



TECHDOCS

PA-400 Series Next-Gen Firewall Hardware Reference

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2020-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

January 24, 2023

Table of Contents

Before You Begin.....	5
Upgrade/Downgrade Considerations for Firewalls and Appliances.....	6
Tamper Proof Statement.....	7
Third-Party Component Support.....	8
Product Safety Warnings.....	9
PA-400 Series Firewall Overview.....	13
PA-400 Series Front Panel.....	14
PA-400 Series Back Panel.....	27
Install the PA-400 Series Firewall.....	31
Install the PA-400 Series Firewall on a Flat Surface.....	32
Install the PA-400 Series Firewall on a Wall.....	34
Install the PA-400 Series Firewall in a 19-inch Equipment Rack.....	42
Install the PA-400 Series Firewall Using the PAN-PA-400-RACKTRAY.....	42
Install Antennas on the PA-400 Series 5G Firewall.....	51
Insert a SIM Card into a PA-400 Series Firewall.....	53
Set Up a Connection to the Firewall.....	54
Connect Power to a PA-400 Series Firewall.....	57
Connect Power to a PA-400 Series Firewall.....	58
Connect Power to a PA-410 Firewall.....	61
Service the PA-400 Series Firewall Hardware.....	63
Interpret the LEDs on a PA-400 Series Firewall.....	64
Replace a Power Adapter on a PA-400 Series Firewall.....	67
PA-400 Series Firewall Specifications.....	71
Physical Specifications.....	72
Electrical Specifications.....	74
Environmental Specifications.....	76
Antenna Specifications.....	78
Miscellaneous Specifications.....	79
PA-400 Series Firewall Compliance Statements Overview.....	81
PA-400 Series Firewall Compliance Statements.....	82

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	<p>Before upgrading the firewall, run the following CLI command to check the flash drive's status: debug system disk-smart-info disk-1.</p> <p>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.</p>	<p>Before downgrading the firewall, run the following CLI command to check the flash drive's status: debug system disk-smart-info disk-1.</p> <p>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.</p>

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.

<ul style="list-style-type: none">  	<p>(All Palo Alto Networks appliances with two or more power supplies)</p> <p>Caution: Shock hazard</p> <p>Disconnect all power cords (AC or DC) from the power inputs to fully de-energize the hardware.</p> <p>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.</p>
<ul style="list-style-type: none">    	<p>(PA-7000 Series firewalls only)</p> <p>Caution: High touch current</p> <p>Connect to earth before connecting to the power supply.</p> <p>Ensure that the protective earthing conductor is connected to the provided ground lug on the rear side of the firewall.</p>
<ul style="list-style-type: none">  	<p>(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.</p> <p>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.</p>

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-400 Series Firewall Overview

The Palo Alto Networks® PA-400 Series Next-Generation firewalls include the PA-410, PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460. These firewalls are designed for small organizations or branch offices and include the following main features: a TPM module for PAN-OS key storage and security, ZTP functionality, active/passive and active/active high availability (HA), 5G capability for select models, and Power Over Ethernet (PoE) support in the PA-415 and PA-445. All PA-400 Series firewalls except for the PA-410 can make use of dual power adapters for power redundancy (second power adapter sold separately). The PA-400 Series firewall enables you to secure your organization through advanced visibility and control of applications, users, and content.

First Supported PAN-OS® Software Release:

- **PAN-OS 10.1.0**—PA-440, PA-450, and PA-460
- **PAN-OS 10.1.2**—PA-410
- **PAN-OS 11.0**—PA-415 and PA-445
- **PAN-OS 11.1**—PA-415-5G and PA-455

The following topics describe the hardware features of the PA-400 Series firewall. To view or compare performance and capacity information, refer to the [Product Selection tool](#).

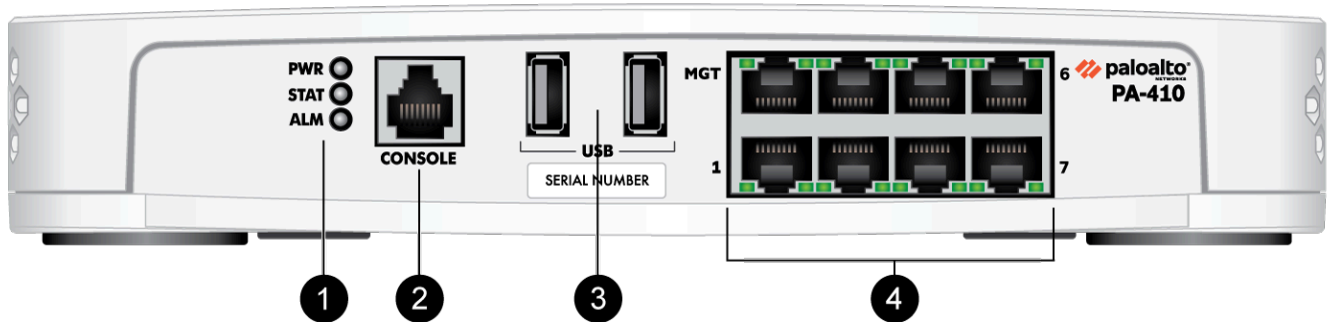
- [PA-400 Series Front Panel](#)
- [PA-400 Series Back Panel](#)

PA-400 Series Front Panel


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

- [PA-410](#)
- [PA-415-5G](#)
- [PA-415 and PA-445](#)
- [PA-455](#)
- [PA-440, PA-450, and PA-460](#)

The following image shows the front panel of the PA-410 and the table describes each front panel component.

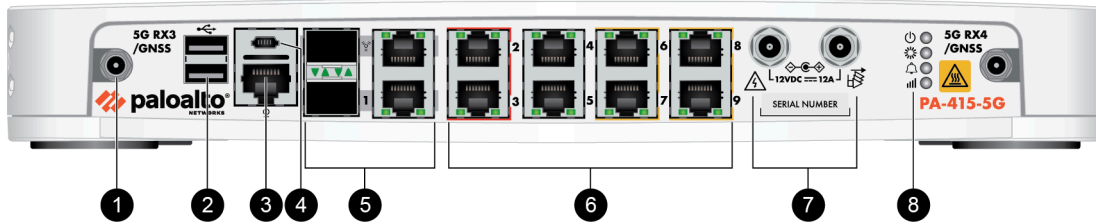



Item	Component	Description
1	LED status indicators	Three LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400 Series Firewall).
2	CONSOLE port	Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 cable and terminal 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
		<p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
3	USB ports	<p>Two USB ports for debugging and administration only. Use one of the two ports to bootstrap the firewall.</p> <p>Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.</p>
4	Ethernet Ports	<p>MGT Port</p> <p>One Ethernet10/100/1000Mbps port (located beside the “MGT” label) that is used 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.</p> <p>Ethernet Ports</p> <p>Seven RJ-4510/100/1000Mbps</p>


Item	Component	Description
		ports for network traffic. You can set the link speed and duplex mode or choose autonegotiate.

The following image shows the front panel of the PA-415-5G and the table describes each front panel component.



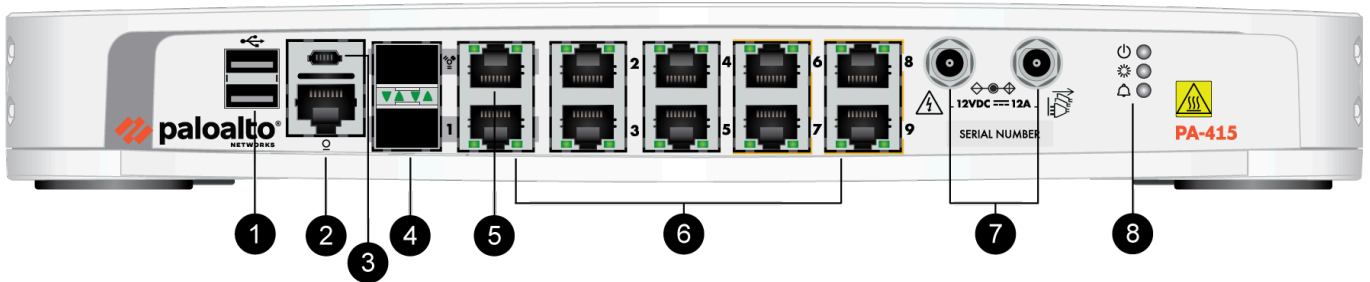
Item	Component	Description
1	Antenna Connector	<p>Four 5G SMA antenna connectors:</p> <ul style="list-style-type: none"> • Main (TX1/RX1) • MIMO1 (TX2/RX2) • MIMO2 (RX3 GNSS L5) • AUX (RX4/GNSS L1) <p>See the Antenna Specifications for more information about the antennas.</p> <p> <i>Two antenna connectors are on the front panel of the device and two antenna connectors are on the PA-400 Series Back Panel.</i></p>
2	USB ports	Two USB ports for debugging and administration only. Use one of these ports to bootstrap the firewall.

Item	Component	Description
3	CONSOLE port (RJ-45)	<p>Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.</p> <p>Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 cable and terminal emulation software.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
4	CONSOLE port (Micro USB)	<p>Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool</p>


Item	Component	Description
		<p>(MRT), and the command line interface (CLI).</p> <p>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.</p>
5	SFP/RJ-45 Combo Ports	<p>Two SFP/RJ-45 combo ports for 10/100/1000Mbps speeds.</p> <p> <i>While facing the front panel of the firewall, the two upper ports that feature the management port are used for management processing. The two lower ports, including Ethernet 1, are used for data processing.</i></p>
6	Ethernet Ports	<p>Eight RJ-45 10/100/1000Mbps ports for network traffic.</p> <p>You can set the link speed and duplex mode or choose auto-negotiate.</p> <p>Ports 5 through 9 are Power Over Ethernet (PoE) ports. They can be configured to transfer power to a connected device.</p>
7	Power adapter inputs	<p>Use the power inputs to connect power to the firewall. The PA-415-5G ships with one 150W power adapter and can utilize an optional second</p>

Item	Component	Description
		power adapter for power redundancy.
8	LED status indicators	Four LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400 Series Firewall).

The front panels of the PA-415 and PA-445 firewalls are visually different but feature the same components. The following image shows the front panel of the PA-415 and the table describes each front panel component.

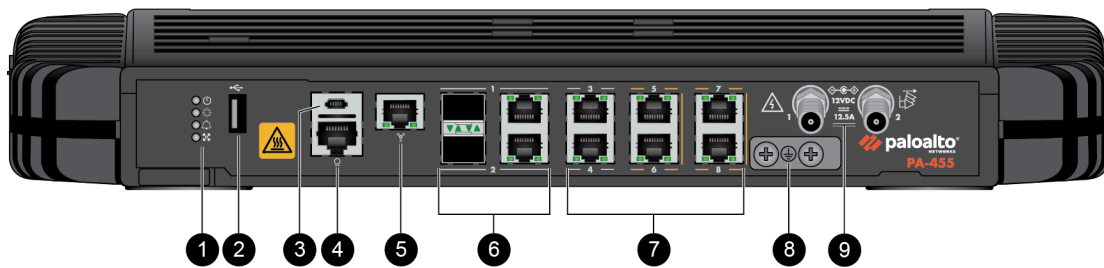


Item	Component	Description
1	USB ports	Two USB ports for debugging and administration only. Use one of the USB ports to bootstrap the firewall. Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.
2	CONSOLE port (RJ-45)	Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 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
		<p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
3	CONSOLE port (Micro USB)	<p>Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p>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.</p>
4	SFP/RJ-45 Combo Ports	Two SFP/RJ-45 combo ports for 10/100/1000Mbps speeds.
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,

Item	Component	Description
		such as retrieving licenses and updating threat and application signatures.
6	Ethernet ports	<p>Eight RJ-45 10/100/1000Mbps ports for network traffic.</p> <p>You can either set the link speed or choose auto-negotiate. The interface duplex mode can only be set to auto-negotiate.</p> <p>Ports 6, 7, 8, and 9 are Power Over Ethernet (PoE) ports. They can be configured to transfer power to a connected device.</p>
7	Power adapter inputs	Use the power inputs to connect power to the firewall. The PA-415 and PA-445 ship with one 150W power adapter and can utilize an optional second power adapter for power redundancy.
8	LED status indicators	Three LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400 Series Firewall).

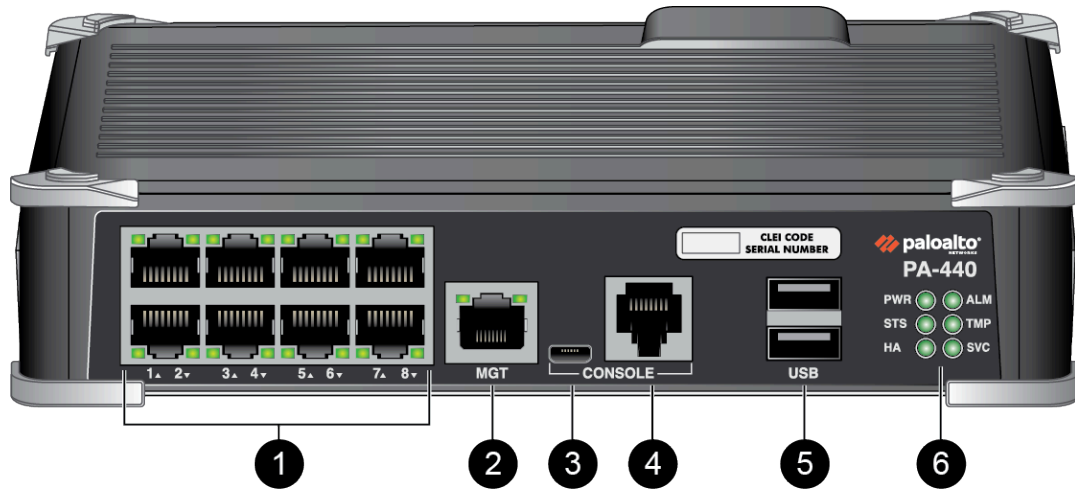
The following image shows the front panel of the PA-455 and the table describes each front panel component.




