paloalto TECHDOCS

PA-400R Series Next-Gen Firewall Hardware Reference

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 1, 2025

Table of Contents

Before You Begin

Read the following topics before you install or service a Palo Alto Networks® next-generation firewall or appliance.**The following topics apply to all Palo Alto Networks firewalls and appliances except where noted.**

- Upgrade/Downgrade Considerations for Firewalls and Appliances
- Tamper Proof Statement
- Third-Party Component Support
- Product Safety Warnings

Upgrade/Downgrade Considerations for Firewalls and Appliances

The following table lists all hardware features that have upgrade or downgrade impact. Make sure you understand all upgrade/downgrade considerations before you upgrade or downgrade from the specified version of PAN-OS.

Feature	Release	Upgrade Considerations	Downgrade Considerations
PA-7000 Log Forwarding Card (LFC)	10.0	If you are using an LFC with a PA-7000 Series Firewall, when you upgrade to PAN-OS 10.0, you must configure the management plane or dataplane interface for the service route because the LFC ports do not support the requirements for the service route. We recommend using the dataplane interface for the Data Services service route.	n/a
Upgrading a PA-7000 Series Firewall with a first generation switch management card (PA-7050-SMC or PA-7080-SMC)	PAN-OS 8.0 and later	Before upgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the upgrade. If the value is less than 20, then contact support for assistance.	Before downgrading the firewall, run the following CLI command to check the flash drive's status: **`debug system disk-smart-info disk-1`**. If the value for attribute ID #232, **Available_Reservd_Space 0x0000**, is greater than 20, then proceed with the downgrade. If the value is less than 20, then contact support for assistance.

Tamper Proof Statement

To ensure that products purchased from Palo Alto Networks were not tampered with during shipping, verify the following upon receipt of each product:

- The tracking number provided to you electronically when ordering the product matches the tracking number that is physically labeled on the box or crate.
- The integrity of the tamper-proof tape used to seal the box or crate is not compromised.
- The integrity of the warranty label on the firewall or appliance is not compromised.

(PA-7000 Series firewalls only) PA-7000 Series firewalls are modular systems and therefore do not include a warranty label on the firewall.

Third-Party Component Support

Before you consider installing third-party hardware, read the Palo Alto Networks Third-Party Component Support statement.

Product Safety Warnings

To avoid personal injury or death for yourself and others and to avoid damage to your Palo Alto Networks hardware, be sure you understand and prepare for the following warnings before you install or service the hardware. You will also see warning messages throughout the hardware reference where potential hazards exist.

All Palo Alto Networks products with laser-based optical interfaces comply with 21 CFR 1040.10 and 1040.11.

The following safety warnings apply to all Palo Alto Networks firewalls and appliances, unless a specific hardware model is specified.

- When installing or servicing a Palo Alto Networks firewall or appliance hardware component that has exposed circuits, ensure that you wear an electrostatic discharge (ESD) strap. Before handling the component, make sure the metal contact on the wrist strap is touching your skin and that the other end of the strap is connected to earth ground.

  French Translation: Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veillez à porter un bracelet antistatique. Avant de manipuler le composant, vérifiez que le contact métallique du bracelet antistatique est en contact avec votre peau et que l'autre extrémité du bracelet est raccordée à la terre.
- Use grounded and shielded Ethernet cables (when applicable) to ensure agency compliance with electromagnetic compliance (EMC) regulations.

  French Translation: Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).
- (PA-3200, PA-5200, PA-5400, PA-7000, and PA-7500 firewalls only) At least two people are recommended for unpacking, handling, and relocating the heavier firewalls.
- Do not connect a supply voltage that exceeds the input range of the firewall or appliance. For details on the electrical range, refer to electrical specifications in the hardware reference for your firewall or appliance.

  French Translation: Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.
- (Devices with serviceable batteries only) Do not replace a battery with an incorrect battery type; doing so can cause the replacement battery to explode. Dispose of used batteries according to local regulations.

  French Translation: Ne remplacez pas la batterie par une batterie de type non adapté, cette dernière risquerait d'exploser. Mettez au rebut les batteries usagées conformément aux instructions.
- I/O ports are intended for intra-building connections only and not intended for OSP (Outside Plant) connections or any network connections subject to external voltage surge events.

• 	(All Palo Alto Networks appliances with two or more power supplies) Caution: Shock hazard Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware. **French Translation:** (Tous les appareils Palo Alto Networks avec au moins deux sources d'alimentation) Débranchez tous les cordons d'alimentation (c.a. ou c.c.) des entrées d'alimentation et mettez le matériel hors tension.
• 	(PA-7000 Series firewalls only) Caution: High touch current Connect to earth before connecting to the power supply. Ensure that the protective earthing conductor is connected to the provided ground lug on the rear side of the firewall.
• 	(PA-7000 Series firewalls only) When removing a fan tray from a PA-7000 Series firewall, first pull the fan tray out about 1 inch (2.5cm) and then wait a minimum of 10 seconds before extracting the entire fan tray. This allows the fans to stop spinning and helps you avoid serious injury when removing the fan tray. You can replace a fan tray while the firewall is powered on but you must replace it within 45 seconds and you can only replace one fan tray at a time to prevent the thermal protection circuit from shutting down the firewall. **French Translation:** (Pare-feu PA-7000 uniquement) Lors du retrait d'un tiroir de ventilation d'un pare-feu PA-7000, retirez tout d'abord le tiroir sur 2,5 cm, puis patientez au moins 10 secondes avant de retirer complètement le tiroir de ventilation. Cela permet aux ventilateurs d'arrêter de tourner et permet d'éviter des blessures graves lors du retrait du tiroir. Vous pouvez remplacer un tiroir de ventilation lors de la mise sous tension du pare-feu. Toutefois, vous devez le faire dans les 45 secondes et vous ne pouvez remplacer qu'un tiroir à la fois, sinon le circuit de protection thermique arrêtera le pare-feu.

The following applies only to Palo Alto Networks firewalls that support a direct current (DC) power source:

French Translation: Les instructions suivantes s'appliquent uniquement aux pare-feux de Palo Alto Networks prenant en charge une source d'alimentation en courant continu (c.c.):

- Do not connect or disconnect energized DC wires to the power supply.

  French Translation: Ne raccordez ni débranchez de câbles c.c. sous tension à la source d'alimentation.
- The DC system must be earthed at a single (central) location.

  French Translation: Le système c.c. doit être mis à la terre à un seul emplacement (central).
- The DC supply source must be located within the same premises as the firewall.

  French Translation: La source d'alimentation c.c. doit se trouver dans les mêmes locaux que ce pare-feu.
- The DC battery return wiring on the firewall must be connected as an isolated DC (DC-I) return.

  French Translation: Le câblage de retour de batterie c.c. sur le pare-feu doit être raccordé en tant que retour c.c. isolé (CC-I).
- The firewall must be connected either directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

  French Translation: Ce pare-feu doit être branché directement sur le conducteur à électrode de mise à la terre du système d'alimentation c.c. ou sur le connecteur d'une barrette/d'un bus à bornes de mise à la terre auquel le conducteur à électrode de mise à la terre du système d'alimentation c.c. est raccordé.
- The firewall must be in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthing conductor of the DC supply circuit and the earthing of the DC system.

  French Translation: Le pare-feu doit se trouver dans la même zone immédiate (des armoires adjacentes par exemple) que tout autre équipement doté d'un raccordement entre le conducteur de mise à la terre du même circuit d'alimentation c.c. et la mise à la terre du système c.c.
- Do not disconnect the firewall in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

  French Translation: Ne débranchez pas le pare-feu du conducteur du circuit de mise à la terre entre la source d'alimentation c.c. et le point de raccordement du conducteur à électrode de mise à la terre.
- Install all firewalls that use DC power in restricted access areas only. A restricted access area is where access is granted only to craft (service) personnel using a special tool, lock and key, or other means of security, and that is controlled by the authority responsible for the location.

  French Translation: Tous les pare-feux utilisant une alimentation c.c. sont conçus pour être installés dans des zones à accès limité uniquement. Une zone à accès limité correspond à une zone dans laquelle l'accès n'est autorisé au personnel (de service) qu'à l'aide d'un outil spécial,

cadenas ou clé, ou autre dispositif de sécurité, et qui est contrôlée par l'autorité responsable du site.

- Install the firewall DC ground cable only as described in the power connection procedure for the firewall that you are installing. You must use the American wire gauge (AWG) cable specified and torque all nuts to the torque value specified in the installation procedure for your firewall.

  French Translation: Installez le câble de mise à la terre c.c. du pare-feu comme indiqué dans la procédure de raccordement à l'alimentation pour le pare-feu que vous installez. Utilisez le câble American wire gauge (AWG) indiqué et serrez les écrous au couple indiqué dans la procédure d'installation de votre pare-feu pare-feu.

- The firewall permits the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment as described in the installation procedure for your firewall.

  French Translation: Ce pare-feu permet de raccorder le conducteur de mise à la terre du circuit d'alimentation c.c. au conducteur de mise à la terre de l'équipement comme indiqué dans la procédure d'installation du pare-feu.

- A suitably-rated DC mains disconnect device must be provided as part of the building installation.

  French Translation: Un interrupteur d'isolement suffisant doit être fourni pendant l'installation du bâtiment.

PA-400R Series Firewall Overview

The Palo Alto Networks® PA-400R Series Next-Generation firewalls include the PA-410R, PA-410R-5G, PA-450R, and PA-450R-5G. These rugged-designed firewalls are built for uncontrolled environments with varying temperature and humidity levels. They include the following main features: a TPM module for PAN-OS key storage and security, active/passive and active/active high availability (HA), 5G capability for select models, local logging (PA-410R and PA-410R-5G only), and ZTP functionality. The PA-400R firewalls enable you to secure your organization through advanced visibility and control of applications, users, and content.

First Supported PAN-OS® Software Release:

- **PAN-OS 11.1**—PA-450R
- **PAN-OS 11.1.3**—PA-410R and PA-450R-5G
- **PAN-OS 11.1.4**— PA-410R-5G

The following topics describe the hardware features of the PA-400R firewalls. To view or compare performance and capacity information, refer to the Product Selection tool.

- PA-400R Series Front Panel
- PA-400R Series Back Panel
- PA-400R Series Top and Bottom Panels
- Interpret the LEDs on a PA-400R Series Firewall

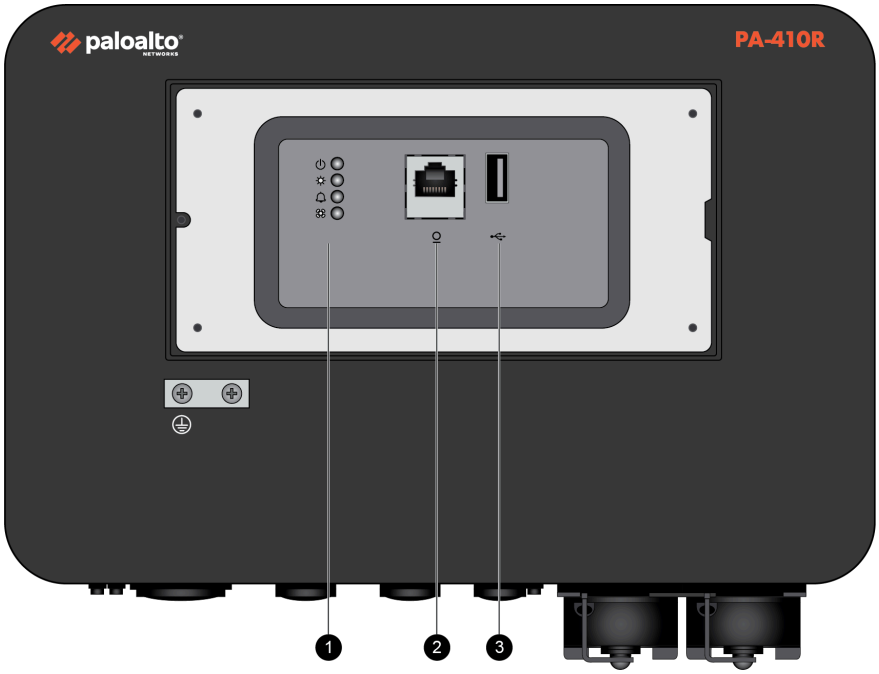
PA-400R Series Front Panel

View the front panel components of your PA-400R Series firewall.

