassis is operating. To replace a fan tray, unscrew the four retention screws and use the handles to pull the fan tray out of the chassis.

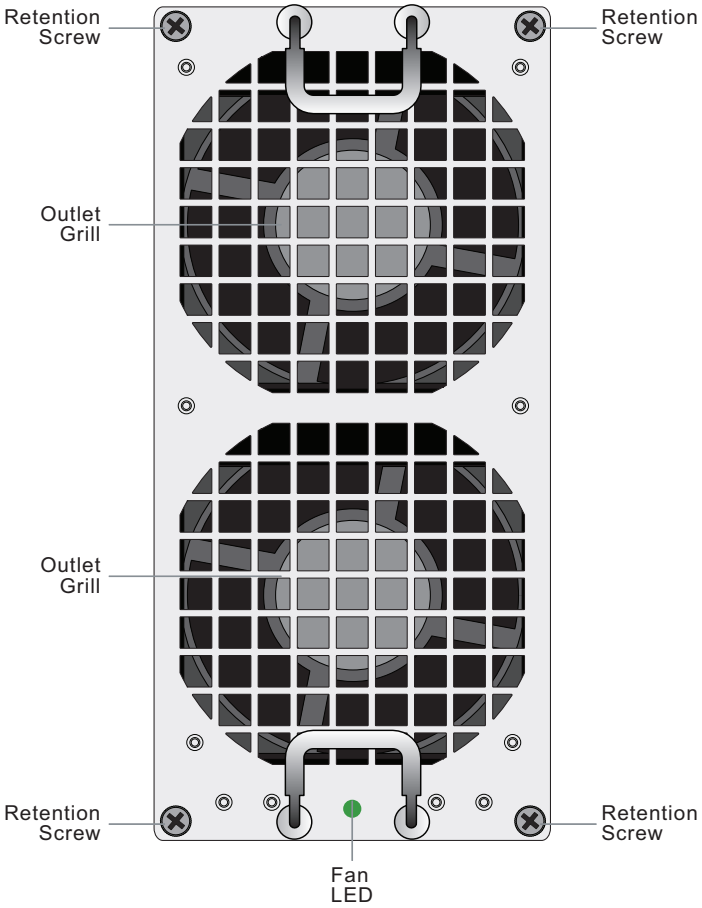
Install a replacement fan tray by sliding it into place in the empty slot and tightening the retention screws. As you slide the new fan into place it will power up and the fan tray LED will light.

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 chassis so do not delay installing the replacement fan tray.

The active SMM monitors the internal temperature of the chassis and adjusts the operating speed of the cooling fans as required. When the chassis is first powered on, all cooling fans run at full speed. Once the active SMM is up and running, it reduces cooling fan speeds to maintain an optimum temperature in the chassis. If an SMM is not available or is not operating correctly, the fans always operate at full speed.

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

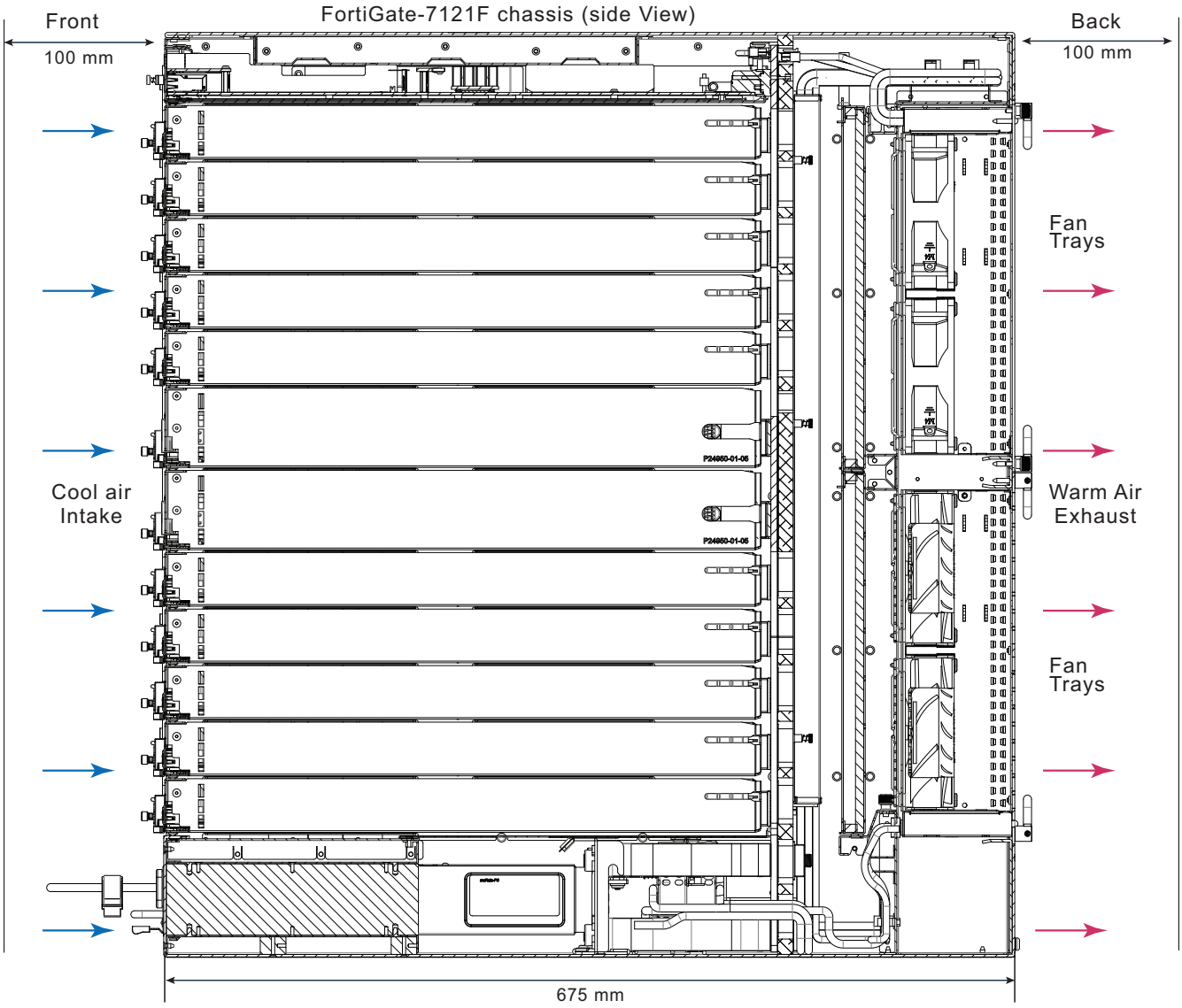
Cooling Fan Tray



Cooling air flow and required minimum air flow clearance

When installing the chassis, make sure there is enough clearance for effective cooling air flow**.** The following diagram shows the cooling air flow through the chassis and the locations 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 7121F cooling air flow and minimum air flow clearance



Cool air enters the chassis through the chassis front panel and warm air exhausts out the back. For optimal cooling, allow 100 mm of clearance at the front and back of the chassis.

Optional air filter

You can purchase an optional NEBS compliant air filter kit that includes a front filter that fits over the front of the chassis. This filter is not required for normal operation but can be added if you require air filtration.

The air filters should be inspected regularly. If dirty or damaged, the filters should be disposed of and replaced. The air filters can be fragile and should be handled carefully.

Power consumption for different FIM-7941F FortiGate 7121F configurations

The tables in this section provide information about how to calculate maximum power consumption for a FortiGate 7121F system with two FIM-7941Fs and with four, six, or ten FPM-7620Fs.

These example calculations should be used as guidelines only. In practice, actual power usage will most likely be higher and the efficiency of PSUs varies for different levels of power consumption and loading. The maximum power consumption of a fully loaded FortiGate 7121F under ideal conditions has been measured as 9754W and the average power consumption is 8296W.

Power consumption calculation with four FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7941Fs and four FPM-7620Fs would require a power allocation of 5524W.

- The capacity of each generation 1 PSU is 2000W. The system would require three PSUs (2000 x 3 = 6000W). You could add up to five extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require three PSUs (2500 x 3 = 7500W). You could add up to five extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7941F	630	2	1260
FPM-7620F	716	4	2864
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	5524

Power consumption calculation with six FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7941Fs and six FPM-7620Fs would require a power allocation of 6956W.

- The capacity of each generation 1 PSU is 2000W. The system would require four PSUs (2000 x 4 = 8000W). You could add up to four extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require three PSUs (2500 x 3 = 7500W). You could add up to five extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7941F	630	2	1260
FPM-7620F	716	6	4296
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	**6956**

Power consumption calculation with ten FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7941Fs and ten FPM-7620Fs would require a power allocation of 9820W.

- The capacity of each generation 1 PSU is 2000W. The system would require five PSUs (2000 x 5 = 10000W). You could add up to three extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require four PSUs (2500 x 4 = 10000W). You could add up to four extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7941F	630	2	1260
FPM-7620F	716	10	7160
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	**9820**

Hot Swapping an AC PSU

Follow these steps to safely hot swap an AC PSU.

You can hot swap a PSU without powering down the FortiGate 7121F as long as four PSUs are connected to power and operating normally. If you need to hot swap one of four operating PSUs, you should do this during a quiet period, because if the FortiGate 7121F is operating with less that four PSUs, some of the FPMs may be shut down.

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 power supply and disconnect the power cord.
3. Press the latch towards the handle until the PSU is detached then pull it out of the chassis.

4. Insert a replacement PSU into the chassis and slide it in until it locks into place.
5. Plug power cables into the FortiGate 7121F PSU connector.
   Slide the connector in until the release tab clicks, locking the cable in place.
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.

Power consumption for different FIM-7921F FortiGate 7121F configurations

The tables in this section provide information about how to calculate maximum power consumption for a FortiGate 7121F system with two FIM-7921Fs and with four, six, or ten FPM-7620Fs.

These example calculations should be used as guidelines only. In practice, actual power usage will most likely be higher and the efficiency of PSUs varies for different levels of power consumption and loading. The maximum power consumption of a fully loaded FortiGate 7121F under ideal conditions has been measured as 9754W and the average power consumption is 8296W.

Power consumption calculation with four FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7921Fs and four FPM-7620Fs would require a power allocation of 5458W.

- The capacity of each generation 1 PSU is 2000W. The system would require three PSUs (2000 x 3 = 6000W). You could add up to four extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require three PSUs (2500 x 3 = 7500W). You could add up to five extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7921F	597	2	1194
FPM-7620F	716	4	2864
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	5458

Power consumption calculation with six FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7921Fs and six FPM-7620Fs would require a power allocation of 6890W.

- The capacity of each generation 1 PSU is 2000W. The system would require four PSUs (2000 x 4 = 8000W). You could add up to four extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require three PSUs (2500 x 3 = 7500W). You could add up to five extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7921F	597	2	1194
FPM-7620F	716	6	4296
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	**6890**

Power consumption calculation with ten FPM-7620Fs

The following table shows that a FortiGate 7121F with two FIM-7921Fs and ten FPM-7620Fs would require a power allocation of 9754W.

- The capacity of each generation 1 PSU is 2000W. The system would require five PSUs (2000 x 5 = 10000W). You could add up to three extra PSUs for redundancy.
- The capacity of each generation 2 PSU is 2500W. The system would require four PSUs (2500 x 4 = 10000W). You could add up to four extra PSUs for redundancy.

Module	Max power consumption (W)	Number of modules	Total max power (W)
FIM-7921F	597	2	1194
FPM-7620F	716	10	7160
Chassis (fans, SMMs etc)	1400	N/A	1400
		Totals	**9754**

AC PSUs and supplying AC power to the chassis

The generation 1 FortiGate 7121F chassis front panel can include up to eight hot swappable 200-240V, 10A, 2000W AC PSUs. The generation 2 FortiGate 7121F chassis front panel can include up to eight hot swappable 200-240V, 16A, 2500W AC PSUs. See FortiGate 7121F front panel on page 8 for locations of the PSUs.

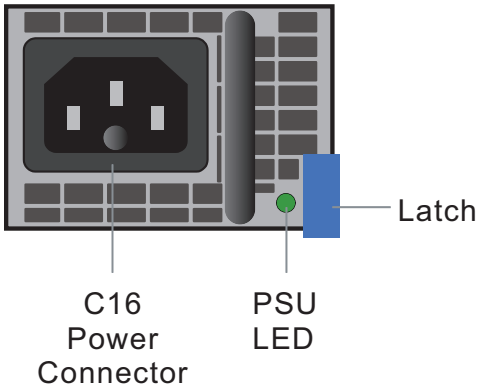
The number of PSUs required by a chassis depends on the number of FIMs and FPMs in the chassis. See Power consumption for different FIM-7941F FortiGate 7121F configurations on page 20 or Power consumption for different FIM-7921F FortiGate 7121F configurations on page 22.

If the chassis does not have enough power because PSUs have failed or become disconnected, the active SMM will begin shutting down FPMs starting at the highest slot number.

All AC PSUs should be connected to AC power. To improve redundancy you can connect each PSU to a separate power source.

Use a C15 Power cable, supplied with the chassis, 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.

AC PSU showing C16 power connector



The PSU LED indicates whether the PSU is operating correctly and connected to power. If this LED is not lit, check to make sure the PSU is connected to power. If the power connection is good then the PSU has failed and should be replaced.

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.

Power distribution unit (PDU) requirements

Due to the power consumption FortiGate 7121F, Fortinet recommends the following PDU requirements if you are operating a FortiGate 7121F that contains two FIM-7921F and ten FPM-7620Fs.

- Two 30A/208V PDUs with no other devices connected to the PSUs. Connect four PSUs to each PDU .
- One 40A/208V/3ph, 1x PDU required and 3xPSU @ L1/L2, 3xPSU @ L2/L3, 2xPSU @ L1/L3. No extra load on PDU.

120V PDUs are not supported since high power PSUs are not designed to work under low AC line input. Max wattage and load balancing across PSUs will be compromised if doing so.