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-400 Series Firewall).
2	USB port	<p>USB port for debugging and administration only. Use this port to bootstrap the firewall.</p> <p>Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.</p>
3	CONSOLE port (Micro USB)	<p>Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p>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.</p>
4	CONSOLE port (RJ-45)	<p>Use this port to connect a management computer to the firewall using a RJ-45 to USB cable and terminal emulation software.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p>Use the following settings to configure your terminal</p>

Item	Component	Description
		emulation software to connect to the console port: <ul style="list-style-type: none"> • 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. You can set the link speed and duplex mode or choose auto-negotiate. Ports 5, 6, 7, and 8 are Power over Ethernet (PoE) ports. They can be configured to transfer power to a connected device.
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 front panels of the PA-440, PA-450, and PA-460 firewalls are identical. The following image shows the front panel of the PA-440 and the table describes each front panel component.



Item	Component	Description
1	Ethernet ports	<p>Eight RJ-45 10/100/1000Mbps ports for network traffic.</p> <p>You can set the link speed and duplex mode or choose auto-negotiate.</p>
2	Management port	<p>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.</p>
3	CONSOLE port (Micro USB)	<p>Use this port to connect a management computer to the firewall using a standard Type-A USB-to-micro USB cable.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p>Refer to Micro USB Console Port for more information and</p>

Item	Component	Description
		<p>to download the Windows driver or to learn how to connect from a Mac or Linux computer.</p>
4	<p>CONSOLE port (RJ-45)</p>	<p>Use this port to connect a management computer to the firewall using a 9-pin serial to RJ-45 cable and terminal emulation software.</p> <p>The console connection provides access to firewall boot messages, the Maintenance Recovery Tool (MRT), and the command line interface (CLI).</p> <p> <i>If your management computer does not have a serial port, use a USB-to-serial converter.</i></p> <p>Use the following settings to configure your terminal emulation software to connect to the console port:</p> <ul style="list-style-type: none"> • Data rate: 9600 • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: None
5	<p>USB ports</p>	<p>Two USB ports for debugging and administration only. Use one of these ports to bootstrap the firewall.</p> <p>Bootstrapping enables you to provision the firewall with a specific PAN-OS configuration and then license it and make it operational on your network.</p>

Item	Component	Description
6	LED status indicators	Six LEDs that indicate the status of the firewall hardware components (see Interpret the LEDs on a PA-400 Series Firewall).



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

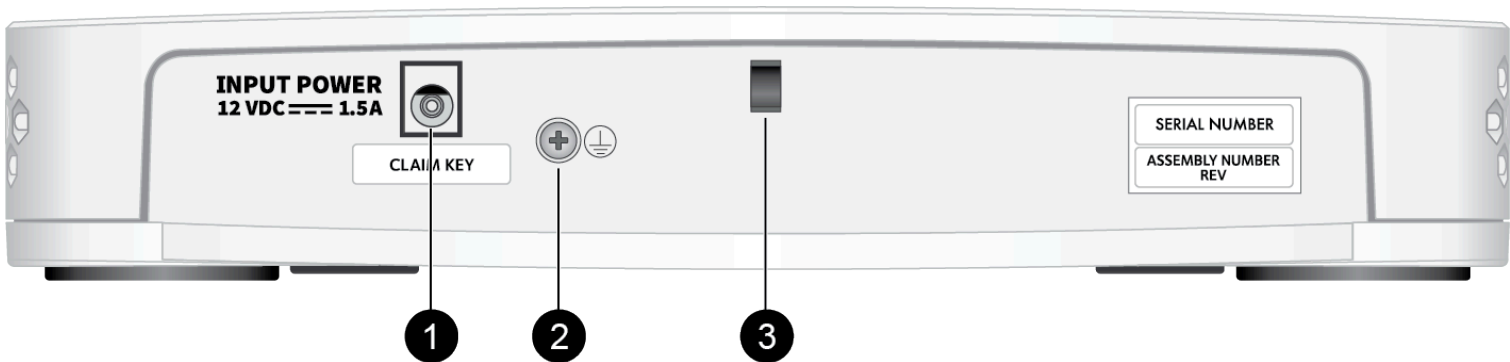
```
admin@PA-400> show system firmware
```


PA-400 Series Back Panel

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

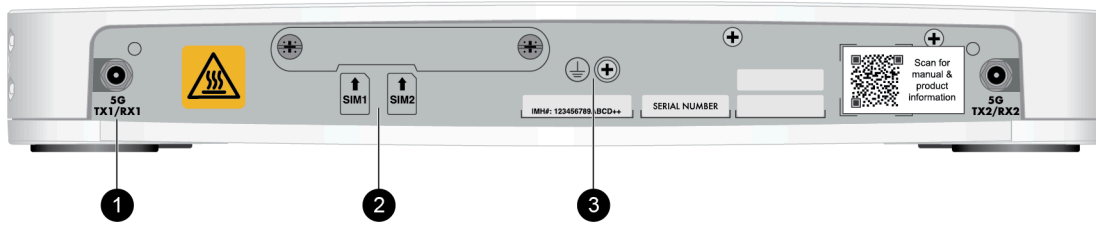
- [PA-410](#)
- [PA-415-5G](#)
- [PA-415 and PA-445](#)
- [PA-455](#)
- [PA-440, PA-450, and PA-460](#)


The following image shows the back panel of the PA-410 and the table describes each back panel component.



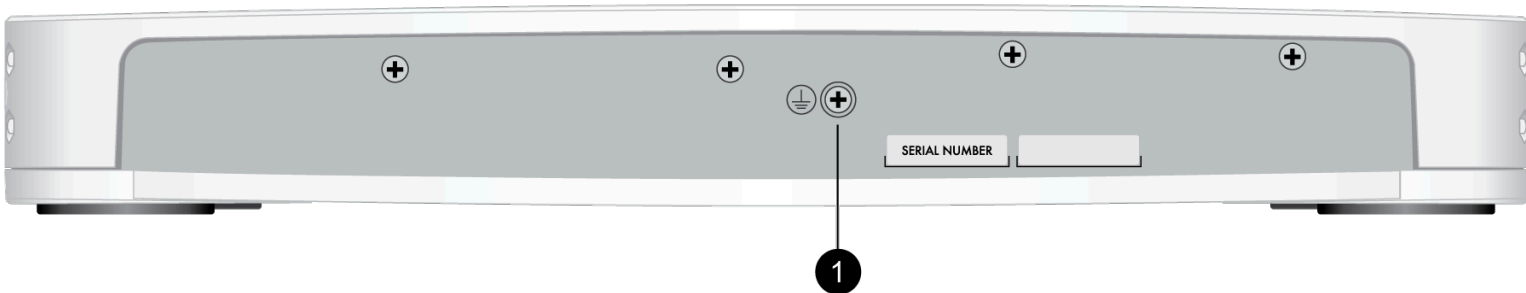
Item	Component	Description
1	Power adapter input	Use the power input to connect power to the firewall. The PA-410 ships with one 25W power adapter.  <i>Use only the PA-400 Series external power adapters provided by Palo Alto Networks.</i>
2	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).
3	Power Cord Retainer	Use the power cord retainer to secure the power cord.

The following image shows the back panel of the PA-415-5G and the table describes each back panel component.



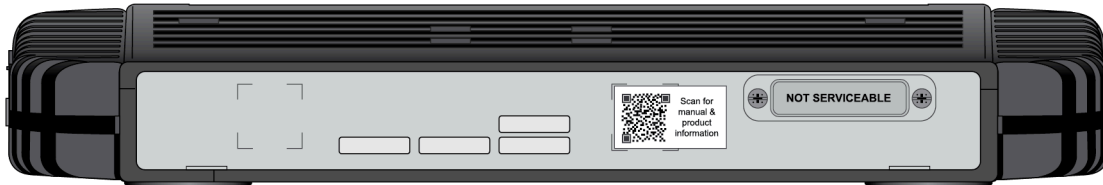
Item	Component	Description
1	Antenna Connector	<p>Four antenna connectors:</p> <ul style="list-style-type: none"> • Main (TX1/RX1) • MIMO1 (TX2/RX2) • MIMO2 (RX3 GNSS L5) • AUX (RX4/GNSS L1) <p> <i>Two antenna connectors are on the back panel of the device and two antenna connectors are on the PA-400 Series Front Panel.</i></p>
2	SIM slots	Two SIM slots for cellular network connectivity.
3	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

The back panels of the PA-415 and PA-445 firewalls are visually different but feature the same components. The following image shows the back panel of the PA-415 and the table describes each back panel component.

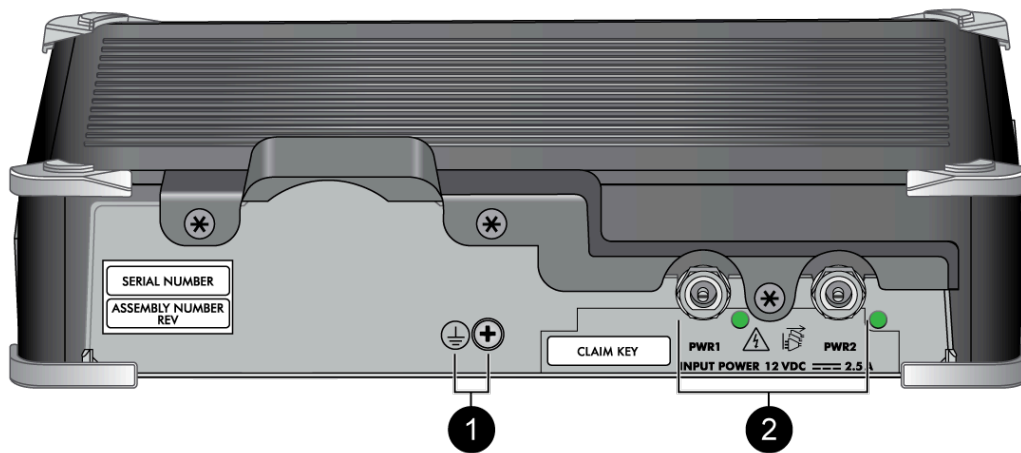


Item	Component	Description
1	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).

The following image shows the back panel of the PA-455. There are no serviceable components on the back panel.



The back panels of the PA-440, PA-450, and PA-460 firewalls are identical. The following image shows the back panel of the PA-440 and the table describes each back panel component.



Item	Component	Description
1	Ground stud	Use the single post ground stud to connect the firewall to earth ground (ground cable not included).
2	Power adapter inputs (PWR 1 and PWR 2)	Use the power inputs to connect power to the firewall. The PA-440, PA-450, and PA-460 ship with one 50W power adapter. A second adapter can be used for redundancy. <div style="display: flex; align-items: center;"> <p><i>Use only the PA-400 Series external power adapters provided by Palo Alto Networks.</i></p> </div>



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

```
admin@PA-400> show system firmware
```

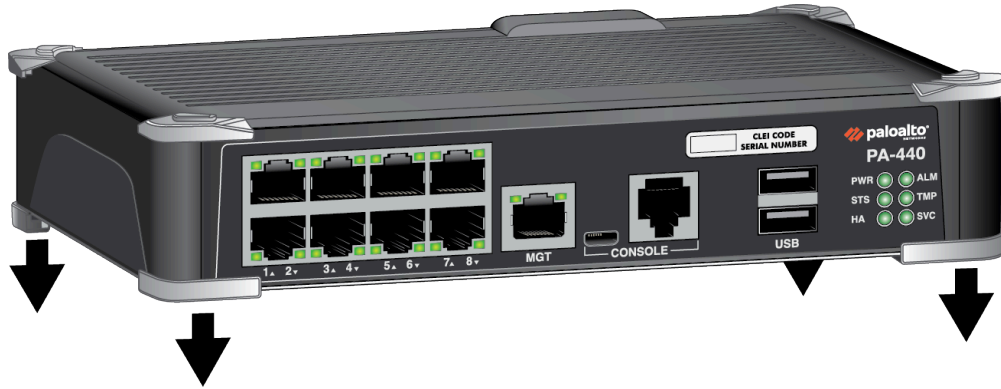
Install the PA-400 Series Firewall

The PA-400 Series next-generation firewall ships with the hardware required to install the firewall on a flat surface or on a wall. For select models, you can also order a rack mount kit to install the firewall in a 19-inch equipment rack.