- PA-410R
- PA-410R-5G
- PA-450R
- PA-450R-5G

To review the specifications of supported Palo Alto Networks® interfaces and transceivers, refer to the datasheet.

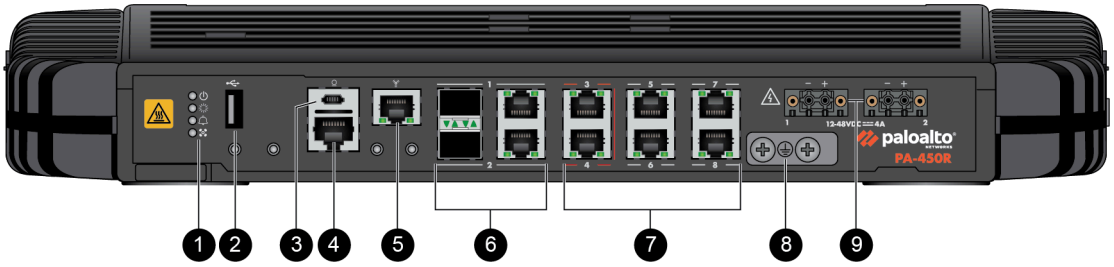
The front panels of the PA-410R and PA-410R-5G are similar except that the PA-410R-5G features antennas and has an additional LED to denote cellular status. The following image shows the front panel of the PA-410R with its cover removed. The table describes each front panel component.



Item	Component	Description
1	LED status indicators	LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400R Series Firewall). The PA-410R has four LEDs and the PA-410R-5G has five LEDs.

Item	Component	Description
2	CONSOLE port	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
3	USB port	Use this USB port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.

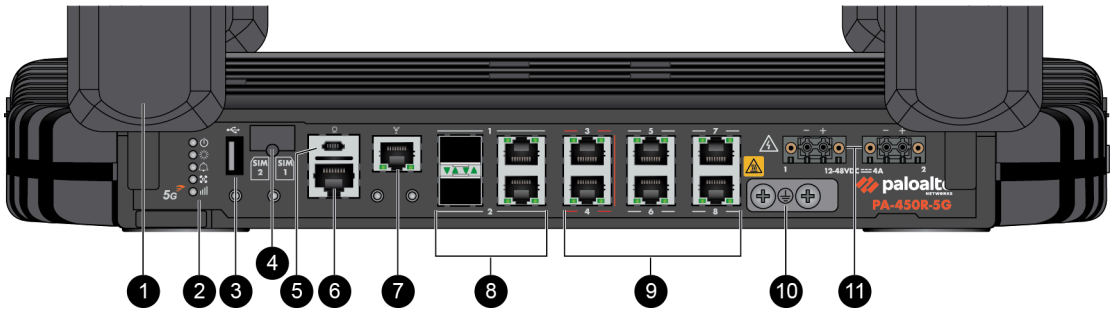
The following image shows the front panel of the PA-450R and the table describes each front panel component.



Item	Component	Description
1	LED status indicators	Four LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400R Series Firewall).
2	USB port	Use this port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.
3	CONSOLE port (Micro USB)	Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable (not included with the firewall). The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Refer to Micro USB Console Port for more information and to download the Windows driver or to learn how to connect from a Mac or Linux computer.
4	CONSOLE port (RJ-45)	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).

Item	Component	Description
		Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
5	Management port	Use this Ethernet 1Gbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures.
6	SFP/RJ-45 combo ports	Two SFP/RJ-45 combo ports for 10/100/1000Mbps speeds.
7	RJ-45 ports	Six RJ-45 10/100/1000Mbps ports for network traffic. Ports 3 and 4 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure.
8	Ground studs	Use a dual screw ground lug to connect the firewall to earth ground (ground cable not included).
9	DC power inputs	Use the DC power inputs to connect power to the firewall. A second power supply can be used for redundancy.

The following image shows the front panel of the PA-450R-5G and the table describes each front panel component.



Item	Component	Description
1	Antennas	Four antennas that provide 5G connectivity to the device. The firewall does not ship with the antennas installed.
2	LED status indicators	Five LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400R Series Firewall).
3	USB port	Use this port to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.
4	SIM slot	Install up to two nano SIMs into this slot to enable mobile network connectivity. *The SIM cards must be rated to 85C.*
5	CONSOLE port (Micro USB)	Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable (not included with the firewall). The console connection provides access to firewall boot messages, the

Item	Component	Description
		Maintenance Recovery Tool (MRT), and the command line interface (CLI). Refer to Micro USB Console Port for more information and to download the Windows driver or to learn how to connect from a Mac or Linux computer.
6	CONSOLE port (RJ-45)	Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software. The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI). Use the following settings to configure your terminal emulation software to connect to the console port: • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
7	Management port	Use this Ethernet 1Gbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures.
8	SFP/RJ-45 combo ports	Two SFP/RJ-45 combo ports for 10/100/1000Mbps speeds.

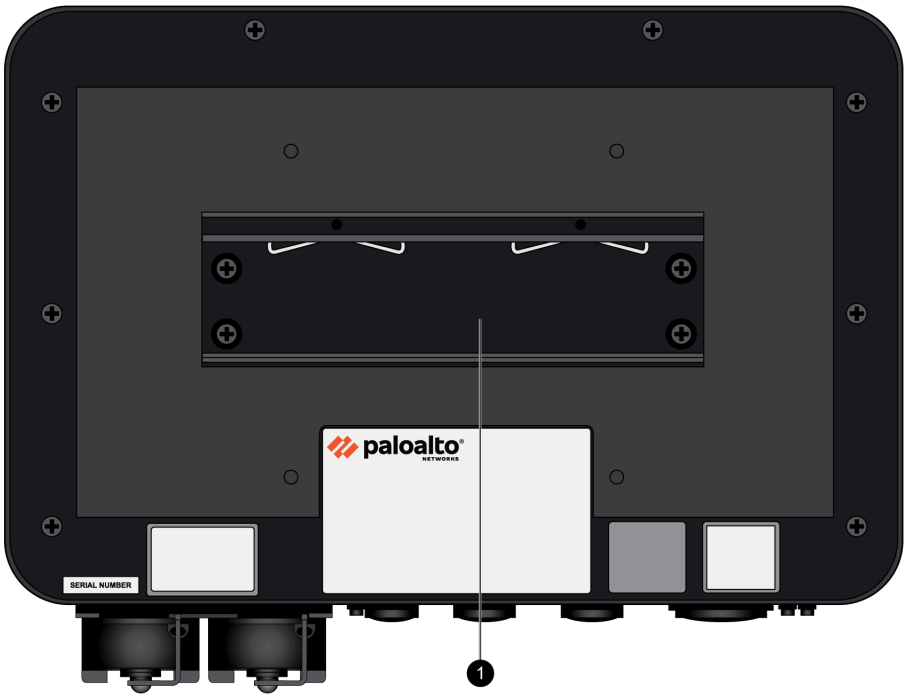
Item	Component	Description
9	RJ-45 ports	Six RJ-45 10/100/1000Mbps ports for network traffic. You can set the link speed and duplex mode or choose auto-negotiate. Ports 3 and 4 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure.
10	Ground studs	Use a dual screw ground lug to connect the firewall to earth ground (ground cable not included).
11	DC power inputs	Use the DC power inputs to connect power to the firewall. A second power supply can be used for redundancy.

PA-400R Series Back Panel

View the back panel components of your PA-400R Series firewall.

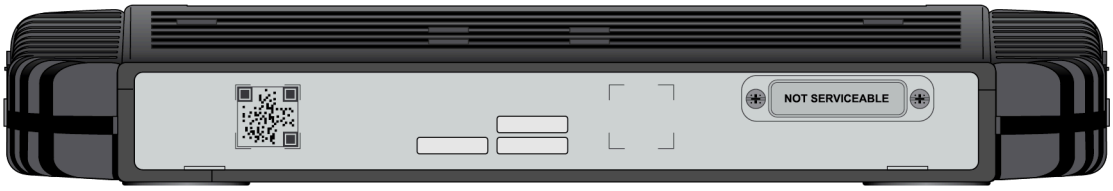
- PA-410R
- PA-410R-5G
- PA-450R
- PA-450R-5G

The back panels of the PA-410R and PA-410R-5G are identical. The following image shows the back panel of the PA-410R and the table describes each back panel component.



Item	Component	Description
1	DIN rail mounting clip	Use this mounting clip to Install the PA-400R Series Firewall on a DIN Rail *The four holes around the DIN rail clip can be used with a 100 x 100 VESA wall mount.*

The following image shows the back panel of the PA-450R. There are no serviceable components on the back panel.



The following image shows the back panel of the PA-450R-5G. There are no serviceable components on the back panel.

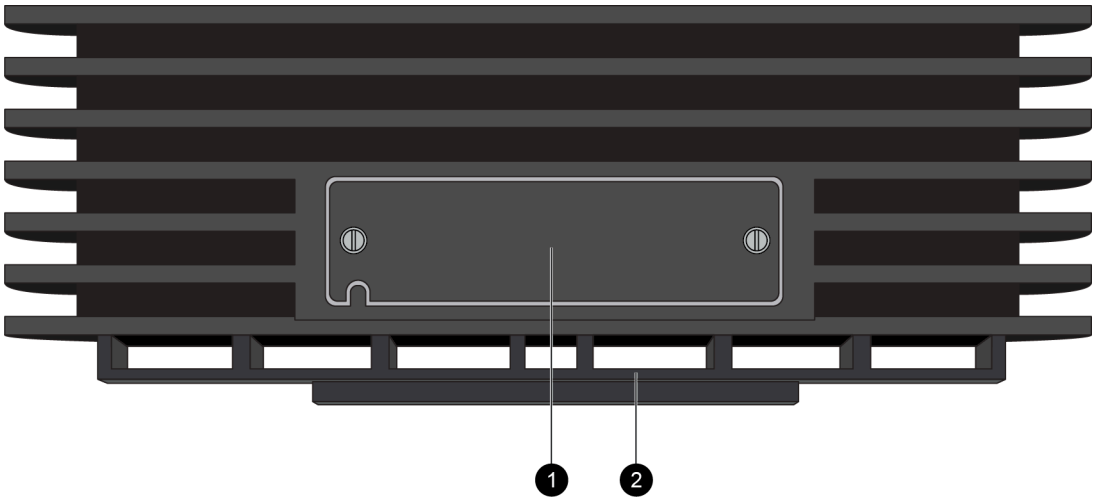
PA-400R Series Top and Bottom Panels

View the top and bottom panel components of your PA-400R Series firewall.

- PA-410R and PA-410R-5G

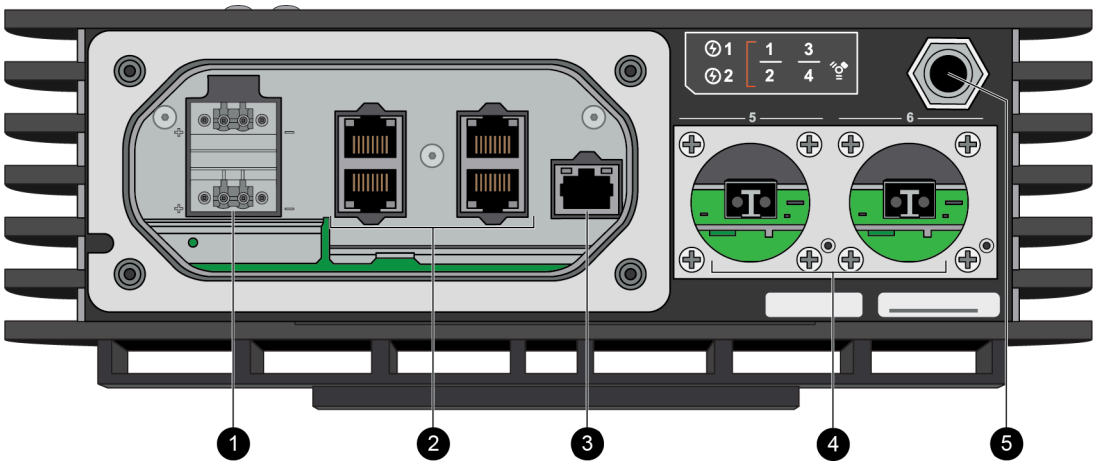
The PA-410R and PA-410R-5G firewalls feature serviceable components on the top and bottom panels.

The top panels of the PA-410R and PA-410R-5G are identical. The following image shows the top panel of the PA-410R and the table describes each back panel component.