Installing AC PSUs

Follow these steps to install an AC PSUs in a FortiGate 7121F chassis.

Install the AC PSUs before connecting them to power.

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. Remove a PSU from its packaging.
3. Insert the PSU into a chassis PSU slot and slide it in until it locks into place.
4. Repeat to install all of the required PSUs.
5. Plug the power cables into each FortiGate 7121F PSU connectors.
   Slide each connector in until the release tab clicks, locking the cable in place.

DC PSUs and supplying DC power to the chassis

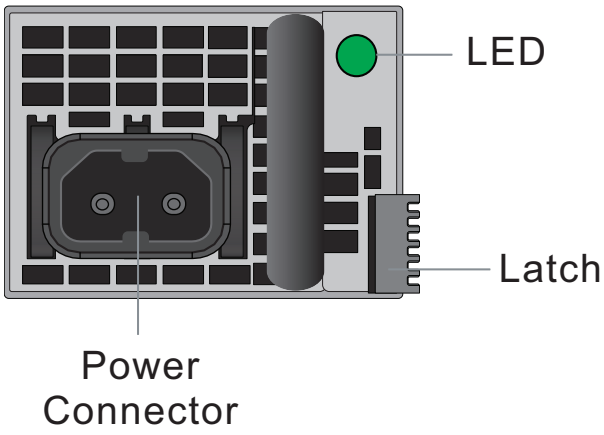
The DC version of the generation 1 FortiGate 7121F chassis front panel can include up to eight hot swappable -48V to -60V, 41-33A, 2000W DC PSUs. The DC version of the generation 2 FortiGate 7121F chassis front panel can include up to eight hot swappable -48V to -60V, 52-42A, 2500W DC PSUs. Each PSU has an Internal 60A/170VDC fast blow fuse on the DC line input. See FortiGate 7121F front panel on page 8 for locations of the PSUs. The diagram shows AC PSUs, with a DC version of the chassis the AC PSUs are replaced with DC PSUs.

The number of PSUs required by a chassis depends on the number of FIMs and FPMs in the chassis. See Power consumption for different FIM-7941F FortiGate 7121F configurations on page 20 or Power consumption for different FIM-7921F FortiGate 7121F configurations on page 22.

Fortinet supplies a DC Combiner that you can install to provide redundant power feeds to each PSU. See Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F on page 29. Because FortiGate 7121F generation 2 PSUs can supply enough power for 4 x 4 redundancy, the DC combiner is not required for the generation 2 FortiGate 7121F.

Each PSU is designed to be installed in a Telecom data center or similar location that has available -48VDC power fed from a listed 80A circuit breaker. To improve redundancy you can connect each power supply to a separate power circuit.

DC PSU



If you are connecting the generation 1 FortiGate 7121F to Fortinet's DC Combiner, Fortinet supplies custom DC power cables that connect the two-prong power connector on each DC PSU to the corresponding connector on the DC Combiner module front panel. The connector on each end of the cable clicks into a release tab that secures the cable into place. For more information about the FortiGate 7121F DC combiner, see Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F on page 29.

If you are connecting the generation 1 FortiGate 7121F directly to data center power, 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.

PSU Power ratings

Max Inrush Current	50A
Max Inrush Current Duration	200ms
Input Voltage	-48Vdc to -60Vdc
Input Current	Average: 203A @ -48Vdc and 163A @ -60Vdc for each PSU

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.

State	Description
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

If you are connecting a generation 2 FortiGate 7121F or not using Fortinet's DC Combiner to connect a generation 1 FortiGate 7121F, the FortiGate 7121F includes eight DC power cords. Each 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 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.

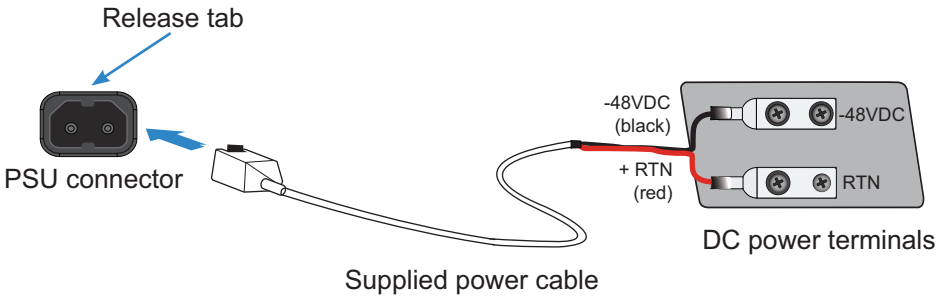
Installing a DC PSU

Follow these steps to install a DC PSU in a chassis.

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. Remove the PSU from its packaging.
3. Insert the PSU into the chassis and slide it in until it locks into place.

Connecting a FortiGate 7121F DC PSU to DC power

The following procedure describes how to connect a FortiGate 7121F DC PSU to DC power. Repeat this procedure to connect each PSU.



You need the following equipment to connect the FortiGate 7121F 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 7121F chassis to ground on page 33 to connect the FortiGate 7121F 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 7121F 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 7121F as long as three PSUs are connected to power and operating normally. If you need to hot swap one of three operating PSUs, you must power down the chassis first.

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 from the PSU.
3. Press the latch towards the handle until the PSU is detached then pull it out of the chassis.
4. Insert a replacement PSU into the chassis and slide it in until it locks into place.
5. Plug the power cable into the FortiGate 7121F PSU connector.
   Slide the connector in until the release tab clicks, locking the cable in place.
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.

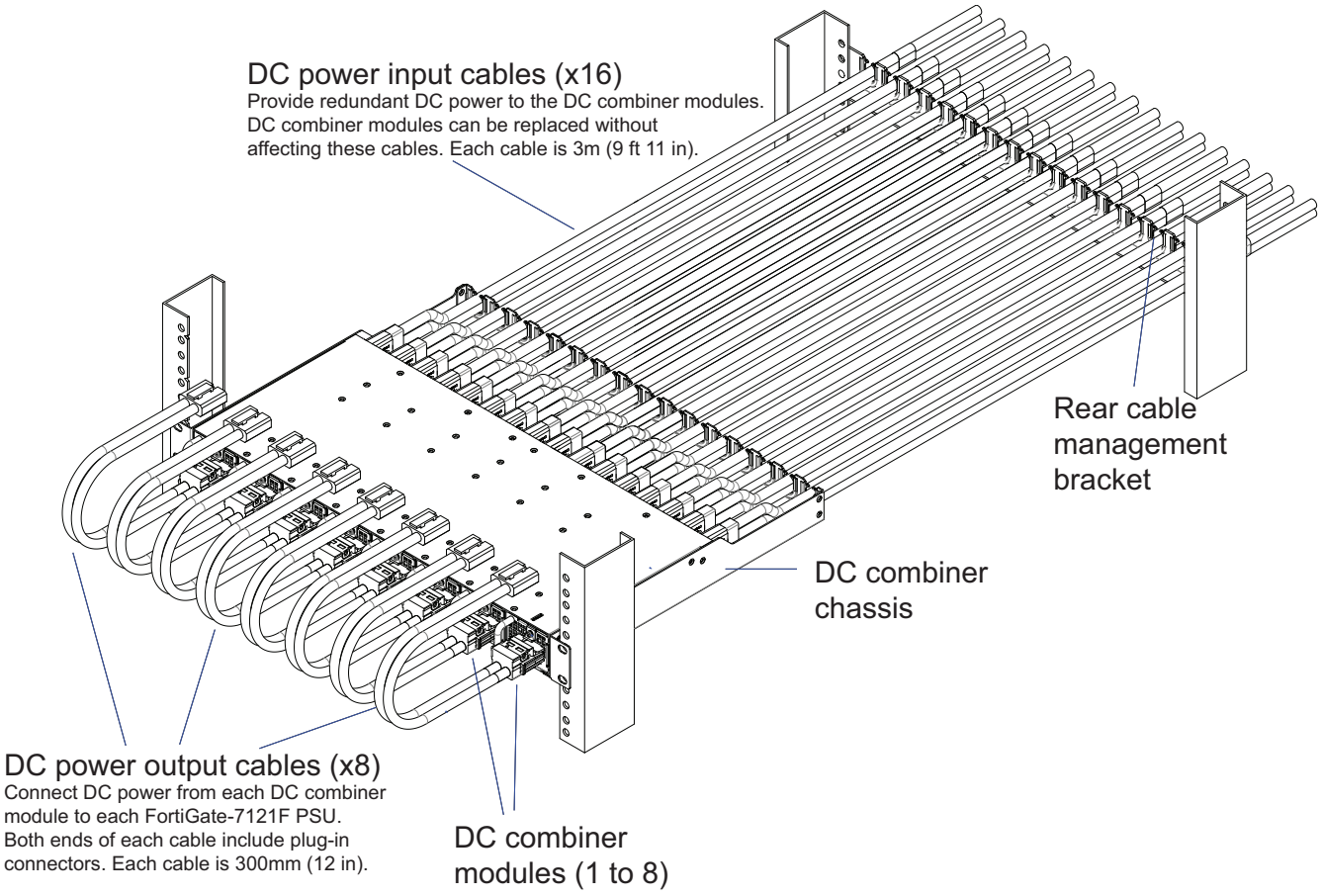
Using the FortiGate 7121F DC Combiner to supply redundant DC power for the FortiGate 7121F

The FortiGate 7121F DC combiner is used to connect the generation 1 FortiGate 7121F to DC power.

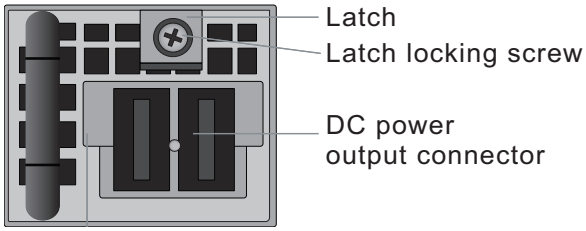
The 1U rack mount FortiGate 7121F DC Combiner contains eight hot-swappable DC combiner modules that provide redundant 48V DC (1+1) power feeds for the eight FortiGate 7121F DC PSUs. Each DC combiner module connects to a FortiGate 7121F PSU and two DC nominal 48V power feeds (Feed A and Feed B). The DC combiner modules include active O-ring controllers that make sure the power feed with the highest voltage supplies power to the connected PSU.

Fortinet also includes sixteen 3m (9 ft 11 in) DC power input cables to connect the DC combiner modules to DC power and eight 300mm (12 in) DC power output cables to connect the DC combiner modules to the FortiGate 7121F DC PSUs.