- [Install the PA-400 Series Firewall on a Flat Surface](#)
- [Install the PA-400 Series Firewall on a Wall](#)
- [Install the PA-400 Series Firewall in a 19-inch Equipment Rack](#)
- [Install Antennas on the PA-400 Series 5G Firewall](#)
- [Insert a SIM Card into a PA-400 Series Firewall](#)
- [Set Up a Connection to the Firewall](#)

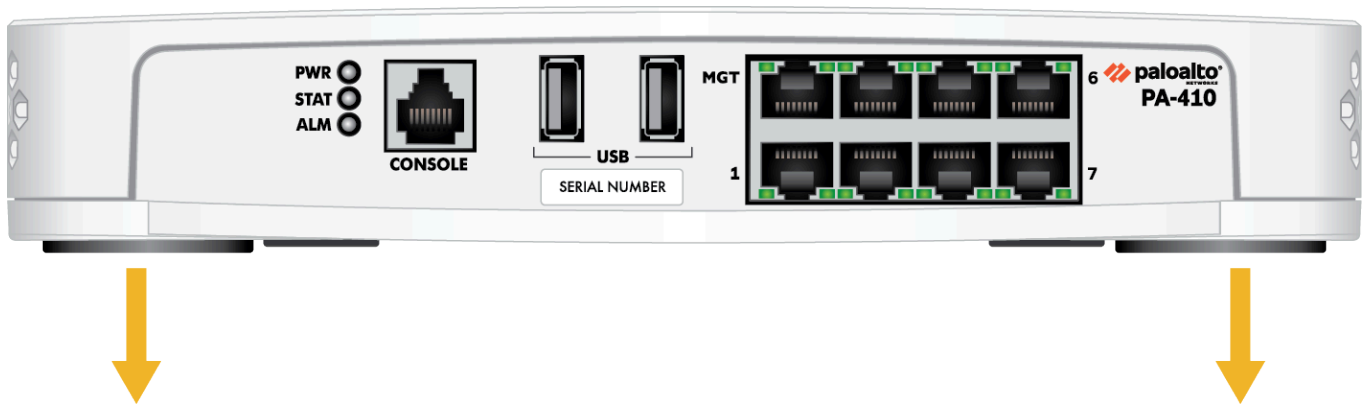
Install the PA-400 Series Firewall on a Flat Surface

The PA-440, PA-450, and PA-460 firewalls ship with rubber “feet” attached to each corner of the device. As pictured below, the PA-440, PA-450, and PA-460 can be situated on a flat surface both horizontally and vertically.




Install the PA-400 Series Firewall

The PA-410, PA-415, PA-415-5G, PA-455, and PA-445 have rubber feet installed on their bottom side so they can only be installed in a horizontal position.



Install the PA-400 Series Firewall on a Wall


Install a PA-400 Series firewall on a drywall or plywood wall using the wall-mount kit as described in the following procedure.


-  If you have a firewall that supports multi-band antennas, make sure that you read how to [install antennas on the 5G firewall](#) before continuing with this procedure.

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

(PA-440, PA-450, and PA-460) Mark three wall mount hole locations.


(PA-410, PA-415, PA-415-5G, PA-455, and PA-445) Mark four wall mount hole locations.

-  To ensure the wall mount screws line up with the firewall mount holes, use the PA-400 Series Quick Start Guide, the PA-410 Firewall Quick Start Guide, or the PA-415 and PA-445 Firewall Quick Start Guide that ship with the firewall as a template. If you do not have a copy of the Quick Start Guide, download and print it. When printing, select landscape and actual size in the print options to ensure the screw hole markers line up correctly.


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

STEP 2 | Use a #1 Phillips-head screwdriver to install the appropriate screws into each of the three or four marked locations:

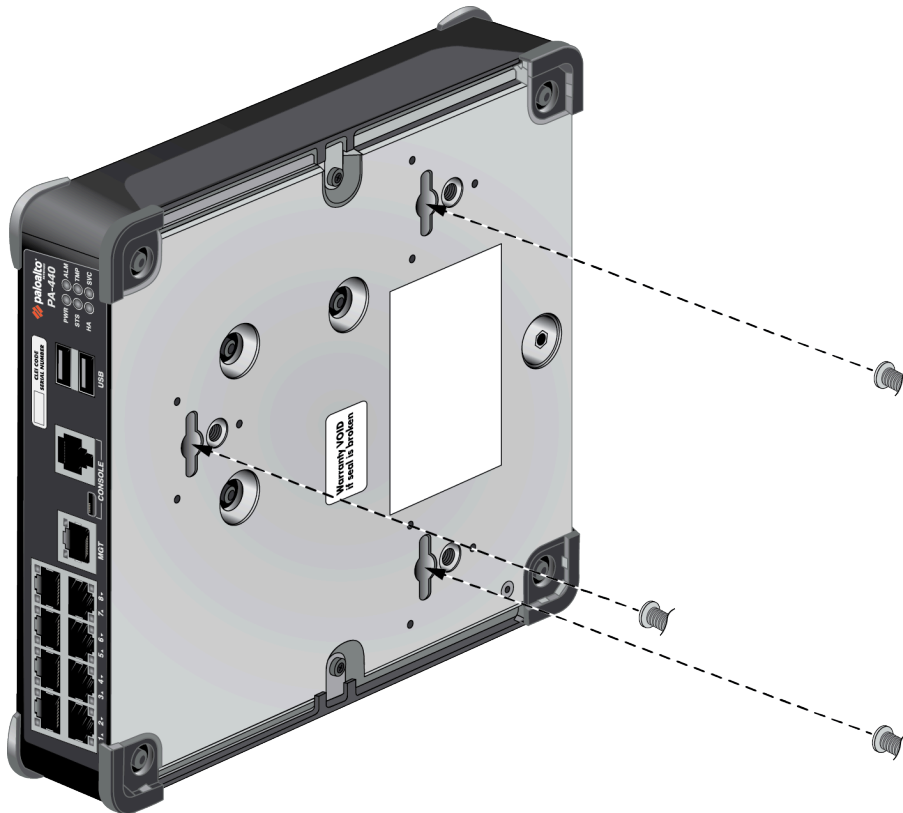
- **Drywall**—Press a drywall anchor slightly into the center of a template mark. Then use your screwdriver to apply pressure while turning the anchor clockwise until the surface of the anchor is flush with the wall. After the drywall anchor is secure, install a 1.25" anchor screw into the anchor until the bottom of the screw head protrudes 1/4" (.6cm) from the wall. Repeat this step for the other screw locations unless either is located over wood, in which case, use a .75" wood screw instead of a drywall anchor and screw.
- **Plywood wall**—Use your screwdriver to insert a .75" wood screw into the center of each template mark that is located over wood until the bottom of the screw heads protrude 1/4" (.6cm) from the wall.

-  (PA-455 only) Do not install the screws in the wall. Instead, proceed to Step 3.

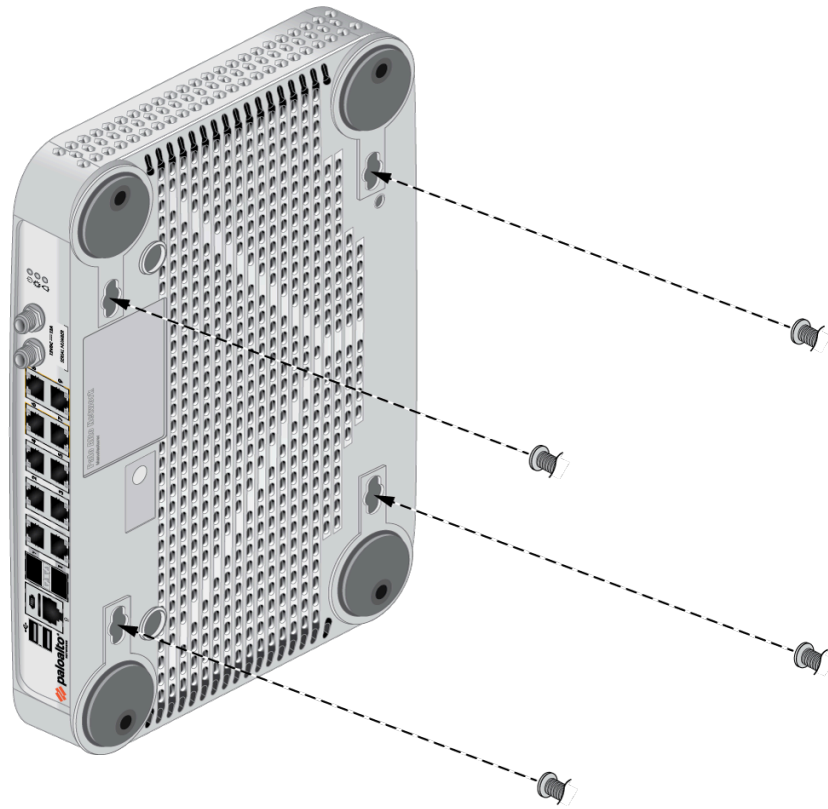
STEP 3 | Align the holes on the bottom of the firewall with the screws on the wall and hang the firewall on the screws. Make sure the firewall is securely connected to each of the screws before you let go.

 *(PA-455 only)* Instead of mounting the firewall directly onto the wall, first attach the firewall to the wall mount using three #6-32 screws. Then attach the wall mount to the wall using four screws that are appropriate for your wall.

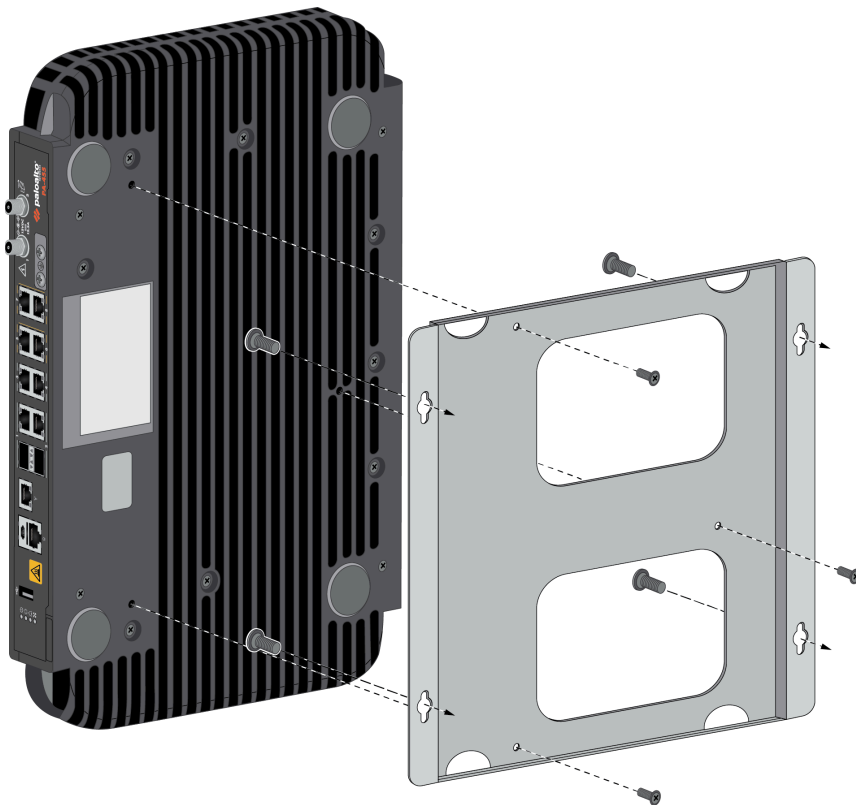
(PA-440, PA-450, and PA-460)



(PA-410, PA-415, PA-415-5G, and PA-445)



(PA-455)

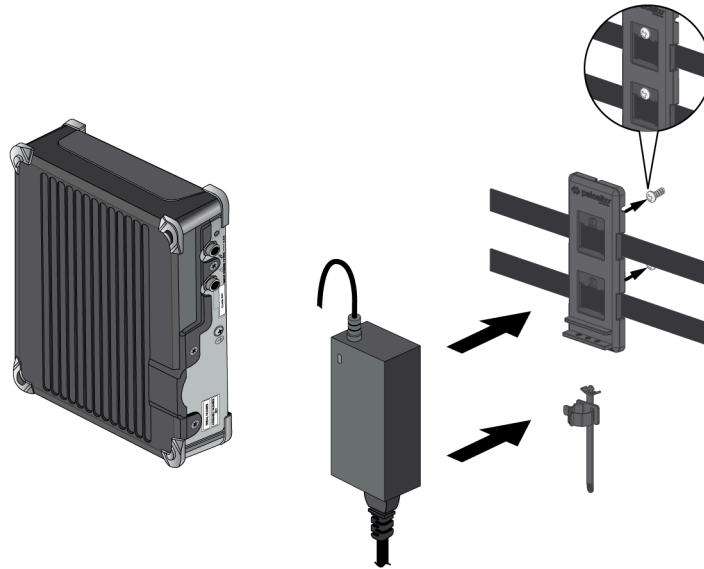


STEP 4 | Install the power adapter in the power adapter wall-mount bracket.

(PA-440, PA-450, and PA-460) Install the power adapter in the power adapter wall-mount bracket using the Velcro straps and cable tie. Make sure to align the cable tie with the notches in the bracket to prevent the power cord from falling out. Next, loop the two Velcro straps through the side openings on the wall mount and over the power adapter. Lastly, loop the Velcro straps back over the top of the power adapter to secure it into place.



Connect the second power adapter through a different circuit breaker to provide power redundancy and allow for electrical circuit maintenance.