Item	Component	Description
1	SIM slot	After removing the cover, install up to two nano SIM cards into this slot to enable multiple mobile network connectivity. *The nano SIM cards installed must be industrial grade and rated to 105C.*
2	DIN rail mounting clip	Use this mounting clip to Install the PA-400R Series Firewall on a DIN Rail

The bottom panels of the PA-410R and PA-410R-5G are identical except that the PA-410R-5G features antennas. The following image shows the bottom panel of the PA-410R after the cover and caps have been removed and the table describes each bottom panel component.



Item	Component	Description
1	DC Power Inputs	The firewall operates on 12-48VDC power. Use the DC power inputs to connect power to the firewall. A second, optional power supply can be used for redundancy.
2	RJ-45 Ports	Four RJ-45 10/100/1000Mbps ports for network traffic. You can set the link speed and duplex mode or choose auto-negotiate. Ports 1 and 2 are fail-open ports. They can be configured to provide a pass-through connection despite power or operating system failure.
3	Management port	Use this Ethernet 1Gbps port to access the management web interface and perform administrative tasks. The firewall also uses this port for management services, such as retrieving licenses and updating threat and application signatures.
4	SFP Ports	Two SFP ports for 10/100/1000Mbps speeds.
5	Breather valve	A breather valve that prevents the buildup of condensation in the sealed enclosure.

Interpret the LEDs on a PA-400R Series Firewall

The following table describes how to interpret the status LEDs on all of the PA-400R Series firewalls.

LED	Description
Front Panel LEDs	
 (Power)	• Green—The firewall is powered on. • Off—The firewall is not powered on or an error has occurred with the internal power system (for example, power is not within tolerance levels).
 (Status)	• Green—The firewall is operating normally. • (PA-410R, PA-410R-5G, PA-450R, and PA-450R-5G) Yellow—The firewall is booting.
 (Alarm)	• Red—A hardware component failed, such as a power supply failure, a firewall failure that caused an HA failover, a drive failure, or hardware is overheating and the temperature is above the high temperature threshold. • Off—The firewall is operating normally.
 (High Availability)	• Green—The firewall is the active peer in an active/passive configuration. • Yellow—The firewall is the passive peer in an active/passive configuration. • Off—High availability (HA) is not operational on this firewall.  *In an active/active configuration, the HA LED only indicates HA status for the local firewall and has two possible states (green or off); it does not indicate HA connectivity of the peer. Green indicates that the firewall is either active-primary or active-secondary and off indicates that the firewall is in any other state (for example, non-functional or suspended).*
(PA-410R-5G and PA-450R-5G only)  (Cellular)	• Green—The firewall has an active signal. • Red—The firewall does not have a signal or the antenna is not connected. • Off—The modem is disabled.

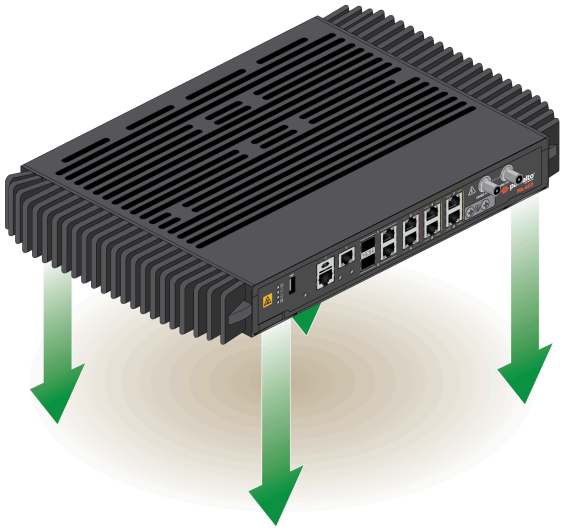
LED	Description
(PA-450R and PA-450R-5G) Ethernet port LEDs	• Left LED—Solid green indicates a network link. • Right LED—Blinking green indicates network activity. *If you configure the link state to **down** on a port, the LEDs on some activse ports will not work. Similarly, if the passive link state is set to **shutdown**, the HA link LEDs on the passive device in the HA pair will not work. To ensure your LEDs display correctly, avoid configuring link states to **down** or using the **shutdown** passive link state unless needed for security reasons.*

Install the PA-400R Series Firewall

The PA-400R Series next-generation firewalls can be installed in a number of different configurations depending on their design. The PA-450R and PA-450R-5G can be installed in a 19-inch equipment rack, on a flat surface, or on a wall. The PA-410R and PA-410R-5G ship with the hardware required to install the firewall on a DIN rail, while the equipment needed to install the firewall on a wall requires your own VESA mount.

Install the PA-400R Series Firewall on a Flat Surface

The PA-450R and PA-450R-5G firewalls have four circular feet on their bottom side that can be used to install the device in a horizontal position.



If you have a firewall that supports multi-band antennas, proceed to Install Antennas on the PA-400R Series 5G Firewall.

Keep the device clean and clear of dust to ensure optimal heat dissipation and maintain proper hardware operation.

Install the PA-400R Series Firewall on a Wall

The PA-450R and PA-450R-5G firewalls can be installed on a wall with the use of PAN-1RU-SMALL-WALLMNT.

The PA-410R and PA-410R-5G firewalls can be installed on a wall using a VESA mount (not provided by Palo Alto Networks). The firewall has a 100 x 100 VESA mount pattern and makes use of four M4 screws.

After installing, make sure to keep the device clean and clear of dust to ensure optimal heat dissipation and maintain proper hardware operation.

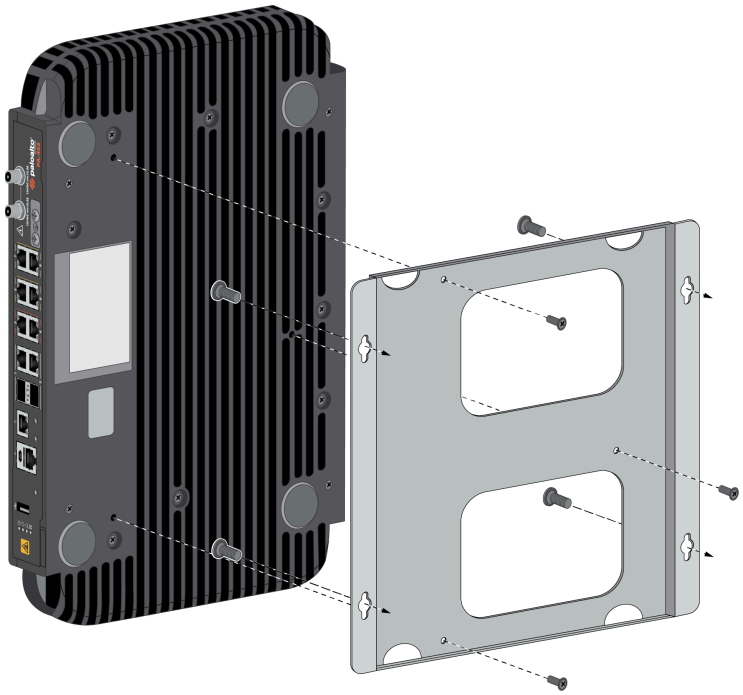
STEP 1 | Mark the locations on the wall that line up with the wall mount holes on the bottom of the wall mount.

Ensure there are no building services (water, gas, or wiring) behind the wall where you intend to install the firewall.

STEP 2 | Drill holes into the marked locations on the wall.

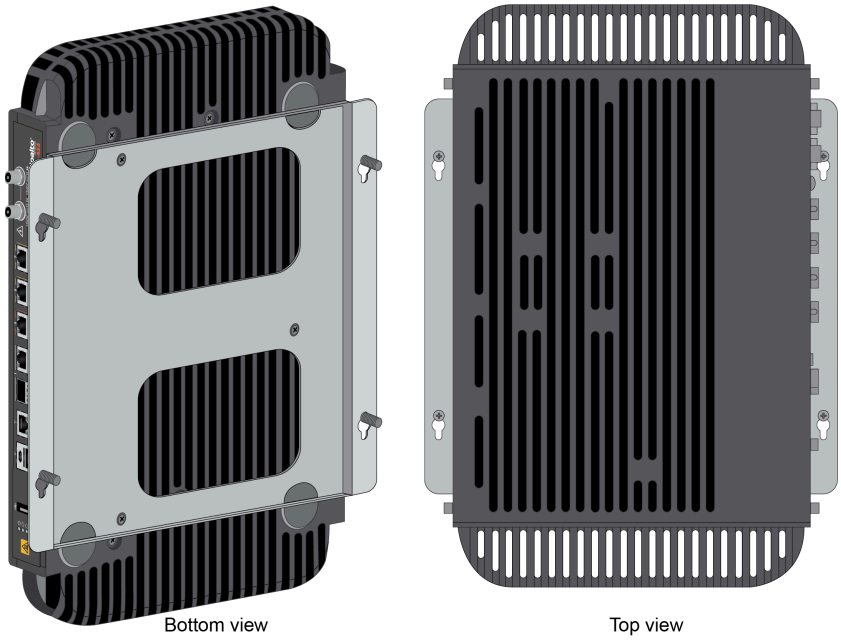
STEP 3 | Attach the firewall to the wall mount.

PA-450R and PA-450R-5G— Attach the firewall to the wall mount using three #6-32 screws and a #2 Phillips-head screwdriver.



STEP 4 | Attach the wall mount to the wall.

PA-450R and PA-450R-5G— Attach the wall mount to the wall using four screws that are appropriate for your wall. Sheet metal and drywall inserts are included with the wall mount kit.



Bottom view

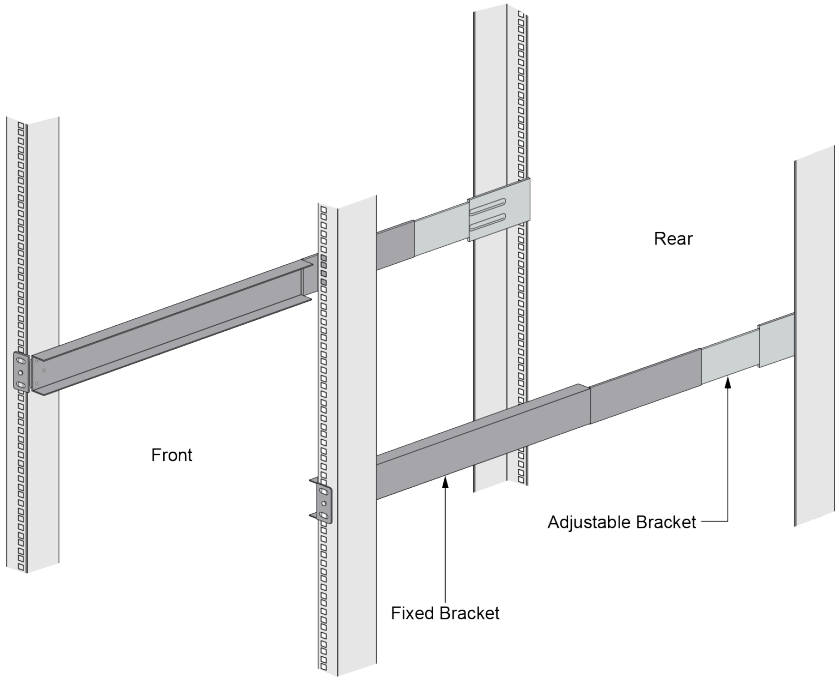
Top view

Install the PA-400R Series Firewall in an Equipment Rack

One PA-450R or PA-450R-5G firewall can be mounted in a 19” equipment rack using the PAN-1RU-SMALL-RACK4. The mounting equipment requires 1 RU of rack space.

After installing, make sure to keep the device clean and clear of dust to ensure optimal heat dissipation and maintain proper hardware operation.