DC combiner chassis and cables



DC combiner module front panel

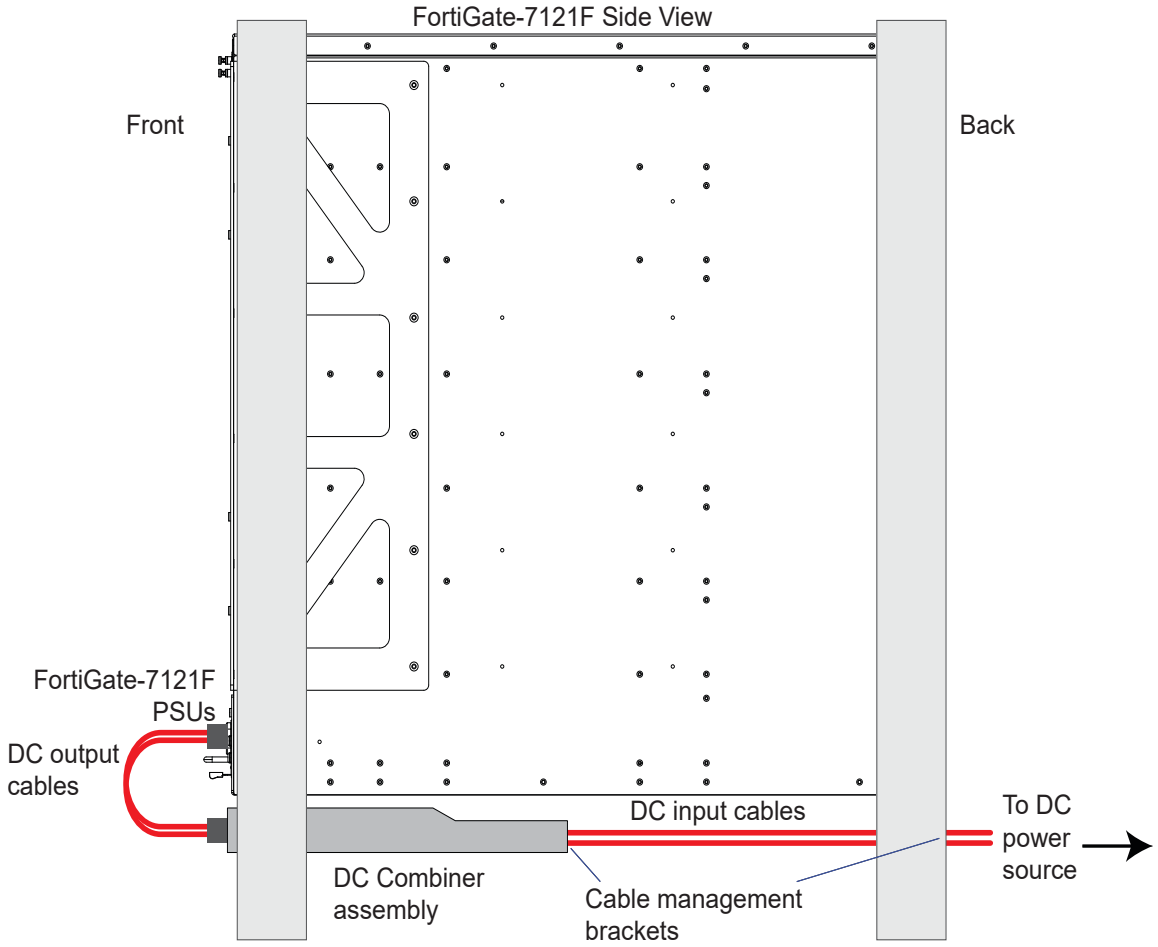


Connecting a FortiGate 7121F to DC power using the FortiGate 7121F DC combiner

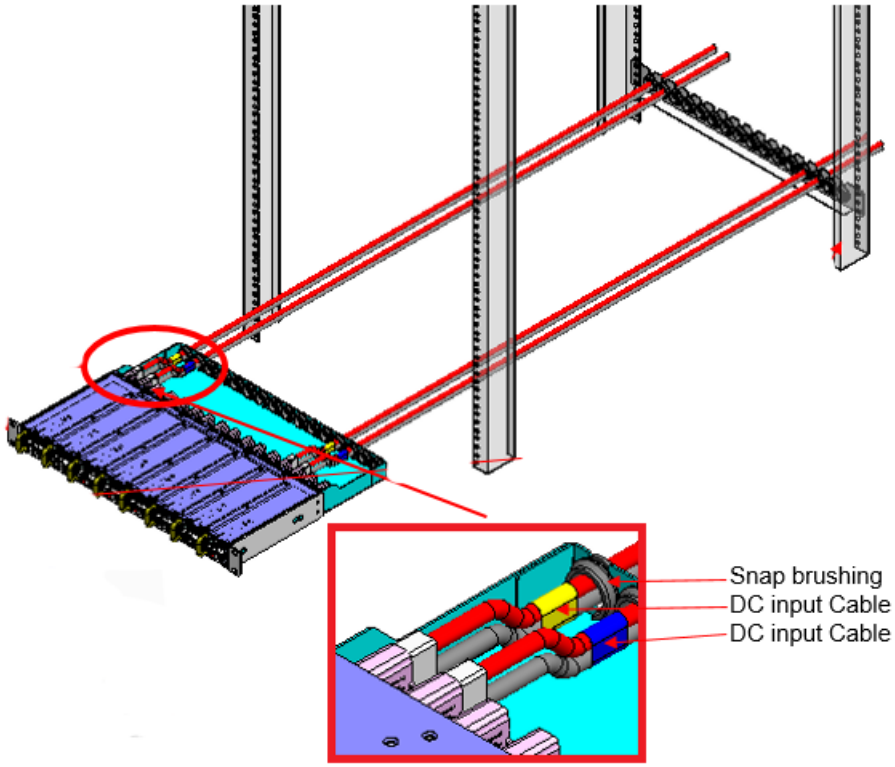
Use the following steps to install the FortiGate 7121F DC combiner and, after installing the FortiGate 7121F chassis, to connect the each DC combiner module to a FortiGate 7121F DC PSUs to provide redundant DC power to the FortiGate 7121F chassis.

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. Use four rack mount screws (not provided) to secure the 1U DC combiner chassis on the front posts of an equipment rack. Install the DC combiner chassis at the bottom of the rack, the FortiGate 7121F chassis must be

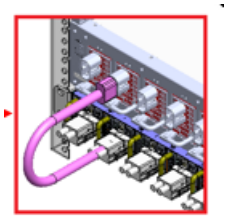
installed directly above the DC combiner in the same rack.



3. Use four rack mount screws (not provided) to install the rear cable management bracket on the rear posts of the equipment rack at the same level as the DC combiner assembly.
4. Select a DC input cable and attach a yellow label to each end. Connect the DC input Cable to power feed A of the first DC combiner module.
5. Select a DC input cable and attach a blue label to each end. Connect the DC input Cable to power feed B of the first DC combiner module.
6. Extend the yellow and blue labeled cables out the back of the DC combiner chassis and use a snap brushing to secure the cables at the back of the chassis. Extend the cables to the rear cable management bracket and secure them to the cable management bracket using another snap brushing.



7. Repeat for all eight DC combiner modules and all sixteen DC input cables.
8. Install the FortiGate 7121F chassis in the rack directly above the DC combiner.
9. Connect DC output cables from each DC combiner module to the corresponding DC PSU in the FortiGate 7121F chassis.



10. Connect all the DC input cables with yellow labels to a DC power source. Connect all the DC input cables with blue labels to a different DC power source.

Hot swapping a DC Combiner Module

You can hot swap a DC combiner module without powering down the FortiGate 7121F as long as three FortiGate 7121F PSUs remain connected to power and operating normally. If you need to hot swap a DC combiner module connected to one of three operating PSUs, you must power down the FortiGate 7121F chassis first.

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. Disconnect the DC power input cable on the front of the DC combiner module that connects the DC combiner module to the FortiGate 7121F PSU.
3. Remove the DC combiner module latch locking screw.
4. Press down on the DC combiner module latch and use the handle to pull the module out of the chassis.
5. Insert a replacement module into the empty slot and tighten the DC combiner module latch locking screw.
6. Reconnect the DC power input cable to the DC combiner module.

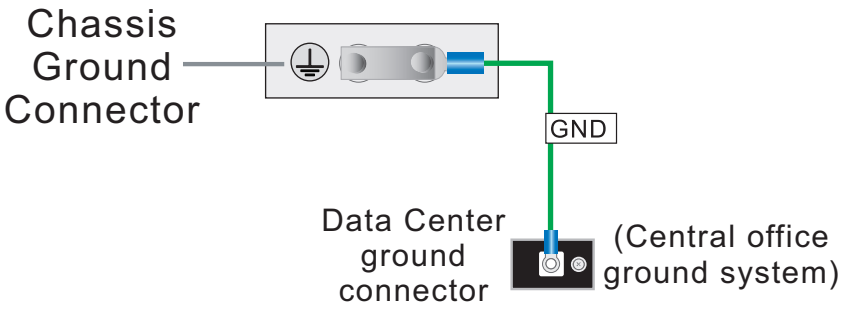
Connecting the FortiGate 7121F chassis to ground

The FortiGate 7121F chassis includes a ground connector on the rear the bottom of the FortiGate 7121F back panel. The ground connector consists of two terminals to be used with a double-holed lug such as Thomas & Betts PN 54850BE. Connect the double-holed lug to the chassis ground connector using the two M5x10 pan-head screws that are already attached to the ground connector.

You need the following equipment to connect the FortiGate 7121F chassis 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 7121F 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 chassis or frame.
2. Make sure that the chassis and ground wire are not energized.
3. Connect the ground wire double-holed lug to the FortiGate 7121F chassis ground connector using the two M5x10 pan-head screws already attached to the ground connector.
4. Connect the other end for the ground wire to a data center ground connector.
5. Optionally label the wire GND.

Turning on FortiGate 7121F chassis power

Connect AC power to PSUs 1 to 8. Once the FortiGate 7121F chassis is connected to power, the chassis powers up. If the chassis is operating correctly, the LEDs on the PSUs and fans should be solid green. As well, the LEDs on the SMMs should be lit.

When the chassis first starts up you should also hear the cooling fans operating.

In addition, if any modules have been installed in the chassis they should power on and their front panel LEDs should indicate that they are starting up and operating normally.

FortiGate 7121F hardware assembly and rack mounting

The FortiGate 7121F chassis must be mounted in a standard 19-inch rack and requires 16U of vertical space in the rack. This chapter describes how to attach accessories to the FortiGate 7121F chassis, how to install the chassis in a 4-post or 2-post rack, and how to install FIM and FPM modules in the chassis front panel slots.

If you install the FortiGate 7121F chassis 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.

The FortiGate 7121F chassis should not be operated as a free-standing appliance.

It is recommended that you mount the FortiGate 7121F chassis near the bottom of the rack to avoid making the rack top-heavy and potentially falling over. If you are going to mount the chassis higher, make sure the rack is well anchored. Since the chassis is over 400 lbs use a lift to raise the chassis into position before mounting it.

Install accessories before mounting the chassis in a rack. Install the FIMs and FPMs after the chassis is rack mounted.

Installing optional accessories

The following accessories are optional and not required for all configurations:

- Front mounting brackets.
- Cable bracket kit.
- Front air filter kit.
- Power cord clamps.

Front mounting brackets

You need to install the front mounting brackets to mount the FortiGate 7121F in a four-post rack (see Mounting the FortiGate 7121F chassis in a four-post rack on page 40). You also need to install the front mounting brackets to be able to attach the left and right cable management brackets.

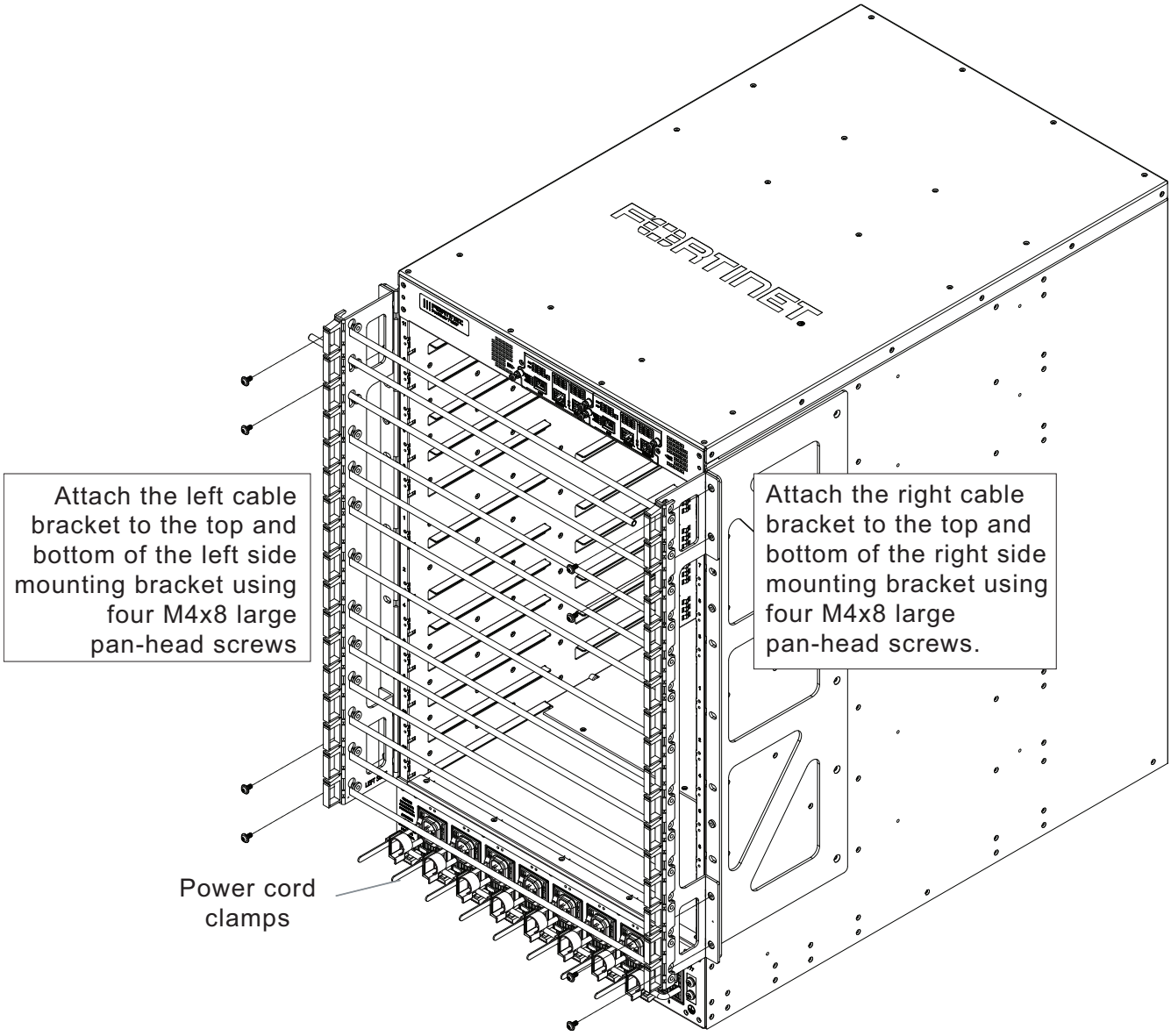
The front mounting brackets are not required to mount the FortiGate 7121F in a two-post rack (see Mounting the FortiGate 7121F chassis in a two-post rack on page 41).

Cable bracket kit

You can install the optional cable bracket kit to help manage the network cables connected to FIMs and FPMs installed in the FortiGate 7121F. Attach the cable bracket kit to the left and right front mounting brackets.

The cable bracket kit includes horizontal cable mount levers that must be installed after the cable kit brackets are attached to the left and right mounting brackets. Once the mount levers are installed you can attach network cables to them.

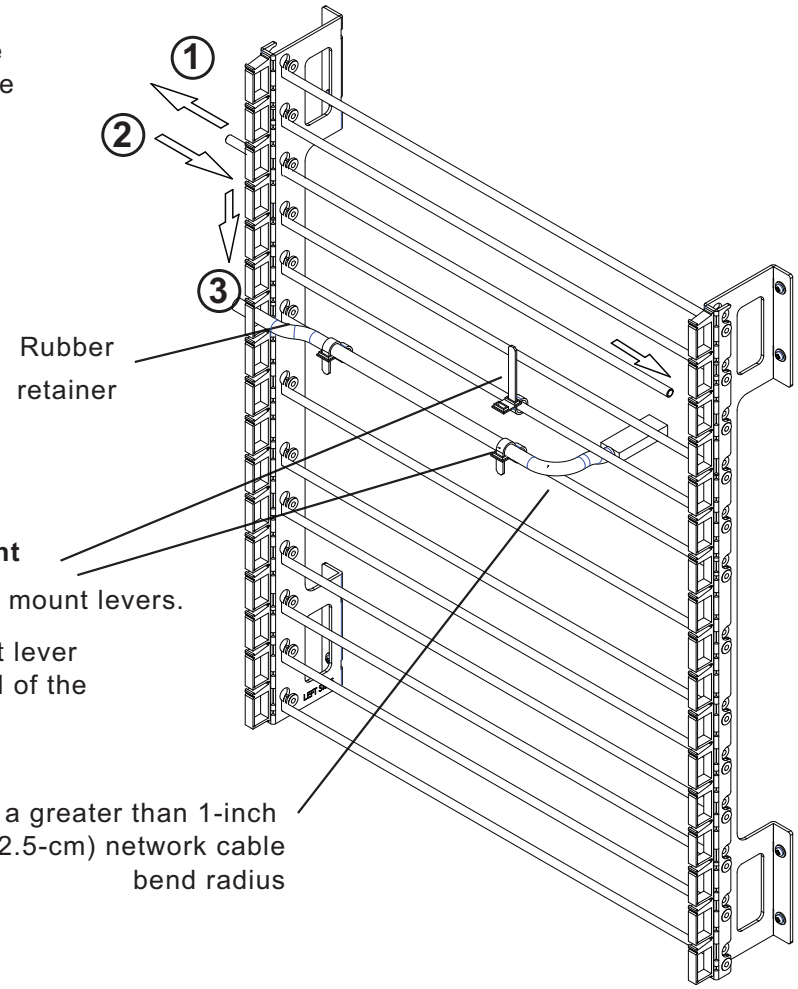
Installing the cable bracket kit



Attaching network cables to the cable mount levers

Installing horizontal cable mount levers

1. From the inside, insert the mount lever through the top hole in the side bracket and extend it a short distance past the side bracket.
2. Insert the other end of the mount lever into the top hole in the bracket on the other side of the chassis.
3. Press the mount lever down until held in place by the rubber retainer in each bracket.



