

# ***PAN-OS CLI Quick Start***

***Version 8.1***

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://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 [www.paloaltonetworks.com/documentation](http://www.paloaltonetworks.com/documentation).
- To search for a specific topic, go to our search page [www.paloaltonetworks.com/documentation/document-search.html](http://www.paloaltonetworks.com/documentation/document-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](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2018-2019 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](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

May 17, 2019

---

# Table of Contents

Get Started with the CLI.....	5
Access the CLI.....	7
Verify SSH Connection to Firewall.....	8
Refresh SSH Keys and Configure Key Options for Management Interface Connection.....	11
Give Administrators Access to the CLI.....	14
Administrative Privileges.....	14
Set Up a Firewall Administrative Account and Assign CLI Privileges.....	15
Set Up a Panorama Administrative Account and Assign CLI Privileges.....	15
Change CLI Modes.....	16
Navigate the CLI.....	17
Find a Command.....	18
View the Entire Command Hierarchy.....	18
Find a Specific Command Using a Keyword Search.....	19
Get Help on Command Syntax.....	21
Get Help on a Command.....	21
Interpret the Command Help.....	21
Customize the CLI.....	24
 Use the CLI.....	 27
View Settings and Statistics.....	29
Modify the Configuration.....	32
Commit Configuration Changes.....	34
Test the Configuration.....	36
Test the Authentication Configuration.....	36
Test Policy Matches.....	37
Load Configurations.....	39
Load Configuration Settings from a Text File.....	39
Load a Partial Configuration.....	40
Use Secure Copy to Import and Export Files.....	44
Export a Saved Configuration from One Firewall and Import it into Another.....	44
Export and Import a Complete Log Database (logdb).....	45
CLI Jump Start.....	46
 CLI Cheat Sheets.....	 49
CLI Cheat Sheet: Device Management.....	51
CLI Cheat Sheet: User-ID.....	53
CLI Cheat Sheet: Networking.....	56
CLI Cheat Sheet: VSYS.....	59
CLI Cheat Sheet: Panorama.....	61



# *Get Started with the CLI*

Every Palo Alto Networks device includes a command-line interface (CLI) that allows you to monitor and configure the device. Although this guide does not provide detailed command reference information, it does provide the information you need to learn how to use the CLI. It includes information to help you find the command you need and how to get syntactical help after you find it.

- > Access the CLI
- > Verify SSH Connection to Firewall
- > Refresh SSH Keys and Configure Key Options for Management Interface Connection
- > Give Administrators Access to the CLI
- > Change CLI Modes
- > Navigate the CLI
- > Find a Command
- > Get Help on Command Syntax
- > Customize the CLI



---

# Access the CLI

Use a terminal emulator, such as PuTTY, to connect to the CLI of a Palo Alto Networks device in one of the following ways:

- **SSH Connection**—If you have completed [initial configuration](#), you can establish a CLI connection over the network using a secure shell (SSH) connection.
- **Serial Connection**—If you have not yet completed initial configuration or if you chose not to enable SSH on the Palo Alto Networks device, you can establish a direct serial connection from a serial interface on your management computer to the Console port on the device.

## STEP 1 | Launch the terminal emulation software and select the type of connection (Serial or SSH).

- To establish an SSH connection, enter the hostname or IP address of the device you want to connect to and set the port to **22**.
- To establish a Serial connection, connect a serial interface on management computer to the Console port on the device. Configure the Serial connection settings in the terminal emulation software as follows:
  - Data rate: **9600**
  - Data bits: **8**
  - Parity: **none**
  - Stop bits: **1**
  - Flow control: **none**

## STEP 2 | When prompted to log in, enter your administrative username.

The default superuser username is **admin**. To set up CLI access for other administrative users, see [Give Administrators Access to the CLI](#).

If prompted to acknowledge the login banner, enter **Yes**.

## STEP 3 | Enter the administrative password.

The default superuser password is **admin**. However, for security reasons you should immediately change the [admin password](#).

After you log in, the [message of the day](#) displays, followed by the CLI prompt in Operational mode:

```
username@hostname>
```

You can tell you are in operational mode because the command prompt ends with a **>**.

---

# Verify SSH Connection to Firewall

Palo Alto Networks firewalls come with Secure Shell (SSH) preconfigured on them; firewalls can act as both an SSH server and SSH client. You can verify your SSH connection to the management port of the firewall during remote access to ensure that when you log in remotely, you are in fact logging into the firewall. You can also refresh the SSH keys and specify other options for the keys.

After you initially log in through the console to the command-line interface (CLI), the firewall boots up and displays six fingerprints (hashed SSH keys). When you then remotely access the management port on the firewall for the first time, the SSH client presents a fingerprint to you and it must match one of the fingerprints you noted from the console login. This match verifies that the firewall you access remotely is indeed your firewall and no malicious device between your device and the firewall is intercepting Hello packets or presenting a false fingerprint.

You can also [Refresh SSH Keys and Configure Key Options for Management Interface Connection](#).



*To ensure you are logging in to your firewall, perform this task when you first access your firewall remotely (when you [Perform Initial Configuration](#)) and whenever you change the default host key type or regenerate the host keys for the management port.*

**STEP 1 | [Perform Initial Configuration](#)** and note the fingerprints that the firewall displays upon booting up.

When you connect to the console port (Step 3 of [Perform Initial Configuration](#)), the firewall boots up and displays SSH fingerprints. Make note of these fingerprints.

If the firewall is in FIPS-CC mode, it displays the fingerprints in sha1 hash in base64 encoding, as in the following example:

```
SSH Fingerprints
-----
256 +nvDTw9G6FpjVRYCN7qYWMmZxB0 (ECDSA)
384 Slx984ndSKeRU+YOkNh9R/4u8IM (ECDSA)
521 sph8wuC3Y/p6zvFr0sGnrzim3wo (ECDSA)
2048 kK3+bBRaJpJQOM+qE8B19SKCQPg (RSA)
3072 gtFBWm65/+D7dqUdDDc3P6hJu1g (RSA)
4096 CQnLFnMF1BfBwV7y5bhYQyawpcc (RSA)
```

If the firewall is in non-FIPS-CC mode, it displays the fingerprints in md5 hash in hex encoding, as in the following example:

```
SSH Public key fingerprints:
256 5c:73:5c:88:ea:ba:04:f7:9a:72:07:67:74:20:0c:09 (ECDSA)
384 f2:69:5c:0b:e2:26:e1:39:ca:2f:46:00:df:d5:aa:c0 (ECDSA)
521 8f:00:fa:d0:b9:a5:c5:4d:9d:f5:cd:0d:2c:86:99:25 (ECDSA)
2048 0c:01:69:54:1e:21:08:9d:65:37:3b:50:4a:03:70:d6 (RSA)
3072 1f:ae:d8:1a:b6:8d:9a:4b:c2:fd:74:ca:dc:4f:ca:19 (RSA)
4096 38:88:fb:62:07:19:cf:89:88:a0:6d:22:4b:fa:f4:23 (RSA)
```



## STEP 2 | (Optional) Display fingerprints from the SSH server (the firewall).

Display the fingerprints using the CLI if you forgot to note the fingerprints that the SSH server displayed upon bootup, or if you have regenerated a host key or changed your default host key type. To be able to effectively compare fingerprints, specify the same format that your SSH client uses (the device from which you will remotely log in): either **base64** or **hex** format, and hash-type format of **md5**, **sha1**, or **sha256**.