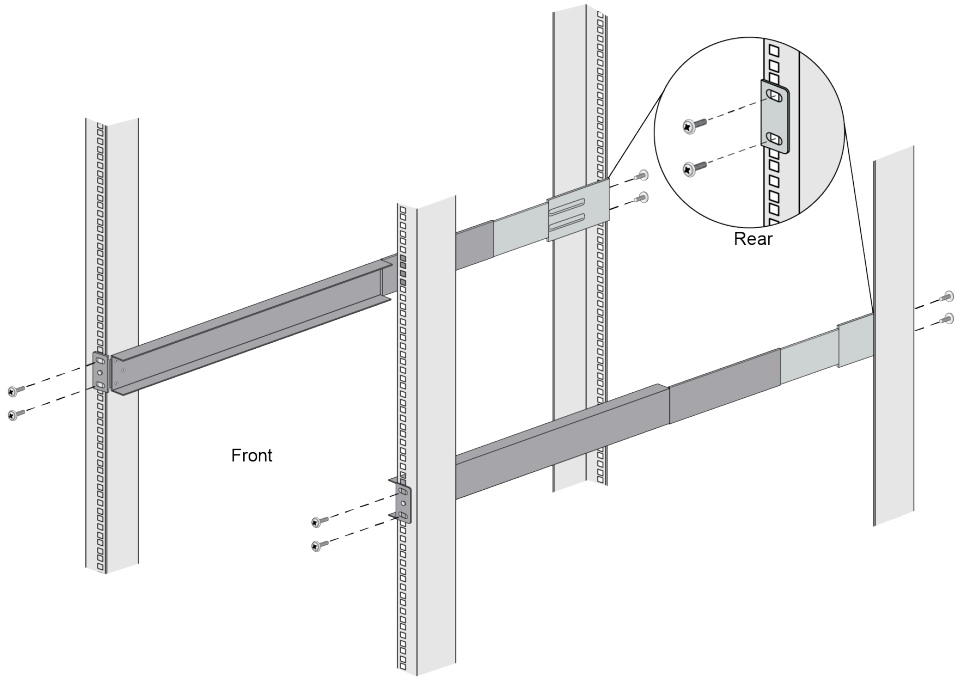
STEP 1 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



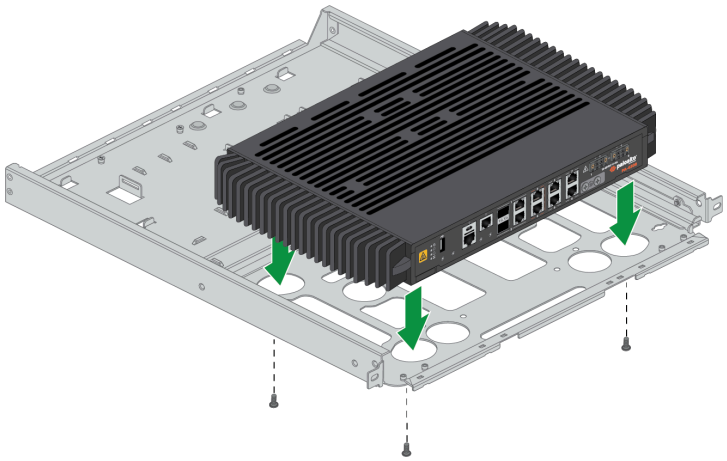
STEP 2 | Align the bottom edge of the mounting rails to the bottom of the 1 RU (1.5 RU if there is another device above) reserved for your firewall. Align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.

The mounting rails are designed for equipment frames that are 26” to 32” deep.

STEP 3 | Secure the rails to the equipment frame with mounting screws (not provided) compatible with your equipment frame. Tighten the screws to their recommended torque value.

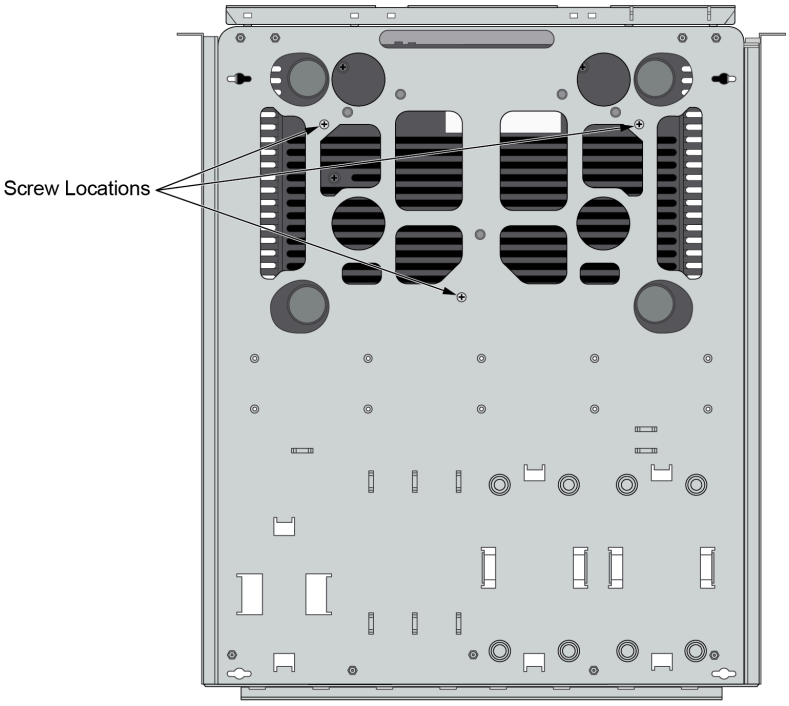


STEP 4 | With the front of the firewall facing forward, align the four rubber feet on the bottom of the device to the slotted holes in the provided mounting tray.



STEP 5 | While holding the firewall, carefully flip the mounting tray over to reveal its underside.

STEP 6 | Secure the firewall in place using three of the provided #6-32 x 3/16” Long Flathead screws.



Underneath Side of the Mounting Tray

STEP 7 | Flip the mounting tray back into an upright position.

STEP 8 | Follow the instructions to Connect DC Power to a PA-400R Series Firewall.

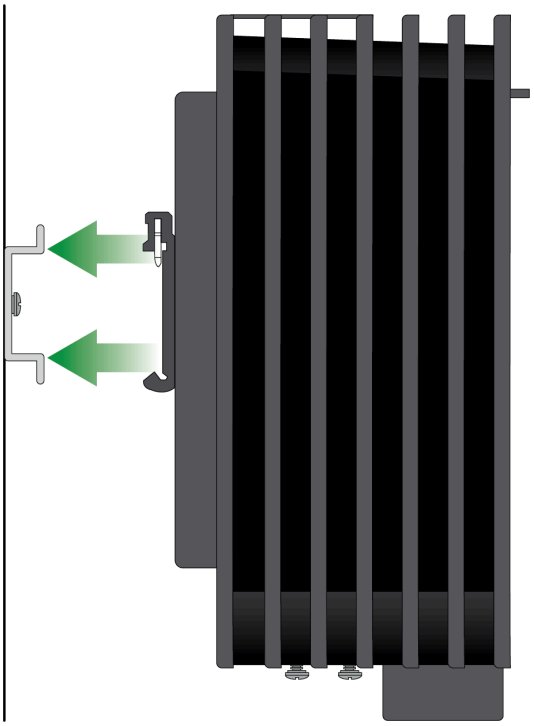
STEP 9 | Slide the mounting tray into the rails previously fixed to the equipment rack. Stop when the front flange on the mounting tray is flush with the front of the rail.

STEP 10 | Align the slotted holes in the mounting tray to the holes in the equipment frame. Secure the mounting tray to the equipment frame on both sides using 3 screws each (not provided). The screws must be compatible with your equipment frame.

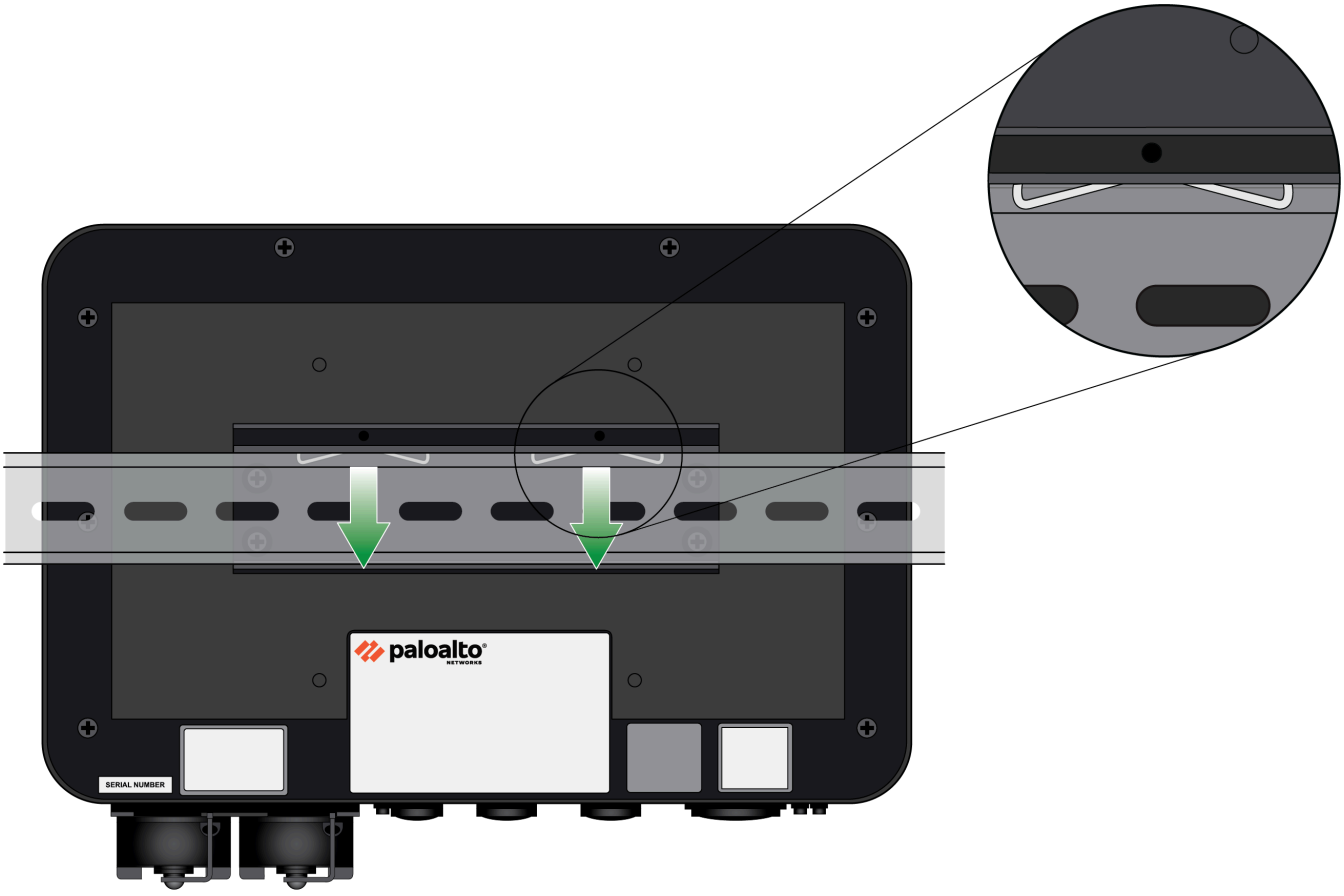
Install the PA-400R Series Firewall on a DIN Rail

The PA-410R and PA-410R-5G firewalls can be installed on a DIN rail using PAN-PA-RGD-DIN-CLIP. This DIN rail mounting clip must be purchased separately.

STEP 1 | Using four M4 screws, install the DIN rail mounting clip to the back panel of the device. Ensure that you orient the firewall so that the bottom panel of the device is facing downwards and the DIN rail mounting clip aligns with the DIN rail.



STEP 2 | Using slight downward pressure, attach the firewall onto the DIN rail so that the two metal clips lock into place.



Keep the device clean and clear of dust to ensure optimal heat dissipation and maintain proper hardware operation.

Connect Cables to the PA-400R Series Firewall

The following procedures describe how to install the waterproof cabling and protective panel of the PA-410R and PA-410R-5G firewall. The process to connect the power cables is covered in Connect Power to a PA-400R Series Firewall.

(PA-410R and PA-410R-5G) You must use IP65 rated cable glands if you want to provide IP65 ingress protection for the firewall. Cable glands can be purchased separately from Palo Alto Networks or from another supplier.

The PAN-PA-RGD-GLND1 includes one M20 (for one power cable) and three M12 glands (for three RJ-45 cables). The PAN-PA-RGD-GLND2 includes a gland for one fiber cable. It takes two of each set to fully populate all the cables in the firewall.

- Connect Ethernet Cables to the PA-400R Series Firewall
- Connect Fiber Cables to the PA-400R Series Firewall

Connect Ethernet Cables to the PA-400R Series Firewall

This topic describes how to connect Ethernet cables to the PA-410R and PA-410R-5G firewall using cable glands.