Front air filter kit

You can attach a front air filter kit if the FortiGate 7121F will be installed in a dusty environment. The following diagrams show how to install the filter kit, special procedures for installing an FPM in slot 11, power cord management, and data cord management when the air filter kit is installed.

Installing the front air filter kit

Installing the channel outlet sealing cover

1. Remove the top cover.

2. Align the four mushroom pins of the cover into the cable channnel key holes. (sealing foam not shown in the diagram).

3. Slide the cover in and then down into place.

4. Re-install the top cover (this holds the channel outlet sealing cover in place).

Installing an FPM in slot 11 if the front filter kit has been installed

1. Remove the top cover.

2. Remove the slot 11 mount lever by pushing it upward and backward.

3. Slide the FPM into slot 11 (not shown).

4. Re-install the slot 11 mount lever and top panel.

Installing the SMM front filter

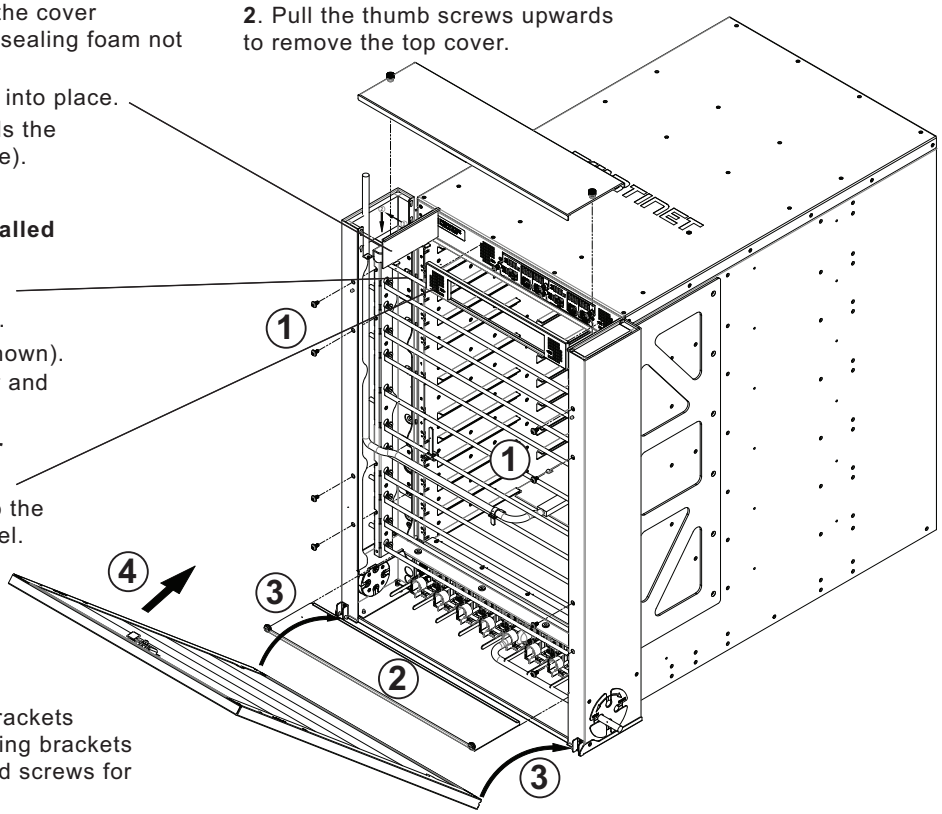
1. Remove the top cover.

2. Attach the SMM front filter to the magnets on the SMM front panel.

Removing the top cover

1. Loosen both thumb screws.

2. Pull the thumb screws upwards to remove the top cover.



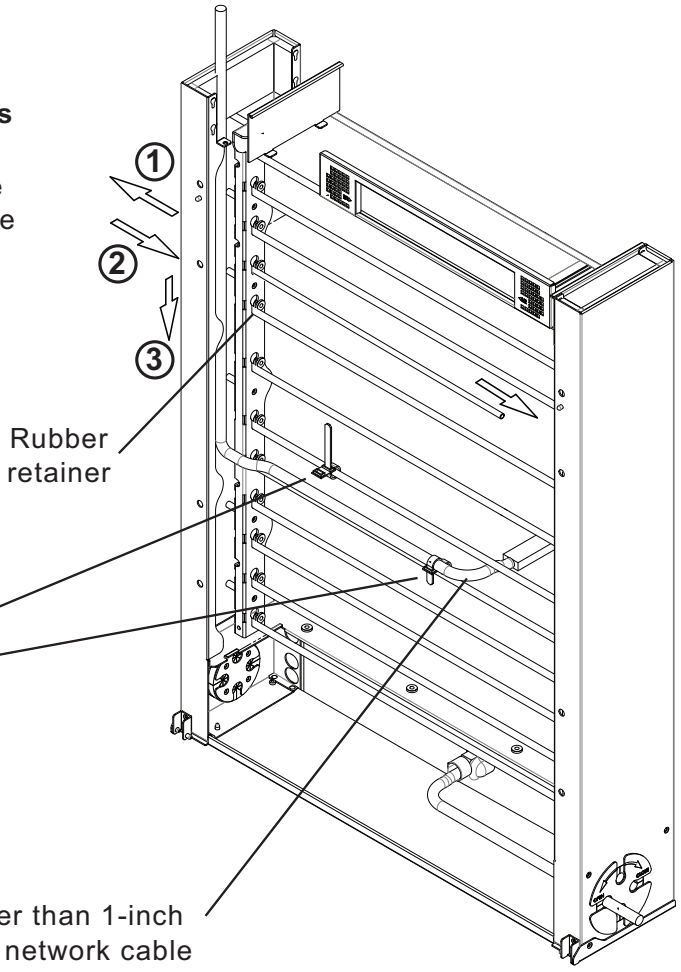
Installing the front air filter kit

1. Attach the front filter kit side brackets to the left and right side mounting brackets using four M4x8 large pan-head screws for each bracket.
2. Slide the bottom plate into the filter enclosure.
3. Mount the front filter cover on the bottom brackets.
4. Close the front panel until it locks into place.

Front air filter kit data and power cable management

Installing horizontal cable mount levers

1. From the inside, insert the mount lever through the top hole in the side bracket and extend it a short distance past the side bracket.
2. Insert the other end of the mount lever into the top hole in the bracket on the other side of the chassis.
3. Press the mount lever down until held in place by the rubber retainer in each bracket.



Cable management

Attach cable ties to the mount levers.

Tie cables to the mount lever using the second round of the cable tie.

Maintain a greater than 1-inch (2.5-cm) network cable bend radius

Managing AC power cords

1. Connect AC power cords to the PSUs and cable clamps.

2. Run the power cords out the side seals at the bottom of both filter kit side brackets.

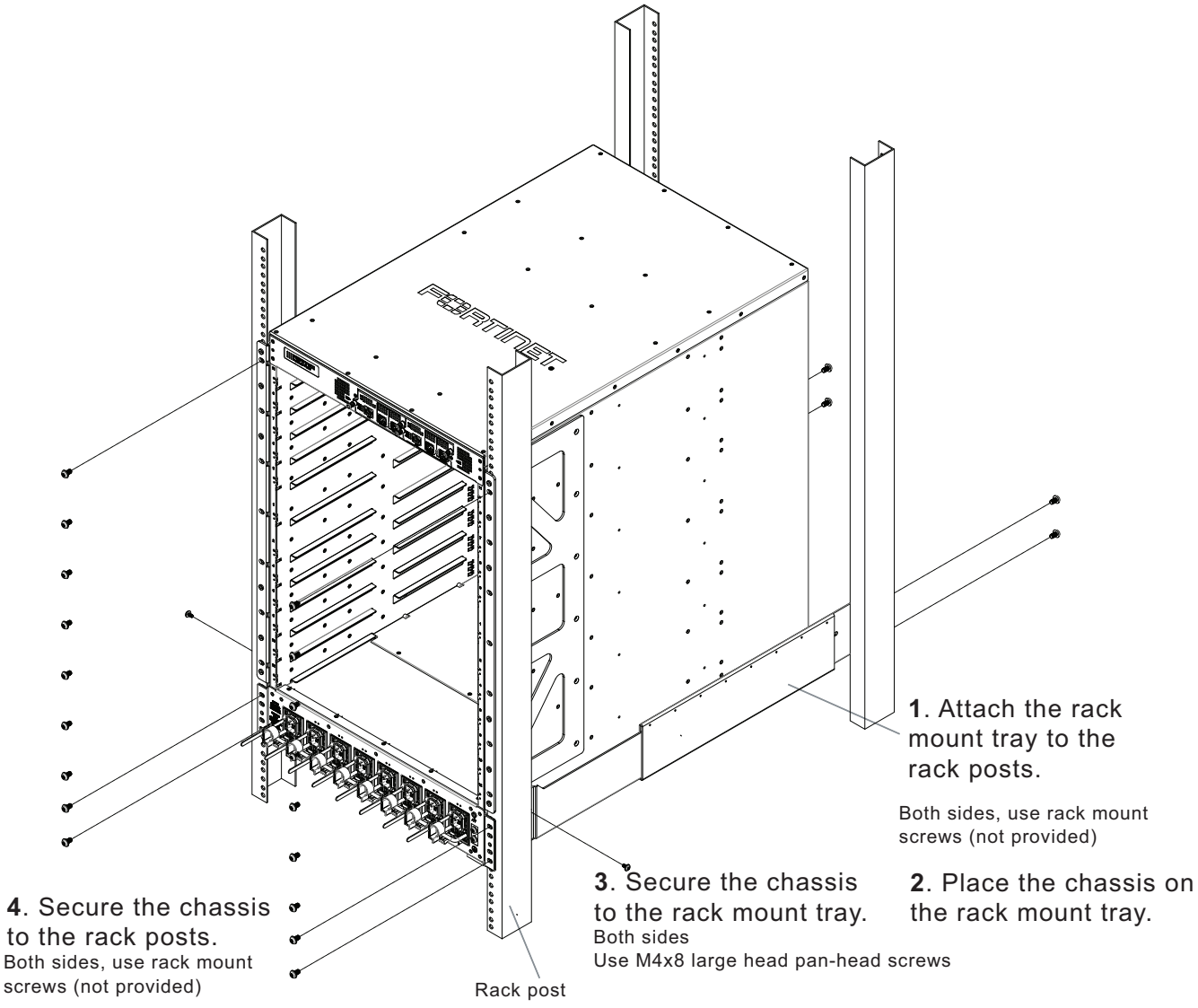
Power cord clamps

You can install power cord clamps onto the front of the chassis beside each PSU. Install the clamps by inserting them into the holes adjacent each PSU. Use the clamps to secure the AC power cords so they are not accidentally disconnected.

Mounting the FortiGate 7121F chassis in a four-post rack

The FortiGate 7121F package includes a set of extendable rack mount trays that you can use to mount the chassis in a 4-post rack. Install the brackets to create a 4-post rack mount tray that the chassis will slide on to. Attach each side of the tray to the 4-post rack as shown below. Make sure you install the tray with enough space above it for the chassis. The length of the tray sides adjusts to match your rack. Once the 4-post rack mount tray has been installed, slide the chassis onto the tray and secure it to the rack mount tray and the rack posts as shown in the diagram.

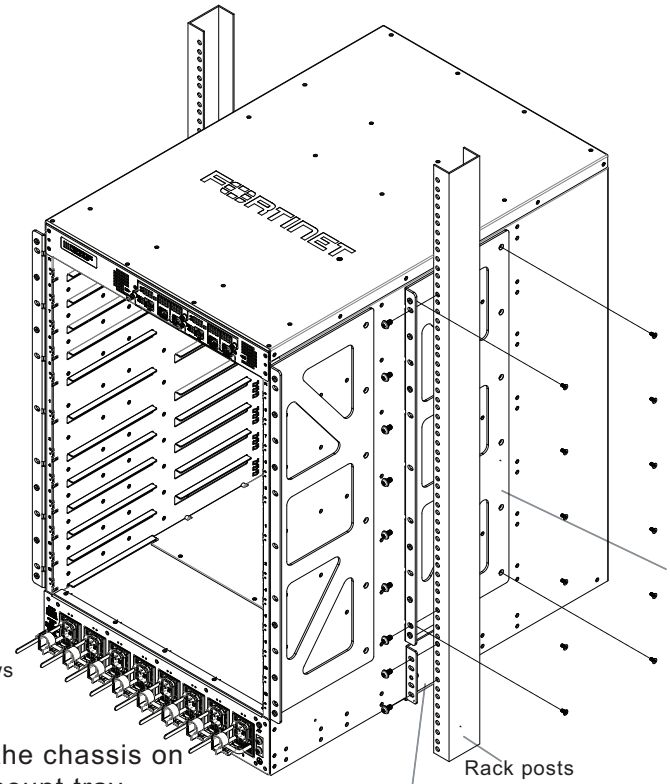
Mounting the chassis in a four-post rack



Mounting the FortiGate 7121F chassis in a two-post rack

The FortiGate 7121F package includes two mid mount trays and two mid-mount brackets that you can use to mount the chassis in a 2-post rack. As shown in the diagram, first attach the mid-mounting brackets to the chassis, them attach the mid mount trays to the rack, making sure to leave enough space above the trays for the chassis. Then place the chassis on the mid-mount tray. Then, use rack mount screws to attach the mid-mount brackets to the rack posts, securing the chassis in the rack.