*There is no md5 hash type in FIPS-CC mode.*

The following example displays SSH server fingerprints in hex format and md5 hash type.

```
admin@PA-3060> show ssh-fingerprints format hex hash-type md5
```

SSH Public key fingerprints:

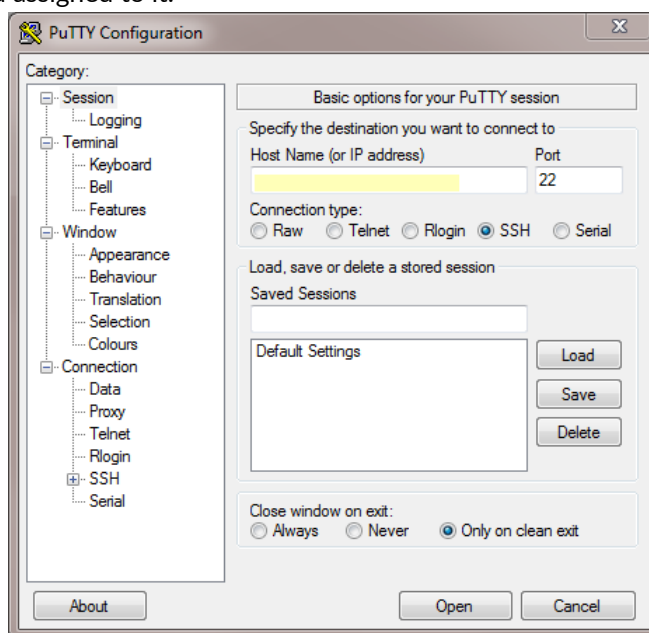
```
256 5c:73:5c:88:ea:ba:04:f7:9a:72:07:67:74:20:0c:09 (ECDSA)
384 f2:69:5c:0b:e2:26:e1:39:ca:2f:46:00:df:d5:aa:c0 (ECDSA)
521 8f:00:fa:d0:b9:a5:c5:4d:9d:f5:cd:0d:2c:86:99:25 (ECDSA)
2048 0c:01:69:54:1e:21:08:9d:65:37:3b:50:4a:03:70:d6 (RSA)
3072 1f:ae:d8:1a:b6:8d:9a:4b:c2:fd:74:ca:dc:4f:ca:19 (RSA)
4096 38:88:fb:62:07:19:cf:89:88:a0:6d:22:4b:fa:f4:23 (RSA)
```

**STEP 3 |** Continue to [Perform Initial Configuration](#) on the firewall so that you assign an IP address to the management interface and commit your changes.

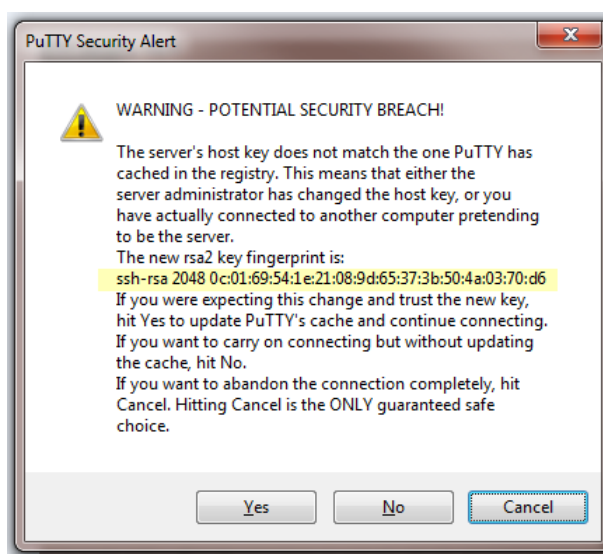
**STEP 4 |** Disconnect the firewall from your computer.


**STEP 5 |** Initiate remote access to the firewall and view the fingerprint.

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



Before you can proceed with the connection, the SSH client presents a fingerprint, as in the following example:




 *If you have already logged in to the firewall (and not changed the key), the SSH client already has the key stored in its database and therefore doesn't present a fingerprint.*

#### STEP 6 | Verify matching fingerprints.

1. Check to see if the fingerprint that the SSH client (PuTTY) presented matches one of the fingerprints you noted from login to the console port in Step 1.
2. If you see a match, that verifies that the firewall you remotely accessed is the same firewall you connected to on the console port. You typically want the SSH client to update its cache, so respond to the warning with **Yes** to continue connecting. In our example, the fingerprint in the preceding graphic matches the RSA 2048 fingerprint from the SSH server (firewall) in Step 1 (and Step 2).

If there is no match or you receive a mismatch warning, you aren't connecting to the expected device; respond with **Cancel** to cancel the connection attempt.

If you see a match but you don't want the SSH client to update its cache, respond with **No**, which allows you to continue connecting. Respond with **No** if the firewall is configured with multiple default host keys and you want to connect using a specific host key, without updating the SSH client cache.

 *To verify your SSH connection to the firewall after you have regenerated a host key or changed the default host key type, perform a procedure similar to this one, starting with logging in to the console port. In this case, Step 2 is required; execute the CLI command **show ssh-fingerprints** (with the applicable format and hash-type) and note the one fingerprint that displays. Omit Step 3 and continue with Step 4, finishing the rest of the procedure. Verify that the fingerprint from the SSH client matches the fingerprint you noted from Step 2.*

---

# Refresh SSH Keys and Configure Key Options for Management Interface Connection

When you [verify your Secure Shell \(SSH\) connection to the firewall](#), the verification uses SSH keys. You can use the CLI to change the default host key type, generate a new pair of public and private SSH host keys, and configure other SSH encryption settings.

The following examples show how to refresh (regenerate) your SSH keys and change various SSH settings after you [Access the CLI](#). The settings marked as recommended provide a stronger security posture.



*If you are using SSH to access the CLI of the firewall in FIPS-CC mode, you must set automatic rekeying parameters for session keys.*



*Each of the following configuration steps includes a commit and an SSH service restart in case you perform only one step, but you can set multiple SSH options and then commit and restart SSH just once.*

- (Optional) Set the default host key type.

The firewall uses a default host key type of RSA 2048 unless you change it. The SSH connection uses only the default host key type (not other host key types) to authenticate the firewall. You can change the default host key type; the choices are ECDSA 256, 384, or 521, or RSA 2048, 3072, or 4096.

Change the default host key type if you prefer a longer RSA key length, or if you prefer ECDSA rather than RSA. This example sets the default host key type to an ECDSA key of 256 bits, which is recommended. It also restarts SSH for the management interface so the new key type can take effect.

