Next-Generation Firewall

Perform the Initial Setup and Configuration for NGFWs

Previous
Integrate NGFWs into Your Network

Next
Set Up Network Access for External Services

Where Can I Use This?

- NGFWs

What Do I Need?

☐ No prerequisites needed for initial setup

Perform the initial configuration for your NGFW. You can perform these initial configuration tasks either from the MGT interface, even if you do not plan to use this interface for your NGFW management, or using a direct serial connection to the console port on the device.

The initial configurations need to be completed before you can begin onboarding your NGFW to your management system of choice.

> The initial configurations for your NGFWs can be performed before you have decided on the management style of choice and will need to be done before you can proceed with onboarding.

> For more information about what needs to be done before you can onboard to Strata Cloud Manager or Panorama, see the cheat sheet here.

By default, the PA-Series NGFW has:

☐ An IP address of 192.168.1.1

☐ A username/password of admin/admin

For security reasons, you must change these settings before continuing with other NGFW configuration tasks.

Standard | Air Gapped

STEP 1 - Install your NGFW and connect power to it.

> If your NGFW model has dual power supplies, connect the second power supply for redundancy. Refer to the hardware reference guide for your model for details.

STEP 2 - Gather the required information from your network administrator.

- IP address and netmask (if the MGT port will have a static address)
- Default gateway (if the MGT port will have a static default gateway address)
- DNS server address

STEP 3 - Connect your computer to the NGFW.

You can connect to the device in one of the following ways:

- Connect a serial cable from your computer to the Console port and connect to the firewall using terminal emulation software (9600-8-N-1). Wait a few minutes for the boot-up sequence to complete; when the NGFW is ready, the prompt changes to the name of the firewall, for example `PA-220 login`.
- Connect an RJ-45 Ethernet cable from your computer to the MGT port on the NGFW. From a browser, go to `https://192.168.1.1`.

> You may need to change the IP address on your computer to an address in the 192.168.1.0/24 network, such as 192.168.1.2, to access this URL.

STEP 4 - When prompted, log in to the NGFW.

You must log in using the default username and password (admin/admin). The NGFW will begin to initialize.

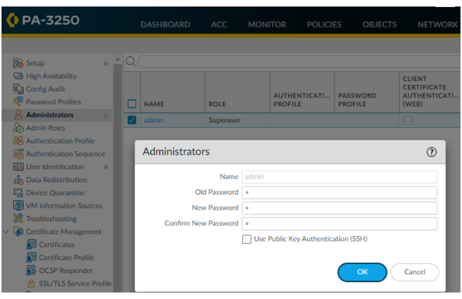
STEP 5 - Set a secure username and password for the admin account.

> The predefined, default administrator password (admin) must be changed on the first login on a device. The new password must be a minimum of eight characters and include a minimum of one lowercase and one uppercase character, as well as one number or special character. Although you don't have to configure a new username, it is a best practice to do so and to use unique usernames and passwords for each administrator. The login must include at least one alphabetical character or symbol (underscore, period, or hyphen, although a hyphen cannot be the first character in the username) and cannot be numbers only.
>
> Be sure to use the best practices for password strength to ensure a strict password and review the minimum password complexity.

① Select **Device > Administrators**.

② Select the **admin** role.

③ Enter the current default password and the new password.



NAME	ROLE
☑ admin	Superuser

Administrators

Name: admin
Old Password: •
New Password: •
Confirm New Password: •
☐ Use Public Key Authentication (SSH)

④ Click **OK** to save your settings.

STEP 6 - Configure the MGT interface.

① Select **Device > Setup > Interfaces** and edit the **Management** interface.

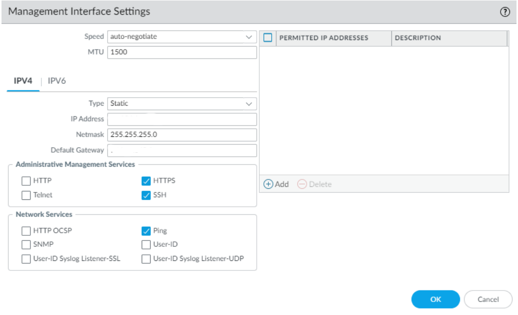
② Set the **Speed** to **auto-negotiate**.

③ Specify the **MTU** in bytes for packets sent on this interface.

④ Select **IPv4** or **IPv6**.

⑤ To configure IPv4 address settings for the MGT interface, select an address **Type**:

- **Static**– Enter the **IP Address**, **Netmask**, and **Default Gateway**.
- **DHCP Client**—To configure dynamic address settings, you must Configure the Management Interface as a DHCP Client.