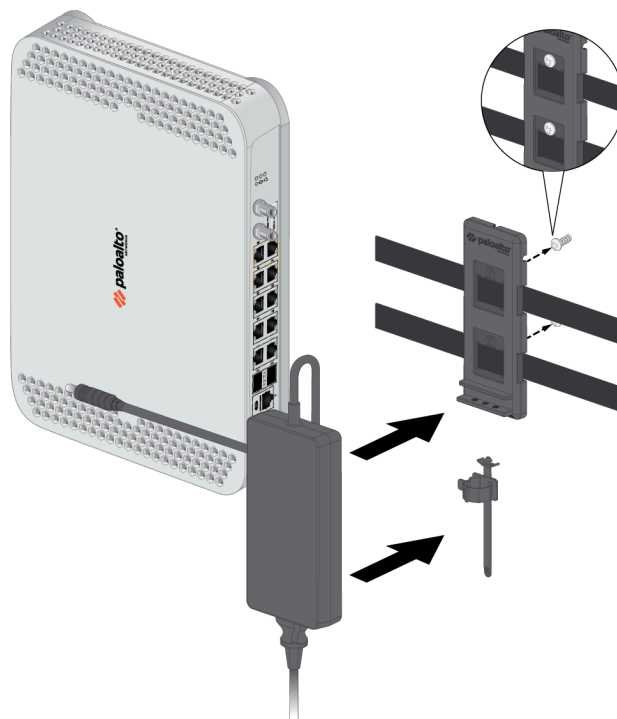


(PA-415, PA-415-5G, PA-455, and PA-445) Install the power adapter in the power adapter wall-mount bracket using the Velcro straps and cable tie. Make sure to align the cable tie with the notches in the bracket to prevent the power cord from falling out. Next, loop the two

Velcro straps through the side openings on the wall mount and over the power adapter. Lastly, loop the Velcro straps back over the top of the power adapter to secure it into place.



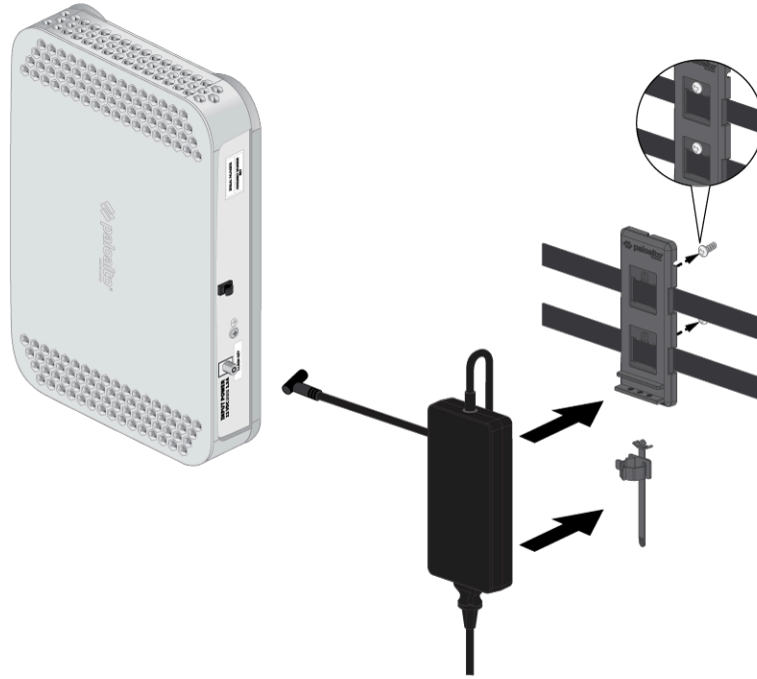
Connect the second power adapter through a different circuit breaker to provide power redundancy and allow for electrical circuit maintenance.



(PA-410) Install the power adapter in the power adapter wall-mount bracket using the Velcro straps and cable tie. Make sure to align the cable tie with the notches in the bracket to prevent the power cord from falling out. Next, loop the two Velcro straps through the side openings on

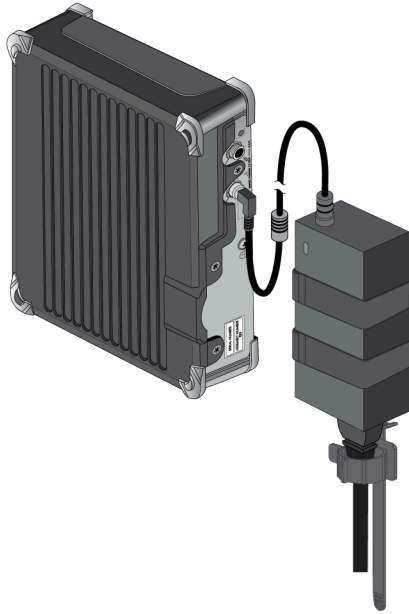
Install the PA-400 Series Firewall

the wall mount and over the power adapter. Lastly, loop the Velcro straps back over the top of the power adapter to secure it into place.

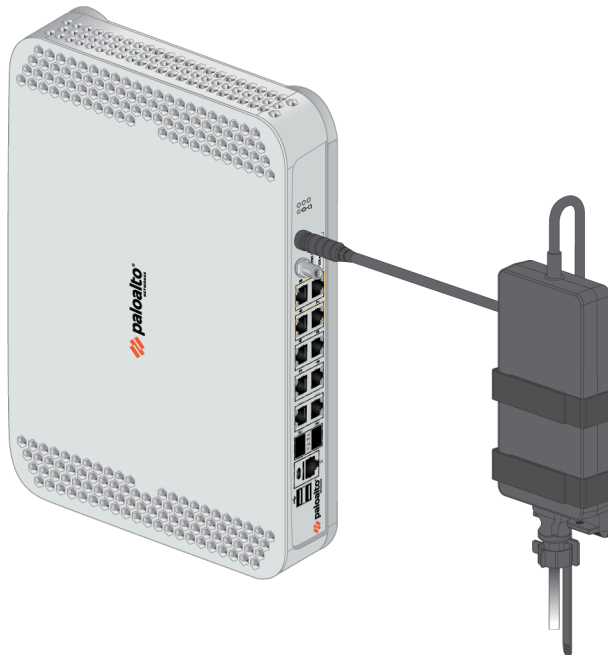


STEP 5 | After you secure the power adapter to the bracket, mount the bracket next to the firewall using wood or drywall screws as appropriate.

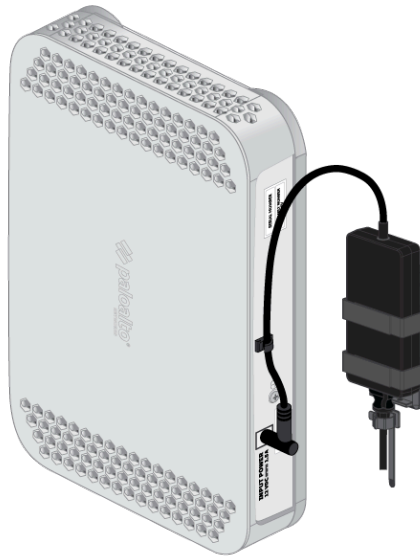
(PA-440, PA-450, and PA-460)



(PA-415, PA-415-5G, PA-455, and PA-445)



(PA-410)



STEP 6 | (PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460) You can install an optional second power adapter next to the first power adapter.

Install the PA-400 Series Firewall in a 19-inch Equipment Rack

The PAN-PA-400-RACKTRAY enables you to install one or two PA-440, PA-450, or PA-460 firewalls in a four-post 19" rack. The installation hardware consists of a metal base and two rails that can be expanded to include up to two firewalls and two PSUs.

The PAN-PA-400-POE-RACKTRAY enables you to install one PA-415 or PA-445 firewall in a four-post 19" rack. The installation hardware consists of a metal base and two rails that can include up to two PSUs.

The PAN-1RU-RGD-RACK-KIT-4POST enables you to install one PA-415-5G in a four-post 19" rack. The installation hardware consists of a metal base and two rails that can include up to two PSUs for the PA-415-5G.

The PAN-1RU-SMALL-RACK4 enables you to install one PA-455 in a four-post 19" rack.



To ease installation, first install the firewall(s) in the rack tray and then install the assembled rack tray into the equipment rack.

- [Install the PA-400 Series Firewall Using the PAN-PA-400-RACKTRAY](#)

Install the PA-400 Series Firewall Using the PAN-PA-400-RACKTRAY

Up to two individual PA-440, PA-450, or PA-460 firewalls can be mounted in a 19" equipment rack using the PAN-PA-400-RACKTRAY. The mounting equipment requires 1 RU of rack space.

One PA-415-5G firewall can be mounted in a 19" equipment rack using the PAN-PA-5G-RACKTRAY-ANT-CABLE. The mounting equipment requires 1 RU of rack space.

One PA-455 firewall can be mounted in a 19" equipment rack using the PAN-1RU-SMALL-RACK4. The mounting equipment requires 1 RU of rack space.

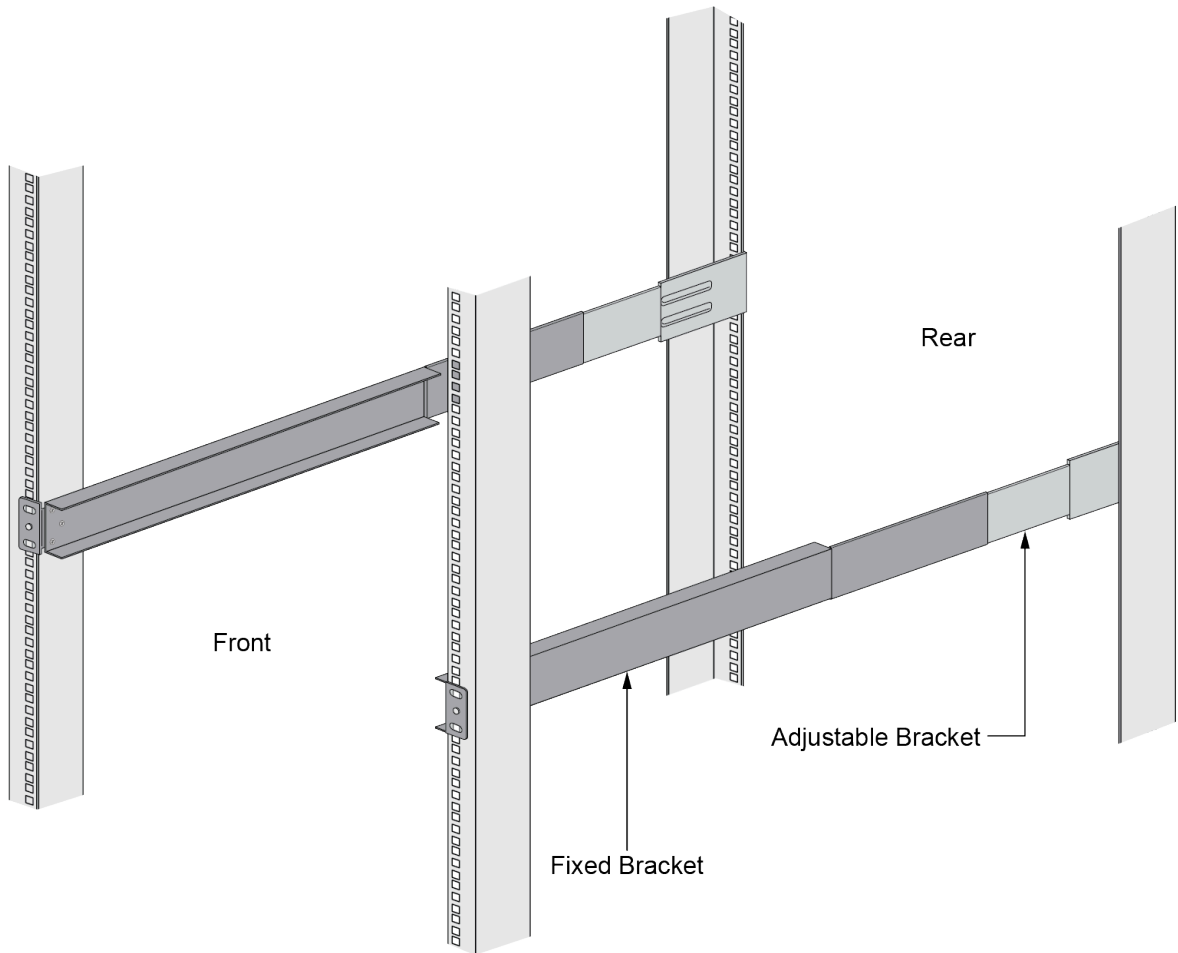
One PA-415 or PA-445 firewall can be mounted in a 19" equipment rack using the PAN-PA-400-POE-RACKTRAY. This mounting equipment requires 1RU of rack space.



If you have a firewall that supports multi-band antennas, make sure that you read how to [install antennas on the 5G firewall](#) before continuing with this procedure.

The procedure to install each set of mounting equipment is the same unless specified otherwise.

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.