1. admin@PA-3060> **configure**
2. admin@PA-3060# **set deviceconfig system ssh default-hostkey mgmt key-type ECDSA key-length 256**
3. admin@PA-3060# **commit**
4. admin@PA-3060# **exit**
5. admin@PA-3060> **set ssh service-restart mgmt**
6. admin@PA-3060> **configure**
7. admin@PA-3060# **show deviceconfig system ssh default-hostkey**

- Establish when automatic rekeying of the session keys occurs for SSH to the management interface by setting parameters.

The session key are used for encrypting the traffic between the remote device and the management interface on the firewall. After any one rekeying parameter reaches its configured value, SSH uses the new session encryption keys. The parameters are data volume, time interval (seconds), and packet count.

If you set more than one parameter, rekeying occurs when the first parameter reaches its configured value, and then the firewall resets all rekeying parameters. You can set a second or third parameter in case you aren't sure that one parameter you configured will reach its value as fast as you want rekeying to occur.

1. admin@PA-3060> **configure**
2. admin@PA-3060# **set deviceconfig system ssh session-rekey mgmt data 32**

Rekeying occurs after the volume of data (in megabytes) is transmitted following the previous rekeying. The default is based on the type of cipher you use, and ranges from 1GB to 4GB. The range

---

is 10 to 4000 MB. Alternatively, you can enter **set deviceconfig system ssh session-rekey mgmt data default**, which sets the data parameter to the default value of the individual cipher you are using.



*If you are configuring the management interface connection with encryption in FIPS-CC mode, you must set a data value (you cannot let it default) and the value must be no greater than 1000 MB.*

3. admin@PA-3060# **set deviceconfig system ssh session-rekey mgmt interval 3600**

Rekeying occurs after the specified time interval (in seconds) passes following the previous rekeying. By default, time-based rekeying is disabled (set to none). The range is 10 to 3600.



*If you are configuring the management interface with encryption in FIPS-CC mode, you must set a time interval within the range; you cannot leave it disabled.*

4. admin@PA-3060# **set deviceconfig system ssh session-rekey mgmt packets 27**

Rekeying occurs after the defined number of packets ( $2^n$ ) are transmitted following the previous rekeying. Specify the exponent to which 2 is raised; for example, 14 configures that a maximum of  $2^{14}$  packets are transmitted before a rekeying occurs. The default is  $2^{28}$ ; the range is 12 to 27 ( $2^{12}$  to  $2^{27}$ ). Alternatively, you can configure **set deviceconfig system ssh session-rekey mgmt packets default**, which sets the value to  $2^{28}$ .



*Choose rekeying parameters based on your type of traffic and network speeds (in addition to FIPS-CC requirements if they apply to you). Don't set the parameters so low that they affect SSH performance.*

5. admin@PA-3060# **commit**
6. admin@PA-3060# **exit**
7. admin@PA-3060> **set ssh service-restart mgmt**
8. admin@PA-3060> **configure**
9. admin@PA-3060# **show deviceconfig system ssh session-rekey mgmt**

- (Optional) Set the SSH server to use the specified encryption ciphers.

Using SSH to encrypt your CLI session to the management interface allows all supported ciphers by default. When you set one or more ciphers, the SSH server advertises only those ciphers while connecting, and if the SSH client tries to connect using a different cipher, the server terminates the connection.

1. admin@PA-3060> **configure**
2. admin@PA-3060# **set deviceconfig system ssh ciphers mgmt cipher**

**aes128-cbc**—AES 128-bit cipher with Cipher Block Chaining

**aes128-ctr**—AES 128-bit cipher with Counter Mode

**aes128-gcm**—AES 128-bit cipher with GCM (Galois/Counter Mode)

**aes192-cbc**—AES 192-bit cipher with Cipher Block Chaining

**aes192-ctr**—AES 192-bit cipher with Counter Mode

**aes256-cbc**—AES 256-bit cipher with Cipher Block Chaining

**aes256-ctr**—(Recommended) AES 256-bit cipher with Counter Mode

**aes256-gcm**—(Recommended) AES 256-bit cipher with GCM

3. admin@PA-3060# **commit**
4. admin@PA-3060# **exit**
5. admin@PA-3060> **set ssh service-restart mgmt**

- 
6. admin@PA-3060> **configure**
  7. admin@PA-3060# **show deviceconfig system ssh ciphers mgmt**

- (Optional) Delete a cipher from the set of ciphers you selected to encrypt your CLI session to the management interface.

This example deletes the AES CBC cipher with 128-bit key.

1. admin@PA-3060> **configure**
2. admin@PA-3060# **delete deviceconfig system ssh ciphers mgmt aes128-cbc**
3. admin@PA-3060# **commit**
4. admin@PA-3060# **exit**
5. admin@PA-3060> **set ssh service-restart mgmt**
6. admin@PA-3060> **configure**
7. admin@PA-3060# **show deviceconfig system ssh ciphers mgmt**

- (Optional) Set the message authentication code (MAC) for SSH to the management interface.

By default the server advertises all of the MAC algorithms to the client.

1. admin@PA-3060> **configure**
2. admin@PA-3060# **set deviceconfig system ssh mac mgmt value**  
**hmac-sha1**—MAC with SHA1 cryptographic hash  
**hmac-sha2-256**—(Recommended) MAC with SHA2-256 cryptographic hash  
**hmac-sha2-512**—(Recommended) MAC with SHA2-512 cryptographic hash
3. admin@PA-3060# **commit**
4. admin@PA-3060# **exit**
5. admin@PA-3060> **set ssh service-restart mgmt**

- Regenerate ECDSA or RSA host keys for SSH to replace the existing keys.

The remote device uses the host keys to authenticate the firewall. This example regenerates the ECDSA 256 default host key because that is the default host key type that was set in the first step.



*Regenerate your default host key at the frequency you determine necessary for security purposes.*



*Regenerating a host key does not change your default host key type. To regenerate the default host key you are using, you must specify your default host key type and length when you regenerate. Regenerating a host key that isn't your default host key type simply regenerates a key that you aren't using and therefore has no effect.*

1. admin@PA-3060> **configure**
2. admin@PA-3060# **set deviceconfig system ssh regenerate-hostkeys mgmt key-type ECDSA key-length 256**
3. admin@PA-3060# **commit**
4. admin@PA-3060> **exit**
5. admin@PA-3060> **set ssh service-restart mgmt**

---

# Give Administrators Access to the CLI

Administrative accounts specify roles and authentication methods for the administrators of Palo Alto Networks firewalls. Every Palo Alto Networks firewall has a predefined default administrative account (admin) that provides full read-write access (also known as superuser access) to the firewall. As a best practice, create an administrative account for each person who will be performing configuration tasks on the firewall or Panorama so that you have an audit trail of changes.