Mounting the chassis in a 2-post rack



4. Secure the chassis by attaching the mid mounting brackets to the rack posts.
Both sides, use rack mount screws (not provided).

1. Attach the mid mount ears to the chassis
Both sides, use M4x8 flat-head screws.

3. Place the chassis on the mid mount tray.

Rack posts

2. Attach the mid mount tray to the rack posts.
Both sides, use rack mount screws (not provided).

Inserting FIMs and FPMs

All FortiGate 7121F chassis are shipped with a protective front panel installed in the chassis to protect internal chassis components. This panel must be removed before you install FIMs and FPMs.

Insert FIMs into chassis slots 1 and 2. Insert FPMs into chassis slots 3 to 12.

Do not operate the FortiGate 7121F chassis with open slots on the front or back panel. For optimum cooling performance and safety, chassis front panel slots 1 and 2 must contain FIMs or FIM blank panels (also called dummy cards). Front panel slots 3 to 12 must contain FPMs or FPM blank panels. In addition, all cooling fan trays, power supplies or power supply slot covers must be installed while the chassis is operating. The FPM blank panels shipped with the chassis should be kept available in case an FPM is removed from the chassis. If an FIM or FPM fails and you don't have a replacement FIM or FPM or an available blank panel, you should keep the failed FIM or FPM in the chassis slot until you receive a replacement.

To insert FIMs and FPMs, see the guide supplied with the module.

FIM and FPM backplane connectors are shipped with a backplane connector protection label and plastic cover. Before inserting the FIM or FPM module into the chassis slot, remove the label and plastic cover and check the backplane connectors to make sure they are clean and undamaged.

To install an FIM or FPM into a chassis, carefully slide the module all the way into the chassis slot, close the module levers to seat the module into the slot, and tighten the secure screws to make sure the module is fully engaged with the backplane and secured. You must also make sure that the power sliders are fully closed by gently pushing them down.

Installation Highlights:

1. Remove backplane connector protection label.
2. Module levers must be closed.
3. Secure screws must be tightened.
4. Power sliders must be fully closed for the module to get power and start up.

If the module is not receiving power all LEDs remain off.

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

Getting started with FortiGate 7121F

Begin by installing your FortiGate 7121F chassis in a rack and installing FIMs and FPMs in it. Then you can power on the chassis and all modules in the chassis will power up.

Whenever a chassis is first powered on, it takes about 5 minutes for all modules to start up and become completely initialized and synchronized. During this time the FortiGate 7121F will not allow traffic to pass through and you may not be able to log into the GUI or CLI. If you manage to log in, the session could time out as the FortiGate 7121F continues starting up.

Review the PSU, fan tray, System Management Module (SMM), FIM, and FPM LEDs to verify that everything is operating normally. Wait until the chassis has completely started up and synchronized before making configuration changes.

When the chassis has initialized, you have a few options for connecting to the FortiGate 7121F GUI or CLI:

- Log in to the GUI by connecting the MGMT1 interface of the FIM in slot 1 to your network. Then browse to https://192.168.1.99.
- Log in to the CLI by connecting the MGMT1 interface of the FIM in slot 1 to your network. Then use an SSH client to connect to 192.168.1.99.
- Log in to the primary FIM CLI by connecting to the RJ-45 RS-232 Console 1 serial port on the System Management Module (SMM) with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.
- Log in to the primary FIM CLI by connecting to the RJ-45 RS-232 Console serial port on the FIM in slot 1 with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate 7121F 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 7121F 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`

FIM in slot 1	MGMT1: FIM01, 1-mgmt1, default IP address 192.168.1.99/24
FIM in slot 2	MGMT2: FIM02, 2-mgmt1, default IP address 192.168.2.99/24
If you choose to only install one FIM, it should be installed in slot 1.	MGMT1: FIM01, 1-mgmt1, default IP address 192.168.1.99/24

All configuration changes must be made from the primary FIM GUI or CLI and not from the secondary FIM or the FPMs.

Configuring the SLBC management interface

To be able to use FortiGate 7121F special SLBC management interface features, such as being able to log into any FIM or FPM using the management interface IP address and a special port number, you need to use the following command to select a FortiGate 7121F management interface to be the SLBC management interface.

You can use any of the FIM or FPM management interfaces to be the SLBC management interface. The following example uses the MGMT 1 interface of the FIM in slot 1. In the GUI and CLI the name of this interface is 1-mgmt1.

Enter the following command to set the 1-mgmt1 interface to be the SLBC management interface:

```
config global
   config load-balance setting
      set slbc-mgmt-intf 1-mgmt1
   end
```

To manage individual FIMs or FPMs using special management ports, the SLBC management interface must be connected to a network.

The `slbc-mgmt-intf` option is set to `1-mgmt1` by default (but this setting may not be visible in the default configuration). If you decide to use a different management interface, you must also change the `slbc-mgmt-intf` to that interface.

Confirming startup status

Before verifying normal operation and making configuration changes and so on you should wait until the FortiGate 7121F is completely started up and synchronized. This can take a few minutes.

The FortiGate 7121F uses the Fortinet Security Fabric for communication and synchronization between the FIMs and the FPMs and for normal GUI operation. By default, the Security Fabric is enabled and must remain enabled for normal operation.

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

```
diagnose  sys  confsync status | grep in_sy
FIM21FTB21000063, Secondary, uptime=79898.73, priority=2, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FIM21FTB21000068, Primary, uptime=79887.77, priority=1, slot_id=1:1, idx=1, flag=0x0, in_sync=1
FPM20FTB21900165, Secondary, uptime=7252.99, priority=17, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20FTB21900186, Secondary, uptime=79751.32, priority=16, slot_id=1:3, idx=3, flag=0x64, in_sync=1
FPM20FTB21900186, Secondary, uptime=79751.32, priority=16, slot_id=1:3, idx=2, flag=0x4, in_sync=1
FIM21FTB21000063, Secondary, uptime=79898.93, priority=2, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FIM21FTB21000068, Primary, uptime=79887.77, priority=1, slot_id=1:1, idx=1, flag=0x0, in_sync=1
FPM20FTB21900165, Secondary, uptime=7252.99, priority=17, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM21FTB21000063, Secondary, uptime=79898.93, priority=2, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FIM21FTB21000068, Primary, uptime=79887.77, priority=1, slot_id=1:1, idx=1, flag=0x0, in_sync=1
...
```

Multi VDOM mode

By default, when you first start up a FortiGate 7121F it is operating in Multi VDOM mode. The default Multi VDOM configuration includes the **root** VDOM and a management VDOM named **mgmt-vdom**. The management interfaces and the HA heartbeat interfaces are in mgmt-vdom and all 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 you can create LAGs that include the interfaces in mgmt-vdom.

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

Changing data interface network settings

To change the IP address of any FortiGate 7121F 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
```

Changing the FortiGate 7121F log disk and RAID configuration

Each FIM-7941F or FIM-7921F installed in a FortiGate 7121F contains two 4TByte SSD log disks in a RAID-1 configuration. In the RAID-1 configuration, you can use the disks for disk logging only.

You can log into the CLI of each FIM and use the `execute disk` command to view and change the configuration and RAID level of the disks. Changing the configuration or RAID level deletes all data from the disks and can disrupt disk logging. A best practice is set the disk configuration and RAID level when initially setting up the FortiGate 7121F.

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 `execute disk raid status` command to show RAID status.

The following command output shows the RAID status of the 4TByte SSDs configured for RAID-1.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 4000GB

Disk 1: OK Used 3815GB
Disk 2: OK Used 3815GB
```

Resetting to factory defaults

At any time during the configuration process, if you run into problems, you can reset the FortiGate 7121F to factory defaults and start over. From the primary FIM CLI enter:

```
config global
   execute factoryreset
```

Restarting the FortiGate 7121F

To restart all of the modules in a FortiGate 7121F, connect to the primary FIM CLI and enter the `execute reboot` command. When you enter this command from the primary FIM, all of the modules restart.

To restart individual FIMs or FPMs, log in to the CLI of the module to restart and run the `execute reboot` command.

Managing individual FortiGate 7121F FIMs and FPMs

You can manage individual FIMs and FPMs using special port numbers or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate 7121F in an HA configuration.

Special management port numbers

In some cases, you may want to connect to individual FIMs or FPMs 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 FIMs or FPMs in a FortiGate 7121F using the SLBC management interface IP address with a special port number.

You use the following command to configure the SLBC management interface:

```
config global
   config load-balance setting
      set slbc-mgmt-intf <interface>
   end
```

Where <interface> becomes the SLBC management interface.

To enable using the special management port numbers to connect to individual FIMs and FPMs, the SLBC management interface must be connected to a network, have a valid IP address, and have management or administrative access enabled. To block access to the special management port numbers, disconnect the mgmt interface from a network, configure the SLBC management interface with an invalid IP address, or disable management or administrative access for the SLBC management interface.

You can connect to the GUI of CLI of individual FIMs or FPMs using the SLBC management interface IP address followed by a special port number. For example, if the SLBC management interface IP address is 192.168.1.99, to connect to the GUI of the FPM in slot 3, browse to:

`https://192.168.1.99:44303`

The special port number (in this case 44303) is a combination of the service port (for HTTPS, the service port is 443) and the slot number (in this example, 03).

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

The following table lists the special port numbers to use to connect to each FortiGate 7121F slot using common management protocols.

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

For example, to connect to the GUI of the FIM in slot 2 using HTTPS you would browse to https://192.168.1.99:44302.

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

Logging in to different FIMs or FPMs allows you to use dashboard widgets, FortiView, or Monitor GUI pages to view the activity of that FIM or FPM. Even though you can log in to different modules, you can only make configuration changes from the primary FIM; which is usually the FIM in slot 1.

FortiGate 7121F special management port numbers (slot numbers in order as installed in the chassis)

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
11	FPM11	8011	44311	2311	2211	16111
9	FPM09	8009	44309	2309	2209	16109
7	FPM07	8007	44307	2307	2207	16107
5	FPM05	8005	44305	2305	2205	16105
3	FPM03	8003	44303	2303	2203	16103
1	FIM01	8001	44301	2301	2201	16101
2	FIM02	8002	44302	2302	2202	16102
4	FPM04	8004	44304	2304	2204	16104
6	FPM06	8006	44306	2306	2206	16106
8	FPM08	8008	44308	2308	2208	16108
10	FPM10	8010	44310	2310	2210	16110
12	FPM12	8012	44312	2312	2212	16112

HA mode special management port numbers

In HA mode, you use the same special port numbers to connect to FIMs and FPMs in chassis 1 (chassis ID = 1) and different special port numbers to connect to FIMs and FPMs in chassis 2 (chassis ID = 2):

FortiGate 7121F HA special management port numbers

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 11	FPM11	8011	44311	2311	2211	16111
Ch1 slot 9	FPM09	8009	44309	2309	2209	16109
Ch1 slot 7	FPM07	8007	44307	2307	2207	16107
Ch1 slot 5	FPM05	8005	44305	2305	2205	16105

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 3	FPM03	8003	44303	2303	2203	16103
Ch1 slot 1	FIM01	8001	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch1 slot 6	FPM06	8006	44306	2306	2206	16106
Ch1 slot 8	FPM08	8008	44308	2308	2208	16108
Ch1 slot 10	FPM10	8010	44310	2310	2210	16110
Ch1 slot 12	FPM12	8012	44312	2312	2212	16112
Ch2 slot 11	FPM11	8031	44331	2331	2231	16131
Ch2 slot 9	FPM09	8029	44329	2329	2229	16129
Ch2 slot 7	FPM07	8027	44327	2327	2227	16127
Ch2 slot 5	FPM05	8025	44325	2325	2225	16125
Ch2 slot 3	FPM03	8023	44323	2323	2223	16123
Ch2 slot 1	FIM01	8021	44321	2321	2221	16121
Ch2 slot 2	FIM02	8022	44322	2322	2222	16122
Ch2 slot 4	FPM04	8024	44324	2324	2224	16124
Ch2 slot 6	FPM06	8026	44326	2326	2226	16126
Ch2 slot 8	FPM08	8028	44328	2328	2228	16128
Ch2 slot 10	FPM10	8030	44330	2330	2230	16130
Ch2 slot 12	FPM12	8032	44332	2332	2232	16132

Managing individual FIMs and FPMs from the CLI

From any CLI, you can use the `execute load-balance slot manage <slot>` command to log into the CLI of different FIMs and FPMs. You can use this command to view the status or configuration of the module, restart the module, or perform other operations. You should not change the configuration of individual FIMs or FPMs because this can cause configuration synchronization errors.

`<slot>` is the slot number of the slot that you want to log in to.

After you log in to a different module in this way, you can't use the `execute load-balance slot manage` command to log in to another module. Instead, you must use the `exit` command to revert back to the CLI of the component that you originally logged in to. Then you can use the `execute load-balance slot manage` command to log into another module.

Connecting to individual FIM and FPM CLIs of the secondary FortiGate 7121F in an HA configuration

From the primary FIM of the primary FortiGate 7121F in an HA configuration, you can use the following command to log in to the primary FIM of the secondary FortiGate 7121F:

```
execute ha manage <id>
```

Where `<id>` is the ID of the other FortiGate 7121F in the cluster. From the primary FortiGate 7121F, use an ID of 0 to log into the secondary FortiGate 7121F. From the secondary FortiGate 7121F, use an ID of 1 to log into the primary FortiGate 7121F. You can enter the ? to see the list of IDs that you can connect to.

