FortiGate-7040E System Guide

FortiGate-7000E 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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 4, 2021
FortiGate-7040E 6.4.2 System Guide
01-642-374321-20210104

TABLE OF CONTENTS

Change log

Date	Change description
January 4, 2021	Added more information about using and retaining the FIM and FPM blank panels to FortiGate-7040E front panel on page 6 and Chassis hardware information on page 10. Added the FPM-7630E, see FPM-7630E on page 8.
June 22, 2020	Changes to Cooling fans, cooling air flow, and minimum clearance on page 12.
June 22, 2020	Changes to Cooling fans, cooling air flow, and minimum clearance on page 12. Updated power consumption information in Physical description of the FortiGate-7040E chassis on page 11. Updated console cable descriptions to reflect that the FortiGate-7040 is now shipped with USB to RJ-45 RS-232 console cables. Other minor changes.
April 13, 2020	Updated console cable descriptions to reflect that the FortiGate-7040 is now shipped with USB to RJ-45 RS-232 console cables. Other minor changes.
March 20, 2020	Renamed management module to System Management Module (SMM). Corrections to Connecting to the SMM using an IPMI tool on page 50.
February 24, 2020	Corrections to the 4-post and 2-post rack mount diagrams.
February 21, 2020	Added DC terminal rings and information about included DC cables. See Optional accessories and replacement parts on page 11 and DC PSUs and supplying DC power to the chassis on page 15.
October 29, 2019	Misc changes throughout.
October 23, 2019	Misc changes throughout.
October 16, 2019	Restructuring and bug fixing.

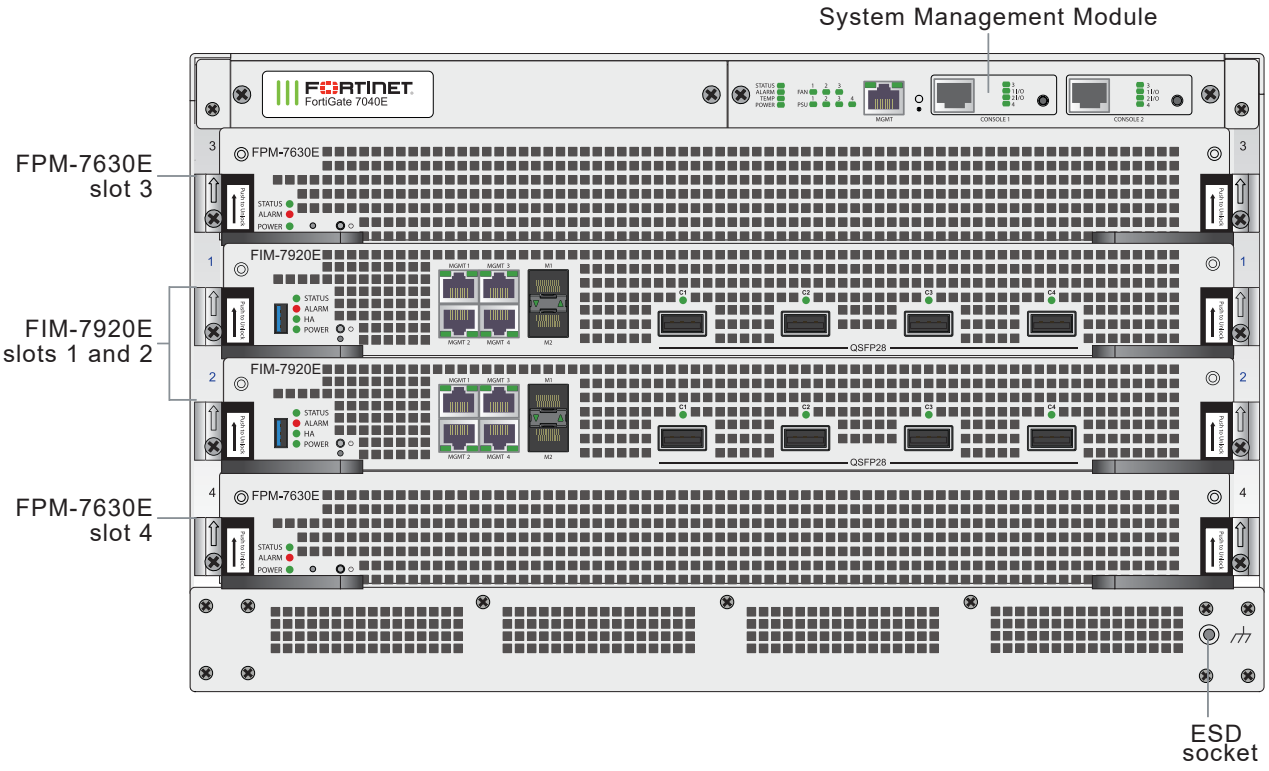
FortiGate-7040E chassis

The FortiGate-7040E is a 6U 19-inch rackmount 4-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots. Power is provided to the chassis using three hot swappable 2+1 redundant 100-240 VAC, 50-60 Hz power supply units (PSUs). You can also optionally add a fourth PSU. The FortiGate-7040E can also be equipped with three or four DC PSUs allowing you to connect the chassis to -48V DC power.

FortiGate-7040E front panel

The FortiGate-7040E chassis is managed by a single System Management Module (SMM) that includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The SMM controls chassis cooling and power management and provides an interface for managing the FIMs and FPMs installed in the chassis. The standard configuration of the FortiGate-7040E includes two FIMs (interface modules) in chassis slots 1 and 2 and two FPMs (processing modules) in chassis slots 3 and 4.

FortiGate-7040E front panel (with FPM-7630Es)



Do not operate the FortiGate-7040E chassis with open slots on the front or back panel. For optimum cooling performance and safety, each chassis front panel slot must contain an FIM or FPM or an FIM or FPM blank panel (also called a dummy card). In addition, all cooling fan trays, power supplies or power supply slot covers must be installed while the chassis is operating. The FIM and FPM blank panels are part of the chassis package and all blank panels should be kept available in case an FIM or FPM is removed from the chassis.

FIM modules

FIM modules are hot swappable interface modules that provide data and management interfaces, base backplane switching and fabric backplane session-aware load balancing for the chassis. The FIM modules include an integrated switch fabric and DP2 processors to load balance millions of data sessions over the chassis fabric backplane to FPM processor modules. The following FIM modules are available:

- The FIM-7901E includes thirty-two front panel 10GigE SFP+ fabric channel interfaces (A1 to A32). These interfaces can be connected to 10Gbps networks. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers.
- The FIM-7904E includes eight front panel 40GigE QSFP+ fabric channel interfaces (B1 to B8). These interfaces can be connected to 40Gbps networks. Using 40GBASE-SR4 multimode QSFP+ transceivers, each QSFP+ interface can also be split into four 10GBASE-SR interfaces and connected to 10Gbps networks.
- The FIM-7910E includes four front panel 100GigE CFP2 fabric channel interfaces (C1 to C4). These interfaces can be connected to 100Gbps networks. Using 100GBASE-SR10 multimode CFP2 transceivers, each CFP2 interface can also be split into ten 10GBASE-SR interfaces and connected to 10Gbps networks.
- The FIM-7920E includes four front panel 100GigE QSFP28 fabric channel interfaces (C1 to C4). These interfaces can be connected to 100Gbps networks. Using a 100GBASE-SR4 QSFP28 or 40GBASE-SR4 QSFP+ transceiver, each QSFP28 interface can also be split into four 10GBASE-SR interfaces and connected to 10Gbps networks.

If you are installing different FIM modules in the FortiGate-7040E chassis, for optimal configuration you should install the module with the lower model number in slot 1 and the module with the higher number in slot 2. For example, if your chassis includes a FIM-7901E and a FIM-7904E, install the FIM-7901E in chassis slot 1 and the FIM-7904E in chassis slot 2. Also, for example, if your chassis includes a FIM-7904E and a FIM-7920E, install the FIM-7904E in chassis slot 1 and the FIM-7920E in chassis slot 2. This applies to any combination of two different interface modules.

FPM-7620E

The FPM-7620E is a hot swappable processor module that provides FortiOS firewalling and security services. FPMs in the chassis function as workers, processing sessions load balanced to them by the FIMs. FPMs include multiple NP6 network processors and CP9 content processors to accelerate traffic.

FPM-7630E

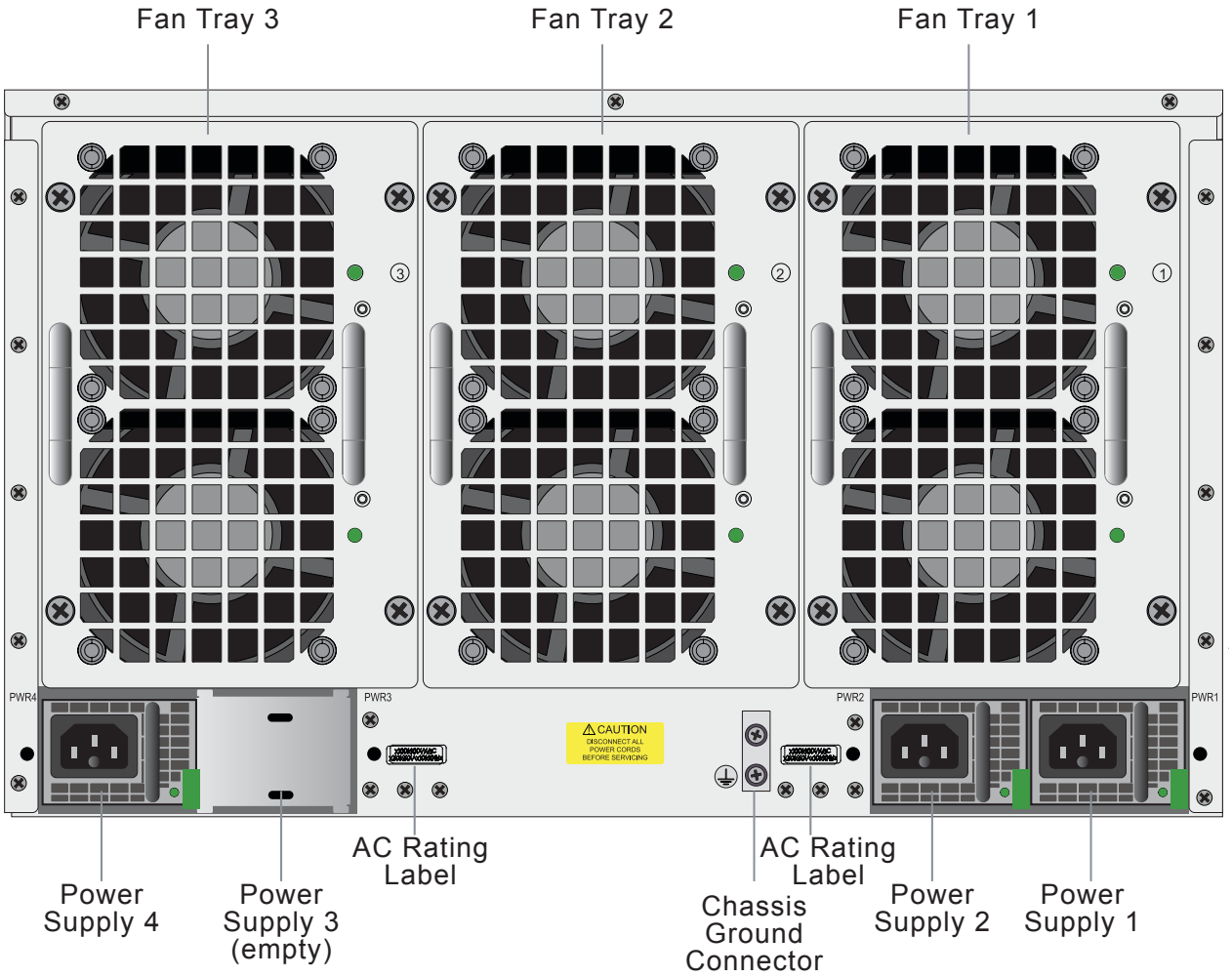
The FPM-7630E is a hot swappable processor module that provides FortiOS firewalling and security services. FPMs in the chassis function as workers, processing sessions load balanced to them by the FIMs. FPMs include multiple NP6 network processors and CP9 content processors to accelerate traffic.