- [Administrative Privileges](#)
- [Set Up a Firewall Administrative Account and Assign CLI Privileges](#)
- [Set Up a Panorama Administrative Account and Assign CLI Privileges](#)

## Administrative Privileges

Privilege levels determine which commands an administrator can run as well as what information is viewable. Each administrative role has an associated privilege level. You can use dynamic roles, which are predefined roles that provide default privilege levels. Or, you can create custom [firewall administrator roles](#) or [Panorama administrator roles](#) and assign one of the following CLI privilege levels to each role:



*You must follow the [Best Practices for Securing Admin Access](#) to ensure that you are securing access to your management network in a way that will prevent successful attacks.*

Privilege Level	Description
superuser	Has full access to the Palo Alto Networks device (firewall or Panorama) and can define new administrator accounts and virtual systems. You must have superuser privileges to create an administrative user with superuser privileges.
superreader	Has complete read-only access to the device.
vsysadmin	Has access to selected virtual systems (vsys) on the firewall to create and manage specific aspects of virtual systems. A virtual system administrator doesn't have access to network interfaces, VLANs, virtual wires, virtual routers, IPsec tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles.
vsysreader	Has read-only access to selected virtual systems on the firewall and specific aspects of virtual systems. A virtual system administrator with read-only access doesn't have access to network interfaces, VLANs, virtual wires, virtual routers, IPsec tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles.
deviceadmin	Has full access to all firewall settings except for defining new accounts or virtual systems.
devicereader	Has read-only access to all firewall settings except password profiles (no access) and administrator accounts (only the logged in account is visible).
panorama-admin	Has full access to Panorama except for the following actions: <ul style="list-style-type: none"><li>• Create, modify, or delete Panorama or device administrators and roles.</li><li>• Export, validate, revert, save, load, or import a configuration.</li><li>• Schedule configuration exports.</li></ul>

---

## Set Up a Firewall Administrative Account and Assign CLI Privileges

To [set up a custom firewall administrative role](#) and assign CLI privileges, use the following workflow:

### STEP 1 | Configure an Admin Role profile.

1. Select **Device > Admin Roles** and then click **Add**.
2. Enter a **Name** to identify the role.
3. For the scope of the **Role**, select **Device** or **Virtual System**.
4. Define access to the **Command Line**:
  - **Device** role—**superuser**, **superreader**, **deviceadmin**, **devicereader**, or **None**.
  - **Virtual System** role—**vsysadmin**, **vsysreader**, or **None**.
5. Click **OK** to save the profile.

### STEP 2 | Configure an administrator account.

1. Select **Device > Administrators** and click **Add**.
2. Enter a user **Name**. If you will use local database authentication, this must match the name of a user account in the local database.
3. If you configured an **Authentication Profile** or authentication sequence for the user, select it in the drop-down. If you select **None**, you must enter a **Password** and **Confirm Password**.
4. If you configured a custom role for the user, set the **Administrator Type** to **Role Based** and select the Admin Role **Profile**. Otherwise, set the **Administrator Type** to **Dynamic** and select a dynamic role.
5. Click **OK** and **Commit**.

## Set Up a Panorama Administrative Account and Assign CLI Privileges

To [set up a custom Panorama administrative role](#) and assign CLI privileges, use the following workflow:

### STEP 1 | Configure an Admin Role profile.

1. Select **Panorama > Admin Roles** and then click **Add**.
2. Enter a **Name** to identify the role.
3. For the scope of the **Role**, select **Panorama**.
4. Select the **Command Line** tab and select an access level: **superuser**, **superreader**, **panorama-admin**, or **None**.
5. Click **OK** to save the profile.

### STEP 2 | Configure an administrator account.

1. Select **Panorama > Administrators** and click **Add**.
2. Enter a user **Name**.
3. If you configured an **Authentication Profile** or authentication sequence for the user, select it in the drop-down. If you select **None**, you must enter a **Password** and **Confirm Password**.
4. If you configured a custom role for the user, set the **Administrator Type** to **Custom Panorama Admin** and select the Admin Role **Profile**. Otherwise, set the **Administrator Type** to **Dynamic** and select a dynamic **Admin Role**.
5. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

---

# Change CLI Modes

The CLI provides two command modes:

- **Operational**—Use operational mode to view information about the firewall and the traffic running through it or to view information about Panorama or a Log Collector. Additionally, use operational mode commands to perform operations such as restarting, loading a configuration, or shutting down. When you log in, the CLI opens in operational mode.
- **Configuration**—Use configuration mode to view and modify the configuration.

You can switch between operational and configuration modes at any time, as follows:

- To switch from operational mode to configuration mode:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

Notice that the command prompt changes from a > to a #, indicating that you successfully changed modes.

- To switch from configuration mode to operational mode, use either the **quit** or **exit** command:

```
username@hostname# quit
Exiting configuration mode
username@hostname>
```

- To enter an operational mode command while in configuration mode, use the **run** command, for example:

```
username@hostname# run ping host 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data
...
username@hostname#
```

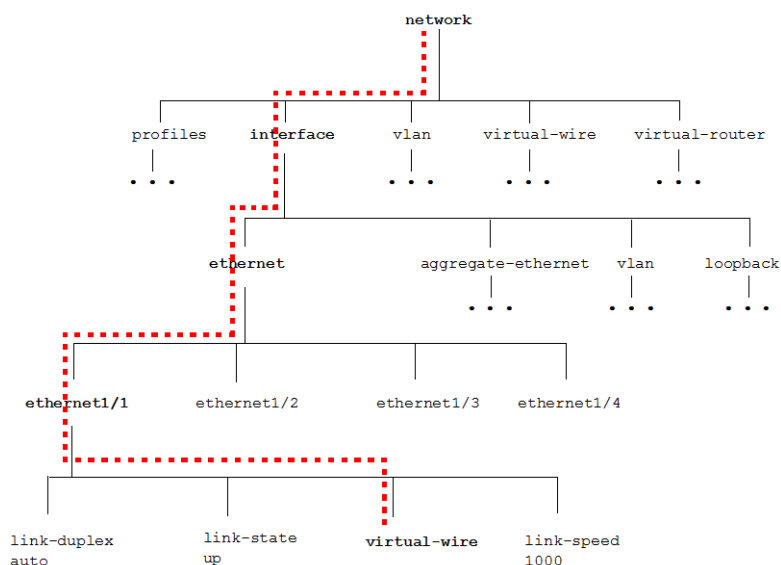


# Navigate the CLI

CLI commands are organized in a hierarchical structure. To display a segment of the current hierarchy, use the **show** command. Entering **show** displays the complete hierarchy, while entering **show** with keywords displays a segment of the hierarchy.