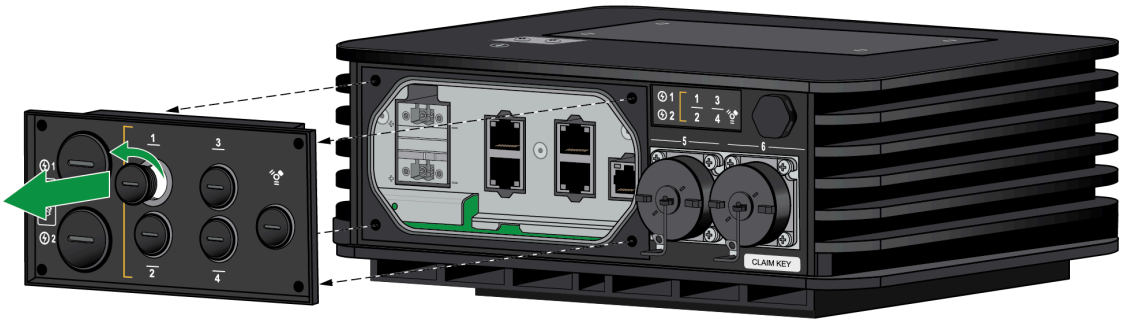
(PA-410R and PA-410R-5G only) The PAN-PA-RGD-GLND1 includes one M20 (for one power cable) and three M12 glands (for three RJ-45 cables). It must be purchased separately.

STEP 1 | Unscrew the four screws on the bottom panel of the firewall.

- **PA-410R and PA-410R-5G**—Use a flathead screwdriver.

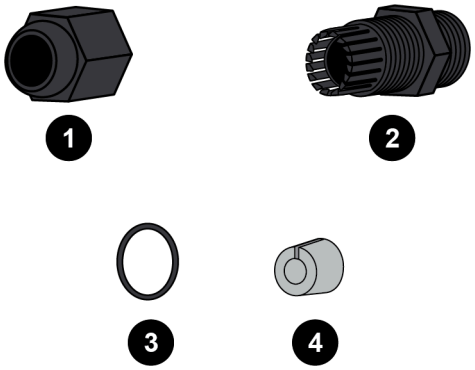
STEP 2 | On the removed panel, unscrew the stopping plug that lines up with the Ethernet port you are connecting to.

- **PA-410R and PA-410R-5G**—Each stopping plug corresponds to one Ethernet port.



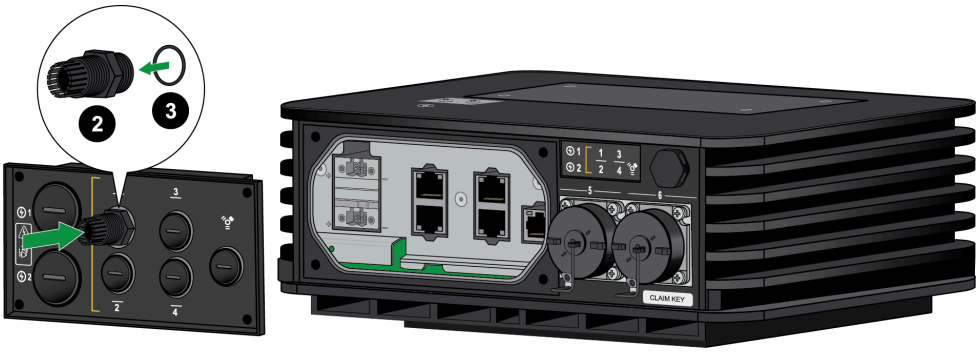
STEP 3 | Unpack the cable glands.

- **PA-410R and PA-410R-5G**—You must have either purchased PAN-PA-RGD-GLND1 or acquired other standard M12 cable glands. There are four necessary items — an end cap, panel connector, seal, and grommet.



STEP 4 | Install the seal onto the shorter end of the panel connector. Make sure to push the seal until it is flush against the nut. Screw the shorter end of the panel connector into the hole that corresponds to the port being connected. Make sure that the connector is secure by torquing to 1.5 Nm.

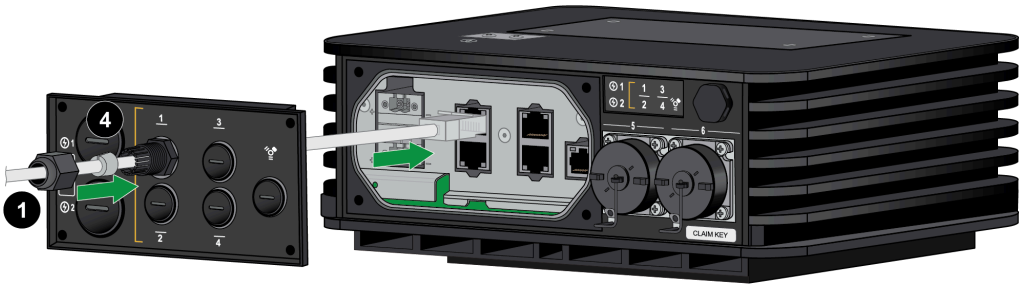
PA-410R and PA-410R-5G



STEP 5 | Thread the cable through the end cap. This is used to secure the cable gland once the panel is reattached at the end of the procedure. Feed the cable through the gray grommet. Move

the cable through the panel connector and gently push the end into the port until you hear a click.

PA-410R and PA-410R-5G



STEP 6 | Repeat Steps 4 and 5 for any additional cables.

STEP 7 | Follow the procedure to Connect DC Power to a PA-400R Series Firewall before you continue to the next step.

STEP 8 | Once all cables are connected, make sure that any unused ports have a stopping plug in the corresponding panel slot.

- **PA-410R and PA-410R-5G**—Ensure that all Ethernet and power cables are connected before continuing to the next step.

STEP 9 | Align the panel with the four screw holes on the firewall. Using the appropriate screwdriver, screw the panel back into its original place.

- **PA-410R and PA-410R-5G**

STEP 10 | Push the end caps along each cable until the end caps reach their respective panel connector.

- **PA-410R and PA-410R-5G**

Connect Fiber Cables to the PA-400R Series Firewall

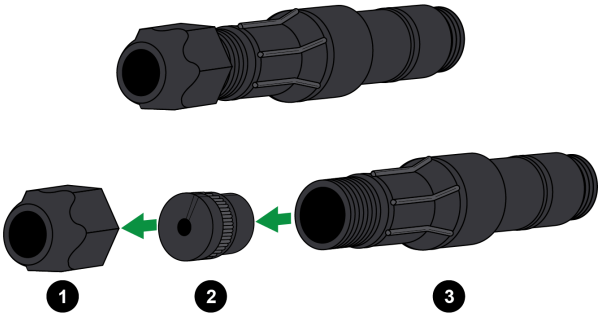
This topic describes how to connect fiber cables to the PA-410R or PA-410R-5G firewall using cable glands.

The PAN-PA-RGD-GLND2 (purchased separately) includes a gland for one fiber cable.

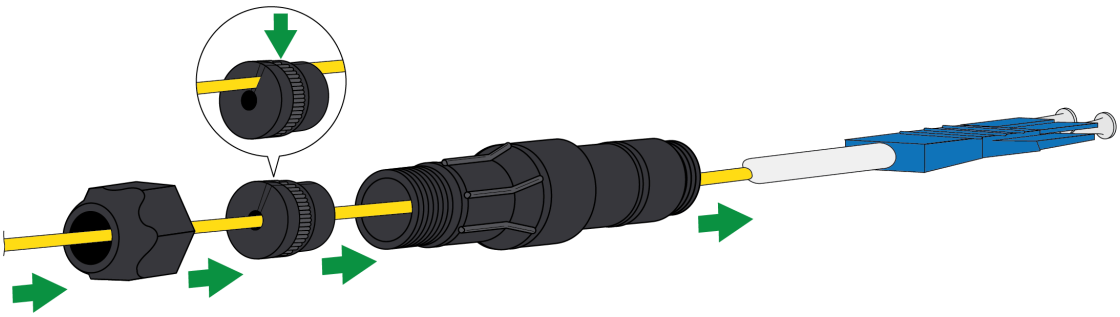
STEP 1 | Insert your transceiver into the SFP port you are connecting the cable to.

The grommet used will differ based on whether you install a copper or fiber transceiver.

STEP 2 | Unpack the fiber cable gland and separate it into three components — the connector, seal, and end cap.



STEP 3 | Thread the fiber cable through the end cap. Unlatch the seal and fit the cable into it, then close the seal latch. Thread the fiber cable through the connector so that the three components are in the order pictured.



STEP 4 | Connect the fiber cable to the installed transceiver. Move the three cable gland components towards the firewall. Push the seal into the connector.

STEP 5 | Push the connector up to the the SFP port and turn the connector clockwise until there is a click. Make sure that the connector is securely locked in place.

STEP 6 | Screw the end cap into the seal and tighten it until the end cap is securely fastened.

STEP 7 | Repeat Steps 1 through 6 on the other SFP port if you are connecting a second fiber cable.

Install Antennas on the PA-400R Series 5G Firewall

The PA-410R-5G and PA-450R-5G firewalls each support four multi-band antennas. The following procedure describes how to install the to the four antenna SMA (F) connectors on the firewall.

(PA-450R and PA-450R-5G only) The antennas must be connected before the firewall is installed in an equipment rack.

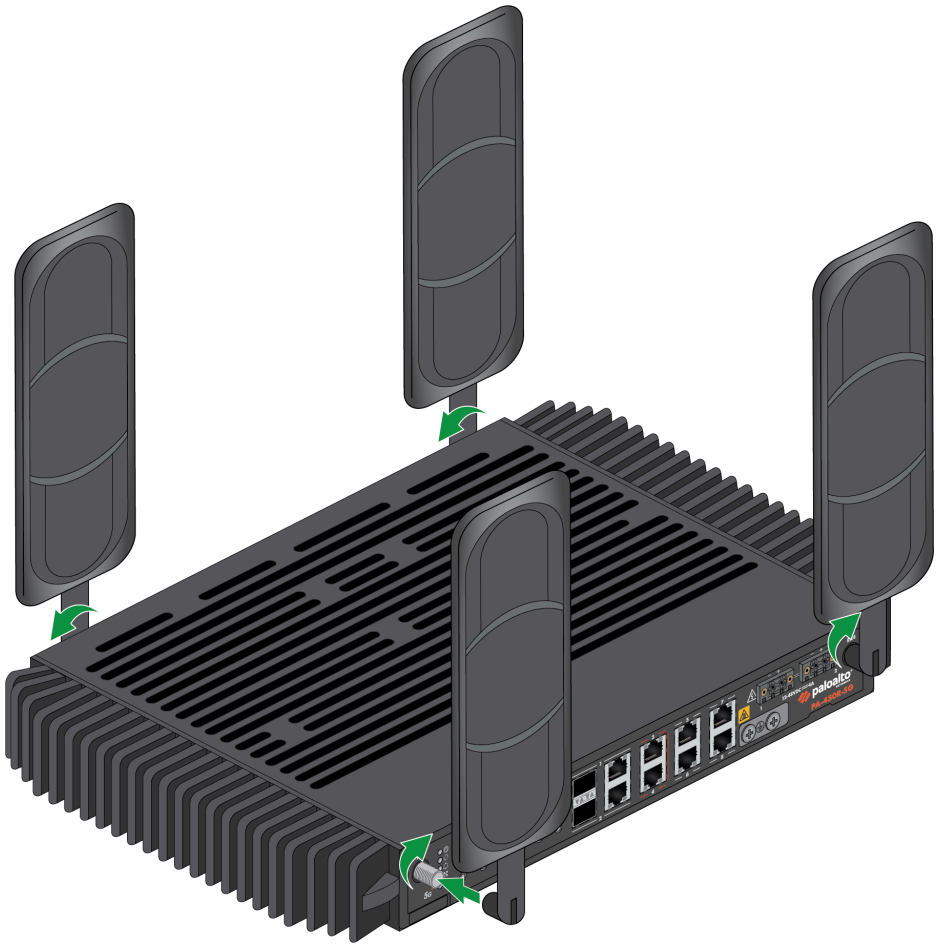
Before installing the firewall, it is recommended that you conduct a cellular location assessment of the installation site to receive the best signal strength before installing the device.

If installing the firewall on a wall or on a flat surface, it is recommended that you orient the antennas upright and slanted slightly outwards, not exceeding 45 degrees, to improve the signal quality.