The FPM-7630E processor module is an update of the FPM-7620E processor module with the same architecture but a newer CPU configuration. You can mix FPM-7630Es and FPM-7620Es in the same FortiGate-7000 chassis. In an HA configuration, both chassis in the HA cluster must have the same FPM modules in the same slots.

FortiGate-7040E back panel

The FortiGate-7040E chassis back panel provides access to three hot swappable cooling fan trays and three hot swappable AC or DC PSUs. A fourth slot is available for including a fourth PSU for additional redundancy. At least two PSUs (PWR1 and PWR2) must be connected to power. PWR4 is a backup power supply. You can add a fourth PSU to PWR3 to provide a second backup PSU. The back panel includes the FortiGate-7040E chassis ground connector that must be connected to ground.

FortiGate-7040E back panel



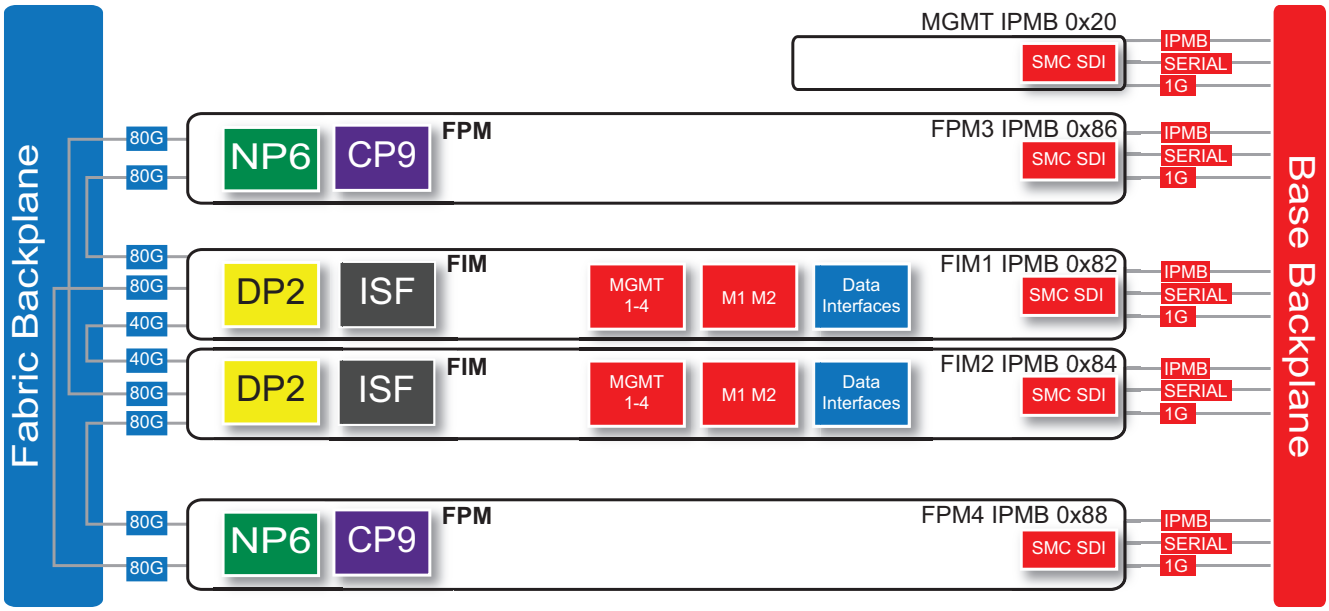
Registering your FortiGate-7040E

FortiGate-7000 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-7040E chassis schematic

The FortiGate-7040E chassis schematic below shows the communication channels between chassis components including the System Management Module (MGMT), the FIMs (called FIM1 and FIM2) and the FPMs (FPM3 and

FPM4).



The SMM (MGMT), with Intelligent Platform Management Bus (IPMB) address 0x20) communicates with all modules in the chassis over the base backplane. Each module, including the SMM, includes a Shelf Management Controller (SMC). These SMCs support IPMB communication between the SMM and the FIM and FPMs for storing and sharing sensor data that the SMM uses to control chassis cooling and power distribution. The base backplane also supports serial communications to allow console access from the SMM to all modules, and 1Gbps Ethernet communication for management and heartbeat communication between modules.

FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

FPM3 and FPM4 (IPMB addresses 0x86 and 0x88) are the FPM processor modules in slots 3 and 4. These worker modules process sessions distributed to them by the FIMs. FPMs include NP6 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing.

Chassis hardware information

This section introduces FortiGate-7040E hardware components and accessories including power requirements and FIMs and FPMs that can be installed in the chassis.

Shipping components

The FortiGate-7040E chassis ships pre-assembled with the following components:

- The 6U FortiGate-7040E chassis.
- Two FIMs.
- Two FPMs.

- One System Management Module (SMM) in the front of the chassis. (The SMM is not field replacable. If the it fails, you must RMA the chassis. The chassis will continue to operate without a functioning SMM.)
- Three Power Supply Units (PSUs) installed in the back of the chassis.
- Three cooling fan trays installed in the back of the chassis.
- One protective front panel installed in the chassis to protect internal chassis components. This panel must be removed before installing FIMs and FPMs.
- Four FIM or FPM blank panels that can be installed in empty chassis slots. The blank panels are part of the chassis package and all blank panels should be kept available in case an FIM or an FPM needs to be removed from the chassis.
- Three power cords with C15 power connectors.
- Four power cord management clamps.
- One set of 4-post rack mounting components.
- One set of 2-post rack mounting components.
- One pair of cable management side brackets.
- Two front mounting brackets.
- Twenty M4x6 flat-head screws.
- Ten M4x8 large head pan-head screws.
- Six 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-7040E-FAN	FortiGate-7040E fan tray.
FG-7040E-PS-AC	1500W AC power supply units (PSUs) for the FortiGate-7040E.
FG-7040E-CHASSIS	FortiGate-7040E chassis including 1x SMM, 3x fan trays, and 3x AC PSUs.

You can also order the following:

- Additional FIMs and FPMs.
- Transceivers.
- DC PSUs (Each PSU ships with a set of two 8 AWG DC power cables and six extra DC terminal rings. The cables are 3 meters (9.84 ft.) long. You can use the DC terminal rings to make custom DC cables.)
- Air Filter kit.
- FPM and FIM single slot cover trays to be installed in empty chassis slots.

Physical description of the FortiGate-7040E chassis

The FortiGate-7040E chassis is a 6U chassis that can be installed in a standard 19-inch rack. The following table describes the physical characteristics of the FortiGate-7040E chassis.

Dimensions (H x W x D)	10.5 x 17.3 x 25.6 in (264 x 440 x 650 mm)
Chassis weight completely assembled with FIM and FPM modules installed	150.3 lbs (68.2 kg)
Operating temperature	32 to 104°F (0 to 40°C)
Storage temperature	-31 to 158°F (-35 to 70°C)
Relative humidity	10% to 90% non-condensing
Noise level	63db
Input voltage range	100 to 240 VAC (50 to 60 Hz)
Power support rating	1500W@240VAC and 1200W@120VAC
Supplied power supply units (PSUs)	3 (for 2+1 redundancy)
Max power supply units (PSUs)	4 (for 2+2 redundancy)
Max power consumption (two FPM-7620Es)	2400W
Average power consumption (two FPM-7620Es)	1800W
Max power consumption (two FPM-7630Es)	2460W
Average power consumption (two FPM-7630Es)	1840W
Max current	110V/15A
Heat dissipation (two FPM-7620Es)	8189 BTU/hr
Heat dissipation (two FPM-7630Es)	8456 BTU/h
Joules/hr	8632 KJ/hr

Cooling fans, cooling air flow, and minimum clearance

The FortiGate-7040E chassis contains three hot swappable cooling fan trays installed in the back of the chassis. Each fan tray includes two fans that operate together. The fan tray includes two LEDs, one for each fan. When these LEDs are green both fans are operating normally. If one of the LEDs turns red or goes off, that fan is not working and the fan tray should be replaced.