For example, the following command displays the configuration hierarchy for the Ethernet interface segment of the hierarchy:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# show network interface ethernet
ethernet {
  ethernet1/1 {
    virtual-wire;
  }
  ethernet1/2 {
    virtual-wire;
  }
  ethernet1/3 {
    layer2 {
      units {
        ethernet1/3.1;
      }
    }
  }
  ethernet1/4;
}
[edit]
username@hostname#
```



---

# Find a Command

The **find command** helps you find a command when you don't know where to start looking in the hierarchy. The command—which is available in all CLI modes—has two forms. Used alone, **find command** displays the entire command hierarchy. Used with the **keyword** parameter, find command keyword displays all commands that contain the specified keyword.



*You can also view a complete listing of all [PAN-OS 8.1 CLI commands](#) or view the [CLI changes](#) between the current and previous PAN-OS release.*

- [View the Entire Command Hierarchy](#)
- [Find a Specific Command Using a Keyword Search](#)

## View the Entire Command Hierarchy

Use **find command** without any parameters to display the entire command hierarchy in the current command mode. For example, running this command from operational mode on a VM-Series Palo Alto Networks device yields the following (partial result):

```
username@hostname> find command
target set <value>
target show
schedule uar-report user <value> user-group <value> skip-detailed-browsing
  <yes|no> title <value> period <value> start-time <value> end-time <value>
  vsys <value>
schedule botnet-report period <last-calendar-day|last-24-hrs> topn <1-500>
  query <value>
clear arp <value>|<all>
clear neighbor <value>|<all>
clear mac <value>|<all>
clear job id <0-4294967295>
clear query id <0-4294967295>
clear query all-by-session
clear report id <0-4294967295>
clear report all-by-session
clear report cache
clear log traffic
clear log threat
clear log config
clear log system
clear log alarm
clear log acc
clear log hipmatch
clear log userid
clear log iptag
clear wildfire counters
clear counter interface
clear counter global name <value>
clear counter global filter category <value> severity <value> aspect <value>
  pac
ket-filter <yes|no>
clear counter all
clear session id <1-4294967295>
clear session all filter nat <none|source|destination|both> ssl-decrypt <yes|
no> type <flow|predict> state <initial|opening|active|discard|closing|closed>
  from <value> to <value> source <ip/netmask> destination <ip/netmask> source-
```

```

user <value> destination-user <value> source-port <1-65535> destination-port
<1-65535> protocol <1-255> application <value> rule <value> nat-rule <value>
qos-rule <value> pbf-rule <value> dos-rule <value> hw-interface <value> min-
kb <1-1048576> qos-node-id <0-5000>|<-2> qos-class <1-8> vsys-name <value>|
<any>
clear application-signature statistics
clear nat-rule-cache rule <value>
clear statistics
clear high-availability control-link statistics
clear high-availability transitions
clear vpn ike-sa gateway <value>
clear vpn ipsec-sa tunnel <value>
clear vpn ike-preferred-version gateway <value>
clear vpn ike-hashurl
clear vpn flow tunnel-id <1-2147483648>
clear dhcp lease all expired-only
clear dhcp lease interface clear dhcp lease interface <name> ip <ip/netmask>
:

```

## Find a Specific Command Using a Keyword Search

Use **find command keyword** to locate all commands that have a specified keyword.

```
username@hostname# find command keyword <keyword>
```

For example, suppose you want to configure certificate authentication and you want the Palo Alto Networks device to get the username from a field in the certificate, but you don't know the command. In this case you might use **find command keyword** to search for commands that contain username in the command syntax.

```
username@hostname > configure
```

```

Entering configuration mode
[edit]
username@hostname # find command keyword username
show shared certificate-profile <name> username-field
set deviceconfig system log-export-schedule <name> protocol ftp username
<value>
set deviceconfig system log-export-schedule <name> protocol scp username
<value>
set deviceconfig setting wildfire session-info-select exclude-username <yes|
no>
set mgt-config password-complexity block-username-inclusion <yes|no>
set network interface ethernet <name> layer3 pppoe username <value>
set shared authentication-profile <name> username-modifier <value>|<validate>|
<%USERINPUT%|%USERINPUT%@@%USERDOMAIN%|%USERDOMAIN%\%USERINPUT%>
set shared certificate-profile <name> username-field
set shared certificate-profile <name> username-field subject <common-name>
set shared certificate-profile <name> username-field subject-alt <email|
principal-name>
set vm-info-source <name> VMware-ESXi username <value>
set vm-info-source <name> VMware-vCenter username <value>
set user-id-collector setting ntlm-username <value>
set user-id-collector syslog-parse-profile <name> regex-identifier username-
regex <value>
set user-id-collector syslog-parse-profile <name> field-identifier username-
prefix <value>

```

---

```
set user-id-collector syslog-parse-profile <name> field-identifier username-  
delimiter <value>  
[edit]  
username@hostname #
```

From the resulting lists of commands, you can identify that the command you need is:

```
username@hostname # set shared certificate-profile <name> username-field
```

If you're not sure exactly what to enter in the command line, you can then [Get Help on Command Syntax](#).

# Get Help on Command Syntax

After you [Find a Command](#) you can get help on the specific command syntax by using the built-in CLI help. To get help, enter a ? at any level of the hierarchy.

- [Get Help on a Command](#)
- [Interpret the Command Help](#)

## Get Help on a Command

For example, suppose you want to configure the primary DNS server settings on the Palo Alto Networks device using **find command keyword** with **dns** as the keyword value, you already know that the command is **set deviceconfig system dns-setting**, but you're not exactly sure how to use the command to set the primary DNS server setting. In this case, you would enter as much of the command as you know (or start typing it and press Tab for automatic command completion), and then add a question mark at the end of the line before pressing Enter, like this:

```
username@hostname# set deviceconfig system dns-setting ?
> dns-proxy-object Dns proxy object to use for resolving fqdns
> servers Primary and secondary dns servers
<Enter> Finish input
```

Notice that the question mark doesn't appear in the command line when you type it, but a list of the available commands appears. You can continue getting syntactical help all through the hierarchy:

```
username@hostname# set deviceconfig system dns-setting servers ?
+ primary Primary DNS server IP address
+ secondary Secondary DNS server IP address
  <Enter> Finish input

