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

March 15, 2024

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

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-450R. 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), 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

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.

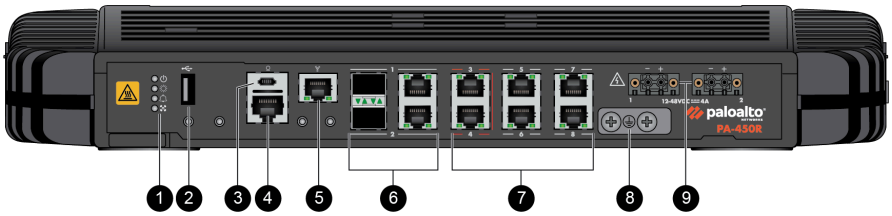
- PA-400R Series Front Panel
- PA-400R Series Back Panel
- Interpret the LEDs on a PA-400R Series Firewall

PA-400R Series Front Panel

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

- PA-450R

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

Item	Component	Description
		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). 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

Item	Component	Description
		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.

To view system firmware versions for any of the PA-400R firewalls, use the following CLI command:

```
admin@PA-450r> show system firmware
```

PA-400R Series Back Panel

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

- PA-450R

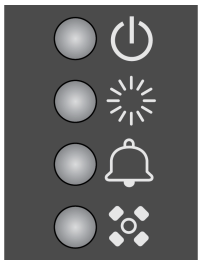
The following image shows the back panel of the PA-450R. There are no serviceable components on the back panel.

To view system firmware versions for any of the PA-400R Series firewalls, use the following CLI command:

```
admin@PA-450r> show system firmware
```

Interpret the LEDs on a PA-400R Series Firewall

The following table describes how to interpret the status LEDs on all off 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. • 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).*

LED	Description
(PA-450R) 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.*

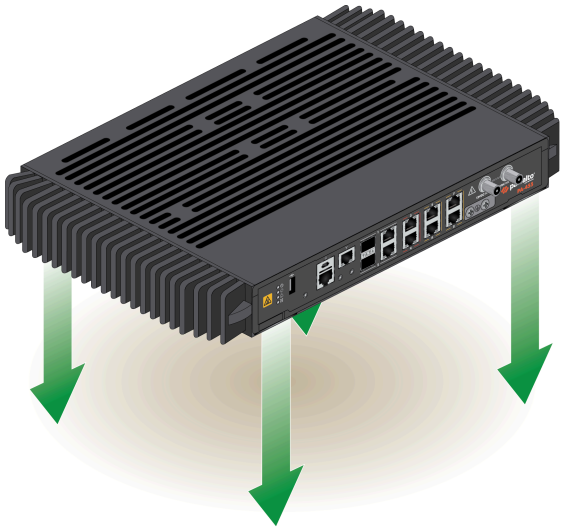
Install the PA-400R Series Firewall

The PA-400R Series next-generation firewalls can be installed in a number of different configurations depending on their design. The PA-450R ships with the hardware required to install the firewall in a 19-inch equipment rack or on a wall.

- Install the PA-400R Series Firewall on a Flat Surface
- Install the PA-400R Series Firewall on a Wall
- Install the PA-400R Series Firewall in an Equipment Rack
- Set Up a Connection to the Firewall

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

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



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

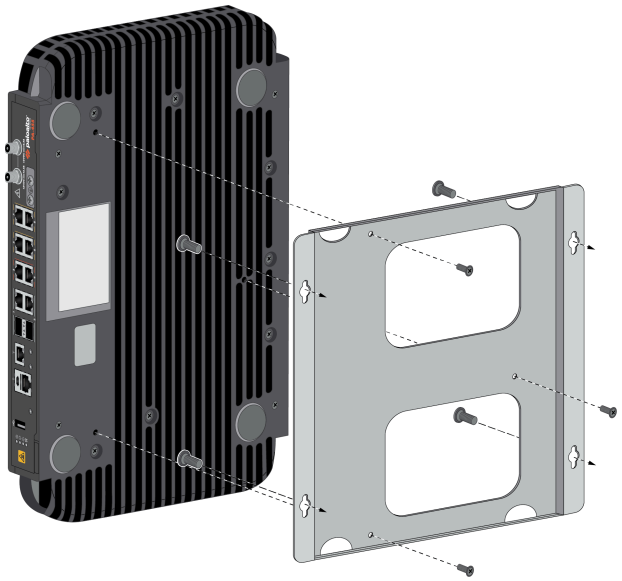
The PA-450R firewalls can be installed on a wall with the use of PAN-1RU-SMALL-WALLMNT.