During normal chassis operation, all three fan trays are active and the fan speed is controlled by the 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 for 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. Then apply the fan outlet

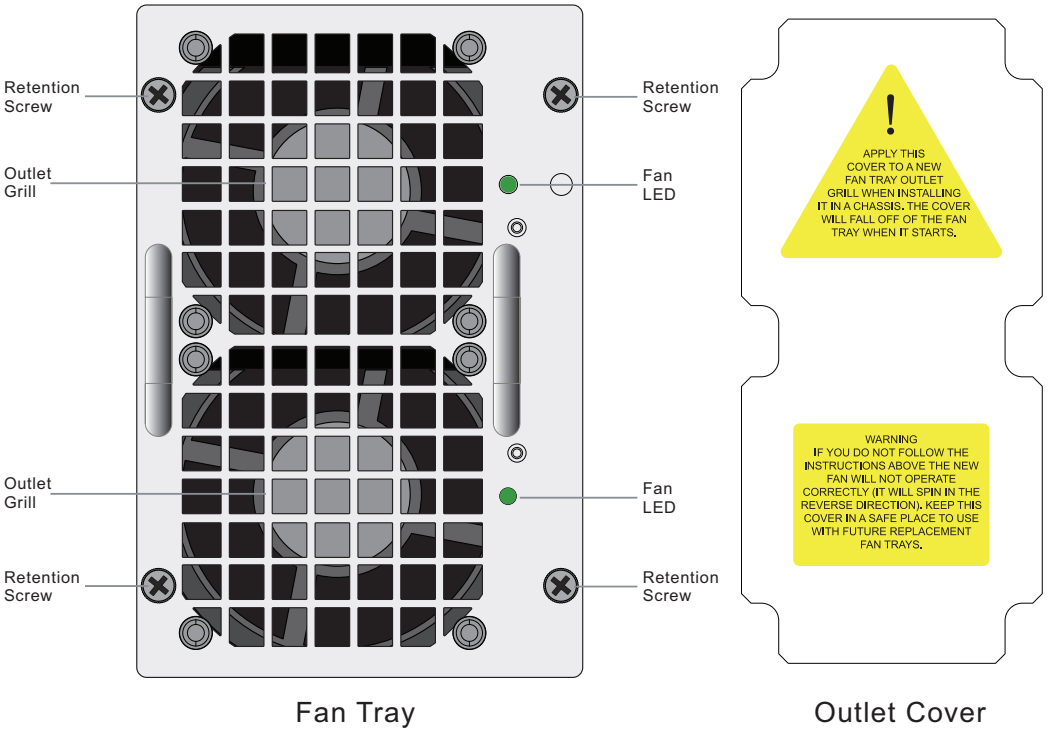
cover to the outlet grill of the new fan tray. Install the new fan tray by sliding it into place. As you slide the new fan into place it will power up and the fan outlet cover will fall off of the fan tray. Tighten the retention screws.

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

The FortiGate-7040E System Management Module (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 SMM is up and running, it reduces cooling fan speeds to maintain an optimum temperature in the chassis. If the SMM is not installed 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 and outlet cover

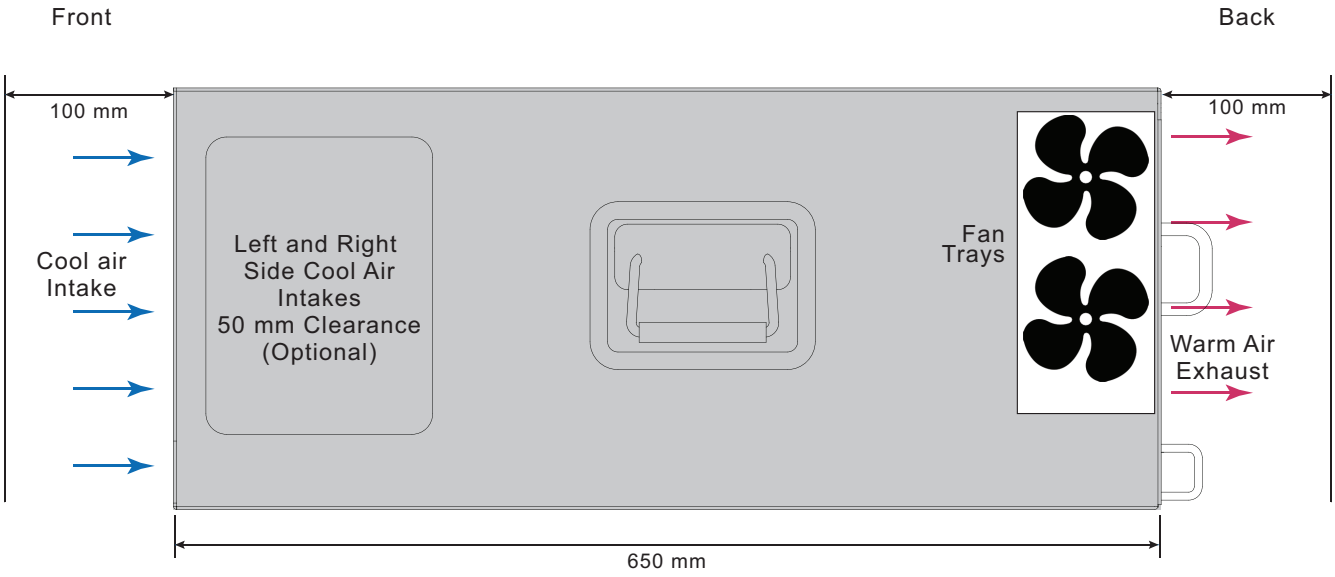


Cooling air flow and required minimum air flow clearance

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.

Most cool air enters the chassis through the chassis front panel and all warm air exhausts out the back. For optimal cooling allow 100 mm of clearance at the front and back of the chassis and 50 mm of clearance at the sides. Under these conditions 80% of cooling air comes from the front panel air intake and 20% from the left and right side panels and 100% exits out the back. Side clearance is optional and chassis cooling will be sufficient if no side clearance is available.

FortiGate-7040E cooling air flow and minimum air flow clearance (chassis side view)



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 and two filters for the side cool air intakes. These filters are 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.

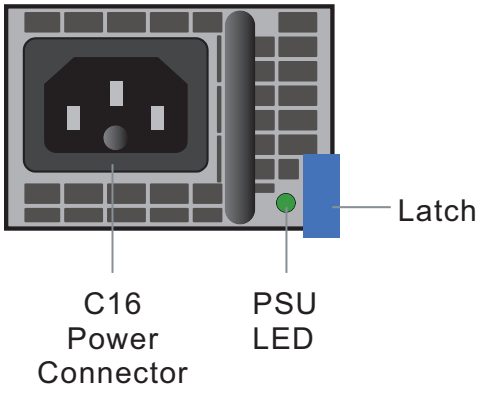
AC PSUs and supplying AC power to the chassis

The AC version of the FortiGate-7040E chassis back panel includes three hot swappable AC PSUs. At least two PSUs (PWR1 and PWR2) must be connected to power. PWR4 is a backup PSU that provides 2+1 redundancy. You can add a fourth power supply to PWR3 to provide a second backup PSU and 2+2 redundancy. See FortiGate-7040E back panel on page 9 for locations of the PSUs.

All 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.

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-7040E as long as two PSUs are connected to power and operating normally. If you need to hot swap one of two 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 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. Connect the PSU power terminals as described above.
6. Turn on power to the PSU.
7. Verify that the PSU status LED is solid green meaning that the PSU is powered up and operating normally.

DC PSUs and supplying DC power to the chassis

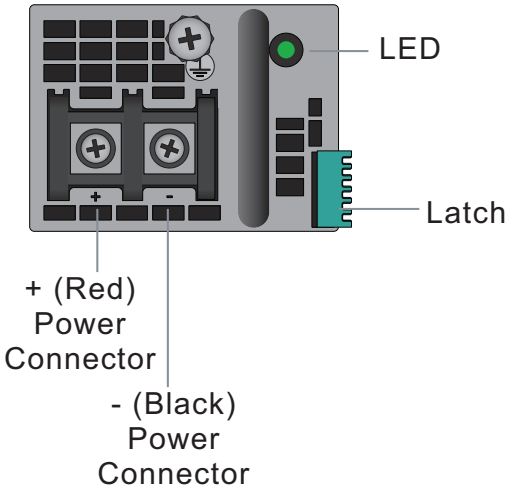
The DC version of the FortiGate-7040E chassis front panel comes with three hot swappable 48-72V to 12V 125A DC PSUs. Each PSU has a Internal 60A/170VDC fast blow fuse on the DC line input.

At least three PSUs (power supplies 1, 2, and 3) must be connected to power. The fourth power supply is a backup power supply and provides 3+1 redundancy. See FortiGate-7040E back panel on page 9 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.

Each PSU is designed to be installed in a Telecom data center or similar location that has available -48VDC power fed from a listed 40A circuit breaker. To improve redundancy you can connect each power supply to a separate power circuit.

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. Make sure DC terminal rings are securely and safely fastened to the PSU terminals.

DC PSU (power connector cover removed)



DC terminals accept UL approved ring terminals for 8/M4 stud with ext ring diameter < 9.8 mm. DC cables must be a minimum of 8 AWG. Each PSU ships with a set of two 8 AWG DC power cables and six extra DC terminal rings. The cables are 3 meters (9.84 ft.) long. You can use the DC terminal rings to make custom DC cables.

PSU Power ratings

Max Inrush Current	50A
Max Inrush Current Duration	200ms
Input Voltage	-40V to -72V
Input Current	Average: 12.5A@48V for each PSU, Max: 44A

PSU LED States

State	Description
Off	DC power not connected.
Flashing Green	The PSU is in standby mode, not supplying power to the chassis.
Green	Normal Operation with DC power connected.
Amber	Input voltage outside of normal operating range, PSU fan not operating, or output voltage outside of normal operating range.
Flashing Amber	Warning that power input or output is close to outside of normal operating range. PSU should be replaced.

Crimping guidelines

To connect the PSUs to data center power you should use 8 AWG or larger wires depending on the wire length and the power requirements of your chassis. The ends of these wires must be fitted with UL approved ring terminals for 8/M4 studs with ext ring diameter < 9.8 mm. Use the following information to crimp and prepare these wires.

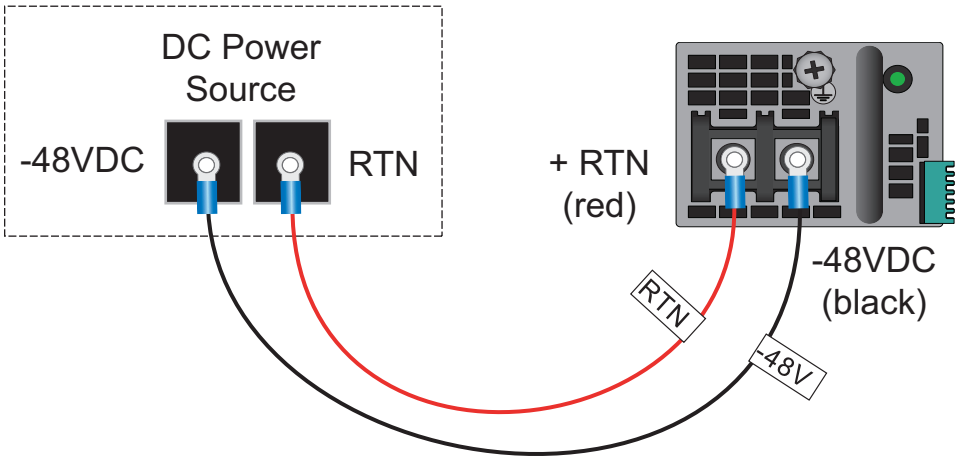
Do not crimp energized wires.