username@hostname# set deviceconfig system dns-setting servers primary ?
<ip> <ip>
```



*Use the Tab key in the middle of entering a command and the command will automatically complete, provided there are no other commands that match the letters you have typed thus far. For example, if you type **set dev** and then press Tab, the CLI will recognize that the command you are entering is **deviceconfig** and automatically finish populating the command line.*

## Interpret the Command Help

Use the following table to help interpret the command options you see when you use the ? to get help.

Symbol	Description
*	Indicates that the option is required.  For example, when importing a configuration over secure copy (SCP), specifying the <b>from</b> parameter is required, as indicated by the * from notation.  username@hostname#> <b>scp import configuration ?</b>

Symbol	Description
	<div>+ remote-port      SSH port number on remote host</div> <div>+ source-ip        Set source address to specified interface address</div> <div>* from              Source (username@host:path)</div>
>	<p>Indicates that there are additional nested commands.</p> <p>For example, when configuring DNS settings, there are additional nested commands for configuring a DNS proxy object and for specifying primary and secondary DNS servers:</p> <pre>username@hostname# set deviceconfig system dns-setting ? &gt; dns-proxy-object    Dns proxy object to use for                       resolving fqdns &gt; servers             Primary and secondary dns servers                       &lt;Enter&gt;            Finish input</pre>
+	<p>Indicates that the option has an associated value that you must enter.</p> <p>For example, when setting up a high availability configuration, notice that the + enabled notation indicates that you must supply a value for this option:</p> <pre>username@hostname# set deviceconfig high-availability ? + enabled            enabled &gt; group              HA group configuration &gt; interface          HA interface configuration                       &lt;Enter&gt;            Finish input Getting help for the enabled option shows that you must enter a value of yes or no: admin@PA-3060# set deviceconfig high-availability enabled ? no            no yes           yes</pre>
	<p>Allows you to filter command output. You can either specify a <b>match</b> value, which will only show command output that matches the value you specify, or you can specify an <b>except</b> value, which will only show command output except for the value you specify.</p> <p>For example, use the   <b>match</b> option to display only the app-version in the output of the show system info command:</p> <pre>username@hostname&gt; show system info   match app-version app-version: 758-4391</pre> <p>Similarly, to show all users in your group lists who are not part of your organization, you should show the user group list, but exclude the organizational unit (ou) for your organization. Notice that, although there are a total of 4555 user-to-group mappings, with the   <b>except</b> filter you can easily see the small list of users who are part of external groups:</p> <pre>username@hostname&gt; show user group list   except ou=acme</pre>

Symbol	Description
	<pre> cn=sap_globaladmin,cn=users,dc=acme,dc=local cn=dnsupdateproxy,ou=admin groups,ou=administrator accounts,dc=acme,dc=local cn=dhcp administrators,ou=admin groups,ou=administrator accounts,dc=acme,dc=local cn=helpservicesgroup,cn=users,dc=acme,dc=local cn=exchange domain servers,cn=users,dc=acme,dc=local cn=network configuration operators,cn=builtin,dc=acme,dc=local cn=dhcp users,ou=admin groups,ou=administrator accounts,dc=acme,dc=local cn=exchange windows permissions,ou=microsoft exchange security groups,dc=acme,dc=local cn=wins users,cn=users,dc=acme,dc=local cn=enterprise read-only domain controllers,cn=users,dc=acme,dc=local cn=print-server-admins,ou=admin groups,ou=administrator accounts,dc=acme,dc=local cn=telnetclients,cn=users,dc=acme,dc=local cn=servicenowpasswordreset,ou=admin groups,ou=administrator accounts,dc=acme,dc=local cn=delegated setup,ou=microsoft exchange security groups,dc=acme,dc=local Total: 4555 * : Custom Group &lt;/result&gt;&lt;/response&gt; username@hostname&gt; </pre>

---

# Customize the CLI

- Specify how long an administrative session to the management interface (CLI or web interface) can remain idle before logging the administrator out:

```
username@hostname# set deviceconfig setting management idle-timeout ?
0          never
<value>    <1-1440>
```



*If you want to set the CLI timeout value to a value different from the global **management idle-timeout** value, use the **set cli timeout** command in operational mode.*

- Specify the format for command output:

```
username@hostname> set cli config-output-format ?
default      default
json         json
set          set
xml          xml
```

For example, in the default setting the config-output-format looks like this:

```
username@hostname# show deviceconfig system dns-setting servers
servers {
  primary 1.2.3.4;
  secondary 1.2.3.5;
}
```

Changing the setting to **set** results in output that looks like this:

```
username@hostname# show deviceconfig system dns-setting servers
set deviceconfig system dns-setting servers primary 1.2.3.4
set deviceconfig system dns-setting servers secondary 1.2.3.5
[edit]
[edit]
```

Changing the setting to **xml** results in output that looks like this:

```
username@hostname# show deviceconfig system dns-setting servers
<response status="success" code="19">
  <result total-count="1" count="1">
    <servers>
      <primary>1.2.3.4</primary>
      <secondary>1.2.3.5</secondary>
    </servers>
  </result>
</response>
```



- 
- Switch to scripting mode. In scripting mode, you can copy and paste commands from a text file directly into the CLI. Although you can do this without scripting-mode enabled (up to 20 lines). If you cut-and-paste a block of text into the CLI, examine the output of the lines you pasted. If you see lines that are truncated or generate errors, you may have to re-paste a smaller section of text, or switch to **scripting-mode**:

```
username@hostname> set cli scripting-mode on
```



*When in scripting-mode, you cannot use Tab to complete commands or use ? to get help on command syntax. When you are done pasting commands, switch back to regular mode using the **set cli scripting-mode off** command.*



# Use the CLI

Now that you know how to Find a Command and Get Help on Command Syntax, you are ready to start using the CLI to manage your Palo Alto Networks firewalls or Panorama. The following topics describe how to use the CLI to view information about the device and how to modify the configuration of the device. In addition, more advanced topics show how to import partial configurations and how to use the test commands to validate that a configuration is working as expected.

- > View Settings and Statistics
- > Modify the Configuration
- > Commit Configuration Changes
- > Test the Configuration
- > Load Configurations
- > Use Secure Copy to Import and Export Files
- > CLI Jump Start



---

# View Settings and Statistics

Use **show** commands to view configuration settings and statistics about the performance of the firewall or Panorama and about the traffic and threats identified on the firewall. You can use **show** commands in both Operational and Configure mode. For example, the **show system info** command shows information about the device itself:

```
admin@PA-3220> show system info

ip-address: 10.10.10.15
public-ip-address: unknown
netmask: 255.255.254.0
default-gateway: 10.10.10.1
ip-assignment: static
ipv6-address: unknown
ipv6-link-local-address: unknown
ipv6-default-gateway:
mac-address: d3:f3:bc:c4:60:4f
time: Thu Dec 28 08:35:19 2017
uptime: 5 days, 22:43:45
family: 3200
model: PA-3220
serial: 027312000404
cloud-mode: non-cloud
sw-version: 8.1.0
global-protect-client-package-version: 0.0.0
app-version: 758-4391
app-release-date: 2017/12/23 12:11:11 PST
av-version: 2474-2968
av-release-date: 2017/12/27 13:37:49 PST
threat-version: 758-4391
threat-release-date: 2017/12/23 12:11:11 PST
wf-private-version: 0
wf-private-release-date: unknown
url-db: paloaltonetworks
wildfire-version: 204587-206907
wildfire-release-date: 2017/12/28 08:01:06 PST
url-filtering-version: 0000.00.00.000
global-protect-datafile-version: unknown
global-protect-datafile-release-date: unknown
global-protect-clientless-vpn-version: 0
global-protect-clientless-vpn-release-date:
logdb-version: 8.1.6
platform-family: 3200
vpn-disable-mode: off
multi-vsyz: on
operational-mode: normal

admin@PA-3220>
```

The **show session info** command shows details about the sessions running through the Palo Alto Networks device.