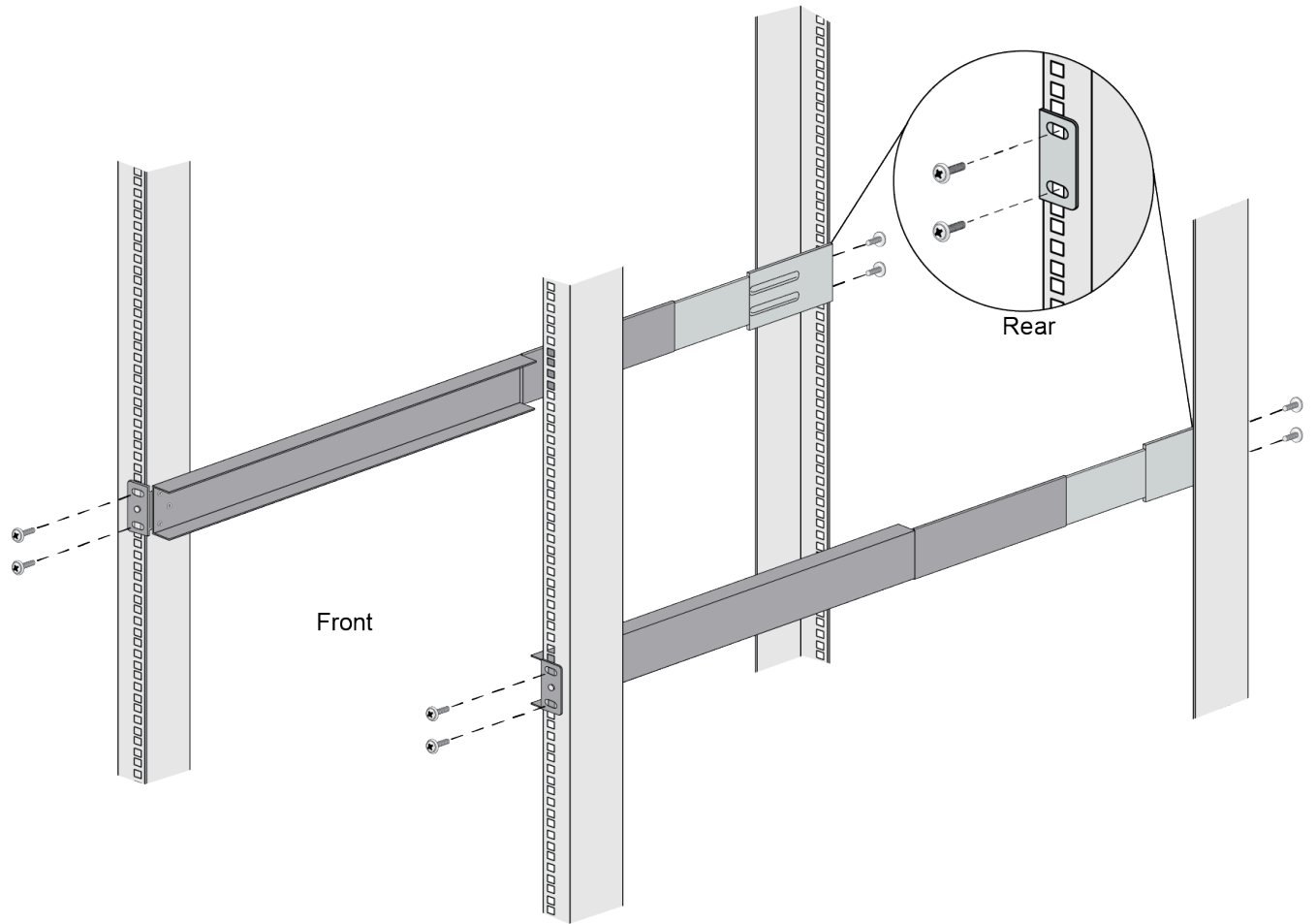


STEP 2 | Align the bottom edge of the mounting rails to the bottom of the 1 RU reserved for your firewall. Align the slotted holes in the adjustable mounting bracket to the holes on the rear of the equipment frame.



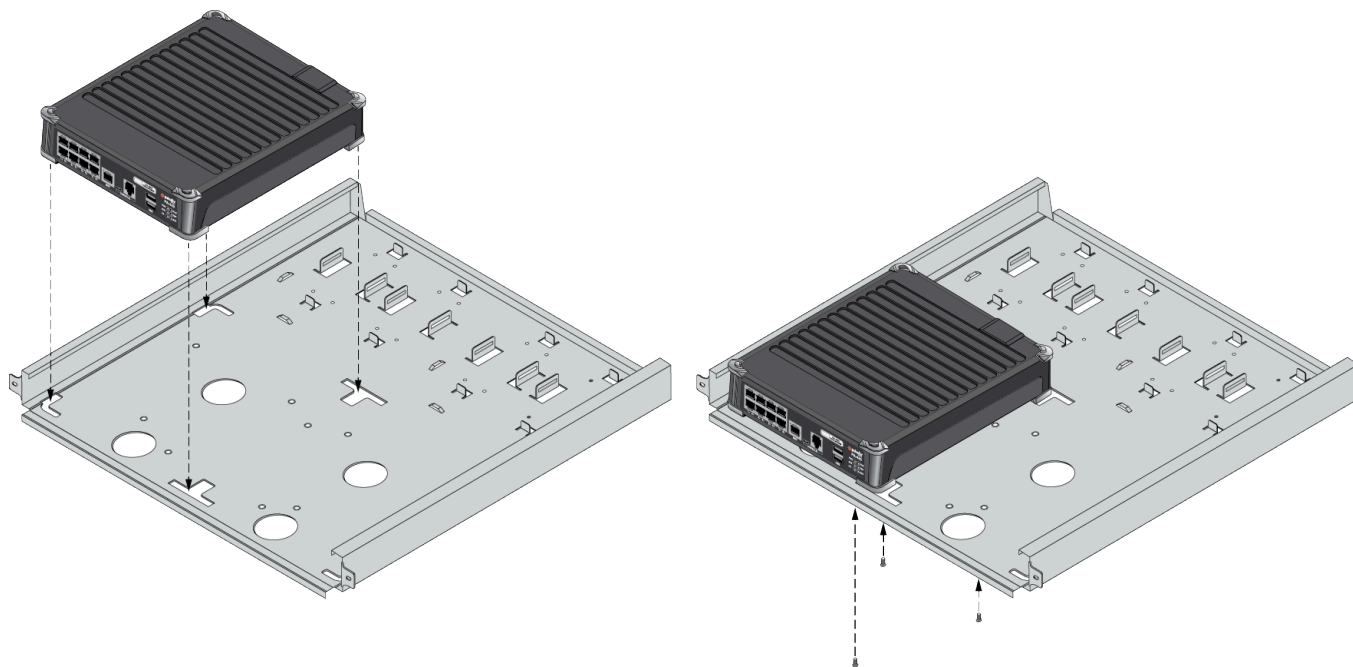
The mounting rails are designed for equipment frames that are 26" to 32" deep.

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.

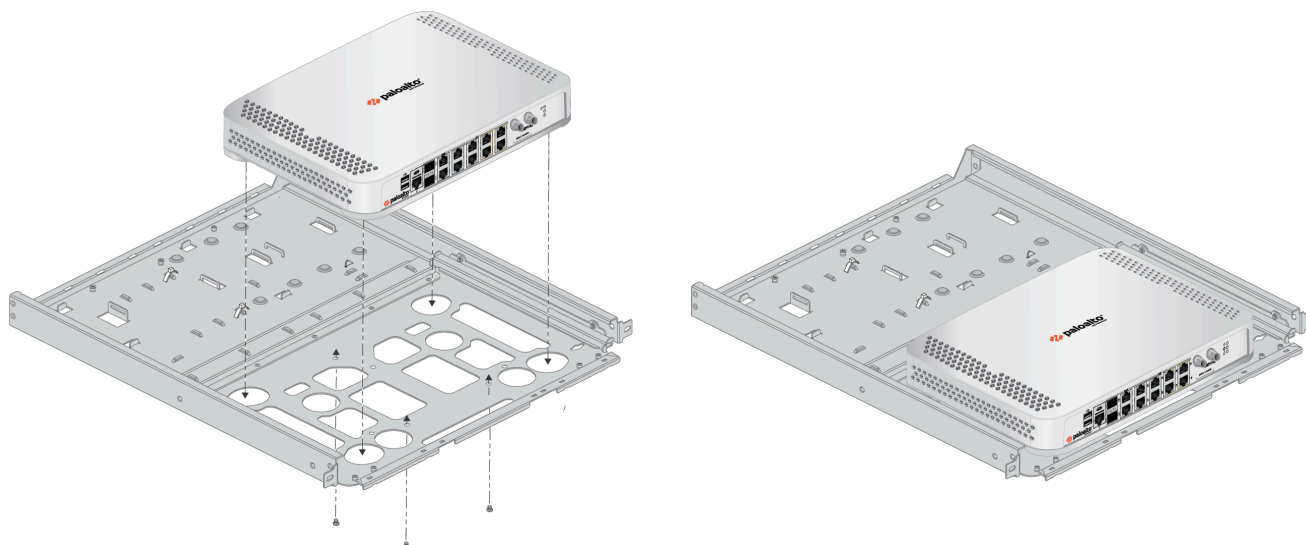


STEP 4 | With the front of the firewall facing forward, align the four rubber feet on the bottom of the device to the slotted holes in the provided mounting tray.

(PA-440, PA-450, and PA-460 firewalls)

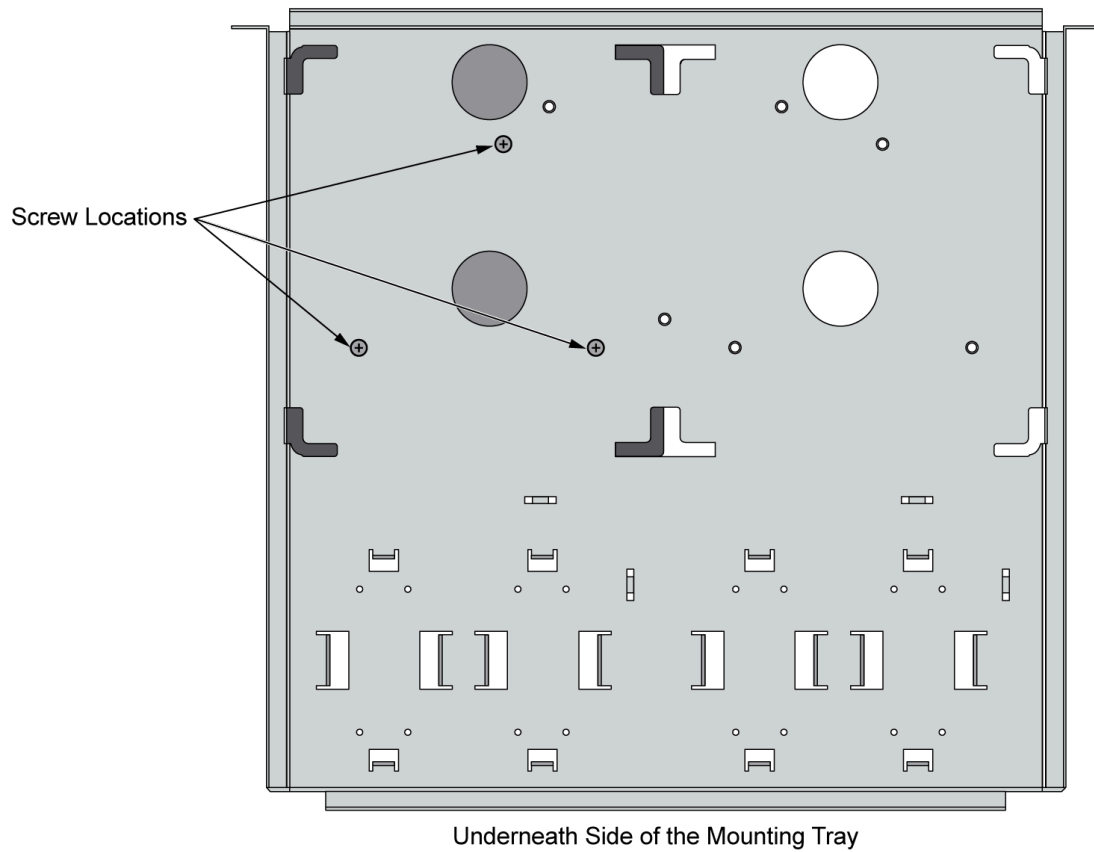


(PA-415, PA-415-5G, PA-455, and PA-445 firewalls)

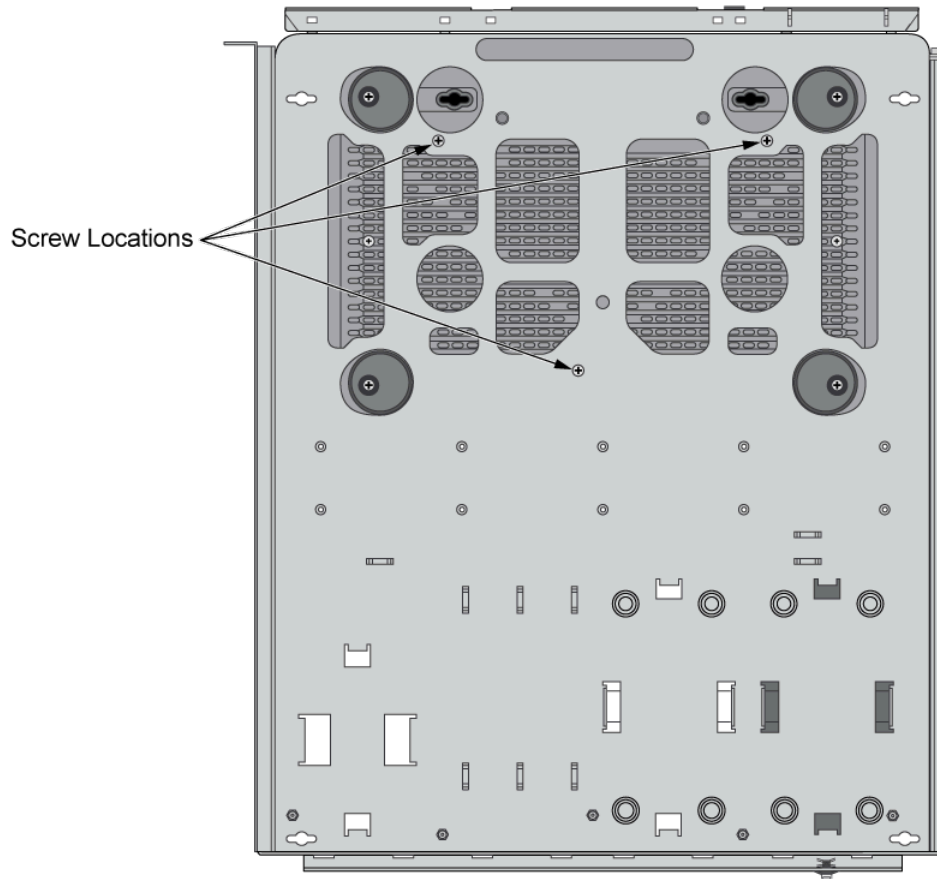


STEP 5 | While holding the firewall, carefully flip the mounting tray over to reveal its underside.