Follow these crimping guidelines:

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

Connecting a FortiGate-7040E PSU to DC power

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



You need the following equipment to connect the FortiGate-7040E PSUs to DC power:

- An electrostatic discharge (ESD) preventive wrist strap with connection cord.
- One black 8 AWG stranded wire with attached UL approved ring terminal for 8/M4 studs with ext ring diameter < 9.8 mm.
- One red 8 AWG stranded wire with attached UL approved ring terminal for 8/M4 studs with ext ring diameter < 9.8 mm.

To connect a 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. Snap the clear plastic cover off of the PSU power terminals.

4. Remove the first set of nuts and lock washers from the connectors on the PSU.
5. Connect the black -48V power wire from your DC power source to the connector on the PSU labeled - using the ring terminal.
6. Connect the red RTN power wire from you RTN power source to the connector on the PSU labeled + using the ring terminal.
7. Use the previously removed nuts and lock washers to secure the connectors. Do not apply torque of more than 3.8 Nm (33.62 lbf.in).
8. Snap the clear plastic cover over the PSU power terminals.
9. Make sure the power wires are secured using tie wraps if required.
10. If required, label the black wire -48V.
11. If required, label the red wire RTN.
12. Turn on power to the PSU.
13. 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-7040E as long as two PSUs are connected to power and operating normally. If you need to hot swap one of two 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.
3. Snap off the terminal cover and remove the wires from the PSU terminals.
4. Press the latch towards the handle until the PSU is detached then pull it out of the chassis.
5. Insert a replacement PSU into the chassis and slide it in until it locks into place.
6. Connect the PSU power terminals as described above.
7. Turn on power to the PSU.
8. Verify that the PSU status LED is solid green meaning that the PSU is powered up and operating normally.

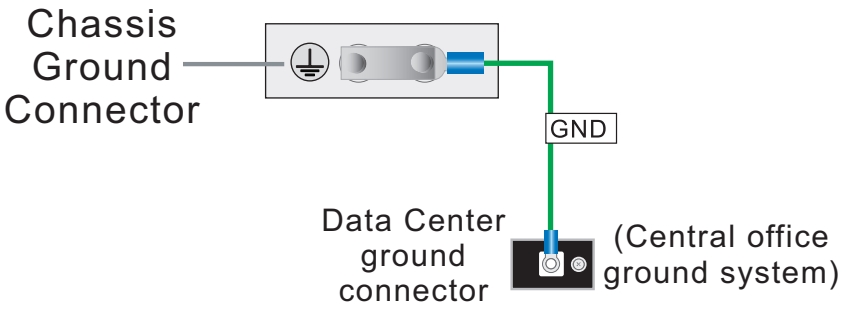
Connecting the FortiGate-7040E chassis to ground

The FortiGate-7040E chassis includes a ground terminal on the rear the bottom of the FortiGate-7040E back panel. The ground terminal provides two connectors to be used with a double-holed lug such as Thomas & Betts PN 54850BE. This connector must be connected to a local ground connection.

You need the following equipment to connect the FortiGate-7040E 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-7040E 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 green ground wire from the local ground to the ground connector on the FortiGate-7040E chassis.
4. Secure the ground wire to the chassis.
5. Optionally label the wire GND.

Turning on FortiGate-7040E chassis power

Connect AC or DC power to PWR1, PWR2 and PWR4. Once the FortiGate-7040E chassis is connected to power the chassis powers up. If the chassis is operating correctly, the LEDs on the PSUs and fans should be lit. As well, the LEDs on the SMM 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-7040E hardware assembly and rack mounting

The FortiGate-7040E chassis must be mounted in a standard 19-inch rack and requires 6U of vertical space in the rack. This chapter describes how to attach accessories to the FortiGate-7040E 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-7040E 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-7040E chassis should not be operated as a free-standing appliance.

Install accessories before mounting the chassis in a rack. Install the modules after the chassis is rack mounted.

Installing optional accessories

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

- Front mounting brackets
- Left and right cable management brackets
- Front cable management brackets
- Power cord clamps

Front mounting brackets

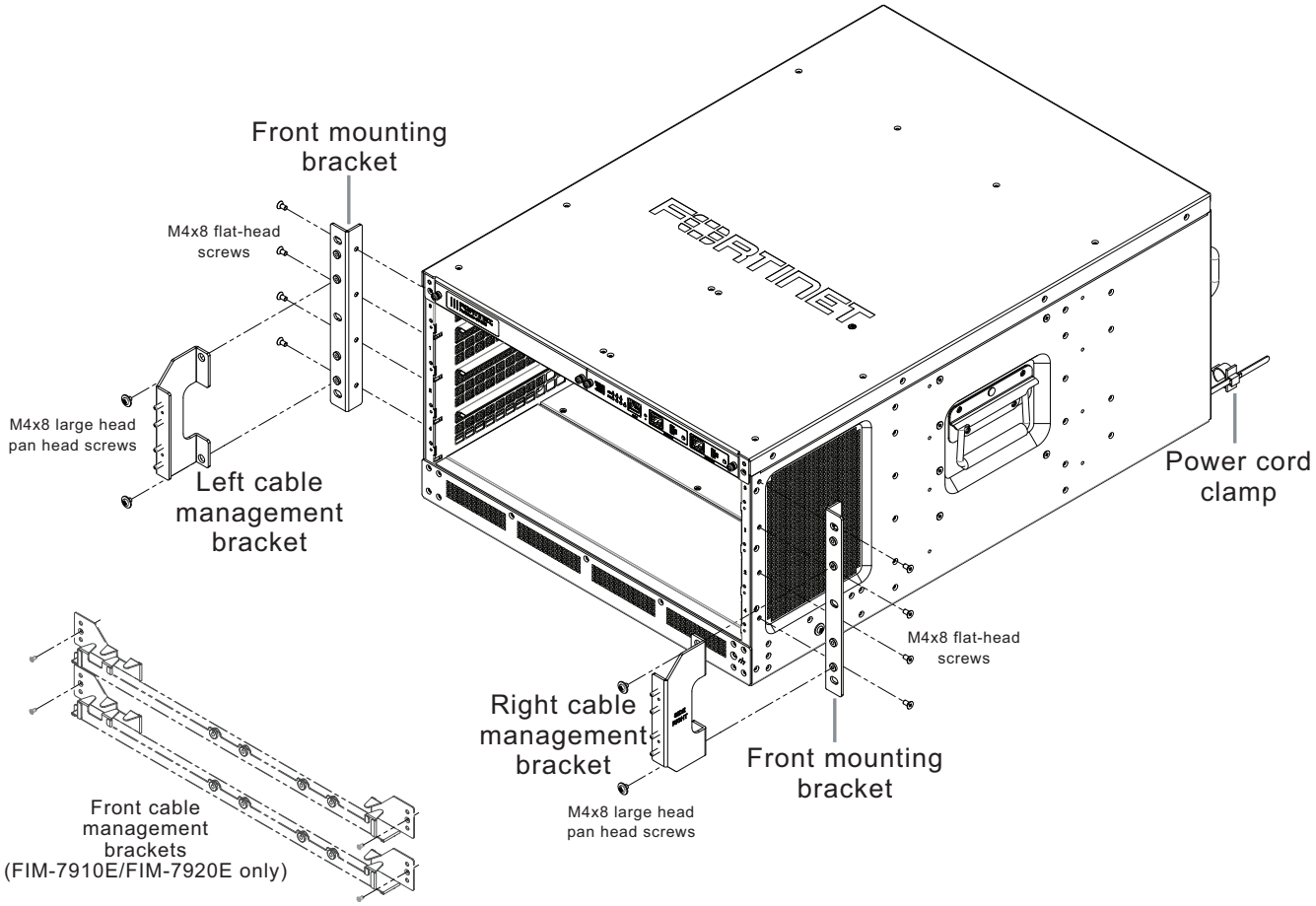
You need to install the front mounting brackets to mount the FortiGate-7040E in a four-post rack (see Mounting the FortiGate-7040E chassis in a four-post rack on page 22). You also need to install the front mounting brackets to be able to attach the left and right cable management brackets.

The front mounting brackets are not required to mount the FortiGate-7040E in a two-post rack (see Mounting the FortiGate-7040E chassis in a two-post rack on page 22).

Left and right cable management brackets

You can optionally install the left and right cable management brackets to help manage the network cables connected to FIM modules installed in the FortiGate-7040E. Install the left and right cable management brackets by attaching them to the left and right front mounting brackets.

Installing FortiGate-7040E optional accessories



Front cable management brackets (FIM-7910E and FIM-7920E only)

These front cable management brackets are not included with the FortiGate-7040E package. Fortinet ships a front cable management bracket with each FIM-7910E and FIM-7920E module. These brackets help support the relatively large CFP2 transceivers used with FIM-7910E modules and QSFP28 transceivers used with FIM-7920E modules.

If you decide to use one or two front cable management brackets, install them by attaching them to the left and right cable management brackets.