STEP 1 | Secure the antennas to the SMA connectors located at the corners of the device. Make sure to tighten each antenna by hand. The antennas are fixed at a 90 degree orientation but can be repositioned after installation.

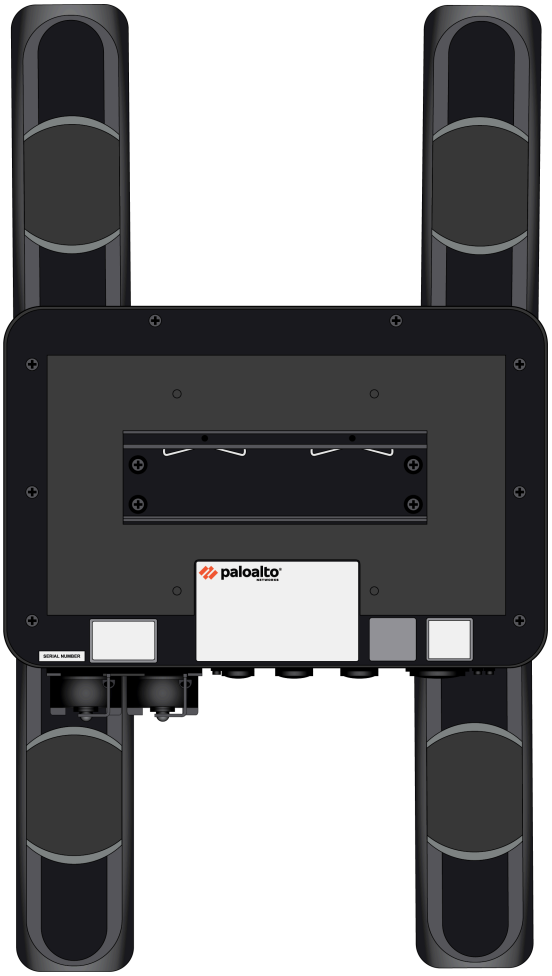
(PA-410R-5G)

(PA-450R-5G)



STEP 2 | (PA-410R-5G only) Fold the antennas at a 90 degree angle so that the device can be appropriately installed on a wall or DIN rail. While viewing the back panel of the device,

ensure that the top two antennas point straight up and that the bottom two antennas point straight down.



STEP 3 | Adjust the antenna orientation to receive the optimal signal strength in your environment.

Check the signal strength of the firewall by viewing the Cellular LED (see Interpret the LEDs on a PA-400R Series Firewall) or by checking the Firewall Web Interface.

- *Do not point the antennas towards one another or place them close to one another.*
- *Ensure that power cables do not cross over the antennas as this can cause signal quality distortion and antenna performance degradation.*

Insert a SIM Card into a PA-400R Series Firewall

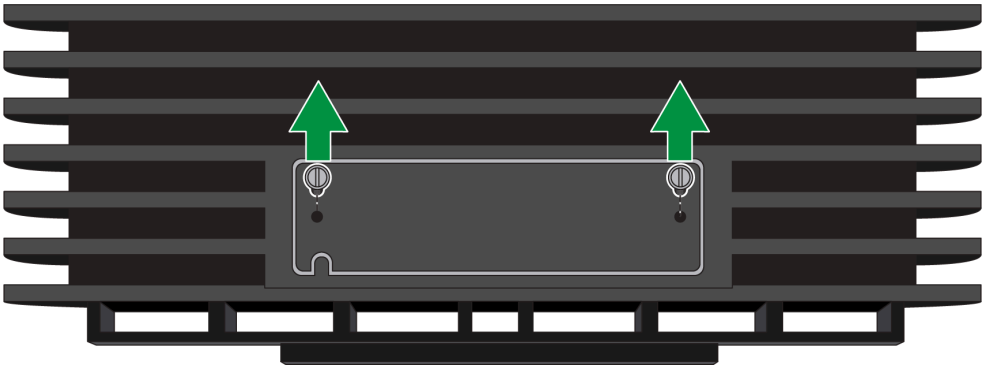
The PA-410R-5G supports two nano SIM cards to enable mobile network connectivity. The SIM slot is located on the top panel of the firewall.

The PA-450R-5G supports two nano SIM cards to enable mobile network connectivity. The SIM slots are located on the front panel of the firewall. SIM 1 is the bottom slot and SIM 2 is the top slot.

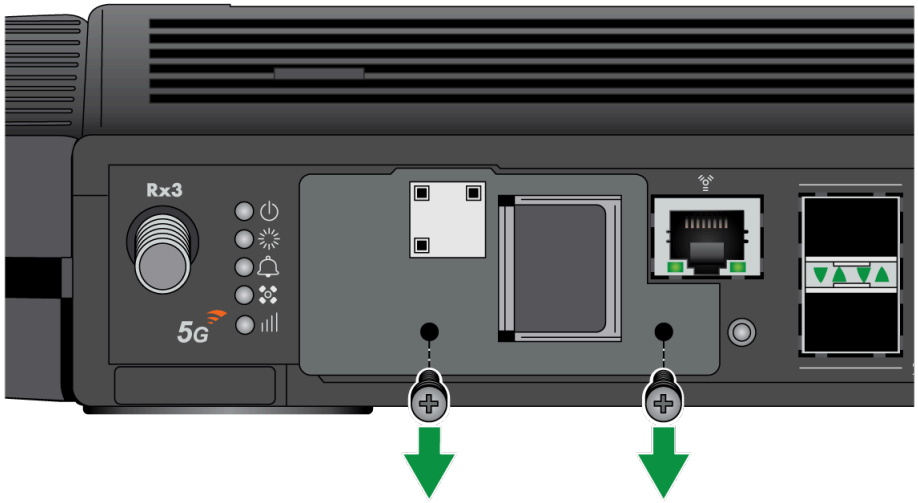
The PA-410R-5G requires industrial grade SIM cards rated for -40° to 105° C. Industrial grade SIM cards are also recommended for other models if they are being deployed in <0° to 40° C temperature.

STEP 1 | Remove the SIM cover.

PA-410R-5G—Unfasten the two screws using a flathead screwdriver.



PA-450R-5G—Unfasten the two screws using a Philips head screwdriver.



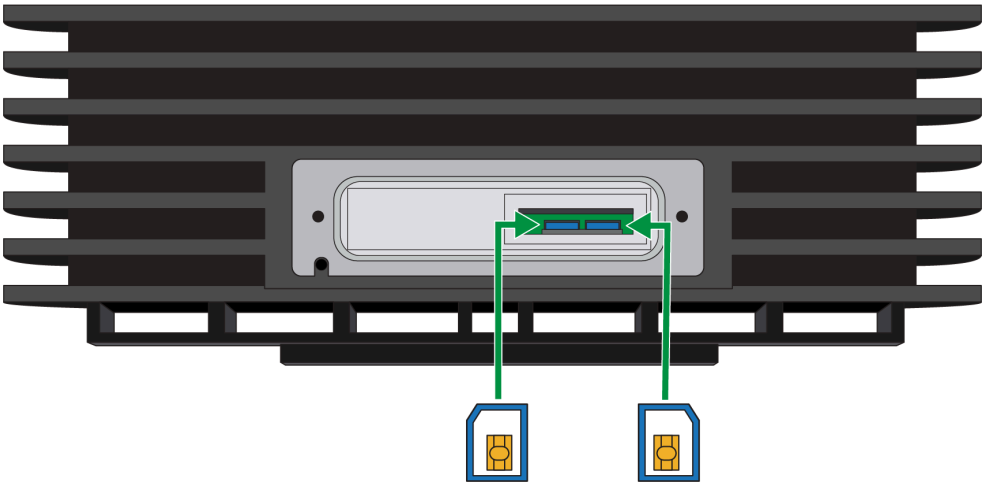
STEP 2 | With the chamfered corner (sloping edge) of the SIM facing towards the slot, gently push the SIM into the SIM 1 or SIM 2 slot until the SIM clicks into position.

The SIM may get damaged if you attempt to insert it into the slot by the wrong end.

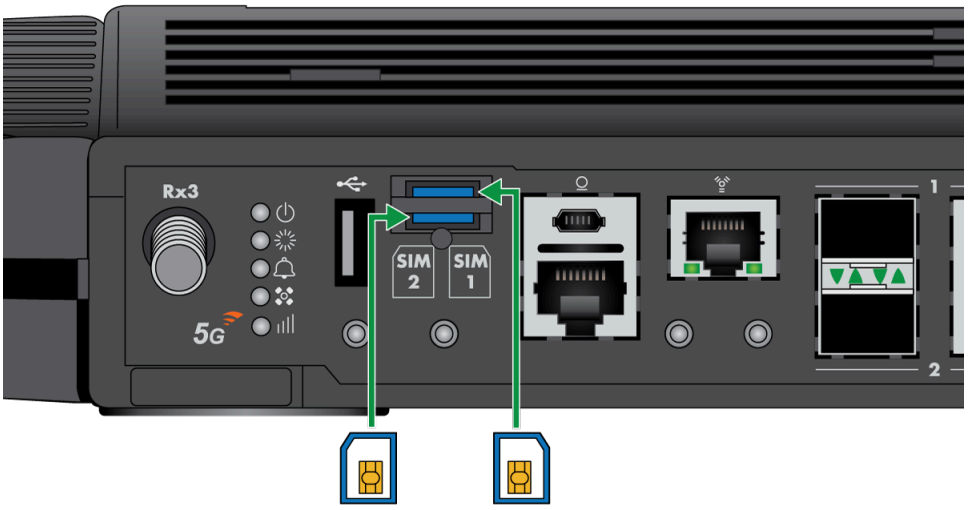
Tweezers may be required to install the SIM cards.

SIM 1 is the primary SIM slot by default. If you intend to use only one SIM, it is recommended to use SIM 1 as the primary slot. If you want to use SIM 2 as the primary slot, you must manually configure SIM 2 as the primary SIM slot using the Web Interface.

(PA-410R-5G)



(PA-450R-5G)



STEP 3 | After inserting the SIM, place the SIM cover back onto the device and refasten the screw(s).

To eject the SIM from the device, gently push the SIM inward using your fingertip. Release your fingertip and pull out the SIM. It is recommended that you use tweezers to extract the SIM.

Set Up a Connection to the Firewall

On first startup, the PA-400R Series firewall boots into Zero Touch Provisioning (ZTP) mode by default. ZTP mode allows you to automate the provisioning process of a new firewall that is added to a Panorama™ management server. To learn more about ZTP, see ZTP Overview. You can also bring the PA-400R Series firewall online in standard mode. See the instructions below to learn how to boot in ZTP or standard mode.

If you have already booted up the firewall and selected the wrong mode, you must perform a factory reset or private-data-reset before continuing.

- Reset the Firewall to Factory Default Settings *describes how to do a factory reset.*
- *To use the private-data-reset command, you must access the firewall CLI and enter the command* ***request system private-data-reset****. This command will remove all logs and restore the default configuration.*

Before you can successfully add a ZTP firewall to Panorama, you must ensure that a Dynamic Host Configuration Protocol (DHCP) server is deployed on the network. A DHCP server is required to successfully onboard a ZTP firewall to Panorama. The ZTP firewall is unable to connect to the Palo Alto Networks ZTP service to facilitate onboarding without a DHCP server.

ZTP mode is disabled if FIPS-CC mode is enabled. If the firewall boots with FIPS-CC mode enabled, the firewall will automatically boot in standard mode.

STEP 1 | Use an RJ-45 Ethernet cable to connect the device to the correct port. The port(s) connected will depend on which mode you intend the firewall to run in.

- (Standard mode) Connect the Ethernet cable from the MGT port on the firewall to the RJ-45 port of your network switch.
- (ZTP mode) Connect the Ethernet cable from the ZTP port (Ethernet port 1) on the firewall to your network switch.

STEP 2 | Confirm that the connection to the MGT port or Ethernet port 1 has an active network switch.

An active switch allows the firewall to trigger a "link up" state on the port you connected to for your desired boot mode.