STEP 6 | Secure the firewall in place using three of the provided #6-32 x 3/16" Long Flathead screws.
(PA-440, PA-450, and PA-460 firewalls)



(PA-415, PA-415-5G, PA-455, and PA-445 firewalls)

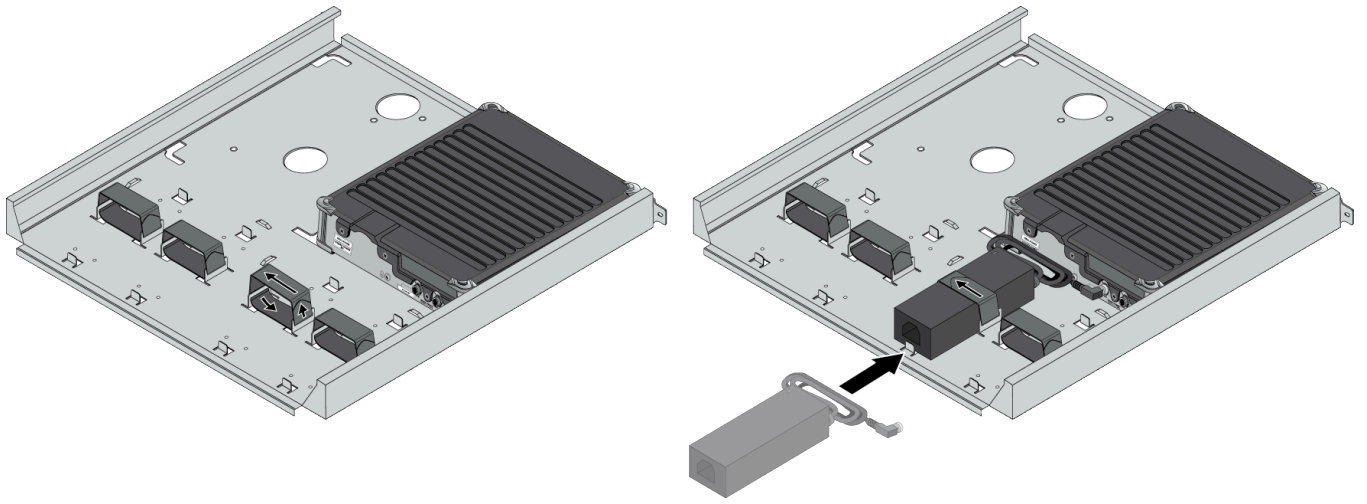


STEP 7 | (If mounting a second firewall) Repeat Steps 4 through 6 for the second firewall. Place the second firewall adjacent to the first firewall in the mounting tray.

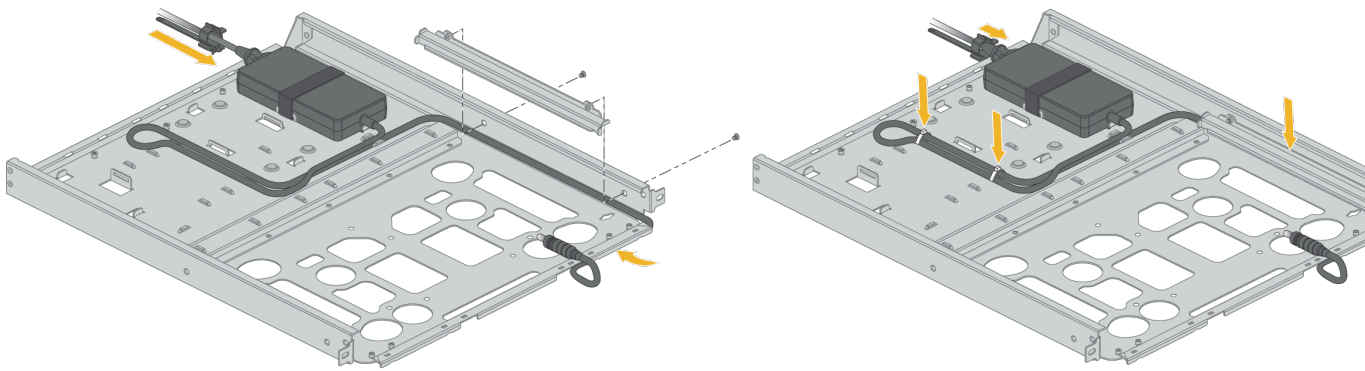
STEP 8 | Flip the mounting tray back into an upright position.


STEP 9 | Slide the firewall power supply into the marked position. Fasten the provided velcro strap around the power supply until it is secure in place.

(PA-440, PA-450, and PA-460 firewalls)




(PA-415, PA-415-5G, PA-455, and PA-445 firewalls)



 For the PA-415 and PA-445 firewalls, use the provided bracket to keep the power adapter cable in place.

STEP 10 | Plug the power supply connector into the back or front of the firewall depending on where the power input is located. Using the provided tie-wraps, bind and secure the power supply cable to the metal hooks in the mounting tray.

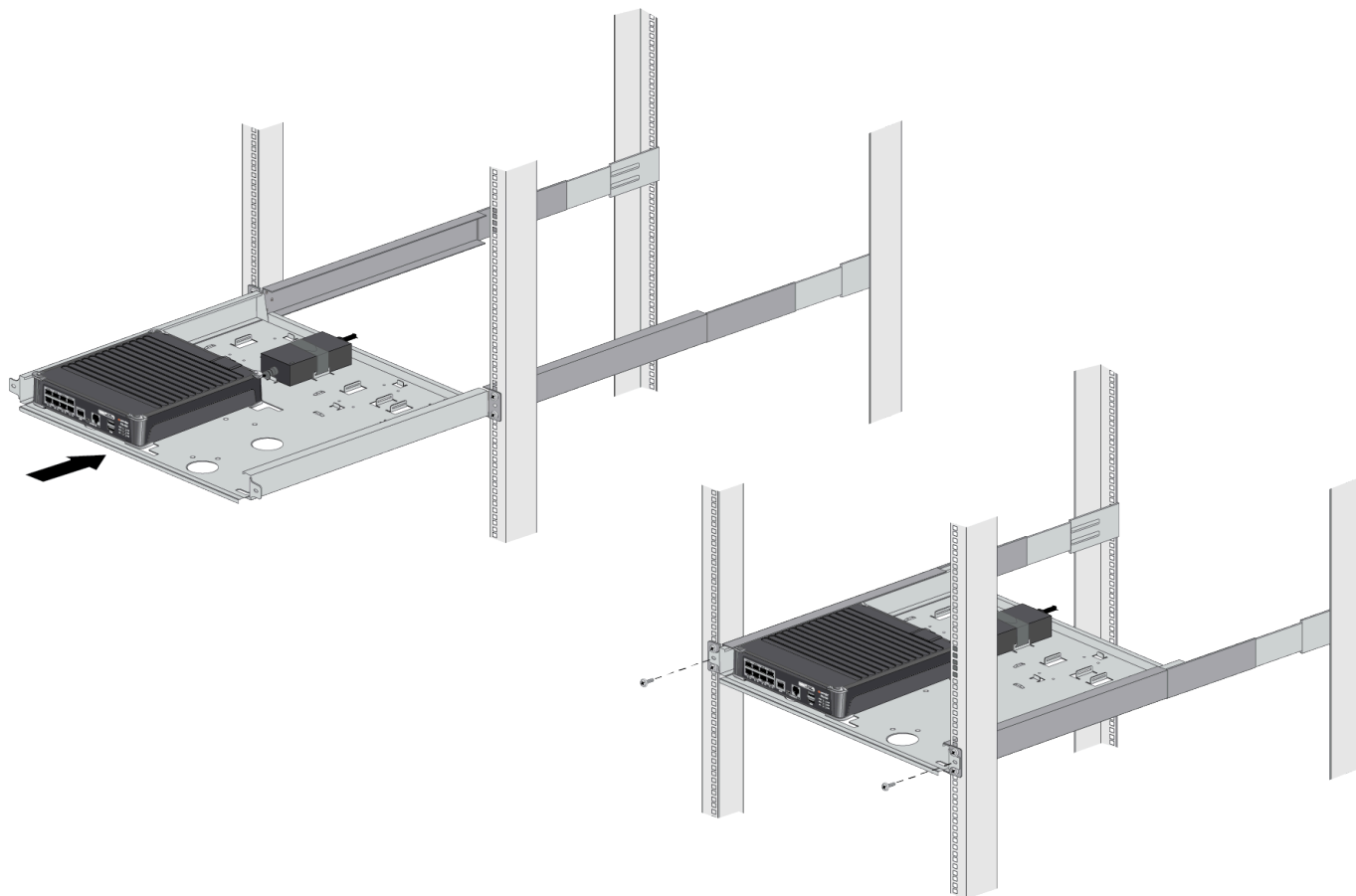
 A redundant power supply can be mounted in the available position next to the primary power supply.

STEP 11 | (If mounting a second firewall) Repeat Steps 9 and 10 for the power supplies of the second firewall.

STEP 12 | 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.

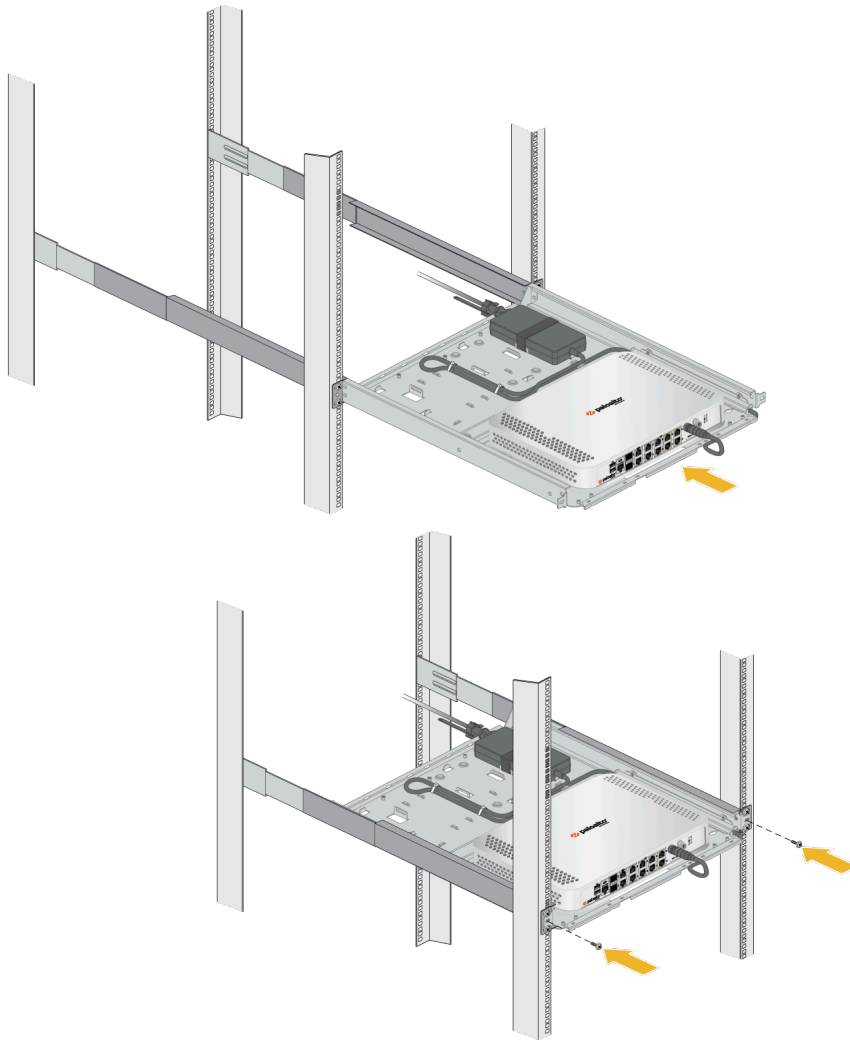
STEP 13 | Align the slotted holes in the mounting tray to the holes in the equipment frame. Secure the mounting tray to the equipment frame on both sides using 3 screws each (not provided). The screws must be compatible with your equipment frame.