Power cord clamps

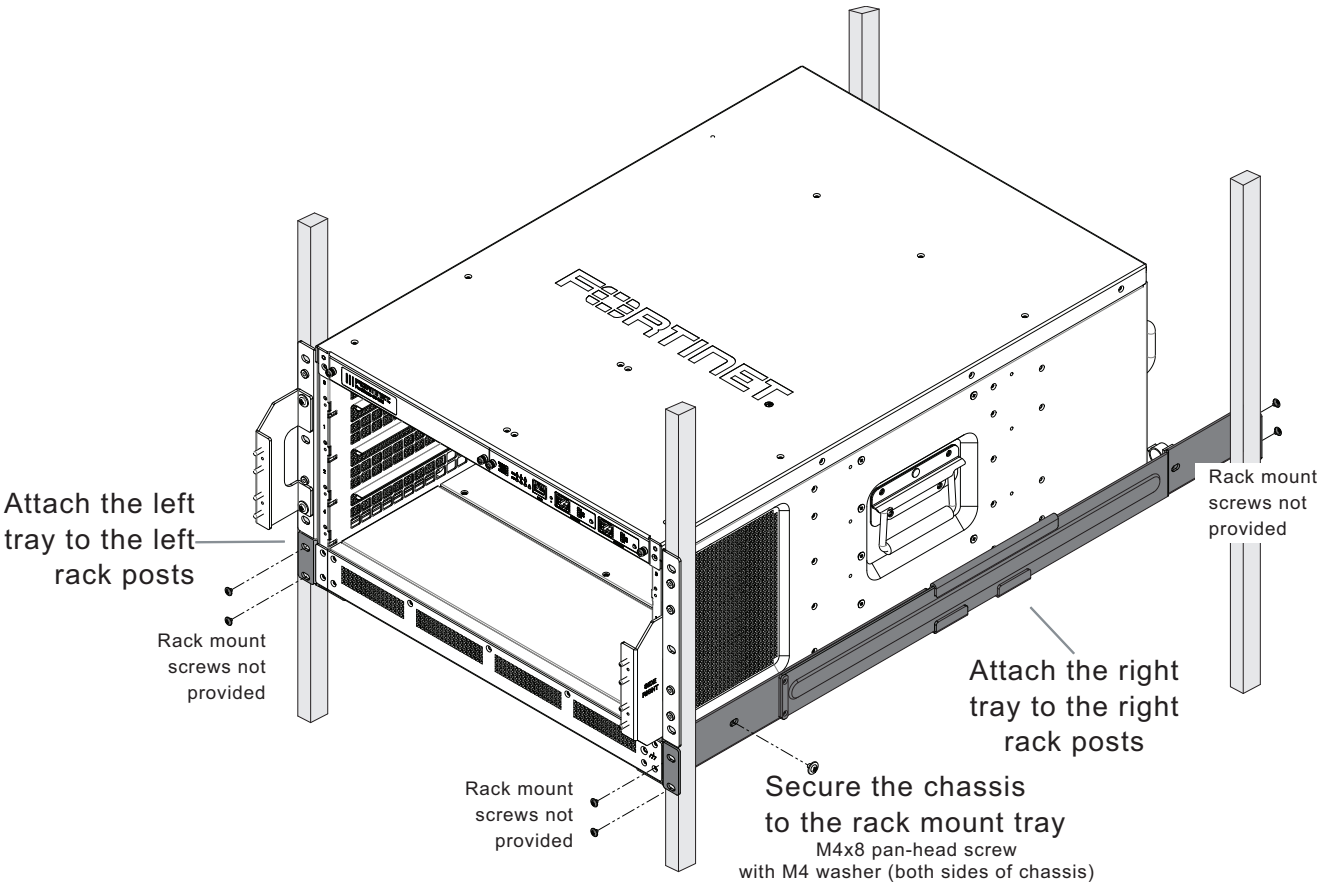
You can also install power cord clamps into the back of the chassis beside each PSU. Install the clamps by inserting them into the holes adjacent each supply at the back of the chassis. Use the clamps to secure the AC power cords so they are not accidentally disconnected.

Mounting the FortiGate-7040E chassis in a four-post rack

The FortiGate-7040E package includes an set of extendable brackets 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 using the front and back brackets 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 as shown in the diagram.

Mounting the chassis in a four-post Rack

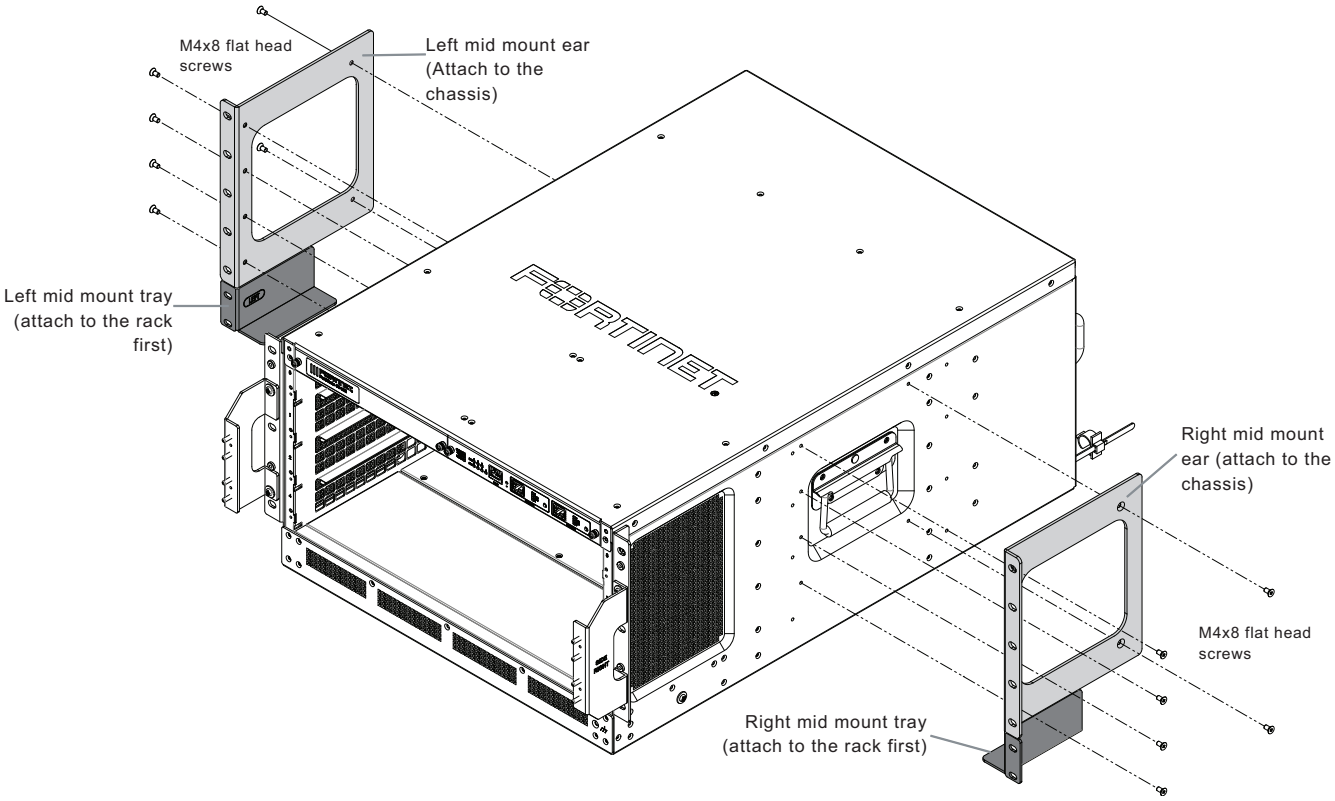


Mounting the FortiGate-7040E chassis in a two-post rack

The FortiGate-7040E package includes two mid-mount trays and two mid-mount ears that you can use the mount the chassis in a 2-post rack. As shown in the diagram, first attach the mid-mount trays to the rack making sure to leave enough space above the trays for the chassis. Then attach the mid-mount ears to the chassis also as shown in the

diagram. Finally line up the mid-mount trays with the mid-mount ears so that the chassis is supported in the rack. Then use screws to attach the mid-mount ears and the chassis to the rack.

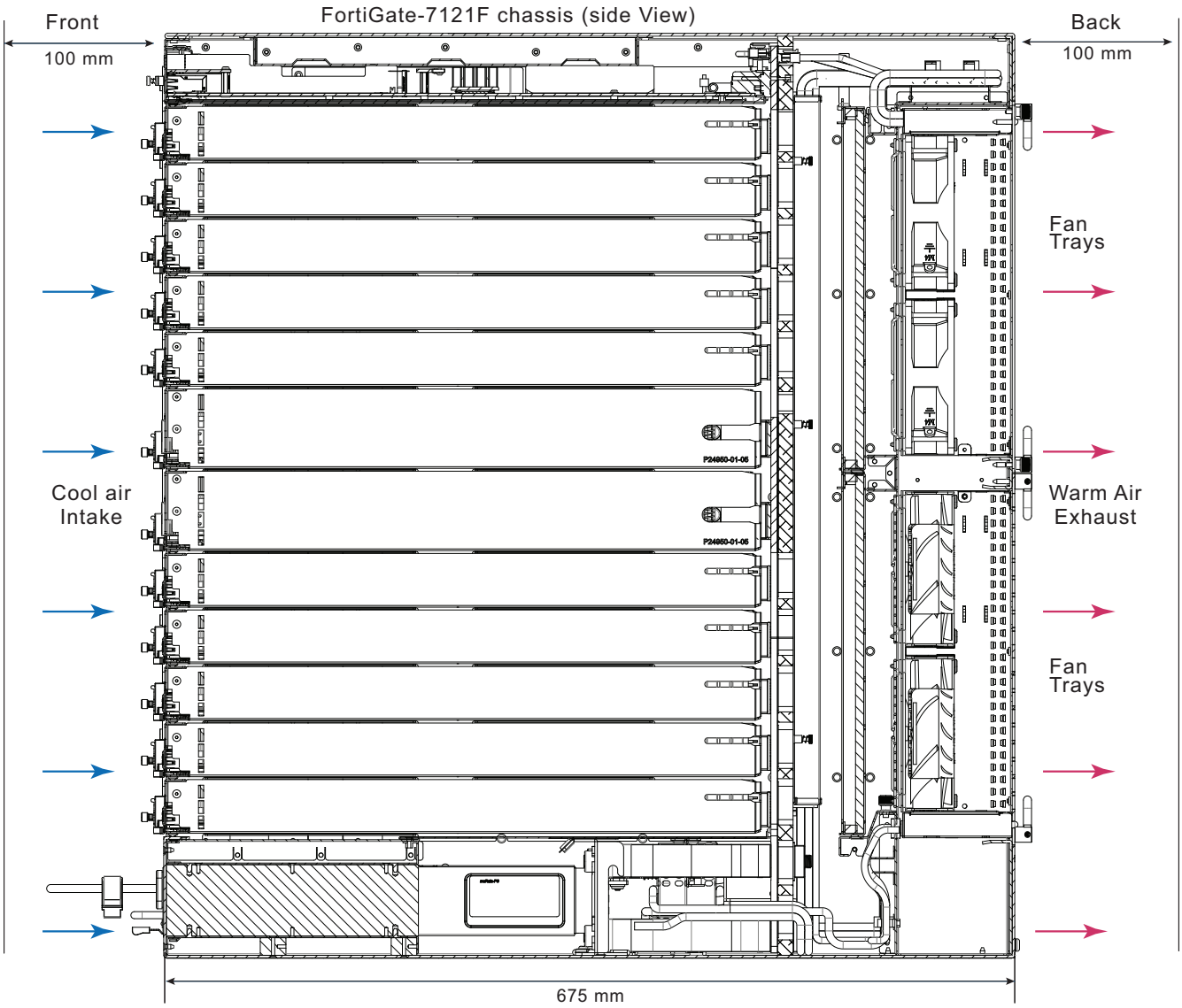
Mounting the chassis in a 2-post rack



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-7040E 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.