After you have logged in, you can manage the secondary FortiGate 7121F from the primary FIM or you can use the `execute-load-balance slot manage` command to connect to the CLIs of the other FIM and the FPMs in the secondary FortiGate 7121F.

Firmware upgrades

In addition to introducing the basics of upgrading FortiGate 7121F firmware, this section describes how to:

- Upgrade the firmware running on individual FIMs and FPMs.
- Upgrade individual FIM or FPM firmware from the BIOS.

Firmware upgrade basics

All of the FIMs and FPMs in your FortiGate 7121F system run the same firmware image. You upgrade the firmware from the primary FIM GUI or CLI just as you would any FortiGate product.

You can perform a graceful firmware upgrade of a FortiGate 7121F FGCP HA 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 7121F, or FortiGate 7121F HA cluster with `upgrade-mode` set to `simultaneous` interrupts traffic because the firmware running on the FIMs and FPMs 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 FIMs and FPMs in your FortiGate 7121F system. Some firmware upgrades may take longer depending on factors such as the size of the configuration.

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 7121F configuration.

To make sure a FortiGate 7121F firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the FIMs and FPMs 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 7121F before a firmware upgrade and then again after the upgrade to make sure the services continues 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.

Verifying that a firmware upgrade is successful

After a FortiGate 7121F firmware upgrade, you should verify that all of the FIMs and FPMs have been successfully upgraded to the new firmware version.

After the firmware upgrade appears to be complete:

1. Log into the primary FIM and verify that it is running the expected firmware version.
   You can verify the firmware version running on the primary FIM from the System Information dashboard widget or by using the `get system status` command.
2. Confirm that the FortiGate 7121F is synchronized.
   Go to **Monitor > Configuration Sync Monitor** to verify the configuration status of the FIMs and FPMs. You can also use the `diagnose sys confsync status | grep in_sy` command to see if the FIMs and FPMs are all synchronized. In the command output, `in_sync=1` means the FIM or FPM is synchronized. `In_sync=0` means the FIM or FPM is not synchronized, which could indicated the FIM or FPM is running a different firmware build than the primary FIM.
3. Optionally, you can also log into the other FIM and FPMs, and in the same way confirm that they are also running the expected firmware version and are synchronized.

Installing firmware on individual FIMs or FPMs

You can install firmware on individual FIMs or FPMs by logging into the FIM or FPM GUI or CLI. You can also setup a console connection to the FortiGate 7121F front panel SMM and install firmware on individual FIMs or FPMs from a TFTP server after interrupting the FIM or FPM boot up sequence from the BIOS.

Normally you wouldn't need to upgrade the firmware on individual FIMs or FPMs because the FortiGate 7121F keeps the firmware on all of the FIMs and FPMs synchronized. However, FIM or FPM firmware may go out of sync in the following situations:

- Communication issues during a normal FortiGate 7121F firmware upgrade.
- Installing a replacement FIM or FPM that is running a different firmware version.
- Installing firmware on or formatting an FIM or FPM from the BIOS.

To verify the firmware versions on each FIM or FPM you can check individual FIM and FPM GUIs or enter the `get system status` command from each FIM or FPM CLI. You can also use the `diagnose sys confsync status | grep in_sy` command to see if the FIMs and FPMs are all synchronized. In the command output, `in_sync=1` means

the FIM or FPM is synchronized. `In_sync=0` means the FIM or FPM is not synchronized, which could indicated the FIM or FPM is running a different firmware build than the primary FIM.

The procedures in this section work for FIMs or FPMs in a standalone FortiGate 7121F. These procedures also work for FIMs or FPMs in the primary FortiGate 7121F in an HA configuration. To upgrade firmware on an FIM or FPM in the secondary FortiGate 7121F in an HA configuration, you should either remove the secondary FortiGate 7121F from the HA configuration or cause a failover so that the secondary FortiGate 7121F becomes the primary FortiGate 7121F.

In general, if you need to update both FIMs and FPMs in the same FortiGate 7121F, you should update the FIMs first as the FPMs can only communicate through FIM interfaces.

Upgrading the firmware on an individual FIM

During the upgrade, the FIM will not be able to process traffic. However, the other FIM and the FPMs should continue to operate normally.

To upgrade the firmware on a individual FIM from the GUI

1. Connect to the FIM GUI using the SLBC management IP address and the special management port number for that FIM. For example, for the FIM in slot 2, browse to https://<SLBC-management-ip>:44302.
2. Start a normal firmware upgrade. For example,
   a. Go to **System > Firmware** and select **Browse** to select the firmware file to install.
   b. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.
3. After the FIM restarts, verify that the new firmware has been installed.
   You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
4. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.
   FIMs and FPMs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FIM or FPM that is not synchronized, log into the CLI of the FIM or FPM and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support at https://support.fortinet.com.
   If you enter the `diagnose sys confsync status | grep in_sy` command before the FIM has completely restarted, it will not appear in the command output. As well, the Configuration Sync Monitor will temporarily show that it is not synchronized.

To upgrade the firmware on a individual FIM from the CLI using TFTP

1. Put a copy of the firmware file on a TFTP server that is accessible from the SLBC management interface.
2. Connect to the FIM CLI by using an SSH client. For example, to connect to the CLI of the FIM in slot 2, connect to <SLBC-management-ip>:2201.
3. Enter the following command to upload the firmware file to the FIM:
   `execute upload image tftp <firmware-filename> comment <tftp-server-ip-address>`
4. After the FIM restarts, verify that the new firmware has been installed.
   You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
5. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.

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

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

Upgrading the firmware on an individual FPM

Use the following procedure to upgrade the firmware running on a single FPM from the GUI.

During this procedure, the FPM will not be able to process traffic. However, the other FPMs and the FIMs should continue to operate normally.

To upgrade the firmware running on a single FPM from the CLI, see Installing FPM firmware from the BIOS after a reboot on page 56.

1. Connect to the FPM GUI using the SLBC management IP address and the special management port number for that FPM. For example, for the FPM in slot 3, browse to https://<SLBC-management-ip>:44303.
2. Start a normal firmware upgrade. For example,
   a. Go to **System > Firmware** and select **Browse** to select the firmware file to install.
   b. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.
3. After the FPM restarts, verify that the new firmware has been installed.
   You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
4. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.
   FIMs and FPMs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FIM or FPM that is not synchronized, log into the CLI of the FIM or FPM and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support at https://support.fortinet.com.
   If you enter the `diagnose sys confsync status | grep in_sy` command before the FPM has completely restarted, it will not appear in the command output. As well, the Configuration Sync Monitor will temporarily show that it is not synchronized.

Installing FIM firmware from the BIOS after a reboot

Use the following procedure to upload firmware from a TFTP server to an FIM. The procedure involves creating a connection between the TFTP server and one of the FIM MGMT interfaces. You don't have to use a MGMT interface on the FIM that you are upgrading.

This procedure also involves connecting to the FIM CLI using a FortiGate 7121F front panel System Management Module console port. From the console session, the procedure describes how to restart the FIM, interrupt the boot process, and follow FIM BIOS prompts to install the firmware.

During this procedure, the FIM will not be able to process traffic. However, the other FIM and the FPMs should continue to operate normally.

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 FIM MGMT interfaces.
3. Using the console cable supplied with your FortiGate 7121F, connect the SMM Console 1 port on the FortiGate 7121F to the 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. Press Ctrl-T to enter console switch mode.
6. Repeat pressing Ctrl-T until you have connected to the FIM to be updated. Example prompt for the FIM in slot 2:

   `<Switching to Console: FIM02 (9600)>`
7. Optionally log in to the FIM's CLI.
8. Reboot the FIM.

   You can do this using the `execute reboot` command from the CLI or by pressing the power switch on the FIM front panel.
9. When the FIM starts up, follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
10. To set up the TFTP configuration, press C.
11. 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 must not be the same as the FortiGate 7121F 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.
12. To quit this menu, press Q.
13. 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.
14. To start the TFTP transfer, press T.

    The firmware image is uploaded from the TFTP server and installed on the FIM. The FIM then restarts with its configuration reset to factory defaults. After restarting, the FIM configuration is synchronized to match the configuration of the primary FIM. The FIM restarts again and can start processing traffic.
15. Once the FIM restarts, verify that the correct firmware is installed.

    You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
16. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIM or FPM is synchronized.

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

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

Installing FPM firmware from the BIOS after a reboot

Use the following procedure to upload firmware from a TFTP server to an FPM. To perform the upgrade, you must first upload the firmware file to the TFTP server on one of the FIMs.

This procedure also involves connecting to the FPM CLI using a FortiGate 7121F front panel SMM console port, rebooting the FPM, interrupting the boot from the console session, and following FPM BIOS prompts to install the firmware from the FIM TFTP server.

During this procedure, the FPM will not be able to process traffic. However, the other FPMs and the FIMs should continue to operate normally.

1. Set up a TFTP server and copy the firmware file into the TFTP server default folder.
2. Set up your network to allow traffic between the TFTP server and the MGMT1 or MGMT2 interface of one of the FIMs.
3. Log into the CLI of the FIM.
4. Enter the following command to upload the firmware file from the TFTP server to the FIM:
   `execute upload image tftp <firmware-filename> comment <tftp-server-ip-address>`
5. Enter the following command to verify that the firmware file has been uploaded to the FIM:
   `fnsysctl ls /data2/tftproot/`
6. Confirm the internal address of FIM, which is also the address of the FIM's TFTP server:
   `fnsysctl ifconfig base-tftp`
   Example output:
   ```
   base-tftp Link encap:Ethernet HWaddr 06:76:A0:75:E8:F1
   inet addr:169.254.254.1 Bcast:169.254.254.255 Mask:255.255.255.0
   ```
   The internal IP addresses of each FIM and FPM is `169.254.254.<slot-number>`.
7. Using the console cable supplied with your FortiGate 7121F, connect the SMM Console 1 port on the FortiGate 7121F to the USB port on your management computer.
8. 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.
9. Press Ctrl-T to enter console switch mode.
10. Repeat pressing Ctrl-T until you have connected to the module to be updated. Example prompt:
    `<Switching to Console: FPM03 (9600)>`
11. Optionally log into the FPM's CLI.
12. Reboot the FPM.
    You can do this using the `execute reboot` command from the FPM's CLI or by pressing the power switch on the FPM front panel.
13. When the FPM starts up, follow the boot process in the terminal session and press any key when prompted to interrupt the boot process.
14. To set up the TFTP configuration, press C.
15. Use the BIOS menu to set the following. Change settings only if required.
    `[P]: Set image download port`: FIM01 TFTP Server (the FIM that you uploaded the firmware file to).
    `[D]: Set DHCP mode`: Disabled.
    `[I]: Set local IP address`: The internal IP address of the FPM. For example, if you are installing firmware on the FPM in slot 5, the local IP address of the FPM in slot 5 is 169.254.254.5.
    `[S]: Set local Subnet Mask`: 255.255.255.0.

`[G]: Set local gateway`: 169.254.254.1.

`[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 internal IP address of the FIM that you uploaded to the firmware file to. For example: 169.254.254.1 for the FIM in slot 1.

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

16. To quit this menu, press Q.
17. 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.
18. To start the TFTP transfer, press T.

    The firmware image is uploaded from the TFTP server of the FIM and installed on the FPM. The FPM then restarts with its configuration reset to factory defaults. After restarting, the FPM configuration is synchronized to match the configuration of the primary FPM. The FPM restarts again and can start processing traffic.
19. Once the FPM restarts, verify that the correct firmware is installed.

    You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
20. Verify that the configuration has been synchronized.

    The following command output shows example FortiGate-7000 sync status. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM21FTB21000068, Secondary, uptime=210445.62, priority=2, slot_id=1:1, idx=1, flag=0x0, in_sync=1
FIM21FTB21000063, Primary, uptime=351403.75, priority=1, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FPM20FTB20990039, Secondary, uptime=351253.83, priority=18, slot_id=1:5, idx=2, flag=0x64, in_sync=1
FPM20FTB20990047, Secondary, uptime=352.27, priority=16, slot_id=1:3, idx=3, flag=0x64, in_sync=1
FPM20FTB20990078, Secondary, uptime=227839.73, priority=17, slot_id=1:4, idx=4, flag=0x64, in_sync=1
FPM20FTB20990091, Secondary, uptime=351248.85, priority=22, slot_id=1:9, idx=5, flag=0x64, in_sync=1
FPM20FTB20990095, Secondary, uptime=351240.13, priority=20, slot_id=1:7, idx=6, flag=0x64, in_sync=1
FPM20FTB21900096, Secondary, uptime=351272.50, priority=24, slot_id=1:11, idx=7, flag=0x64, in_sync=1
FPM20FTB21900179, Secondary, uptime=351247.07, priority=19, slot_id=1:6, idx=8, flag=0x64, in_sync=1
FPM20FTB21900182, Secondary, uptime=351242.02, priority=25, slot_id=1:12, idx=9, flag=0x64, in_sync=1
FPM20FTB21900203, Secondary, uptime=351228.51, priority=21, slot_id=1:8, idx=10, flag=0x64, in_sync=1
FPM20FTB21900211, Secondary, uptime=351252.93, priority=23, slot_id=1:10, idx=11, flag=0x64, in_sync=1
FPM20FTB20990047, Secondary, uptime=351252.27, priority=16, slot_id=1:3, idx=2, flag=0x4, in_sync=1
FIM21FTB21000063, Primary, uptime=351403.75, priority=1, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FIM21FTB21000068, Secondary, uptime=210445.62, priority=2, slot_id=1:1, idx=1, flag=0x0, in_sync=1
FPM20FTB20990078, Secondary, uptime=227839.73, priority=17, slot_id=1:4, idx=2, flag=0x4, in_sync=1
```

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

    The command output also shows that the uptime of the FPM in slot 3 is lower than the uptime of the other modules, indicating that the FPM in slot 3 has recently restarted.

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

Synchronizing FIMs and FPMs after upgrading the primary FIM firmware from the BIOS

After you install firmware on the primary FIM from the BIOS after a reboot, the firmware version and configuration of the primary FIM will most likely be not be synchronized with the other FIMs and FPMs. You can verify this from the primary FIM CLI using the `diagnose sys confsync status | grep in_sy` command.