(PA-440, PA-450, and PA-460 firewalls)



(PA-415, PA-415-5G, PA-455, and PA-445 firewalls)




Install the PA-400 Series Firewall



STEP 14 | Proceed to [Connect Power to a PA-400 Series Firewall](#)

Install Antennas on the PA-400 Series 5G Firewall

The PA-415-5G firewalls support four multi-band antennas. The following procedure describes how to install the to the four antenna SMA (F) connectors on the firewall.

-  *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 | Connect the antennas.

PA-415-5G

Secure the antennas to the SMA connectors located at the corners of the device. Rotate the antennas at 180-degree movement about the SMA connectors. Tighten the antennas by hand.



STEP 2 | 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](#) 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-400 Series Firewall


The PA-415-5G firewalls support two SIM slots to enable mobile network connectivity.


STEP 1 | Remove the SIM cover.

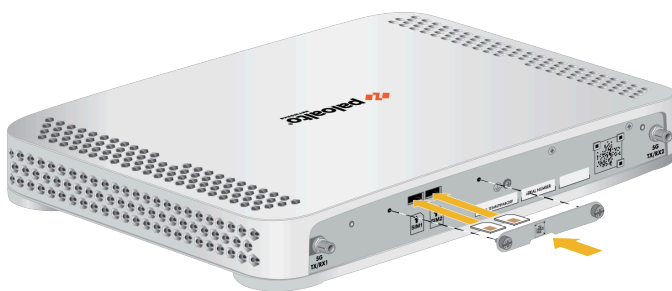
The SIM cover is on the back of the firewall. Unfasten the two M3 screws on the SIM cover using a type one Phillips screwdriver. Remove the SIM cover.




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.*

 *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.*



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

 *To eject the SIM from the device, gently push the SIM inward using a finger tip. Release the finger tip and pull out the SIM.*

Set Up a Connection to the Firewall

On first startup, the PA-400 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-400 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.

```
SSH Public key fingerprints:
Generating SSH2 RSA host key of length 2048: [ OK ]
2048 MD5:28:5a:a8:4e:3d:69:99:a8:b0:4a:77:9c:12:f6:62:ce no comment (RSA)
Starting sshd: [ OK ]
Starting PAN Software: ERROR: Module us[ 73.058994] intel_qat: module verification failed: signature and/or required key missing - tainting kernel
dm_drv does not exist in /proc/modules
ERROR: Module qat_c3xxx does not exist in /proc/modules
ERROR: Module intel_qat does not exist in /proc/modules
FATAL: Module qat_c3xxx not found.
Restarting all devices.
Processing /etc/c3xxx_dev0.conf
Checking status of all devices.
There is 1 QAT acceleration device(s) in the system:
qat_dev0 - type: c3xxx, inst_id: 0, node_id: 0, bsf: 0000:01:00.0, #accel: 3 #engines: 6 state: up
CPLD RSU not supported for ver 0x0
***** FIPS-CC Plugin Self-Tests Stage-2 begins *****
***** FIPS-CC Plugin Self-Tests Stage-2 passed *****
Zero touch provisioning (ZTP) of the firewall is in progress.
Do you want to exit ZTP mode and configure your firewall in standard mode (yes/no)[no]:y\y/no
[ OK ]
```



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-400 Series Firewall

All PA-400 Series firewalls are powered by an external power adapter that converts an AC power source to DC power.


All firewalls, except for the PA-410, 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.


- [Connect Power to a PA-400 Series Firewall](#) (PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460)
- [Connect Power to a PA-410 Firewall](#)

Connect Power to a PA-400 Series Firewall

The following procedure describes how to connect power to a PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460 firewall.

 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](#).


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.

 *(PA-415 and PA-445 only)* A ground connection is not required during normal operation. For these firewalls, skip to Step 3 of the following procedure.

STEP 1 | Remove the screw and star washer from the ground point on the back of the firewall.

STEP 2 | Crimp a 14AWG ground cable to a ring lug (cable and lug not included), place the ring lug over the screw and star washer, then replace the screw to attach the cable to the firewall. Torque the screw to 25 in-lbs and then connect the other end of the cable to earth ground.

STEP 3 | Connect the DC connector from the power adapter into the PWR 1 port on the firewall and tighten the connector nut to secure the cable to the firewall.

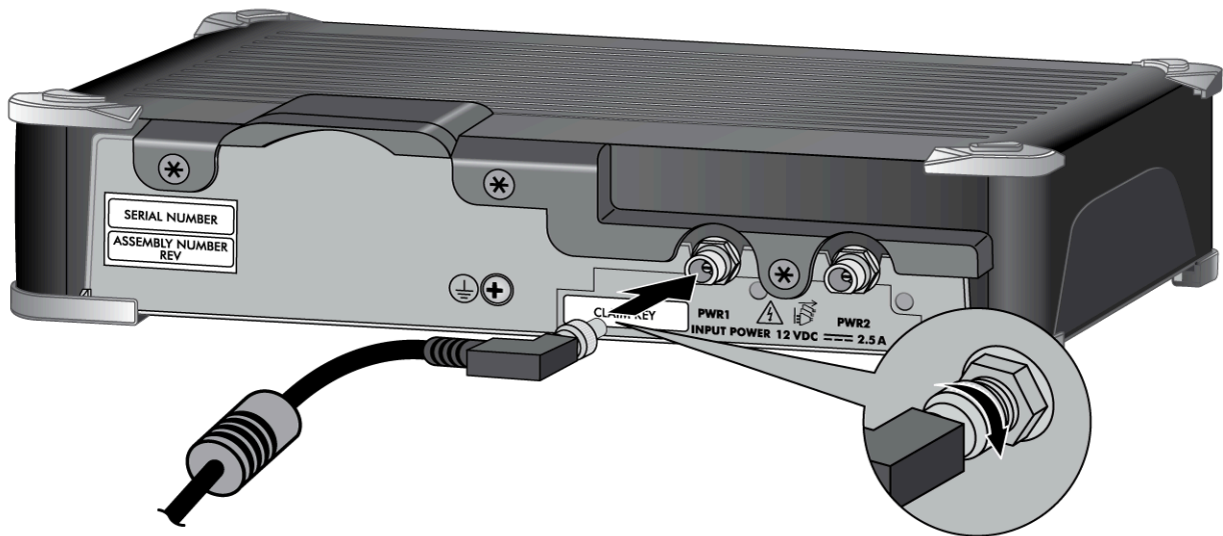
 The power adapter inputs for the PA-440, PA-450, and PA-460 are on the back panel of the device. The power adapter inputs for the PA-415, PA-415-5G, PA-455, and PA-445 are on the front panel of the device.

Ensure the power adapter itself is appropriately positioned (see [Install the PA-400 Series Firewall](#)).

(PA-415, PA-415-5G, PA-455, and PA-445 (PA-415 pictured))







(PA-440, PA-450, and PA-460)




STEP 4 | Plug the AC connector from the power adapter into your AC power source. After power is connected, the firewall powers on as indicated by the green power LED next to the PWR 1 port. The front PWR LED shows green when a functioning power adapter is connected.

STEP 5 | (Optional for PA-415, PA-415-5G, PA-440, PA-445, PA-450, and PA-460) Connect the DC connector from a second power adapter (purchased separately) into the PWR 2 port and plug the AC connector into an AC power source.

-  For the PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460, connect the second power adapter through a different circuit breaker to provide power redundancy and to allow for electrical circuit maintenance.
-  On the PA-440, PA-450, and PA-460, the control check on the power supply can detect if a connection is present but does not check for voltage. As a result, if the power cable is connected to the firewall but disconnected from a power source, the system still reads the power connection as inserted.
-  On some PA-440, PA-450, and PA-460 models, the **show system environmentals** command in the CLI displays the status of a second power supply when a second power supply is not connected.
-  Before powering on the firewall, ensure that you have connected your Ethernet cables in accordance to the mode you wish to boot the firewall in (standard mode or Zero Touch Provisioning mode) as specified in [Set Up a Connection to the Firewall](#).

Connect Power to a PA-410 Firewall


The following procedure describes how to connect power to a PA-410 firewall.

-  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](#).

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.

- STEP 1 |** Crimp a 14AWG ground cable to a ring lug (cable and lug not included), place the ring lug over the screw and star washer, then replace the screw to attach the cable to the firewall. Torque the screw to 25 in-lbs and then connect the other end of the cable to earth ground.
- STEP 2 |** Insert the DC connector from the power adapter into the port on the back of the firewall. Snap the DC connector cable to the cord retainer.



- STEP 3 |** Ensure the power adapter itself is appropriately positioned (see [Install the PA-400 Series Firewall](#)).
 - STEP 4 |** Plug the AC connector from the power adapter into your AC power source. After power is connected, the firewall powers on as indicated by the green power LED next to the PWR port. The front PWR LED shows green when a functioning power adapter is connected.
-  Before powering on the firewall, ensure that you have connected your Ethernet cables in accordance to the mode you wish to boot the firewall in (standard mode or Zero Touch Provisioning mode) as specified in [Set Up a Connection to the Firewall](#).


Service the PA-400 Series Firewall Hardware




The following topics describe how to interpret the PA-400 Series status LEDs and how to replace a PA-400 Series power adapter. The power adapter is the only serviceable component on the PA-400 Series firewall.




- [Interpret the LEDs on a PA-400 Series Firewall](#)
- [Replace a Power Adapter on a PA-400 Series Firewall](#)



Interpret the LEDs on a PA-400 Series Firewall

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

-  The PA-410, PA-415, and PA-445 firewall only have PWR, STAT, and ALM front panel LEDs. They do not have any back panel LEDs.



LED	Description
Front Panel LEDs	
<ul style="list-style-type: none"> (PA-410, PA-440, PA-450, and PA-460) HA (High Availability) (PA-415, PA-415-5G, PA-455, and PA-445)  	<ul style="list-style-type: none"> 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. <p> <i>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).</i></p>
<ul style="list-style-type: none"> (PA-410, PA-440, PA-450, and PA-460) STAT (Status) (PA-415, PA-415-5G, PA-455, and PA-445)  	<ul style="list-style-type: none"> Green—The firewall is operating normally. (PA-410, PA-440, PA-450, and PA-460) Yellow—The firewall is booting. (PA-415, PA-415-5G, PA-455, and PA-445) Red—The firewall is booting.
<ul style="list-style-type: none"> (PA-410, PA-440, PA-450, and PA-460) ALM (Alarm) (PA-415, PA-415-5G, 	<ul style="list-style-type: none"> Red—A hardware component failed, such as a power adapter 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.

LED	Description
<p>PA-455, and PA-445)</p> 	
<p>TEMP (Temperature)</p>	<ul style="list-style-type: none"> • Green—The firewall temperature is normal. • Yellow—The firewall temperature is outside tolerance levels.
<ul style="list-style-type: none"> • (PA-410, PA-440, PA-450, and PA-460) <p>PWR (Power)</p> <ul style="list-style-type: none"> • (PA-415, PA-415-5G, PA-455, and PA-445) 	<ul style="list-style-type: none"> • 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).
<p>SVC (Service)</p>	<p>This LED is disabled by default but can be enabled by a remote administrator to illuminate the device for a local operator. To enable the LED, use the following CLI command:</p> <pre>admin@PA-440> set system setting service-led enable yes</pre> <ul style="list-style-type: none"> • Off—The LED is disabled. • Blinking Red and Green—The firewall has been instructed to enable the LED.
<p>Cellular</p>  <p>(PA-415-5G only)</p>	<ul style="list-style-type: none"> • 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.
<p>Ethernet port LEDs</p>	<ul style="list-style-type: none"> • Left LED—Solid green indicates a network link. • Right LED—Blinking green indicates network activity.

LED	Description
	<p> If you configure the link state to down on a port, the LEDs on some active 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.</p>
<p>Back Panel LEDs</p>	
<p>(PA-440, PA-450, and PA-460 only) PWR 1 and PWR 2</p>	<p>The following describes the power adapter LEDs on the back of the firewall:</p> <ul style="list-style-type: none"> • Green—The power input is receiving power. • Off—The power input is not receiving power. <p> The PWR LED on the front of the firewall shows green if one or both power adapters are connected to the back power inputs. If both power adapters are connected and one power adapter fails, the PWR LED on the back of the firewall turns off and the ALM LED turns red.</p>


Replace a Power Adapter on a PA-400 Series Firewall

The PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460 firewalls can operate on one power adapter or you can install a second power adapter for power redundancy. If two power adapters are installed and one fails, you can replace the failed power adapter without interruption. The PA-410 can only operate on one power adapter.