Inserting FIMs and FPMs

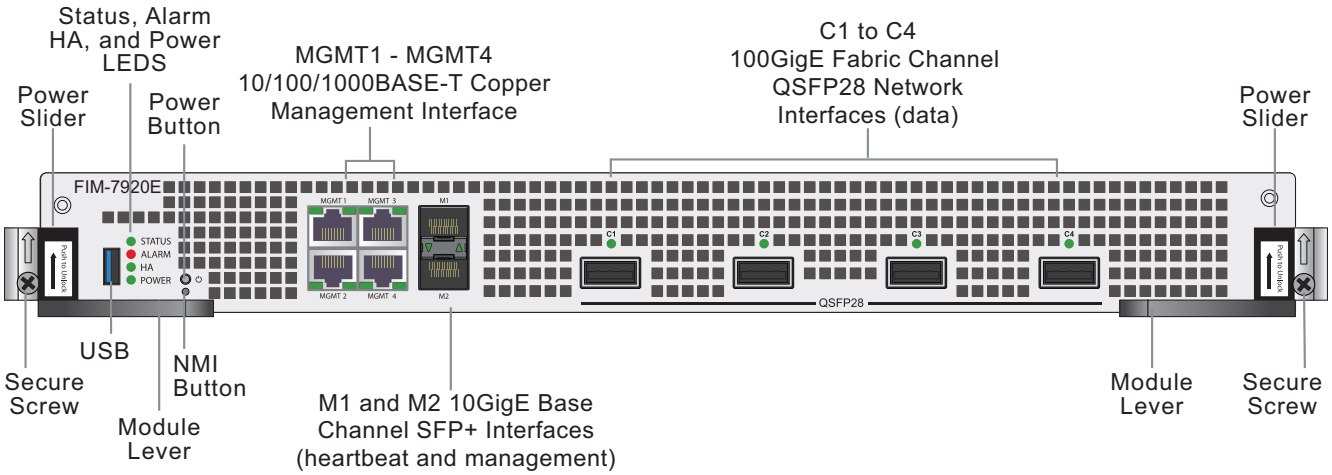
All FortiGate-7040E chassis are shipped with a protective front panel installed in the chassis to protect internal chassis components. This panel must be removed before you install FIMs and FPMs.

Insert FIMs into chassis slots 1 and 2. Insert FPMs into chassis slots 3 and 4.

Do not operate the FortiGate-7040E chassis with open slots on the front or back panel. For optimum cooling performance and safety, each chassis front panel slot must contain an FIM or FPM or an FIM or FPM blank panel (also called a dummy card). In addition, all cooling fan trays, power supplies or power supply slot covers must be installed while the chassis is operating. The FIM and FPM blank panels are part of the chassis package and all blank panels should be kept available in case an FIM or FPM is removed from the chassis.

To insert FIM and FPM modules, see the guide supplied with the module.

FIM-7920E front panel



You must carefully slide the FIM or FPM 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. Module levers must be closed.
2. Secure screws must be tightened.
3. 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.

Recommended slot locations for FIMs

If you are installing different FIMs in the FortiGate-7040E chassis, for optimal configuration you should install the FIM with the lower model number in slot 1 and the module with the higher model number in slot 2.

For example:

- if your chassis includes a FIM-7901E and a FIM-7904E, install the FIM-7901E in chassis slot 1 and the FIM-7904E in chassis slot 2.
- If your chassis includes a FIM-7904E and a FIM-7920E, install the FIM-7904E in chassis slot 1 and the FIM-7920E in chassis slot 2.

This applies to any combination of two different FIMs.

Getting started with FortiGate-7000

Begin by installing your FortiGate-7000 chassis in a rack and installing FIM interface modules and FPM processing modules 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 chassis will not allow traffic to pass through and you may not be able to log into the GUI, or if you manage to log in, the session could time out as the FortiGate-7000 continues negotiating.

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 system has initialized, you have a few options for connecting to the FortiGate-7000 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 and use the same admin account to log in.
- Log in to the primary FIM CLI by connecting to the RJ-45 RS-232 Console 1 serial port on the FortiGate-7000 SMM with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate-7000 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-7000 to your network.
MGMT1 IP/Netmask	192.168.1.99/24 (the MGMT1 interface is part of the mgmt redundant interface that also includes MGMT2, MGMT3, and MGMT4).

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

All other management communication (for example, SNMP queries, remote logging, and so on) use the management aggregate interface and are handled by the primary FIM.

Multi VDOM mode

By default, when you first start up a FortiGate-7000 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 interface (mgmt) and the HA heartbeat interfaces (M1, M2) are in mgmt-vdom and all of the data interfaces are in the root VDOM.

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

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

Confirming startup status

Before verifying normal operation and making configuration changes and so on you should wait until the FortiGate-7000 is completely started up and synchronized. This can take a few minutes.

To confirm that the FortiGate-7000 is synchronized, go to **Monitor > Configuration Sync Monitor**. If the system is synchronized, all of the FIMs and FPMs should be visible and their **Configuration Status** should be **In Sync**. The Configuration Sync Monitor also indicates if any modules are not synchronized.

Serial	Slot ID	Configuration Status	Role	Up Time	Last Heartbeat
FIM10E3E17000043	1	In Sync	Master	1d 5m	
FIM20E3E17000068	2	In Sync	Slave	1d 5m	12 seconds ago
FPM20E3E16900213	4	In Sync	Slave	1d 5m	12 seconds ago
FPM20E3E17900152	5	In Sync	Slave	1d 5m	12 seconds ago
FPM20E3E17900223	3	In Sync	Slave	1d 5m	12 seconds ago
FPM30E3E17900003	6	In Sync	Slave	1d 5m	12 seconds ago

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

From the menu bar at the top of the GUI, you can click on the host name and pull down a list of the FIMs and FPMs in the FortiGate-7000. From the list you can see the status of each FIM or FPM, change the host name, or log into the GUI using the special management port number.

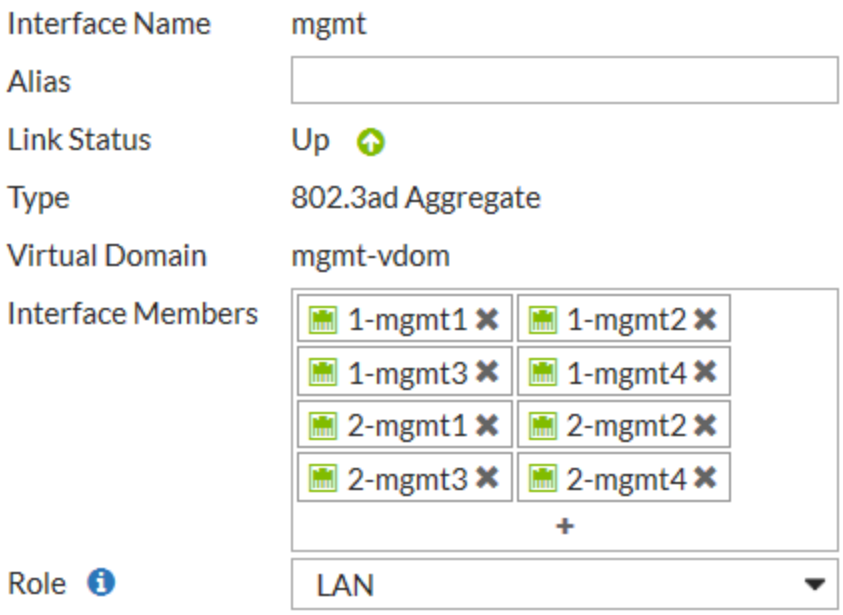
From the CLI you can use the `diagnose sys confsync status | grep in_sy` command to view the synchronization status of the FIMs and FPMs. If all of the FIMs and FPMs are synchronized, each output line should include `in_sync=1`. If a line ends with `in_sync=0`, that FIM or FPM is not synchronized. The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