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

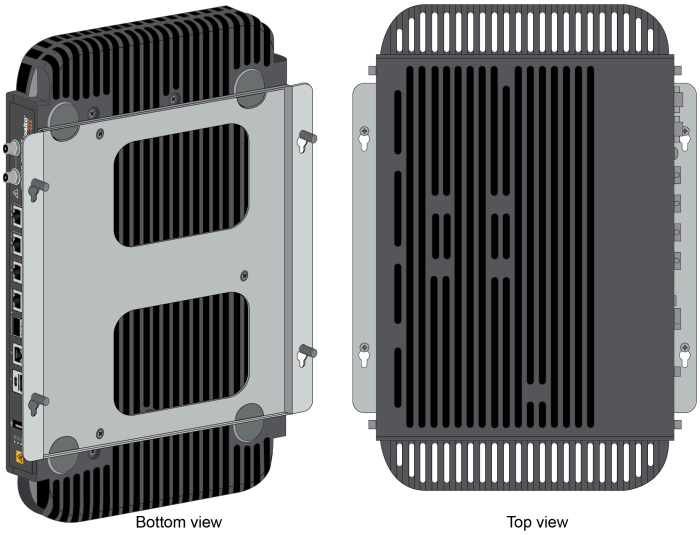
STEP 1 | Mark the locations on the wall that line up with the wall mount holes on the bottom of the wall mount.

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

STEP 2 | Attach the firewall to the wall mount using three #6-32 screws and a #2 Phillips-head screwdriver.



STEP 3 | 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

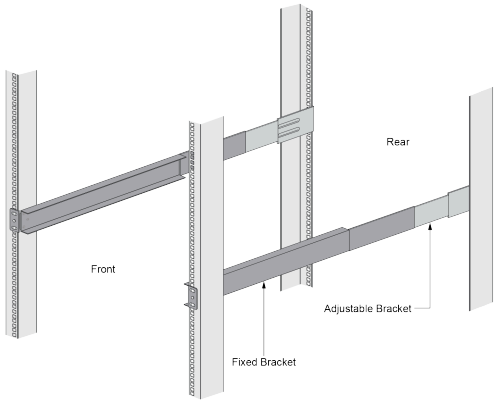
Top view

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

One PA-450R 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.

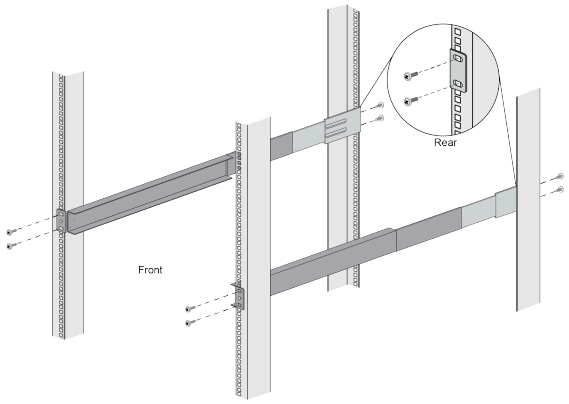
STEP 1 | Slide one of the adjustable mounting brackets into one of the fixed mounting brackets to create a mounting rail. Repeat for the second mounting rail. The adjustable and fixed brackets are the same for the left and right side.



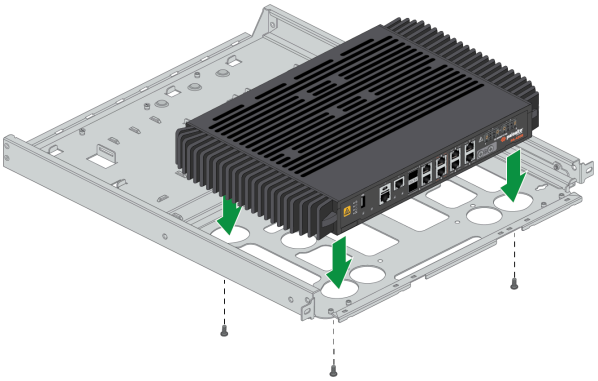
STEP 2 | Align the bottom edge of the mounting rails to the bottom of the 1 RU (1.5 RU if there is another device above) reserved for your firewall. Align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.