-  *The CLI cannot be used to determine the status of the PA-400 Series firewalls power adapter. To manually interpret the status of the power adapter, verify that your power cable connections are secure and that the LED on the power adapter is on. If the LED is not illuminated even though the power cable connections are secure, your power adapter has failed.*
-  *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](#).*

STEP 1 | Disconnect the failed power adapter.

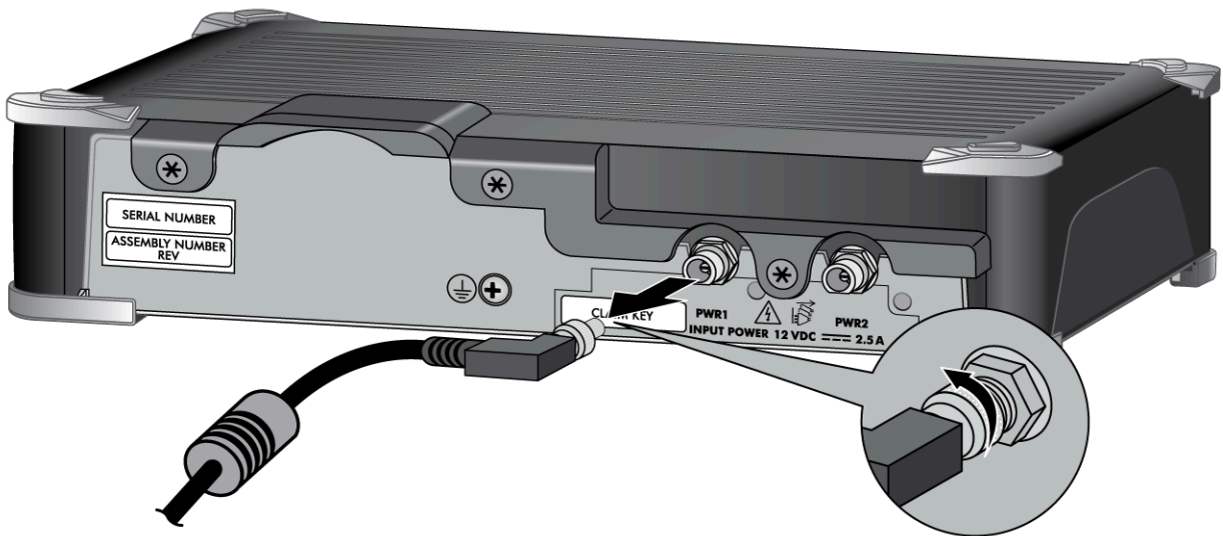
(PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460) Unplug the failed power adapter from the AC power source and then turn the power cable connector nut counterclockwise to release the cable. Pull the cable away from the firewall to remove it.

 *The power adapter inputs for the PA-440, PA-450, and PA-460 are on the back panel of the device. The power adapter inputs for the rest of the PA-400 Series firewalls are on the front panel of the device.*

(PA-415, PA-415-5G, PA-455, and PA-445 (PA-415 pictured))



(PA-440, PA-450, and PA-460)



(PA-410) Unplug the failed power adapter from the AC power source and pull the power cable out of the firewall to remove it.

STEP 2 | Connect a new power adapter.

(PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460) Connect the DC connector from the new power adapter to the power input (PWR 1 or PWR 2) port on the firewall and, if applicable, tighten the connector nut to secure the cable to the firewall.

(PA-410) Connect the DC connector from the new power adapter to the power input port on the firewall.

STEP 3 | Plug the AC connector from the power adapter into an AC power source.

PA-400 Series Firewall Specifications

The following topics describe the PA-400 Series firewall hardware specifications. For feature, capacity, and performance information, refer to the [datasheet](#).

- [Physical Specifications](#)
- [Electrical Specifications](#)
- [Environmental Specifications](#)
- [Antenna Specifications](#)
- [Miscellaneous Specifications](#)

Physical Specifications

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

Specification	Value
Rack units and dimensions	<p>PA-410</p> <ul style="list-style-type: none"> Height: 1.73", Width: 9.53", Depth: 6.60" (Height: 4.39 cm, Width: 24.21 cm, Depth: 16.76 cm) <p>PA-415 and PA-415-5G</p> <ul style="list-style-type: none"> Height: 1.73", Width: 13", Depth: 9" (Height: 4.40 cm, Width: 33.02 cm, Depth: 22.86 cm) Rack units—1U <p>PA-445</p> <ul style="list-style-type: none"> Height: 1.66", Width: 13", Depth: 8.88" (Height: 4.22 cm, Width: 33.02 cm, Depth: 22.56 cm) Rack units—1U <p>PA-455</p> <ul style="list-style-type: none"> Height: 1.7", Width: 15.4", Depth: 9.4" (Height: 4.32 cm, Width: 39.12 cm, Depth: 23.88 cm) Rack units—1U <p>PA-440, PA-450, and PA-460</p> <ul style="list-style-type: none"> Height: 1.75", Width: 8", Depth: 8.8" (Height: 4.45 cm, Width: 20.3 cm, Depth: 22.35 cm) Rack units—1U Rack kit dimensions—Height: 1.75" X Width: 17.5" X Depth: 14" (4.44cm X 44.45cm X 35.56cm)
Antenna dimensions	<p>PA-415-5G</p> <ul style="list-style-type: none"> Length: 9.02" (22.91 cm), Width: 1.10" (2.79 cm), Thickness: 0.55" (1.40 cm)
Weight	<p>PA-410</p> <ul style="list-style-type: none"> Firewall weight—3.0 lbs (1.36 kg) Shipping weight—6.0 lbs (2.72 kg) <p>PA-415</p> <ul style="list-style-type: none"> Firewall weight—7.85 lbs (3.56 kg) Shipping weight—12.21 lbs (5.54 kg) <p>PA-415-5G</p>

Specification	Value
	<ul style="list-style-type: none">• Firewall weight—7.85lbs (3.56 kg)• Shipping weight—TBD
	PA-445
	<ul style="list-style-type: none">• Firewall weight—8.69 lbs (3.94 kg)• Shipping weight—12.6 lbs (5.72 kg)
	PA-455
	<ul style="list-style-type: none">• Firewall weight—9.8 lbs (4.45 kg)• Shipping weight—12.8 lbs (5.81 kg)
	PA-440, PA-450, and PA-460
	<ul style="list-style-type: none">• Firewall weight—5.0 lbs (2.27 kg)• Shipping weight—7.8 lbs (3.54 kg)

Electrical Specifications

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

Specification	Value
Power adapter	<p>The PA-400 Series firewalls operate on DC power that is provided by the external power adapter (provided).</p> <p>The firewall can operate on one power adapter or you can install a second power adapter for power redundancy.</p>
Input voltage	<p>PA-410</p> <ul style="list-style-type: none"> Power adapter (AC side)—100-240V AC 50-60Hz The power adapter converts the AC power to 12VDC to provide power to the firewall. <p>PA-415, PA-415-5G, and PA-445</p> <ul style="list-style-type: none"> Power adapter (AC side)—100-240V AC 50-60Hz The power adapter converts the AC power to 12VDC to provide power to the firewall. <p>PA-455</p> <ul style="list-style-type: none"> DC power—12-48VDC <p>PA-440, PA-450, and PA-460</p> <ul style="list-style-type: none"> Power adapter (AC side)—100-240V AC 50-60Hz The power adapter converts the AC power to 12VDC to provide power to the firewall.
Power consumption	<p>PA-410</p> <ul style="list-style-type: none"> Maximum—24W <p>PA-415</p> <ul style="list-style-type: none"> Maximum—135W <p>PA-415-5G</p> <ul style="list-style-type: none"> Maximum—135W <p>PA-440</p> <ul style="list-style-type: none"> Maximum—30W <p>PA-445</p> <ul style="list-style-type: none"> Maximum—135W <p>PA-450 and PA-460</p> <ul style="list-style-type: none"> Maximum—36W

Specification	Value
	<p>PA-455</p> <ul style="list-style-type: none"> • Maximum—147W
Maximum current consumption	<p>PA-410</p> <ul style="list-style-type: none"> • Firewall—2A@12VDC <p>PA-415</p> <ul style="list-style-type: none"> • Firewall—11.3A@12VDC <p>PA-415-5G</p> <ul style="list-style-type: none"> • Firewall—TBD@12VDC <p>PA-440</p> <ul style="list-style-type: none"> • Firewall—2.5A@12VDC <p>PA-445</p> <ul style="list-style-type: none"> • Firewall—11.3A@12VDC <p>PA-450 and PA-460</p> <ul style="list-style-type: none"> • Firewall—3A@12VDC <p>PA-455</p> <ul style="list-style-type: none"> • Firewall—13A@12VDC
Power over Ethernet (PoE)	<p>PA-415 and PA-445</p> <ul style="list-style-type: none"> • Supported on ports 6, 7, 8, and 9 • Maximum reserved power—60W • Total PoE budget allowed (across all ports) —91W

Environmental Specifications

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

Specification	Value
Operating temperature range	<p>PA-410, PA-415-5G, PA-440, PA-450, and PA-460</p> <ul style="list-style-type: none"> • 32°F to 104°F (0° to 40°C) <p>PA-415 and PA-445</p> <ul style="list-style-type: none"> • 32°F to 113°F (0° to 45°C) <p>PA-455</p> <ul style="list-style-type: none"> • -40°F to 158°F (-40° to 70°C)
Non-operating temperature	<p>PA-410, PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460</p> <ul style="list-style-type: none"> • -4°F to 158°F (-20° to 70°C)
Humidity tolerance	10% to 90% non-condensing
Airflow	The other PA-400 Series firewalls use passive cooling and do not contain fans.
Maximum BTUs/hour	<p>PA-410</p> <ul style="list-style-type: none"> • 82/hour <p>PA-415</p> <ul style="list-style-type: none"> • 461/hour <p>PA-415-5G</p> <ul style="list-style-type: none"> • 461/hour <p>PA-440</p> <ul style="list-style-type: none"> • 102/hour <p>PA-445</p> <ul style="list-style-type: none"> • 460/hour <p>PA-450 and PA-460</p> <ul style="list-style-type: none"> • 123/hour <p>PA-455</p> <ul style="list-style-type: none"> • 502/hour

Specification	Value
Electromagnetic Interference (EMI)	FCC Class B, CE Class B, VCCI Class B
Acoustic noise	Emits no sound.
Maximum operating altitude	10,000ft (3,048m)

Antenna Specifications

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

Specification	Value
Antennas	PA-415-5G <ul style="list-style-type: none"> Four 5G multi-band antennas
Supported radio frequency (RF) bands	5G NR Sub-6GHz (FR1): n2, n3, n5, n66, n71, n77, n78, n79 LTE: B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B46, B48, B66, B71 3G: B1, B2, B4, B5, B6, B8, B9, B19
Frequency range	PA-415-5G <ul style="list-style-type: none"> 615-960MHz / 1500-1600MHz / 1710-2690MHz / 3300-3700MHz
Peak gain	PA-415-5G <ul style="list-style-type: none"> 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
Voltage standing wave ratio (VSWR)	PA-415-5G <ul style="list-style-type: none"> <3:1
Feed impedance	PA-415-5G <ul style="list-style-type: none"> 50Ω
Power handling	PA-415-5G <ul style="list-style-type: none"> 30 dBm
Interface	SMA (F) Connectors
Cellular Carrier/Regulatory Certification	<ul style="list-style-type: none"> AT&T PTCRB GCF

Miscellaneous Specifications

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

Specification	Value
Storage capacity	PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460 <ul style="list-style-type: none">• One 128 GB eMMC PA-410 <ul style="list-style-type: none">• One 64 GB eMMC
Mean time between failures (MTBF)	29 years

PA-400 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-400 Series firewall, see [PA-400 Series Firewall Compliance Statements](#)

PA-400 Series Firewall Compliance Statements

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

- **BSMI EMC Statement:** (PA-415 and PA-445) This is a Class A product. When used in a residential environment it may cause radio interference. In this case, the user will be required to take adequate measures.
- **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.
- (PA-415 and PA-445 VCCI Class A requirements)

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

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.

- (PA-410, PA-440, PA-450, and PA-460 VCCI Class B requirements)

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI – B

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):**
 - (PA-410, PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460 firewalls)

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.
 - (PA-415-5G firewall)
- This device is herewith confirmed to comply with the requirements set out in the Radio Equipment Directive (2014/53/EU).

- **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.

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

- **TUV:** Product Ambient Temperature:
 - (PA-410, PA-440, PA-450, PA-455, and PA-460) 0~40 degrees C
 - (PA-415, PA-415-5G, and PA-445) 0~45 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**

- **PA-415, PA-415-5G, PA-455, and PA-445 Class A requirements**

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.
- **PA-410, PA-440, PA-450, and PA-460 Class B requirements**

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:

- 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**

- (PA-415, PA-415-5G, PA-455, and PA-445 Class A requirements)

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.

- (PA-410, PA-440, PA-450, and PA-460 Class B requirements)

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.

- **United Kingdom Declaration of Conformity (UKCA) Directives**

- (PA-410, PA-415, PA-415-5G, PA-440, PA-445, PA-450, PA-455, and PA-460 firewalls)

This equipment complies with the requirements set out in the UK Electrical Equipment (Safety) Regulations 2016 and Electromagnetic Compatibility Regulations 2016.

- (PA-415-5G firewall)

This equipment complies with the requirements set out in the UK Radio Equipment Regulations 2017.