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000062, Slave, uptime=53740.68, priority=2, slot_id=2:2, idx=3, flag=0x10, in_sync=1
FIM04E3E16000010, Slave, uptime=53790.94, priority=3, slot_id=1:1, idx=0, flag=0x10, in_sync=1
FIM04E3E16000014, Master, uptime=53781.29, priority=1, slot_id=2:1, idx=1, flag=0x10, in_sync=1
FIM10E3E16000040, Slave, uptime=53707.36, priority=4, slot_id=1:2, idx=2, flag=0x10, in_sync=1
FPM20E3E16900234, Slave, uptime=53790.98, priority=16, slot_id=2:3, idx=4, flag=0x64, in_sync=1
FPM20E3E16900269, Slave, uptime=53783.67, priority=17, slot_id=2:4, idx=5, flag=0x64, in_sync=1
FPM20E3E17900113, Slave, uptime=53783.78, priority=116, slot_id=1:3, idx=6, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=53784.11, priority=117, slot_id=1:4, idx=7, flag=0x64, in_sync=1
...
```

Setting up management connections

When your FortiGate-7000 first starts up, the MGMT1 to MGMT4 interfaces of both of the FIMs are part of a static 802.3 aggregate interface with a default IP address of 192.168.1.99. On the GUI or CLI the 802.3 aggregate interface is named **mgmt**.

Example mgmt interface configuration



For security reasons you should add a password to the admin account before connecting the chassis to your network.

Setting up a single management connection

You can configure and manage your FortiGate-7040E by connecting an Ethernet cable to any of the MGMT1 - 4 interfaces of the FIM in slot 1 or slot 2 and logging into the GUI using HTTPS or the CLI using SSH. The default IP address is 192.168.1.99 and you can log in with the **admin** administrator account with no password.

For security reasons you should add a password to the admin account before connecting the chassis to your network.

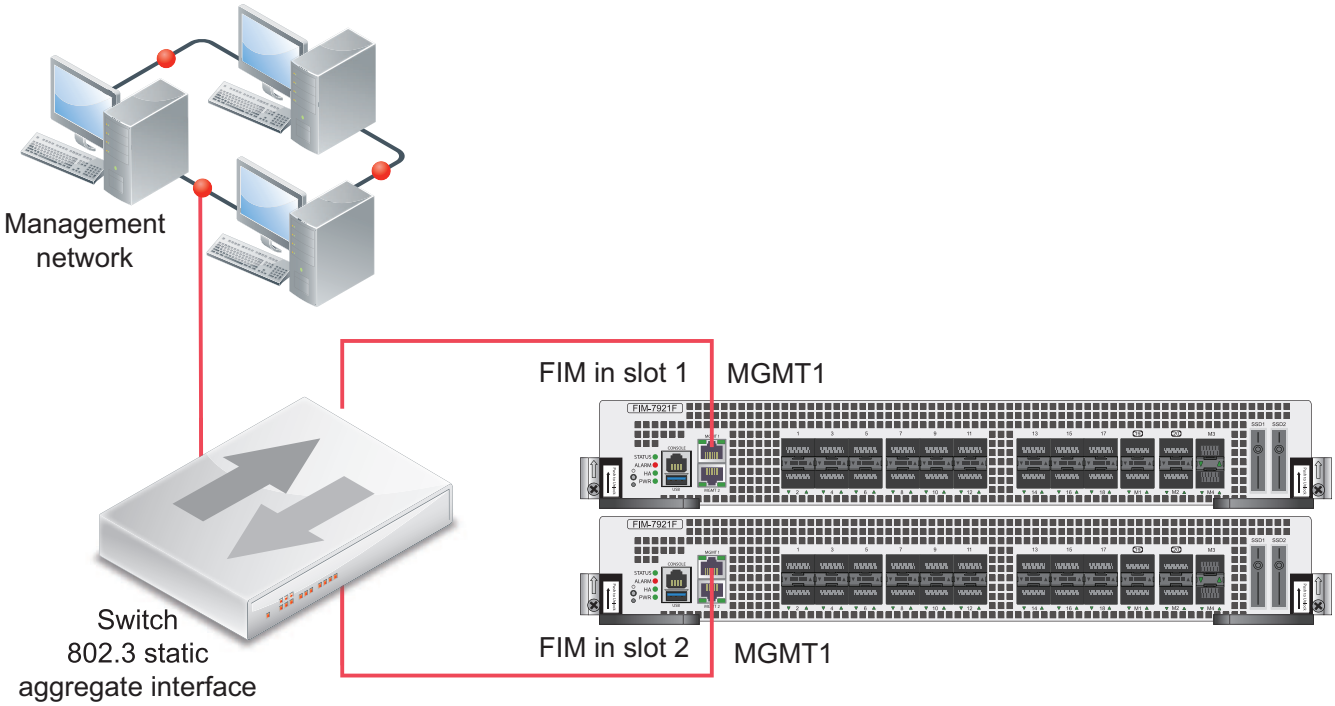
Setting up redundant management connections

You can set up redundant management connections to your FortiGate-7000 by adding a static 802.3 aggregate interface to a switch and setting up multiple connections between the switch and the FIM MGMT ports. Then connect the switch to your network.

LACP is not supported for the mgmt aggregate interface.

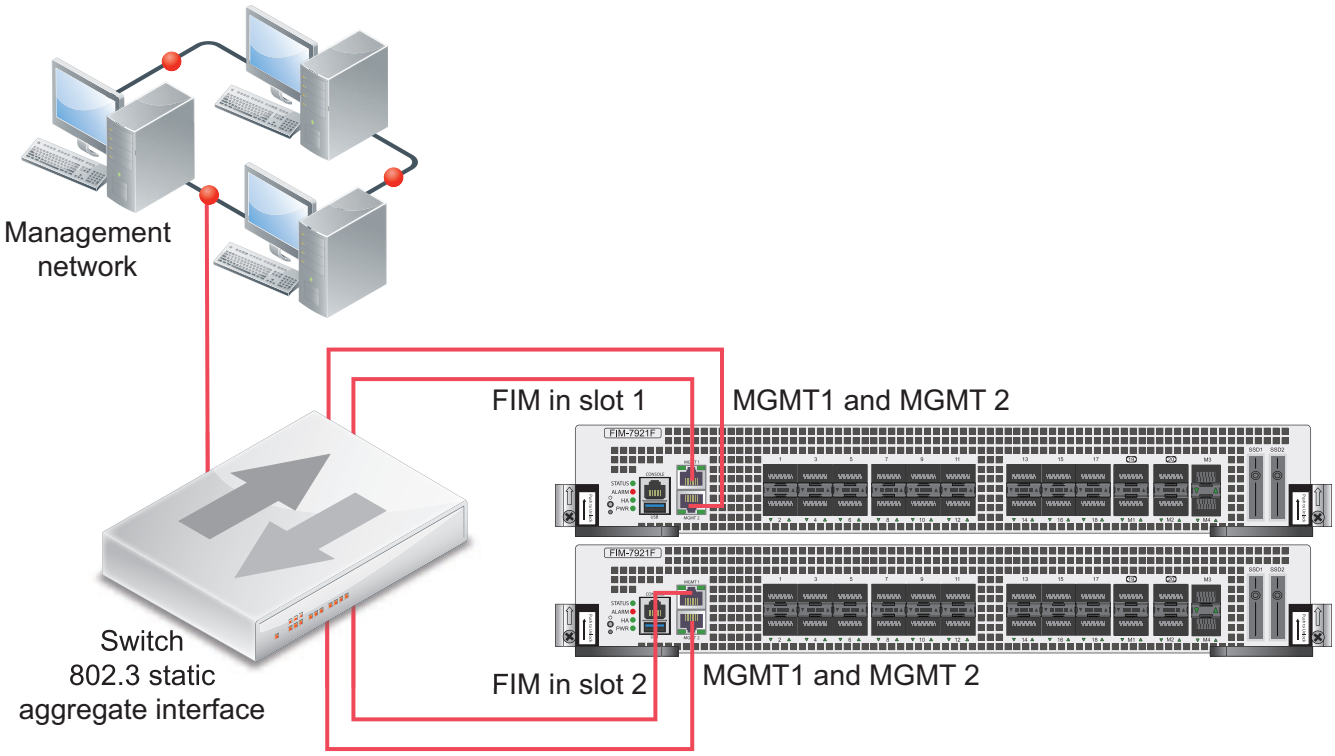
You do not have to change the configuration of the FortiGate-7000 to set up redundant management connections. The following example shows connections between the MGMT1 interfaces of each FIM to a switch. The switch is configured with a 802.3 static aggregate interface that includes two ports, one for each MGMT1 interface. The switch also connects the MGMT1 interfaces to a management network.

Example FortiGate-7000 redundant management connections



The following example shows redundant connections between both FIMs and the switch. In this case you need to add more switch ports to the static aggregate interface on the switch. You do not have to change the configuration of the FortiGate-7000 to set up this redundant management connection configuration.

Example FortiGate-7000 redundant management connections with redundant connections to each FIM



In either of these configurations, for additional redundancy you can use two switches. If you use two redundant switches, the static aggregate interface should span across both switches.

Adding a password to the admin administrator account

For security purposes one of the first things you should do is add a password to the admin account.

Depending on your firmware version, when you first log into the GUI you maybe presented with an option to change the admin account password.

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
```

Changing data interface network settings

To change the IP address of any FortiGate-7040E data interface:

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

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

Resetting to factory defaults

At any time during the configuration process, if you run into problems, you can reset the FortiGate-7040E to factory defaults and start over. From the primary FIM CLI enter:

```
config global
   execute factoryreset
```

Restarting the FortiGate-7040E

To restart all of the modules in a FortiGate-7040E, 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-7000 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-7000 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-7000 using the mgmt interface IP address with a special port number.

To enable using the special management port numbers to connect to individual FIMs and FPMs, the mgmt 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 mgmt interface with an invalid IP address, or disable management or administrative access for the mgmt interface.

For example, if the mgmt interface IP address is 192.168.1.99, you can connect to the GUI of the FPM in slot 3 using the mgmt interface IP address followed by the special port number, for example:

`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-7000 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.

FortiGate-7000 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)
3	FPM03	8003	44303	2303	2203	16103

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
1	FIM01	8001	44301	2301	2201	16101
2	FIM02	8002	44302	2302	2202	16102
4	FPM04	8004	44304	2304	2204	16104

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 module 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 slot address in the format `<hostname> [<slot address>] #`.

Logging in to different modules allows you to use FortiView or Monitor GUI pages to view the activity of that module. 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.

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-7000 HA special management port numbers

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 3	FPM03	8005	44303	2303	2203	16103
Ch1 slot 1	FIM01	8003	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch2 slot 3	FPM03	8025	44323	2323	2223	16123
Ch2 slot 1	FIM01	8023	44321	2321	2221	16121
Ch2 slot 2	FIM02	8022	44322	2322	2222	16122
Ch2 slot 4	FPM04	8024	44324	2324	2224	16124

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-7000 in an HA configuration

From the primary FIM of the primary FortiGate-7000 in an HA configuration, you can use the following command to log in to the primary FIM of the secondary FortiGate-7000:

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

Where `<id>` is the ID of the other FortiGate-7000 in the cluster. From the primary FortiGate-7000, use an ID of 0 to log into the secondary FortiGate-7000. From the secondary FortiGate-7000, use an ID of 1 to log into the primary FortiGate-7000. 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-7000 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-7000.

Firmware upgrades

In addition to introducing the basics of upgrading FortiGate-7040E firmware, this section describes how to:

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

Firmware upgrade basics

All of the FIMs and FPMs in your FortiGate-7000 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-7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption. For more information about graceful HA upgrades, see HA cluster firmware upgrades.

Upgrading the firmware of a standalone FortiGate-7000, or FortiGate-7000 HA cluster with `uninterrupable-upgrade` disabled 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-7000 system. Some firmware upgrades may take longer depending on factors such as the size of the configuration and whether an upgrade of the DP2 processor is included.

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

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path as documented in the release notes.
- Back up your FortiGate-7000 configuration.

Fortinet recommends that you review the services provided by your FortiGate-7000 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-7000 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-7000 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.

Upgrading the firmware running 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-7000 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-7000 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-7000 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-7000. These procedures also work for FIMs or FPMs in the primary FortiGate-7000 in an HA configuration. To upgrade firmware on an FIM or FPM in the secondary FortiGate-7000 in an HA configuration, you should either remove the secondary FortiGate-7000 from the HA configuration or cause a failover so that the secondary FortiGate-7000 becomes the primary FortiGate-7000.

In general, if you need to update both FIMs and FPMs in the same FortiGate-7000, you should update the FIMs first as the FPMs can only communicate through FIM interfaces.

Upgrading FIM firmware

Use the following procedure to upgrade the firmware running on a single FIM. For this procedure to work, you must connect at least one of the FIM MGMT interfaces to a network. You must also be able to log in to the FIM GUI or CLI from that MGMT interface. If you perform the firmware upgrade from the CLI, the FIM must be able to communicate with an FTP or TFTP server.

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

1. Log into the FIM GUI or CLI and perform a normal firmware upgrade.
   You may need to use the special port number to log in to the FIM in slot two (for example, browse to https://192.168.1.99:44302).
2. Once 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.
3. Verify that the configuration has been synchronized to the upgraded FIM. The following command output shows the synchronization status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, 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 example output also shows that the uptime of the FIM in slot 2 is lower than the uptime of the other modules, indicating that the FIM in slot 2 has recently restarted.