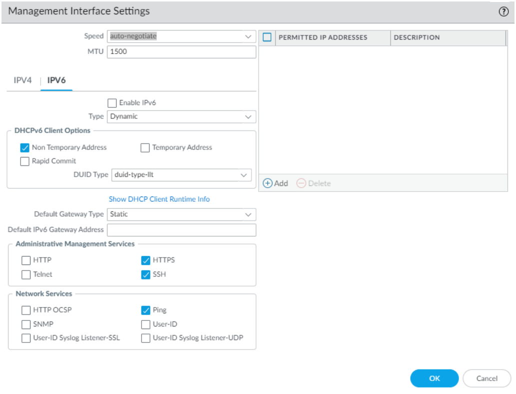
Speed: auto-negotiate
MTU: 1500
Type: Static
IP Address:
Netmask: 255.255.255.0
Default Gateway:

Administrative Management Services
☐ HTTP ☑ HTTPS
☐ Telnet ☑ SSH

Network Services
☐ HTTP OCSP ☑ Ping
☐ SNMP ☐ User-ID
☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

⑥ To configure IPv6 address settings for the MGT interface, **Enable IPv6** and select an address **Type**:

- **Static**– Enter the **IPv6 Address/Prefix Length**. Additionally, select a **Default Gateway Type**: **Static** (enter the **Default IPv6 Gateway Address**) or **Dynamic** (the NGFW learns the default gateway address from the Router Advertisement message that the router sent).
- **DHCP Client**—To configure dynamic IPv6 address settings, you must Configure the Management Interface for Dynamic IPv6 Address Assignment.



Speed: auto-negotiate
MTU: 1500
☐ Enable IPv6
Type: Dynamic

DHCPv6 Client Options
☑ Non Temporary Address ☐ Temporary Address
☐ Rapid Commit
DUID Type: duid-type-llt

Default Gateway Type: Static
Default IPv6 Gateway Address:

Administrative Management Services
☐ HTTP ☑ HTTPS
☐ Telnet ☑ SSH

Network Services
☐ HTTP OCSP ☑ Ping
☐ SNMP ☐ User-ID
☐ User-ID Syslog Listener-SSL ☐ User-ID Syslog Listener-UDP

⑦ To prevent unauthorized access to the management interface, it is a an administrative best practice to **Add** the **Permitted IP Addresses** from which an administrator can access the MGT interface.

⑧ Select which management services to allow on the interface.

> Make sure **Telnet** and **HTTP** aren't selected because these services use plaintext and aren't as secure as the other services; they could compromise administrator credentials.

⑨ Click **OK**.

STEP 7 - Specify the update server, and configure DNS settings and proxy server settings.

> You must manually configure at least one DNS server on the NGFW or it won't be able to resolve hostnames; it won't use DNS server settings from another source, such as an ISP.

① Select **Device > Setup > Services**.

- For multi-virtual system platforms, select **Global** and edit the Services section.
- For single virtual system platforms, edit the Services section.

② On the **Services** tab, **Update Server** represents the IP address or host name of the server from which to download updates from Palo Alto Networks. The current value is **updates.paloaltonetworks.com**. Don't change this setting unless instructed by technical support.

③ Select **Verify Update Server Identity**.

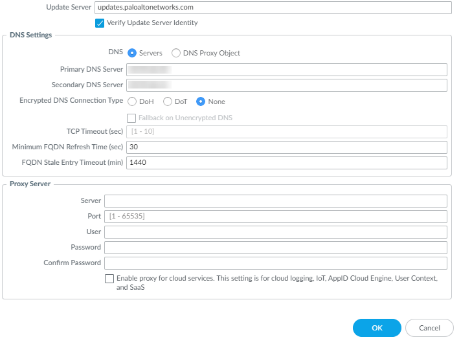
> It's a best practice to enable this option, which causes the firewall or Panorama to verify that the server from which the software or content package is downloaded has an SSL certificate signed by a trusted authority.

④ For **DNS**, select the way for the MGT interface to get DNS services:

- **Servers**—Enter the **Primary DNS Server** address and **Secondary DNS Server** address.
- **DNS Proxy Object**—From the drop-down, select the **DNS Proxy** that you want to use to configure global DNS services, or click **DNS Proxy** to configure a new DNS proxy object.

> Beginning with PAN-OS 11.2.1 and later releases, you can enable encrypted DNS on the MGT interface (whether the interface uses a DNS server or DNS proxy) by configuring DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT).
>
> - To configure encrypted DNS when the MGT interface uses DNS servers, refer to the Networking Administrator's Guide, Use Case 1: Firewall Requires DNS Resolution..
> - To configure encrypted DNS when the MGT interface uses DNS proxy, refer to the Networking Administrator's Guide, Configure a DNS Proxy Object.

Services
Services
NTP



Update Server: updates.paloaltonetworks.com

☑ Verify Update Server Identity

DNS Settings

DNS: ● Servers ○ DNS Proxy Object

Primary DNS Server

Secondary DNS Server

Encrypted DNS Connection Type: ○ DoH ○ DoT ● None

☐ Fallback on Unencrypted DNS

TCP Timeout (sec): [1 - 10]

Minimum FQDN Refresh Time (sec): 30

FQDN Stale Entry Timeout (min): 1440

Proxy Server

Server

Port: [1 - 65535]

User

Password

Confirm Password

☐ Enable proxy for cloud services. This setting is for cloud logging, IoT, AppID Cloud Engine, User Context, and SaaS

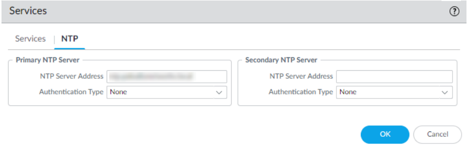
⑤ Click **OK**.