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.

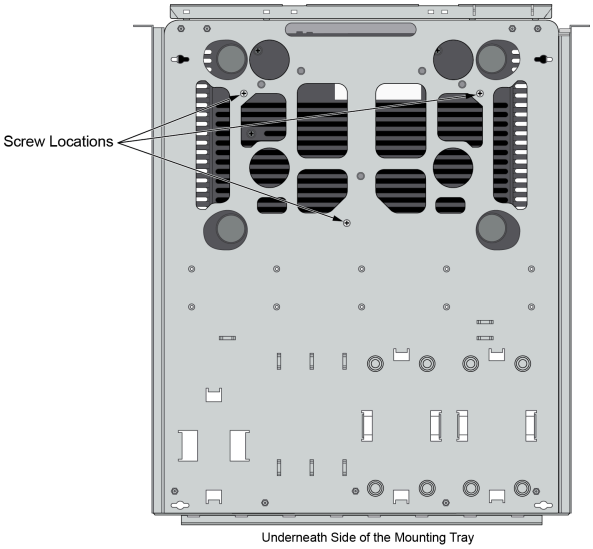


STEP 4 | With the front of the firewall facing forward, align the four rubber feet on the bottom of the device to the slotted holes in the provided mounting tray.



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.



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

STEP 8 | Follow the instructions to Connect 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.

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-400 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.

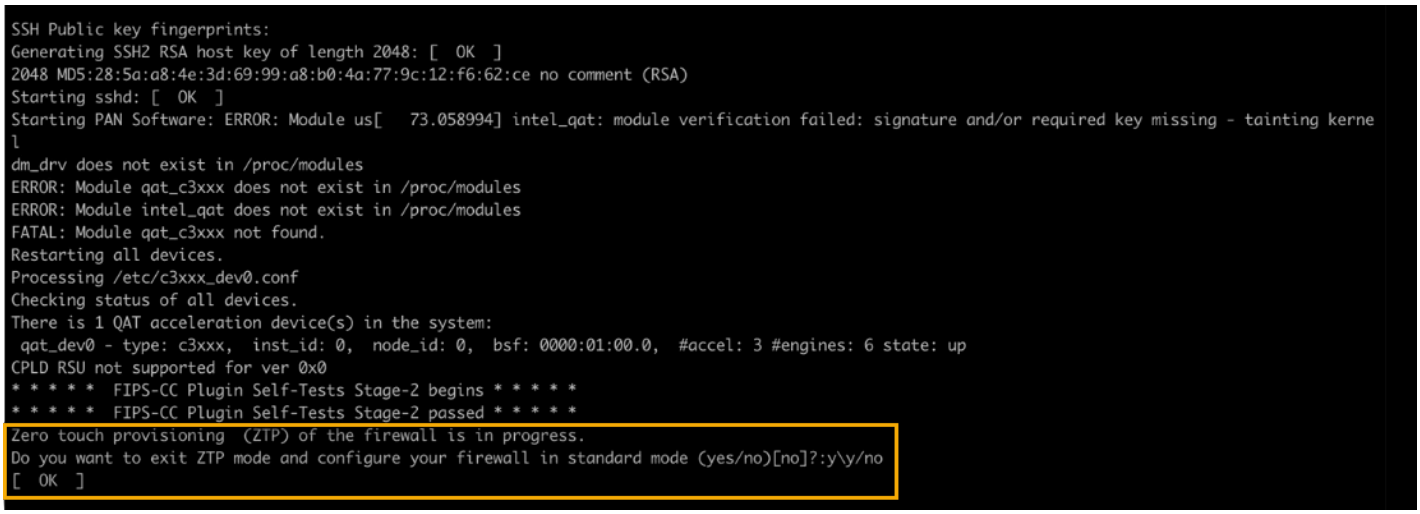
STEP 3 | (Standard mode only) If you intend to boot the firewall in standard mode, you will need access to the firewall CLI to respond to a prompt during bootup. Connect a console cable from the firewall console port to your computer. Once the firewall is powered on, use a terminal emulator such as PuTTY 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 Power to a PA-400R Series Firewall

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

Use the following information to gather and prepare the hardware that is required to Connect Power to a PA-400R Series Firewall.