   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 FPM firmware

Use the following procedure to upgrade the firmware running on an individual FPM. To perform the upgrade, you must enter a command from the primary FIM CLI to allow ELBC communication with the FPM. Then you can just log in to the FPM GUI or CLI and perform the firmware upgrade.

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

After verifying that the FPM is running the right firmware, you must log back into the primary FIM CLI and return the FPM to normal operation.

1. Log in to the primary FIM CLI and enter the following command:
   `diagnose load-balance switch set-compatible <slot> enable elbc`
   Where `<slot>` is the number of the FortiGate-7000 slot containing the FPM to be upgraded.
2. Log in to the FPM GUI or CLI using its special port number (for example, for the FPM in slot 3, browse to https://192.168.1.99:44303 to connect to the GUI) and perform a normal firmware upgrade of 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. Verify that the configuration has been synchronized. The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, 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 4 is lower than the uptime of the other modules, indicating that the FPM in slot 4 has recently restarted.

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.

5. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:

   ```
   diagnose load-balance switch set-compatible <slot> disable
   ```

   Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

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-7000 front panel System Management Module console port. From the console session, the procedure describes how to restart the FIM, interrupting 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.

   If the MGMT interface you are using is one of the MGMT interfaces connected as a LAG to a switch, you must shutdown or disconnect all of the other interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs.
3. Using the console cable supplied with your FortiGate-7000, connect the SMM Console 1 port on the FortiGate-7000 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-7000 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 FPM CLI using the `get system status` command.
16. Verify that the configuration has been synchronized.
    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, 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 FIM in slot 2 is lower than the uptime of the other modules, indicating that the FIM in slot 2 has recently restarted.

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 enter a command from the primary FIM CLI to allow the FPM BIOS to communicate through an FIM MGMT interface. The procedure involves creating a connection between the TFTP server and one of the FIM MGMT interfaces.

This procedure also involves connecting to the FPM CLI using a FortiGate-7000 front panel SMM console port, rebooting the FPM, interrupting the boot from the console session, and following FPM BIOS prompts to install the firmware.

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

After you verify that the FPM is running the right firmware, you must log back in to the primary FIM CLI and return the FPM to normal operation.

1. Set up a TFTP server and copy the firmware file into the TFTP server default folder.
2. Log into to the primary FIM CLI and enter the following command:
   `diagnose load-balance switch set-compatible <slot> enable bios`
   Where `<slot>` is the number of the FortiGate-7000 slot containing the FPM to be upgraded.
3. Set up your network to allow traffic between the TFTP server and a MGMT interface of one of the FIMs.
   You can use any MGMT interface of either of the FIMs. When you set up the FPM TFTP settings below, you select the FIM that can connect to the TFTP server. If the MGMT interface you are using is one of the MGMT interfaces connected as a LAG to a switch, you must shutdown or disconnect all of the other interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs
4. Using the console cable supplied with your FortiGate-7000, connect the SMM Console 1 port on the FortiGate-7000 to the USB port on your management computer.
5. 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.
6. Press Ctrl-T to enter console switch mode.
7. Repeat pressing Ctrl-T until you have connected to the module to be updated. Example prompt:
   `<Switching to Console: FPM03 (9600)>`
8. Optionally log into the FPM's CLI.
9. 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.
10. When the FPM starts up, follow the boot process in the terminal session and press any key when prompted to interrupt the boot process.
11. To set up the TFTP configuration, press C.
12. Use the BIOS menu to set the following. Change settings only if required.
    `[P]: Set image download port`: FIM01 (the FIM that can communicate with the TFTP server).
    `[D]: Set DHCP mode`: Disabled.

`[I]: Set local IP address`: The IP address of the MGMT interface of the selected FIM that you want to use to connect to the TFTP server. This address must not be the same as the FortiGate-7000 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.

13. To quit this menu, press Q.
14. 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.
15. To start the TFTP transfer, press T.

    The firmware image is uploaded from the TFTP server 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.
16. 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.
17. Verify that the configuration has been synchronized.

    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, 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 4 is lower than the uptime of the other modules, indicating that the FPM in slot 4 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.
18. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:

    `diagnose load-balance switch set-compatible <slot> disable`

    Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

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. The `in_sync=0` entries in the following example output show that the management board (serial number ending in 10) is not synchronized with the other FIM and the FPMs shown in the example.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=0
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=0
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
...
```

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

To re-synchronize the FortiGate-7000, 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.

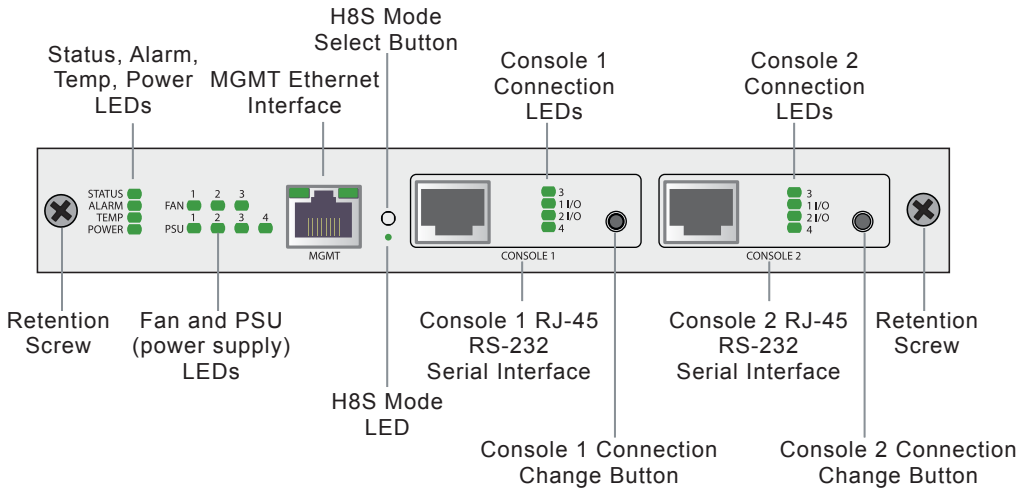
   Installing firmware synchronizes the firmware build and configuration from the primary FIM to the other FIM and the FPMs.
3. Check the synchronization status from the Configuration Sync Monitor or using the `diagnose sys confsync status | grep in_sy` command. The following example ForGate-7040E shows that the primary FIM is synchronized with the other FIM and all of the FPMs because each line includes in_sync=1:

   ```
   diagnose sys confsync status | grep in_sy
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_sync=1
   ```

FortiGate-7040E System Management Module

The FortiGate-7040E chassis includes a System Management Module (SMM) or shelf manager, located at the top right of the chassis front panel. The SMM is factory installed and configured and is not field replaceable.

FortiGate-7040E SMM front panel



The 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 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 4.

The 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 SMM through the module's IPMB. FIM and FPM module power on/off requires authorization from the SMM and the 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 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 the SMM fails, you should RMA the chassis. The chassis and the modules in it will continue to operate with no functioning SMM 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-7040E 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.
	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.
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

LED	State	Description
		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 three 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.
	Blinking red	The fan tray is not working. Chassis cooling may be sufficient but redundancy is lost and the fan tray that is not working should be replaced.
	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 (LEDs for each of four PSUs)	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 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 6 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-7000, connect the SMM Console 1 port on the FortiGate-7000 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-7000, connect the SMM Console 1 port on the FortiGate-7000 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-7000, connect the SMM Console 1 port on the FortiGate-7000 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: FIM03-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.

Connecting to the SMM using an IPMI tool

You can install an IPMI tool on a management computer and then use this tool to send IPMI commands over your network to the SMM MGMT interface. The IPMI tool allows you to communicate with the SMM by entering IPMI commands. The IPMI commands are the same as the CLI commands described in this chapter but include parameters such as the MGMT interface IP address and SMM administrator username and password.

For example, you can use the following IPMI command to change the SMM MGMT interface IP address:

```
sudo ipmitool -I lanplus -H <mgmt-ip> -k gkey -U <username> -P <password> lan set 4 ipaddr
     172.20.120.30
```

Use the following IPMI command to change the SMM password:

```
sudo ipmitool -I lanplus -H <mgmt-ip> -k gkey -U <username> -P <password> user set password 2
     <password>
```

To perform an operation on a module according to its chassis slot include the `-t <slot>` parameter in the IPMI command. For example, to list the sensors on the FIM module in chassis slot 2 (0x82), use the following IPMI command:

```
sudo ipmitool -I lanplus -H <mgmt-ip> -k gkey -U <username> -P <password0> -t 0x82 sensor
```

FortiGate-7040E chassis slots IPMB addresses

The following table lists the IPMB addresses of the FortiGate-7040E chassis slots.

Chassis slot number	Name	IPMB Address (FRUID)
SMM	MGMT	0x20
3	FPM3	0x86
1	FIM1	0x82
2	FIM2	0x84
4	FPM4	0x88

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 4) or an IPMB address number (0x82 to 0x88)

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
```

Use the following IPMI command to reset the module SMC to reboot the FPM in slot 3:

```
sudo ipmitool -I lanplus -H 10.160.19.30 -k gkey -U admin -P admin -t 0x86 mc reset warm
```

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

```
sudo ipmitool -I lanplus -H 10.160.19.30 -k gkey -U admin -P admin -t 0x88 picmg deactivate 0
```

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

```
sudo ipmitool -I lanplus -H 10.160.19.30 -k gkey -U admin -P admin -t 0x84 picmg activate 0
```

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`

Description	SMC CLI Commands	IPMI commands
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 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.

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

Action	SMC CLI Commands	IPMI Commands
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 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	`verbose <level>`	N/A
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 set name <user-id> <name>`	`user set name <user-id> <name>`

Action	SMC CLI Commands	IPMI Commands
user name. Available on the passive module.		
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 IPMI <channel>. If a <channel> is not specified the privilege level is set for all IPMI channels. Available on the passive module.	`user priv <user-id> {callback | user | operator | administrator | no_access} [<channel>]`	`user priv <user id> <privilege level> [<channel number>]`
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	`serial set sdi disable <slot>`	N/A

Action	SMC CLI Commands	IPMI Commands
passive module.		
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 chassis	N/A	`chassis power cycle`
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` `lan enable`	`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>`
	`fan_set_switch`
	`<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).

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

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

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

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

Safety

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

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

Warning: Equipment intended for installation in Restricted Access Location.

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

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

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

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

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

警告

本電池如果更換不正確會有爆炸的危險

請依製造商說明書處理用過之電池

CAUTION:

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

WARNUNG:

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

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

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

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

CAUTION: Shock Hazard. Disconnect all power sources.

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

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

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

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

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

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

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

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

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

Regulatory notices

Federal Communication Commission (FCC) – USA

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

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

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

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

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

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

CAN ICES-3 (A) / NMB-3 (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

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

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。