STEP 8 - Configure date and time (NTP) settings.

① Select **Device > Setup > Services**.

- For multi-virtual system platforms, select **Global** and edit the Services section.
- For single virtual system platforms, edit the Services section.

② On the **NTP** tab, to use the virtual cluster of time servers on the Internet, enter the hostname pool.ntp.org as the **Primary NTP Server** or enter the IP address of your primary NTP server.



Services

Primary NTP Server

NTP Server Address

Authentication Type: None

Secondary NTP Server

NTP Server Address

Authentication Type: None

③ (**Optional**) Enter a **Secondary NTP Server** address.

④ (**Optional**) To authenticate time updates from the NTP server(s), for **Authentication Type**, select one of the following for each server:

- **None**—(Default) Disables NTP authentication.
- **Symmetric Key**—NGFW uses symmetric key exchange (shared secrets) to authenticate time updates.
  - **Key ID**—Enter the Key ID (1-65534).
  - **Algorithm**—Select the algorithm to use in NTP authentication: **MD5**, **SHA1**, (**PAN-OS 12.1.2 & later**) **SHA256**, or **SHA512**.
- **Autokey**—NGFW uses autokey (public key cryptography) to authenticate time updates.

⑤ Click **OK**.

STEP 9 - (**Optional**) Configure general NGFW settings as needed.

① Select **Device > Setup > Management** and edit the General Settings.

② Enter a **Hostname** for the NGFW and enter your network **Domain** name. The domain name is just a label; it will not be used to join the domain.

③ Enter **Login Banner** text that informs users who are about to log in that they require authorization to access the NGFW management functions.

> As a best practice, avoid using welcoming verbiage. Additionally, you should ask your legal department to review the banner message to ensure it adequately warns that unauthorized access is prohibited.

④ Enter the **Latitude** and **Longitude** to enable accurate placement of the NGFW on the world map.

⑤ Click **OK**.

STEP 10 - Commit your changes.

> When the configuration changes are saved, you lose connectivity to the web interface because the IP address has changed.

Click **Commit** at the top right of the web interface. The NGFW can take up to 90 seconds to save your changes.

STEP 11 - Connect the NGFW to your network.

① Disconnect the NGFW from your computer.

② (**All NGFWs except for the PA-5450**) Connect the MGT port to a switch port on your management network using an RJ-45 Ethernet cable. Make sure that the switch port you cable the device to is configured for auto-negotiation.

③ (**PA-5450 only**) Connect the MGT port to a switch port on your management network using a Palo Alto Networks certified SFP/SFP+ transceiver and cable.

STEP 12 - Open an SSH management session to the NGFW.

Using a terminal emulation software, such as PuTTY, launch an SSH session to the firewall using the new IP address you assigned to it.

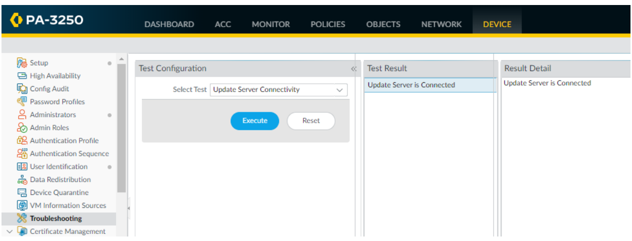
STEP 13 - Verify network access to external services required for NGFW management, such as the Palo Alto Networks Update Server.

You can do this in one of the following ways:

- If you do not want to allow external network access to the MGT interface, you will need to set up a data port to retrieve required service updates. Continue to Set Up Network Access for External Services.
- If you do plan to allow external network access to the MGT interface, verify that you have connectivity and then proceed to Register the NGFW and Activate Subscription Licenses.

① Use update server connectivity test to verify network connectivity to the Palo Alto Networks Update server as shown in the following example:

1. Select **Device > Troubleshooting**, and select **Update Server Connectivity** from the Select Test drop-down.
2. **Execute** the update server connectivity test.



Select Test: Update Server Connectivity

Test Result: Update Server is Connected

Result Detail: Update Server is Connected

② Use the following CLI command to retrieve information on the support entitlement for the firewall from the Palo Alto Networks update server:

```
request support
check
```

If you have connectivity, the update server will respond with the support status for your NGFW. If your firewall is not yet registered, the update server returns the following message:

```
Contact Us

https://www.paloaltonetworks.com/company/contact-us.html

Support Home

https://www.paloaltonetworks.com/support/tabs/overview.html

Device not found on this update server
```

Previous
Integrate NGFWs into Your Network

Next
Set Up Network Access for External Services

© 2026 Palo Alto Networks, Inc. All rights reserved.