Due to the various cable lengths required for a given installation site, DC power and ground cables are not included with the firewall.

Required Hardware

- **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 | 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 Power to a PA-400R Series Firewall

The following procedure describes how to connect DC power to a 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.

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 | 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 3 | Insert the positive and negative DC cables into the terminal block. The terminal connectors support 12 to 30 AWG cables, but 16 AWG is recommended. Secure each cable using a 1/8” flat head screwdriver. Turn the terminal screws clockwise until tight. Do not torque the screws to more than 2 in-lbs.

STEP 4 | (Optional) Connect a second DC power source for redundancy.

STEP 5 | Plug the cabled DC terminal block into the DC inputs on the firewall. Secure the terminal block by turning the two screws on each side of the block clockwise and torque to 3 in-lbs.

STEP 6 | 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-450R** • Height: 8.78", Width: 10.63", Depth: 4.45" (Height: 22.3 cm, Width: 27 cm, Depth: 11.3 cm) • Rack units—1U
Weight	**PA-450R** • Firewall weight—15 lbs (6.8 kg) • Shipping weight—18 lbs (8.2 kg)

Electrical Specifications

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

Specification	Value
Power input	The PA-400R Series firewalls operate on 12-48VDC power. The firewall can operate on one power supply or you can install a second power supply for power redundancy.
Power consumption	**PA-450R** • Maximum—50W
Maximum current consumption	**PA-450R** • Firewall—6A@12VDC

Environmental Specifications

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

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

Miscellaneous Specifications

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

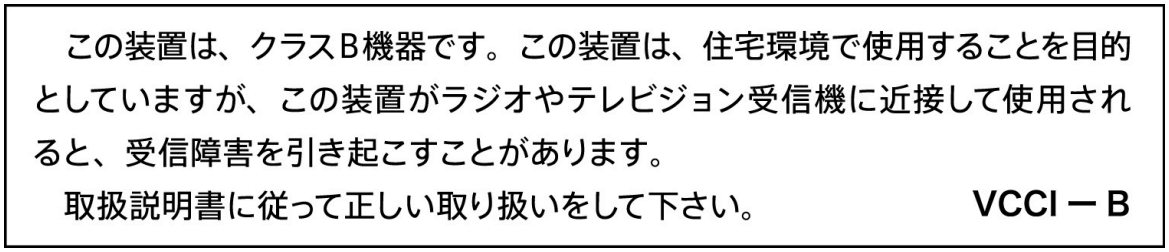
Specification	Value
Storage capacity	**PA-450R** • One 128 GB eMMC
Mean time between failures (MTBF)	8.7 years

PA-400R Series Firewall Compliance Statements Overview

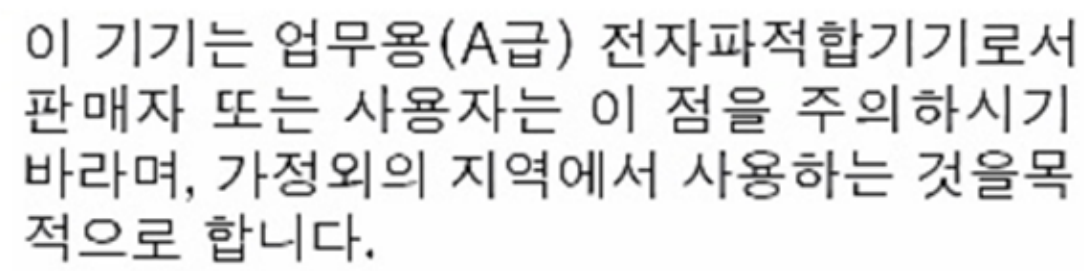
Palo Alto Networks obtains regulatory compliance certifications to comply with the laws and regulations in each country where there are requirements applicable to our products. Our products meet standards for product safety and electromagnetic compatibility when used for their intended purpose. To view 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 B 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.

- **TUV**: Product Ambient Temperature:
  - (PA-450R) 4~21 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 and B digital device or peripheral**: This equipment has been tested and found to comply with the limits for a Class B 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 B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