```
admin@PA-3220> show session info
```

```

target-dp:                                     *.dp0
-----
Number of sessions supported:                  1048574
Number of allocated sessions:                  0
Number of active TCP sessions:                 0
Number of active UDP sessions:                 0
Number of active ICMP sessions:                0
Number of active GTPc sessions:                0
Number of active GTPu sessions:                0
Number of pending GTPu sessions:               0
Number of active BCAST sessions:               0
Number of active MCAST sessions:               0
Number of active predict sessions:             0
Number of active SCTP sessions:                0
Number of active SCTP associations:            0
Session table utilization:                     0%
Number of sessions created since bootup:       1577
Packet rate:                                  0/s
Throughput:                                    0 kbps
New connection establish rate:                 0 cps
-----
Session timeout
  TCP default timeout:                         3600 secs
  TCP session timeout before SYN-ACK received: 5 secs
  TCP session timeout before 3-way handshaking: 10 secs
  TCP half-closed session timeout:             120 secs
  TCP session timeout in TIME_WAIT:            15 secs
  TCP session delayed ack timeout:             250 millisecs
  TCP session timeout for unverified RST:      30 secs
  UDP default timeout:                         30 secs
  ICMP default timeout:                       6 secs
  SCTP default timeout:                       3600 secs
  SCTP timeout before INIT-ACK received:       5 secs
  SCTP timeout before COOKIE received:        60 secs
  SCTP timeout before SHUTDOWN received:      30 secs
  other IP default timeout:                   30 secs
  Captive Portal session timeout:              30 secs
  Session timeout in discard state:
    TCP: 90 secs, UDP: 60 secs, SCTP: 60 secs, other IP protocols: 60 secs
-----
Session accelerated aging:                     True
  Accelerated aging threshold:                 80% of utilization
  Scaling factor:                              2 X
-----
Session setup
  TCP - reject non-SYN first packet:           True
  Hardware session offloading:                 True
  Hardware UDP session offloading:             True
  IPv6 firewalling:                           True
  Strict TCP/IP checksum:                     True
  Strict TCP RST sequence:                    True
  Reject TCP small initial window:            False
  ICMP Unreachable Packet Rate:               200 pps
-----
Application trickling scan parameters:
  Timeout to determine application trickling:  10 secs
  Resource utilization threshold to start scan: 80%
  Scan scaling factor over regular aging:      8
-----
Session behavior when resource limit is reached: drop
-----

```

---

```
Pcap token bucket rate : 10485760
```

```
-----  
Max pending queued mcast packets per session : 0  
-----
```

---

# Modify the Configuration

You can also modify the device configuration from the CLI using the **set**, **delete**, and **edit** commands (if your administrative role has a [Privilege Level](#) that allows you to write to the configuration). In most cases you must be in Configure mode to modify the configuration.

- To change the value of a setting, use a **set** command. For example, to configure an NTP server, you would enter the complete hierarchy to the NTP server setting followed by the value you want to set:

```
admin@PA-3060# set deviceconfig system ntp-servers primary-ntp-server ntp-server-address pool.ntp.org
```



*To target a command to a specific virtual system (vsys), enter the following operational mode command: **set system setting target-vsys <vsys-name>**. To go back to issuing commands that apply to the firewall instead of the targeted vsys, use **set system target-vsys none**.*

- To change to a different location in the configuration hierarchy and/or to modify a setting, use the **edit** command. The **edit** commands are very similar to the **set** commands, except that when you enter an **edit** command, you switch context to the corresponding node in the command hierarchy. This can be useful if you need to enter several commands in a node that is nested far down in the command hierarchy. For example, if you want to configure all of the NTP server settings, instead of entering the full command syntax each time using the **set** command, you could use the **edit** command to move to the **ntp-servers** node as follows:

```
[edit]
admin@PA-3060# edit deviceconfig system ntp-servers
[edit deviceconfig system ntp-servers]
admin@PA-3060#
```

Notice that when you enter the command, your new location in the command hierarchy is displayed. You can now use the **set** command to configure the NTP server settings without entering the entire command hierarchy:

```
admin@PA-3060# set secondary-ntp-server ntp-server-address 10.1.2.3
```



*Use the **up** command to move up a level in the command hierarchy. Use the **top** command to move back to the top of the command hierarchy.*

- To delete an existing configuration setting, use a **delete** command. For example, to delete the secondary NTP server address, you would enter the following command:

```
admin@PA-3060# delete deviceconfig system ntp-servers secondary-ntp-server ntp-server-address
```



*When deleting configuration settings or objects using the CLI, the device does not check for dependencies like it does in the web interface. Therefore, when you use **delete***



---

from the CLI, you must manually search the configuration for other places where the configuration object might be referenced. For example, before you delete an application filter group named *browser-based business*, you should search the CLI for that value to see if it is used anywhere in profiles or policies, using the following command:

```
admin@PA-3060> show config running / match "browser-based  
business"
```

Notice that because the object you are matching on has a space in it, you must enclose it in quotation marks.

# Commit Configuration Changes

Any change in the Palo Alto Networks device configuration is first written to the candidate configuration. The change only takes effect on the device when you commit it. Committing a configuration applies the change to the running configuration, which is the configuration that the device actively uses. Upon commit, the device performs both a syntactic validation (of configuration syntax) and a semantic validation (whether the configuration is complete and makes sense). As a best practice, **validate** configuration changes prior to committing so that you can fix any errors that will cause a commit failure, thereby ensuring that the commit will succeed. This is particularly useful in environments with a strict change window.

The firewall and Panorama queue commit operations so that you can initiate a new commit while a previous commit is in progress. The firewall and Panorama perform commits in the order you and other administrators initiate them but prioritize automatic commits such as content database installations and FQDN refreshes. If the queue already has the maximum number of administrator-initiated commits (this varies by appliance model), the firewall or Panorama must begin processing a commit (remove it from the queue) before you can initiate a new commit.



*To see details (such as queue positions or Job-IDs) about commits that are pending, in progress, completed, or failed, run the operational command **show jobs all**. To see the messages and description for a particular commit, run **show jobs id <job-id>**.*

## STEP 1 | (Optional but recommended) Validate the configuration:

1. Enter the validate command:

```
admin@PA-3060> configure
admin@PA-3060# validate full
Validate job enqueued with jobid 3041
3041
```

2. View the validation results using the job ID that was displayed when you entered the validate command. Verify that the job finished (FIN) and that the configuration is valid as shown in the following example:

```
[edit]
admin@PA-3060# exit
Exiting configuration mode
admin@PA-3060> show jobs id 3041
```

Enqueued	Dequeued	ID	Type	Status	Result	Completed
2015/05/18						
14:00:40	14:00:40	3041	Validate	FIN	OK	14:01:11

Warnings:EBL(vsys1/Palo Alto Networks Malicious IP List) Unable to fetch external list. Using old copy for refresh.

vsys1 (vsys1)

vsys1: Rule 'rule1' application dependency warning:

- Application 'propalms' requires 'web-browsing' be allowed
- Application 'open-vpn' requires 'ssl' be allowed
- Application 'open-vpn' requires 'web-browsing' be allowed
- Application 'files.to' requires 'web-browsing' be allowed
- Application 'gigaup' requires 'ftp' be allowed
- Application 'dazhihui' requires 'web-browsing' be allowed
- Application 'fasp' requires 'ssh' be allowed
- Application 'vidsoft' requires 'web-browsing' be allowed