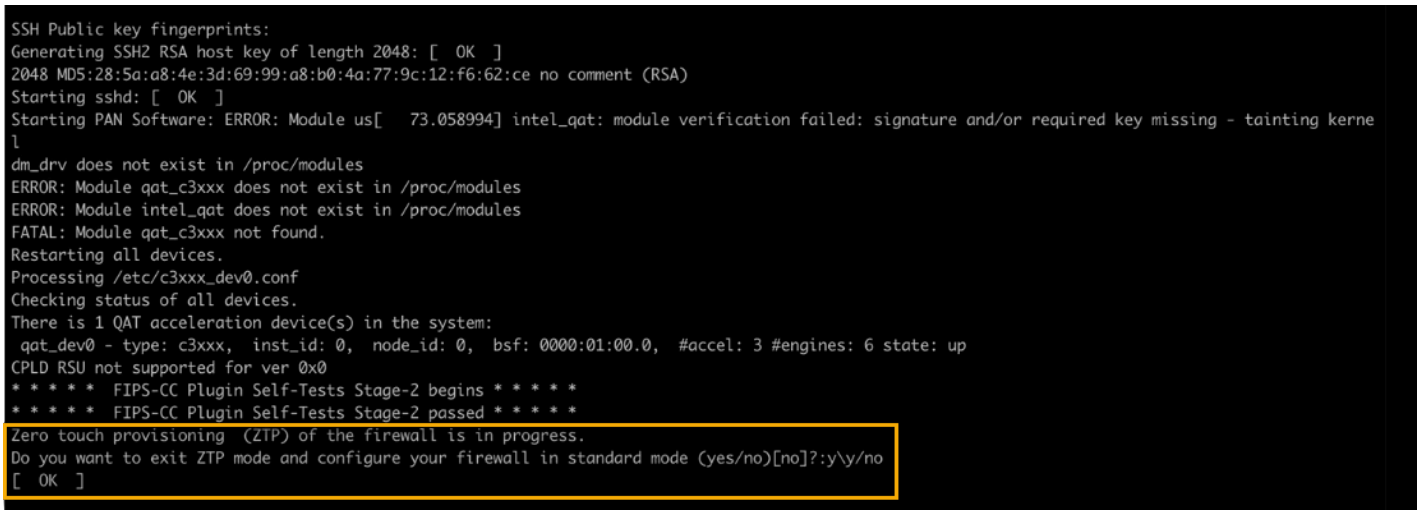
STEP 3 | (Standard mode only) If you intend to boot the firewall in standard mode, you will need access to the firewall CLI to respond to a prompt during bootup. Connect a console cable from the firewall console port to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY to access the CLI. See Access the CLI for more information.

STEP 4 | Power on the firewall. See Connect Power to a PA-400R Series Firewall to learn how to connect power to the firewall.

- (Standard mode) Using your terminal emulator, watch for the following CLI prompt as the firewall boots:

```
Do you want to exit ZTP mode and configure your firewall in
 standard mode (yes/no)[no]?
```

  Enter **yes**. The system will then ask you to confirm. Enter **yes** again to boot in standard mode.



> *If you miss the above CLI prompt, you can also change your boot mode using the web interface. Go to the firewall login screen at any point before or during the startup process. A prompt will ask if you wish to continue booting in ZTP mode or if you would like to switch to standard mode. Select **Standard Mode** and the firewall will begin rebooting in standard mode.*

- (ZTP mode) Stand by as the firewall boots up.

STEP 5 | Set up the firewall manually if using standard mode. If using ZTP mode, the device group and template configuration defined on the Panorama management server are automatically pushed to the firewall by the ZTP service.

- (Standard mode) Change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2. From a web browser, go to https://192.168.1.1. When prompted, log in to the web interface using the default username and password (admin/admin).
- (ZTP mode) Follow the instructions provided by your Panorama administrator to register your ZTP firewall. You will have to enter the serial number (12-digit number identified as S/N) and claim key (8-digit number). The claim key is required to add a ZTP firewall to the Panorama management server. These numbers are stickers attached to the back of the device.

Connect Power to a PA-400R Series Firewall

The PA-400R Series firewalls are powered by DC power and support power redundancy.

Learn how to Set Up a Connection to the Firewall based on your desired boot mode prior to powering on the firewall for the first time.

- Prepare to Connect Power to a PA-400R Series Firewall
- Connect DC Power to a PA-400R Series Firewall

Prepare to Connect Power to a PA-400R Series Firewall

The following information describes how to prepare the hardware that is required to connect power to a PA-410R or PA-410R-5G only.

On the other hand, the PA-450R and PA-450R-5G ship with the equipment needed to connect power to the firewall.

- **PA-410R, PA-410R-5G, PA-450R, and PA-450R-5G firewalls**— Connect DC power to the firewall.

(PA-410R and PA-410R-5G only) Due to the various cable lengths required for a given installation site, DC power and ground cables are not included with the firewall. The DC terminal blocks for connecting the DC power cables to the firewall is included in the accessories kit.

Required Hardware (PA-410R and PA-410R-5G only)

- **AWG cable (minimum 8 AWG)**—Use this cable for the ground cable and DC power cables.
- **Dual screw ground lug**—Use this lug to connect a ground cable to the screw-on ground points on the firewall.
- **Cable/wire strippers**—Use this tool to strip the cable shielding off the ends of the DC power and ground cables.
- **Screwdrivers**—Use these tools to attach the ground cable and DC power cables: use a Phillips-head screwdriver for the screw-on ground point and a small flat-head screwdriver to secure cables to the DC terminal block inputs.

Prepare for the Installation

STEP 1 | Read the Electrical Specifications for power requirements.

STEP 2 | (PA-410R and PA-410R-5G only) Measure and cut the DC power cables and ground cable. Ensure that the DC power cables reach from the firewall to your DC power source and that the ground cable reaches from the firewall to your ground location.

You will need one ground cable and two DC cables (one for the positive connection and one for the negative connection). To provide power redundancy for the firewall, prepare two additional DC power cables to connect the second set of DC power inputs.

Connect DC Power to a PA-400R Series Firewall

The following procedure describes how to connect DC power to a PA-410R , PA-410R-5G, PA-450R-5G, and PA-450R firewall. Before you continue, read how to Prepare to Connect Power to a PA-400R Series Firewall. The DC terminal block for connecting the DC power cables to the firewall is included in the accessories kit.

The PA-410R and PA-410R-5G firewalls use cable glands (purchased separately) to waterproof the inside of the device. The PAN-PA-RGD-GLND1 includes one M20 (for one power cable) and three M12 glands (for three RJ-45 cables).

To avoid injury to yourself or damage to your Palo Alto Networks® hardware or the data that resides on the hardware, read the Product Safety Warnings.

Power off the DC power sources that you will connect to the power supplies before you continue.

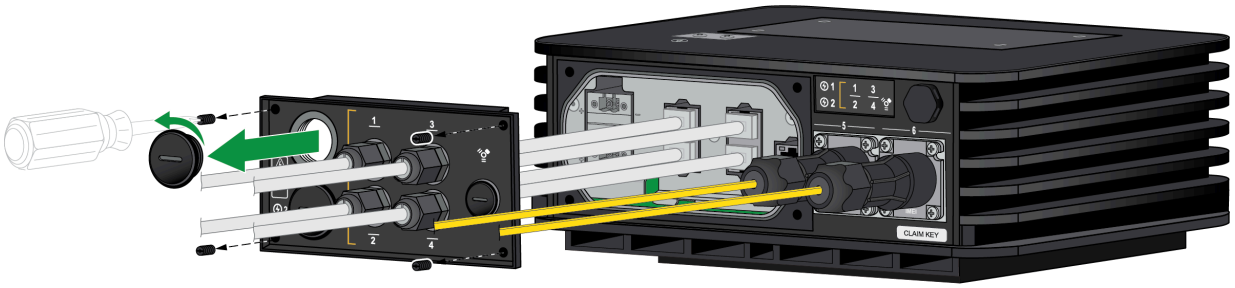
STEP 1 | Verify that the DC power source that will power the firewall is powered off.

In the following procedure, connect the DC power cables—and ground cable if you do not use the screw-on ground point—to the DC terminal block before you attach the DC terminal block to the firewall.

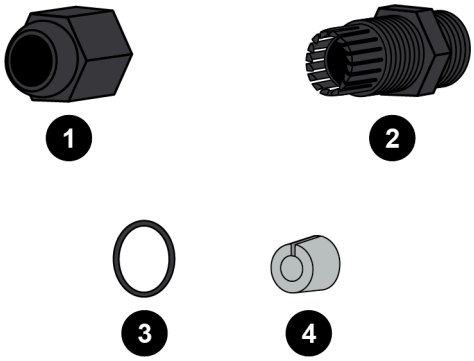
STEP 2 | (PA-410R and PA-410R-5G only) Prepare to install the power cables using cable glands.

1. Using a Phillips-Head screwdriver, unscrew the four screws on the bottom panel of the firewall.

2. On the removed panel, unscrew the stopping plug that lines up with the DC power input you are connecting to.

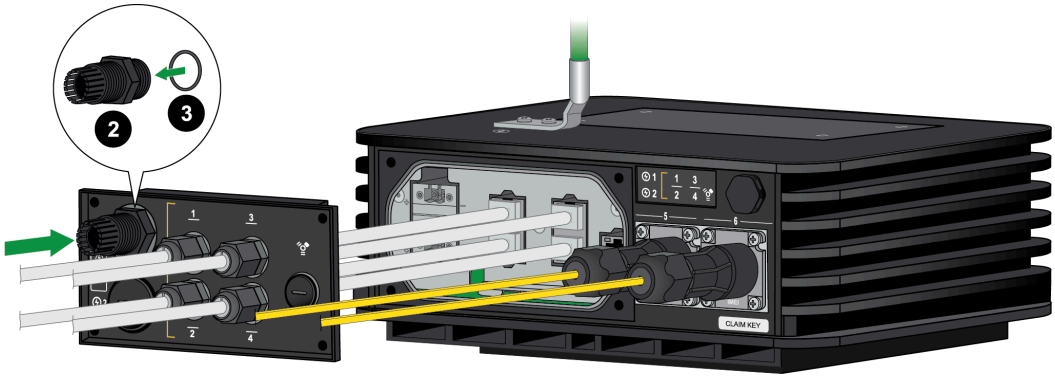


3. Unpack the power cable glands. There are four items — an end cap, panel connector, lock nut, and seal.



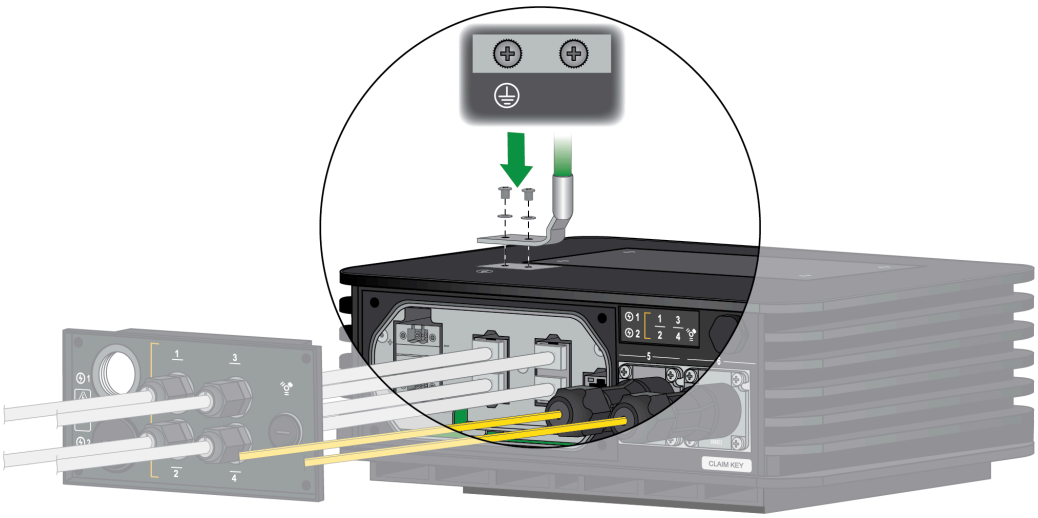
4. Loop the seal onto the shorter end of the panel connector. Make sure to push the seal until it is flush against the nut. Screw the shorter end of the panel connector into the

hole that corresponds to the DC power input being connected. Make sure that the connector is secure.



5. Thread the power cable through the end cap. This is used to secure the cable gland once the panel is reattached at the end of the procedure.