```
FortiCarrier-7000F [FIM01] (global) # diagnose  sys confsync status | grep in_sy
FIM21FTB21000063, Secondary, uptime=327.36, priority=2, slot_id=1:2, idx=0, flag=0x0, in_sync=1
FIM21FTB21000068, Primary, uptime=327729.56, priority=1, slot_id=1:1, idx=1, flag=0x0, in_sync=0
FPM20FTB21900165, Secondary, uptime=327578.35, priority=17, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20FTB21900168, Secondary, uptime=327527.53, priority=24, slot_id=1:11, idx=3, flag=0x64, in_sync=0
FPM20FTB21900170, Secondary, uptime=327520.91, priority=18, slot_id=1:5, idx=4, flag=0x64, in_sync=1
FPM20FTB21900179, Secondary, uptime=327556.85, priority=19, slot_id=1:6, idx=5, flag=0x64, in_sync=1
FPM20FTB21900182, Secondary, uptime=327579.41, priority=25, slot_id=1:12, idx=6, flag=0x64, in_sync=1
FPM20FTB21900186, Secondary, uptime=327559.41, priority=16, slot_id=1:3, idx=7, flag=0x64, in_sync=1
FPM20FTB21900189, Secondary, uptime=327591.45, priority=22, slot_id=1:9, idx=8, flag=0x64, in_sync=1
...
```

You can also verify synchronization status from the primary FIM Configuration Sync Monitor.

To re-synchronize the FortiGate 7121F, which has the effect of resetting the other FIM and the FPMs, re-install firmware on the primary FIM.

You can also manually install firmware on each individual FIM and FPM from the BIOS after a reboot. This manual process is just as effective as installing the firmware for a second time on the primary FIM to trigger synchronization to the FIM and the FPMs, but takes much longer.

1. Log into the primary FIM GUI.
2. Install a firmware build on the primary FIM from the GUI or CLI. The firmware build you install on the primary FIM can either be the same firmware build or a different one.

   Installing firmware synchronizes the firmware build and configuration from the primary FIM to the other FIM and the FPMs.
3. Check the synchronization status from the Configuration Sync Monitor or using the `diagnose sys confsync status | grep in_sy` command.

FortiGate 7121F System Management Module

The FortiGate 7121F chassis includes two System Management Modules (SMMs) or shelf managers, located at the top of the chassis front panel. The SMMs are factory installed and configured and are not field replaceable.

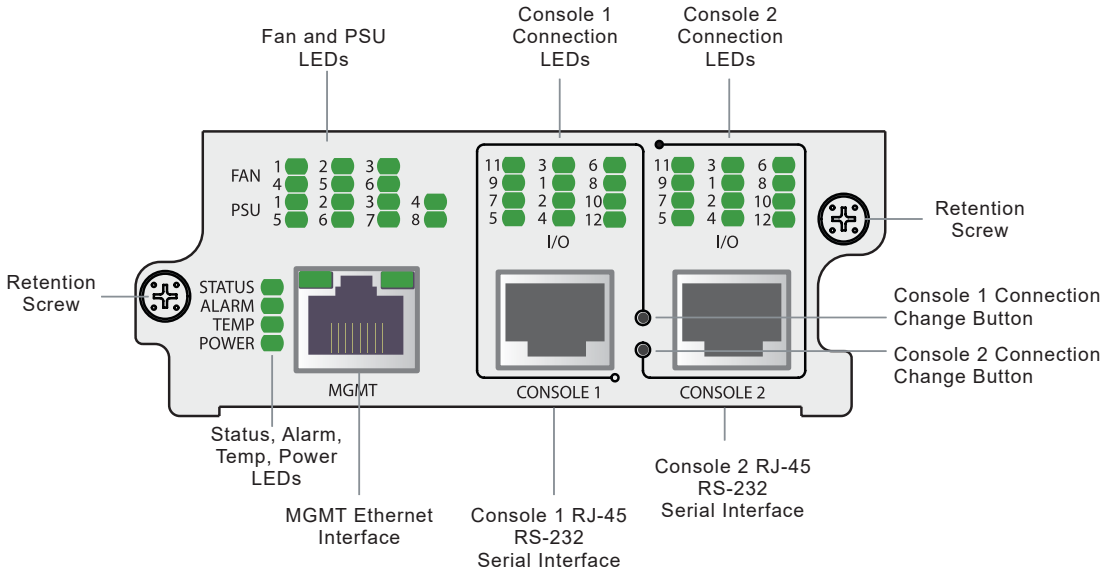
The SMMs operate in an active-passive redundant configuration. By default, when the system starts up the SMM in slot M2 is active and the SMM in slot M1 is passive. The active SMM always has IPMB address 0x20 and the passive SMM always has IPMB address 0x22. Active and passive refers to the SMM that is controlling the chassis. The MGMT interfaces and console ports on both SMMs are always available if the SMM is operating.

If the passive SMM fails, the chassis just keeps operating with the active SMM. If the active SMM fails, the passive SMM becomes active.

The active SMM synchronizes the following data to the passive SMM:

- Chassis state and chassis policy
- LAN parameters for each LAN channel, including, the IP address, gateway IP address, channel enable status, local interface/non-local interface setting, and the session support flag.

FortiGate 7121F SMM front panel



The active SMM communicates with module SMCs in the chassis, each of which is responsible for local management of one or more Field Replaceable Units (FRUs), including FIM and FPM modules, fan trays, and power supplies. Management communication within a chassis occurs over the Intelligent Platform Management Bus (IPMB).

The active SMM includes LED indicators that report on the status of many of the chassis components, including fan trays and power supplies. You can also use the SMM console ports to connect to the SMM CLI and to the CLI of the modules in chassis slots 1 to 12.

The active SMM controls chassis power allocation, monitors chassis operating parameters, monitors and controls chassis cooling, and generates alarms if the chassis encounters problems. All FIM and FPM modules installed in the chassis communicate with the active SMM through the module's IPMB. FIM and FPM module power on/off requires

authorization from the active SMM and the active SMM controls the power supplied by the chassis power systems to the modules.

Each module in the chassis includes its own module Shelf Manager Controller (SMC) Serial Debug Interface (SDI) or SMC SDI console that communicates with the SMM SMC SDI. You can connect a serial cable to the active SMM console ports to connect to the SMM SMC SDI and to connect to each module's SMC SDI console. You can also interact with the SMC SDI consoles using an Intelligent Platform Management Interface (IPMI) tool.

System Management Module failure

If one or both of the SMMs fails, you should RMA the chassis. The chassis and the modules in it will continue to operate with one or no functioning SMMs until you can replace the chassis. If there is no functioning SMM, the chassis fans operate at maximum speed and the FIM and FPM modules in the chassis switch to standalone mode and manage their own power.

System Management Module LEDs

The following table describes the SMM LED indicators:

FortiGate 7121F SMM LEDs

LED	State	Description
Status	Off	The SMM is powered off or not initialized.
	Solid red	The SMM is not operating normally either because it is starting up or because it has failed.
	Blinking red	The active SMM cannot communicate with the passive SMM.
	Solid green	The SMM has started up and is operating normally.
	Blinking green	The SMM is passive.
Alarm	Off	No alarms
	Red	One or more analog sensors in the chassis or on a module in the chassis (other than PSUs) 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	One or more analog sensors in the chassis or on a module in the chassis (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.

LED	State	Description
Temp	Solid green	All temperature sensors indicated acceptable operating temperatures.
	Blinking green	At least one temperature sensor is detecting a high temperature outside of the normal operating range. In this case an upper non-critical (UNC) temperature. The SMM increases fan speed to increase cooling and reduce the temperature.
	Blinking red	At least one temperature sensor is detecting a temperature outside of the acceptable operating range. In this case an upper critical (UC) temperature. The SMM increases fan speed to the maximum level. This also indicates possible problems with the cooling system and could mean that the ambient temperature is too high. Also causes a major or critical (CR) alarm.
	Solid red	At least one temperature sensor is detecting a temperature outside of the allowed operating range. In this case an upper non-recoverable (UNR) temperature. The SMM increases fan speed to the maximum level. The temperature is high enough to potentially cause physical damage. Also causes a critical or non-recoverable (NR) alarm.
Power	Solid green	Normal operation.
	Blinking green	Chassis 12V disabled. This means that the administrator has entered commands into the SMM CLI to power off the PSU main 12V outputs. All fans, FIM and FPM modules are completely powered off but the SMM is still running.
	Red	Chassis 12V enabled but not OK. This means the SMM has enabled the main 12V outputs for all chassis components, but the power OK (PWOK) signal of at least one PSU has not been sent. When a PSU is powering up, it would be normal for this LED to be red for a second (before PSU outputs are stabilized), but if LED remains red, it indicates a problem (such as a failed PSU). SMM or FIM or FPM module voltage sensors would most likely also trigger alarms if this happens since the PSUs may not be delivering enough power.
FAN (LEDs for each of six fan trays)	Off	Fan tachometer sensors disabled. This could happen if the administrator disabled them from the SMM CLI.
	Green	The fan tray is operating normally.
	Red	A fan tachometer sensor in this fan tray has registered an alert because a critical or non-recoverable (NR) threshold has been crossed.
PSU	Off	The PSU is not installed in the chassis.
	Green	The PSU is present and operating normally.
	Blinking red	The PSU module is installed but no power is being delivered (not plugged in).
	Red	The PSU's sensors have detected an alert condition. The PSU's analog sensors crossed critical or non-recoverable (NR) thresholds, or the PSU Status Failure bit has been set.
Console 1 and 2	Off	This console port is not connected or is connected to the SMM SMM CLI.
	Green	This console port is connected to this module host console in this chassis slot.
	Amber	This console port is connected to this module's SMC console.

About SMM alarm levels

Minor, major, and critical alarms are defined based on both IPMI, ATCA, and Telco standards for naming alarms.

- A minor alarm (also called an IPMI non-critical (NC) alarm) indicates that a temperature or a power level was detected by a sensor that is outside of the normal operating range but is not considered a problem. In the case of a minor temperature alarm the system could respond by increasing fan speed. A non-critical threshold can be an upper non-critical (UNC) threshold (for example, a high temperature or a high power level) or a lower non-critical (UNC) threshold (for example, a low power level).
- A major alarm (also called an IPMI critical or critical recoverable (CR) alarm) indicates a temperature or power level was detected by a sensor that is far enough outside of the normal operating range to require attention from the operator. It could also mean that the system itself cannot correct the alarm. For example, the cooling system cannot provide enough cooling to reduce the temperature. It could also mean that conditions are close to being outside of the allowed operating range. For example, the temperature is close to exceeding the allowed operating temperature. A critical threshold can also be an upper critical (UC) threshold (for example, a high temperature or a high power level) or a lower critical (LC) threshold (for example, a low power level).
- A critical alarm (also called an IPMI non-recoverable (NR) alarm) indicates a temperature or power level was detected by a sensor that is outside of the allowed operating range and could potentially cause physical damage.

You can use the SMM CLI to get details about alarm sensors, thresholds, and the events that trigger alarms.

Using the console ports

The active SMM includes two console ports named Console 1 and Console 2 that can be used to connect to any serial console in the chassis. This includes the SMM CLI, the FortiOS CLIs (also called host CLIs) of the FIM and FPM modules in chassis slots 1 to 12 and all of the SMC SDI consoles in the chassis.

The FIMs, FPMs, and SMM, all have an SMC SDI console. These consoles are used for low level programming of the module using an IPMI tool and are disabled by default. You can enable serial access to individual SMC SDI consoles from the SMM SMC SDI CLI using the command `serial set sdi enable <slot>`. During normal operation you may want to access the SMM SMC SDI CLI, you shouldn't normally require access to individual FIM and FPM SMC SDI consoles.

By default when the chassis first starts up Console 1 is connected to the FortiOS CLI of the FIM module in slot 1 and Console 2 is disconnected.

The default settings for connecting to each console port are: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

The FIMs and FPMs use the standard FortiOS CLI. The SMC SDI CLIs are described in this chapter.

You can use the console connection change buttons to select the CLI that each console port is connected to.

- Press the button to cycle through the FIM and FPM FortiOS CLIs and disconnect this console.
- Press and hold the button to connect to the SMM SMC SDI CLI. You can also cycle through each module's SMC SDI CLI if they are enabled.

The console's LEDs indicate what it is connected to. If no LED is lit the console is either connected to the SMM SMC SDI console or disconnected. Both console ports cannot be connected to the same CLI at the same time. If a console button

press would cause a conflict that module is skipped. If one of the console ports is disconnected then the other console port can connect to any CLI.

If you connect a PC to one of the SMM console ports with a serial cable and open a terminal session you begin by pressing Ctrl-T to enable console switching mode, then you can do the following:

- Press Ctrl-T multiple times to cycle through the FIM and FPM module FortiOS CLIs (the new destination is displayed in the terminal window). If you press Ctrl-T after connecting to the FPM module in slot 6 the console is disconnected. Press Ctrl-T again to start over again at slot 1.
- Press Ctrl-R multiple times to cycle through the FIM and FPM module SMC SDI CLIs if they are enabled (the new destination is displayed in the terminal window). After cycling through all of the enabled SMC SDI CLIs the next press of Ctrl-R disconnects the console port.

Once the console port is connected to the CLI that you want to use, press Enter to enable the CLI and log in. The default administrator account for accessing the FortiOS CLIs is `admin` with no password. The default administrator account for the SMC SDI CLIs is `admin`/`admin`.

When your session is complete you can press Ctrl-T until the prompt shows you have disconnected from the console.

Connecting to the FortiOS CLI of the FIM in slot 1

Use the following steps to connect to the FortiOS CLI of the FIM in slot 1:

1. Using the console cable supplied with your FortiGate 7121F, connect the SMM Console 1 port on the FortiGate 7121F to the USB port on your management computer.
2. 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.
3. Press Ctrl-T to enter console switch mode.
4. Repeat pressing Ctrl-T until you have connected to slot 1. Example prompt:
   ```
   <Switching to Console: FIM01 (9600)>
   ```
5. Login with an administrator name and password.
   The default is `admin` with no password.
   For security reasons, it is strongly recommended that you change the password.
6. When your session is complete, enter the `exit` command to log out.

Connecting to the FortiOS CLI of the FIM in slot 2

Use the following steps to connect to the FortiOS CLI of the FIM in slot 2:

1. Using the console cable supplied with your FortiGate 7121F, connect the SMM Console 1 port on the FortiGate 7121F to the USB port on your management computer.
2. 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.
3. Press Ctrl-T to enter console switch mode.
4. Repeat pressing Ctrl-T until you have connected to slot 2. Example prompt:
   ```
   <Switching to Console: FIM02 (9600)>
   ```

5. Login with an administrator name and password.
   The default is `admin` with no password.
   For security reasons, it is strongly recommended that you change the password.
6. When your session is complete, enter the `exit` command to log out.

Connecting to the SMC SDI CLI of the FPM in slot 3

Use the following steps to connect to the FortiOS CLI of the FPM in slot 3:

1. Using the console cable supplied with your FortiGate 7121F, connect the SMM Console 1 port on the FortiGate 7121F to the USB port on your management computer.
2. 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.
3. Press Ctrl-T to enter console switch mode.
4. Press Ctrl-R to switch to the SMM SMC SDI CLI switching mode.
5. Repeat pressing Ctrl-R until you have connected to slot 3. Example prompt:
   `<Switching to Console: FPM03-MC (9600)>`
6. Login with an administrator name and password.
   The default administrator name and password are `admin`/`admin`.
   For security reasons, it is strongly recommended that you change the password.
7. You can begin entering commands at the `admin@FPM03-MC #` prompt.
8. When your session is complete, enter the `exit` command to log out.

Changing the SMM admin account password

Use the following procedure to change the SMM admin account password.

1. Enter the following command to show all users and their user IDs.
   `user list`
   The output should show that the `admin` user has a user ID of 2.
2. Use the command `user set password <user-id> [<password>]` to add a password for the admin account. For example:
   `user set password 2 <password>`
3. Enter and confirm a new password for the `admin` account.
   The password should be between 5 and 20 characters long and should include a combination of upper and lower case letters and numbers.
   You can change the admin account password at any time.

FortiGate 7121F chassis slots IPMB addresses

The following table lists the IPMB addresses of the FortiGate 7121F chassis slots.

Chassis slot number	Name	IPMB Address (FRUID)
SMM 1	MGMT1	if active 0x20, if passive (the default) 0x22
SMM 2	MGMT2	if active (the default) 0x20, if passive 0x22
11	FPM11	0x96
9	FPM9	0x92
7	FPM7	0x8E
5	FPM5	0x8A
3	FPM3	0x86
1	FIM1	0x82
2	FIM2	0x84
4	FPM4	0x88
6	FPM6	0x8C
8	FPM8	0x90
10	FPM10	0x94
12	FPM12	0x98

You can use the IPMB address or chassis slot number to reference a chassis slot when entering commands in the SMM CLI. For example, enter either of the following commands to display sensor readings for the FIM in slot 2:

```
sensor 0x84
sensor 2
```

When command syntax descriptions in this chapter include the <slot> variable you can replace it with a slot number (1 to 12) or an IPMB address number (0x82 to 0x98).

Rebooting an FIM or FPM from the SMC SDI CLI

A common use of the SMC SDI CLI is being able to remotely reboot a FIM or FPM.

From any SMC SDI CLI use the following command to reboot the FPM in slot 3:

```
mc reset 3 warm
```

Use the following command to power off the FPM in slot 4:

```
fru deactivate 4
```

Use the following command to power on the FIM in slot 2 (IPMI address 0x84):

```
fru activate 0x84
```

Comlog

All FIM and FPM SMCs include a comlog system for writing and saving console log messages. When enabled, the comlog saves log messages in a local comlog file. Log messages include all local host console messages including BIOS boot up messages. In the comlog these messages include the following headers:

Header	Cause
\n--- COMLOG SYSTEM BOOT: YYYY/MM/DD hh:mm:ss ---\n	The module is starting up after being powered on or reset.
\n--- COMLOG DISABLED: YYYY/MM/DD hh:mm:ss ---\n	Logging is disabled.
\n--- COMLOG ENABLED: YYYY/MM/DD hh:mm:ss ---\n	Logging is enabled
\n--- COMLOG TIME: YYYY/MM/DD hh:mm:ss ---\n	This message is written every hour when the module is powered on and logging is enabled.

The following comlog-related CLI commands are available:

Description	SMC CLI Commands	IPMI commands

Display comlog information. Available on the passive module.	`comlog getinfo`
	`Status Disabled`
	`COM Speed 9600`
	`Storage Size 0x00400000`
	`Log Start 0x00000000`
	`Log End 0x00000C37`
	`Log Size 3127 Bytes`	

Display a module's comlog. Available on the passive module.	`comlog getinfo <slot>` `comlog print <slot>`	`fortinetoem comlog getinfo` `fortinetoem comlog print`
Clear a module's comlog. Either by resetting the a comlog start location in flash (reset_loc) or erasing all of the flash storage (chip_erase). Available on the passive module.	`comlog clear [reset_loc] [chip_erase]`	`fortinetoem comlog clear`
Disable a module's comlog. Available on the passive module.	`comlog disable`	`fortinetoem comlog clear`
Enable comlog. Available on the passive module.	`comlog enable`	`fortinetoem comlog clear`
Set comlog baud rate. `<speed>` can be 9600, 19200, 38400,57600, 115200, or expressed as level 1 to 4. Available on the passive module.	`comlog setbaud <speed>`	`fortinetoem comlog setbaud <speed>`

System event log (SEL)

The SMC in each FIM and FPM generates system event log (SEL) messages that record system events as they occur. All SEL messages are stored by individual FIM and FPM SMCs. They are also all collected and stored by the SMM SMC. From the SMM you can use the following commands from the active or passive SMM to view and clear SEL messages.

Operation	SMC CLI Commands	IPMI Commands

Display the local SEL for a module.	`sel <slot>`	`sel list`
		`sel elist`
		`-v sel list`

Clear the local SEL.	`sel clear`	`sel clear`
Get SEL information.	N/A	`sel info`
Get SEL time	`time get`	`sel time get`
Set SEL time	`time set <yyyy/mm/dd hh:mm:ss>`	`sel time set`

Sensor data record (SDR)

The sensor data record (SDR) contains static information about the sensors in all parts of the chassis including the FIMs and FPMs. Information includes the Sensor ID string, sensor type, sensor event/reading type, entity ID, entity instance, sensor unit, reading linearization parameters, sensor thresholds, and so on. The following commands display information stored in the SDR.

Operation	SMC CLI Commands	IPMI Commands

Display current local sensor values and sensor SDRs or sensor thresholds for a module. Available on the passive module.	`sensor <slot>`
	`sensor_thresholds <slot>`
		`sensor`
		`sensor hexlist`
		`sdr list`
		`sdr elist`
		`-v sdr list`
		(`-v` required when using the Windows command prompt)

Set Sensor thresholds	N/A	`sensor thres help` (use this command to display online help for setting sensor thresholds)

Common SMM CLI operations

The following table lists many of the operations you can perform from the SMM CLI and the commands you use to perform them. Only a subset of these commands are available on the passive SMM as indicated below. Also, the

<slot> option is not available on the passive SMM.

Action	SMC CLI Commands	IPMI Commands
Log into the CLI.	Ctrl-R	N/A
Log out of the CLI. Available on the passive module.	exit (followed by Ctrl-R)	N/A
Display all commands. Available on the passive module.	help	help
Display information about all SMC firmware in the chassis.	info	mc info
Display SMC device ID, Build Date/Number, SMC firmware information, address info, entity map for the device in the slot. Available on the passive module.	info <slot>	N/A
Switching active SMM. The active SMM becomes passive and the passive becomes active. Available on the passive module.	smm_switch	N/A
Display status, power budget and hot swap state for all modules. Available on the passive module.	status	N/A
List the IPMI channels.	channel list	channel info [<channel-number>]
Change the SDI verbosity level. <level> can be: 0: Alerts + Errors 1: Alerts + Errors + Verbose + Low-Level	verbose <level>	N/A

Action	SMC CLI Commands	IPMI Commands
Errors 2: Alerts + Errors + Verbose + Low-Level Errors + PI traffic 3: Alerts + Errors + Verbose + Low-Level Errors + PI traffic + IPMB traffic + LAN Interface traffic 4: Same as 3		
Display the SMM time. Available on the passive module.	`time get`	`sel time get`
Set the SMM time. Available on the passive module.	`time set <yyy/mm/dd hh:mm:ss>`	`sel time set <yyy/mm/dd hh:mm:ss>`
Synchronize all module SMC times.	`time sync`	N/A
List SMM user accounts. Available on the passive module.	`user list`	`user list [<channel number>]`
Disable a user account. Available on the passive module.	`user disable <user-id>`	`user disable <user-id>`
Enable a user account. Available on the passive module.	`user enable <user-id>`	`user enable <user-id>`
Set a user account user name. Available on the passive module.	`user set name <user-id> <name>`	`user set name <user-id> <name>`
Set a user account password. Available on the passive module.	`user set password <user-id> <password>`	`user set password <user-id> <password>`
Set the privilege level that a user account has for a specified session-based	`user priv <user-id> {callback | user | operator | administrator | no_access} [<channel>]`	`user priv <user id> <privilege level> [<channel number>]`

Action	SMC CLI Commands	IPMI Commands
IPMI <channel>. If a <channel> is not specified the privilege level is set for all IPMI channels. Available on the passive module.		
View a summary of users.	N/A	`user summary`
User test command.	N/A	`user test`
Display the SMM serial interface settings. Available on the passive module.	`serial print`	N/A
Set the SDI baud rate. Available on the passive module.	`serial set sdi baud <speed>`	N/A
Set the sniff baud rate when the console is disabled. Available on the passive module.	`serial set sdi default_sniff_baud <speed>`	N/A
Enable a console connection from the SMM to another module.	`serial set sdi enable <slot>`	N/A
Disable the console connection between the SMM and another module. Available on the passive module.	`serial set sdi disable <slot>`	N/A
Cold or warm reset a module.	`mc reset <slot> cold` `mc reset <slot> warm`	`mc reset cold` `mc reset warm`
Run a module self test.	N/A	`mc selftest`
Power on a module.	`fru activate <slot> [<fruid>]`	`picmg activate`
Power off a module.	`fru deactivate <slot> [<fruid>]`	`picmg deactivate`
Reset a module.	`fru reset <slot> [<fruid>]`	`picmg reset`
Power cycle the	N/A	`chassis power cycle`

Action	SMC CLI Commands	IPMI Commands
chassis		
Get chassis sttatus	N/A	`chassis status`
Display the LAN configuration. Available on the passive module.	`lan print <channel>`	

Set LAN configuration. The `kgkey` and `krkey` options are used for RCMP+.	`lan set <channel> ipaddr <ip> [<netmask>]`
	`lan set <channel> macaddr <mac>`
	`lan set <channel> defgw ipaddr <ip>`
	`lan set <channel> defgw macaddr <mac>`
	`lan set <channel> kgkey <value>`
	`lan set <channel> krkey <value>`
		`lan set help`
		(use this command to display online help for LAN settings)

Enable or disable all LAN interfaces.	`lan disable <channel>` `lan enable <channel>`	`fortinetoem param set 0 1` `fortinetoem param set 0 0`

Set fan levels. Change or switch the active fan set.	`fan_min_level <level>`
	`fan_max_level <level>`
	`<level>` range is 0 - 20.
		N/A

Change LED settings.	N/A	`picmg led set help` (use this command to display online help for LED settings)
Display HPM.1 status.	N/A	`hpm check`
Run an HPM.1 upgrade.	N/A	`hpm upgrade <.img> hpm upgrade <.img> all activate`

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).

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.

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.

Skilled person must install the equipment.

L'équipement doit être installé par une personne qualifiée

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.

Warning: A UL Listed external disconnect device, i.e. circuit breaker or other, with over current protection suitable for local code(Generation 1 rated 200-240V, 10A recommended. Generation 2 rated 200-240V, 16A recommended.) shall be installed with this equipment.

Avertissement: Un dispositif de déconnection externe homologué UL, exemple d'un disjoncteur ou autre, avec des protections de surintensité appropriées (Génération 1 nominal 200-240V, 10A recommandé. Génération 2 nominal 200-240V, 16A recommandé.) à l'installation de ce matériel.

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.

Regulatory notices

Federal Communication Commission (FCC) – USA

This device complies with Part 15 of the 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。

請仔細閱讀以下說明

本設備勿置於潮濕處。

連接至電源前, 請先檢查電壓。

當設備不用時, 請將所有電源線拔除, 避免電壓不穩而造成傷害。

勿將任何液體濺入設備中, 避免線路短路。

基於安全理由, 只有受到專業訓練的從業人員, 才可以打開本設備。

請勿自行調整或修理已通電的設備, 以確保您的安全。

如不小心受傷, 請立刻找急救人員給予您適當的救護, 千萬別因傷勢輕微而忽略自己的傷勢。

請依照台灣法規處置電池。

若不正確替換電池可能導致爆炸危險, 替換電池時, 請使用設備生產商推薦使用的電池。

請勿拆卸、刺穿或以其他方式損壞電池。

雷射設備非用戶維修設備, 請與生產商聯繫維修事宜。

注意: 要斷開電源, 請將所有電源線從本機上拔下

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

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。这种情况下，可能需要用户对其采取切实可行的措施。

Agência Nacional de Telecomunicações (ANATEL) – Brazil (for the FortiGate 7121F AC model)

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.