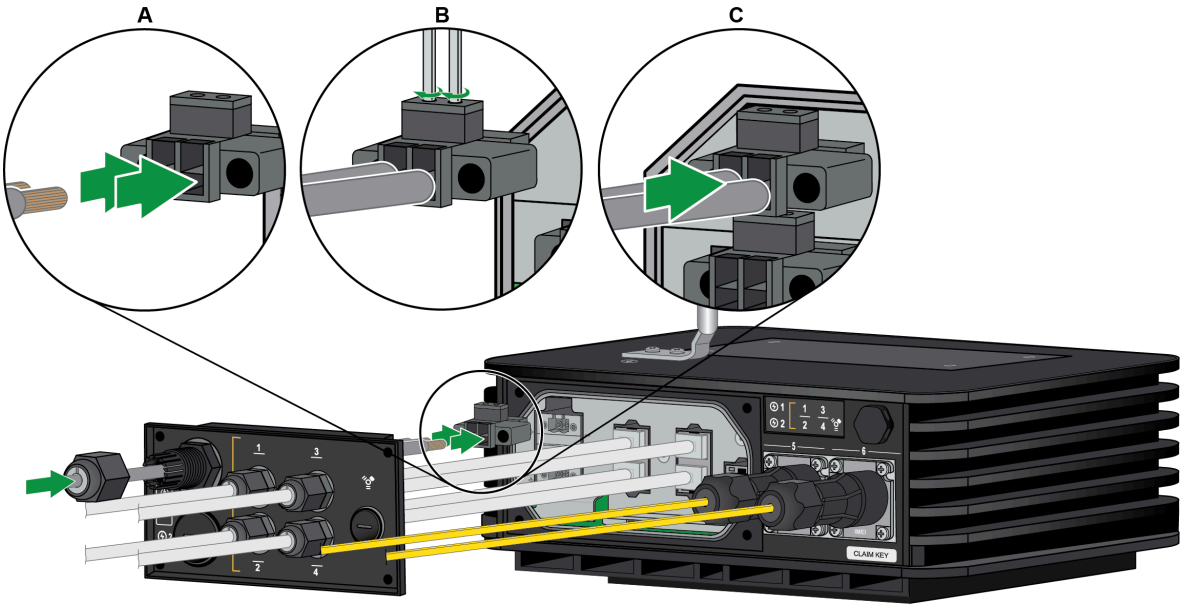
STEP 3 | Connect one end of a 8 AWG ground cable (not included) to the dual-hole ground lug. Connect the other end of the cable to earth ground. Remove the two ground screws from the ground point on the front panel of the firewall. Hold the ground lug (that you previously attached to the ground cable) over the screw holes, and then re-attach the screws to secure the cable to the firewall. Do not torque the screws to more than 6 in-lbs.



STEP 4 | (PA-410R and PA-410R-5G only) Thread the power cable through the hole in the removed bottom panel that corresponds to the power inputs.

STEP 5 | Insert the positive and negative DC cables into the connector. The connector supports 12 to 30 AWG cables, but 16 AWG is recommended. Secure each cable using a 1/8” flat head

screwdriver. Turn the connector screws clockwise until tight. Do not torque the screws to more than 2 in-lbs.

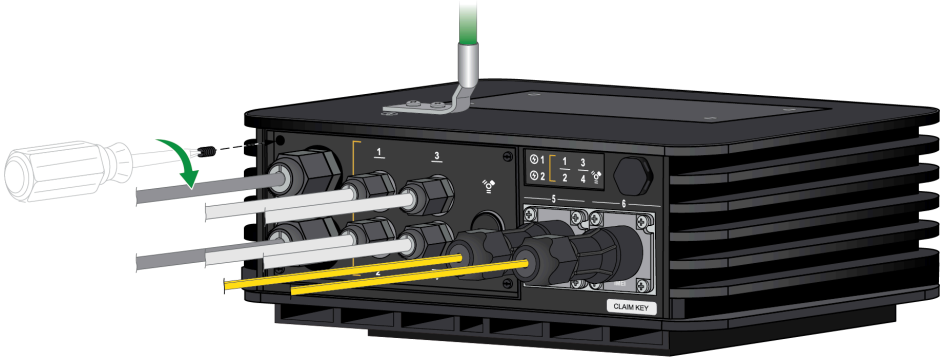


STEP 6 | Plug the cabled DC connector into the DC input on the firewall. Secure the connector by turning the two screws on each side clockwise and torque them to 3 in-lbs.

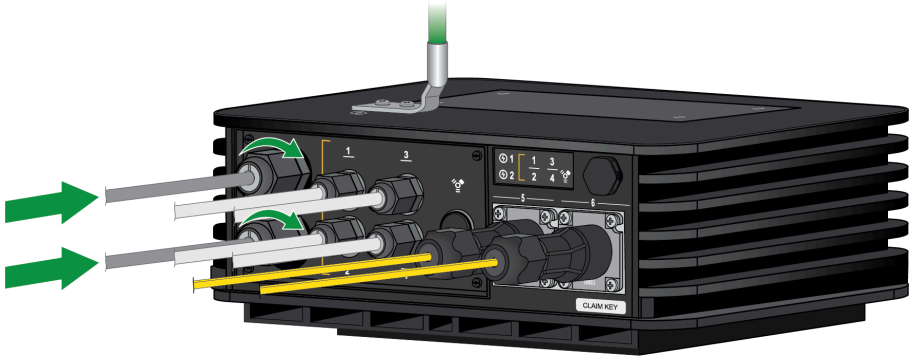
STEP 7 | (Optional) Connect a second DC cable for redundancy.

STEP 8 | (PA-410R and PA-410R-5G only) Follow the procedure to Connect Ethernet Cables to the PA-400R Series Firewall before you screw the bottom panel back into place.

1. Once all Ethernet and power cables are connected, make sure that any unused ports have a stopping plug in the corresponding panel slot.
2. Align the panel with the four screw holes on the firewall. Using a Phillips-Head screwdriver, screw the panel back into its original place.



3. Push the end caps along each Ethernet and power cable until the end caps reach their respective panel connector. Screw the end caps onto each panel connector, making sure that it is tight and secure.



STEP 9 | Power on the DC power source to power on the firewall. The firewall powers on and the power LED turns green.

PA-400R Series Firewall Specifications

The following topics describe the PA-400R Series firewall hardware specifications. For feature, capacity, and performance information, refer to the datasheet.

Physical Specifications

The following table describes PA-400R Series firewall physical specifications.

Specification	Value
Rack units and dimensions	**PA-410R and PA-410R-5G** • Height: 8.07", Width: 10.63", Depth: 3.66" (Height: 20.5 cm, Width: 27 cm, Depth: 9.3 cm) *The above dimensions do not take the cable glands and covers into account.* • Not rack mounted **PA-450R and PA-450R-5G,** • Height: 1.73", Width: 15.35", Depth: 9.71" (Height: 4.39 cm, Width: 38.99 cm, Depth: 24.66 cm) • Rack units—1U
Antenna dimensions	**PA-410R-5G and PA-450R-5G** • Height: 7.76", Width: 2.28", Depth: 1.67" (Height: 19.7 cm, Width: 5.8 cm, Depth: 4.2 cm)
Weight	**PA-410R** • Firewall weight—9 lbs (4.08 kg) • Shipping weight—12.3 lbs (5.58 kg) **PA-410R-5G** • Firewall weight—9 lbs (4.08 kg) • Shipping weight—12.8 lbs (5.81 kg) **PA-450R and PA-450R-5G,** • Firewall weight—10 lbs (4.5 kg) • Shipping weight—14.5 lbs (6.6 kg)

Electrical Specifications

The following table describes PA-400R Series firewall electrical specifications.

Specification	Value
Power input	**PA-410R, PA-410R-5G, PA-450R, and PA-450R-5G**—12-48VDC power.
Maximum power consumption	**PA-410R and PA-410R-5G**—28.9W **PA-450R**—50W **PA-450R-5G**—50W
Maximum current consumption	**PA-410R and PA-410R-5G**—2.4A@12VDC **PA-450R and PA-450R-5G**—6A@12VDC

Environmental Specifications

The following table describes PA-400R Series firewall environmental specifications.

Specification	Value
Operating temperature range	-40°F to 158°F (-40°C to 70°C)
Humidity tolerance	10% to 90% non-condensing
Airflow	The PA-400R Series firewalls use passive cooling and do not contain fans.
Maximum BTUs/hour	**PA-450R and PA-450R-5G**—170 BTUs/hour
Acoustic noise	Emits no sound.
Maximum operating altitude	10,000 ft (3048m)

Antenna Specifications

The following table describes the PA-400R Series firewall antenna specifications.

Specification	Value
Antennas	**PA-410R-5G and PA-450R-5G** • Four 5G multi-band antennas
Frequency range	**PA-410R-5G and PA-450R-5G** • 615-960MHz / 1500-1600MHz / 1710-2690MHz / 3300-3700MHz
Peak gain	**PA-410R-5G and PA-450R-5G** • 2.3dBi in 800MHz band, 4.4dBi in 1575MHz band, 2.6dBi in 2170MHz band, 1.7dBi in 3300MHz band, 3.8dBi in 4400MHz band
VSWR	**PA-410R-5G and PA-450R-5G** • <3:1
Feed impedance	**PA-410R-5G and PA-450R-5G** • 50Ω
Power handling	**PA-410R-5G and PA-450R-5G** • 30 dBm
Interface	**PA-410R-5G and PA-450R-5G**—SMA (F) Connectors

Miscellaneous Specifications

The following table describes PA-400 Series firewall miscellaneous specifications.

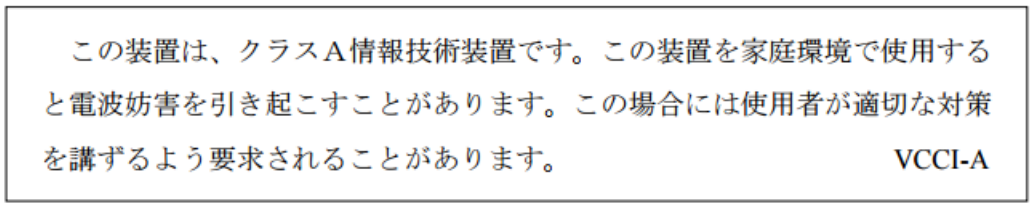
Specification	Value
Storage capacity	One 128 GB eMMC
Mean time between failures (MTBF)	8.7 years

PA-400R Series Firewall Compliance Statements Overview

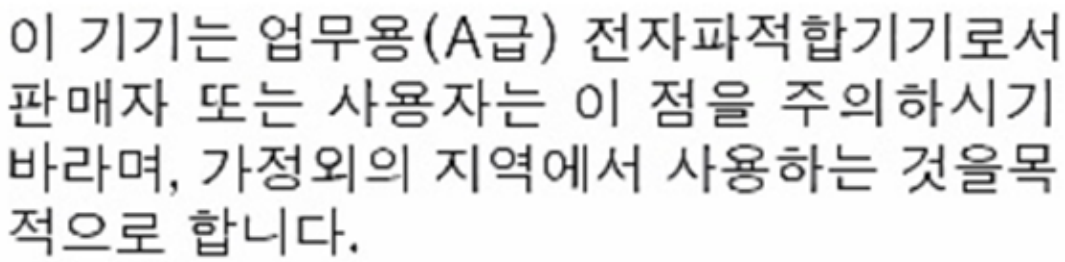
Palo Alto Networks obtains regulatory compliance certifications to comply with the laws and regulations in each country where there are requirements applicable to our products. Our products meet standards for product safety and electromagnetic compatibility when used for their intended purpose. To view compliance statements for the PA-400R Series firewall, see PA-400R Series Firewall Compliance Statements.

PA-400R Series Firewall Compliance Statements

The following lists the PA-400R Series firewall hardware compliance statements:

- **VCCI**: This section provides the compliance statement for the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), which governs radio frequency emissions in Japan.
  - 

    Translation: 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 corrective actions.
- **CE**: European Union (EU) Electromagnetic Compatibility Directive.This device is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive (2014/30/EU). The above product conforms with Low Voltage Directive 2014/35/EU and complies with requirements relating to electrical equipment designed for use within certain voltage limits.
- **KCC**: This equipment is an electromagnetic compatible device for business purposes (Class A). The provider or user should be aware that the equipment is intended for use outside the home.

- **Safety**: Product Ambient Temperature:
  - -40~70 degrees C

  Risk of explosion if battery is replaced by an incorrect type. Dispose of used battery according to local regulations.
- **Federal Communications Commission (FCC) statement for a Class A digital device or peripheral**: 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 in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be

determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit that is different from the one to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

- **ICES**: Canadian Department Compliance Statement: This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.