```
Application 'ipp' requires 'web-browsing' be allowed
Application 'flexnet-installanywhere' requires 'web-browsing' be
allowed
(Module: device)
Details:Configuration is valid
```

3. If the validation fails, fix any errors and then repeat steps 1 and 2.

**STEP 2** | After successfully validating the configuration, save it to the running configuration by performing a commit of all or a portion of the configuration:

- Commit the entire configuration:

```
admin@PA-3060> configure
admin@PA-3060# commit
```

- Commit part of the configuration on a firewall with multiple virtual systems:

```
admin@PA-3060# commit partial ?
+ description          Enter commit description
+ device-and-network   device-and-network
+ shared-object        shared-object
> admin                admin
> no-vsyz              no-vsyz
> vsyz                 vsyz
<Enter>               Finish input
```

When doing a partial commit from the CLI, you must specify what part of the configuration to exclude from the commit. You can also filter the configuration changes by administrator. For example, the following command commits only the changes that an administrator with the username jsmith made to the vsys1 configuration and to shared objects:

```
admin@PA-3060# commit partial admin jsmith vsyz vsyz1 device-and-network
excluded
```

- Commit part of the configuration on a firewall that does not have multiple virtual systems mode enabled:

```
admin@PA-200# commit partial ?
+ description          Enter commit description
+ device-and-network   device-and-network
+ policy-and-objects   policy-and-objects
+ shared-object        shared-object
> admin                admin
<Enter>               Finish input
```

For example, if you made a change in the Security policy only, you might want to commit just the policy and objects portion of the configuration as follows:

```
admin@PA-200# commit partial device-and-network excluded
```



*If the commit takes a long time, you can press Ctrl+C to access the command line while the commit continues as a background process.*

---

# Test the Configuration

Use the CLI-only **test** commands to test that your configuration works as expected. For example, you can test that your policy rulebases are working as expected, that your authentication configuration will enable the Palo Alto Networks device to successfully connect to authentication services, that a custom URL category matches expected sites, that your IPSec/IKE VPN settings are configured properly, that your User-ID syslog parsing profiles are working properly, and many more things.

The following sections show examples of how to use some of the **test** commands:

- [Test the Authentication Configuration](#)
- [Test Policy Matches](#)

## Test the Authentication Configuration

Use the **test authentication** command to determine if your firewall or Panorama management server can communicate with a back-end authentication server and if the authentication request was successful. You can additionally test authentication profiles used for GlobalProtect and Captive Portal authentication. You can perform authentication tests on the candidate configuration, so that you know the configuration is correct before committing.

Connectivity testing is supported for local database authentication and for external authentication servers that use multi-factor authentication (MFA), RADIUS, TACACS+, LDAP, or Kerberos.

**STEP 1 |** (**Vsys-specific authentication profiles only**) Specify which virtual system contains the authentication profile you want to test. This is only necessary if you are testing an authentication profile that is specific to a single virtual system (that is, you do not need to do this if the authentication profile is shared).

```
admin@PA-3060> set system setting target-vsys <vsys-name>
```

For example, to test an authentication profile in vsys2 you would enter the following command:

```
admin@PA-3060> set system setting target-vsys vsys2
```



*The **set system setting target-vsys** command is not persistent across sessions.*

**STEP 2 |** Test an authentication profile by entering the following command:

```
admin@PA-3060> test authentication authentication-profile <authentication-profile-name> username <username> password
```

You will be prompted for the password associated with the user account.



*Profile names are case-sensitive. Also, if the authentication profile has a username modifier defined, you must enter it with the username. For example, if the username modifier is **%USERINPUT%@%USERDOMAIN%**, for a user named **bzobrist** in domain **acme.com**, you would need to enter **bzobrist@acme.com** as the username.*

For example, run the following command to test connectivity with a Kerberos server defined in an authentication profile named Corp, using the login for the LDAP user credentials for user bzobrist:

```
admin@PA-3060> test authentication authentication-profile Corp username
bzobrist password
Enter password :

Target vsys is not specified, user "bzobrist" is assumed to be configured
with a
shared auth profile.

Do allow list check before sending out authentication request...
name "bzobrist" is in group "all"

Authentication to KERBEROS server at '10.1.2.10' for user 'bzobrist'
Realm: 'ACME.LOCAL'
Egress: 10.55.0.21
KERBEROS configuration file is created
KERBEROS authcontext is created. Now authenticating ...
Kerberos principal is created
Sending authentication request to KDC...
Authentication succeeded!

Authentication succeeded for user "bzobrist"
```

To test a SAML-based authentication profile, enter the following command, then copy the URL from the output and paste it into a browser:

```
admin@PA-VM-8.0> test generate-saml-url <captive-portal|global-
protect|management><interface> authprofile<authentication-profile-
name>vsys <vsysid>ip-hostname <ip-address>
```

For example, run the following command to test the SAML authentication for Captive Portal that is defined in the authentication profile named Admin\_AuthProfile on the virtual system vsys1 for IP address 192.0.2.0:

```
admin@PA-VM-8.0> test generate-saml-url captive-portal authprofile
Admin_AuthProfile
```

```
https://192.0.2.0/SAML20/SP/TEST?vsys=vsys1&authprofile=Admin_AuthProfile
```

## Test Policy Matches

You can use **test** commands to verify that your policies are working as expected.

- Test a security policy rule.

Use the **test security-policy-match** command to determine whether a security policy rule is configured correctly. For example, suppose you have a user mcanha in your marketing department who is responsible for posting company updates to Twitter. Instead of adding a new rule just for that user, you want to test whether twitter will be allowed via an existing rule. By running the following test command, you can see that the user mcanha is indeed allowed to post to twitter based on your existing Allowed Personal Apps security policy rule:

```
admin@PA-3060> test security-policy-match application twitter-posting
source-user acme\mcanha destination 199.59.150.7 destination-port 80 source
10.40.14.197 protocol 6
```

```
"Allowed Personal Apps" {
    from trust;
    source any;
    source-region none;
    to untrust;
    destination any;
    destination-region none;
    user any;
    category any;
    application/service [ twitter-posting/tcp/any/80 twitter-posting/
tcp/any/443 finger/tcp/any/79 finger/udp/any/79 irc-base/tcp/any/6665-6669
vidsoft/tcp/any/51222 vidsoft/tcp/any/80 vidsoft/tcp/any/443 vidsoft/tcp/
any/1853 vidsoft/udp/any/51222 vidsoft/udp/any/1853 rtsp/tcp/any/554 rtsp/
udp/any/554 kkbox/tcp/any/80 yahoo-mail/tcp/any/80 yahoo-mail/tcp/any/143 0
msn-base/tcp/any/443 msn-base/tcp/any/1863 msn-base/tcp/any/7001 msn-base/
udp/any/7001 ebuddy/tcp/any/80 gmail-base/tcp/any/80 gmail-base/tcp/any/443
hovrs/tcp/any/443 hov application/service(implicit) [ http/tcp/any/80 http/
tcp/any/443 http/tcp/any/6788 http/tcp/any/6789 http/tcp/any/7456 http/tcp/
any/8687 http/tcp/any/9100 http/tcp/any/9200 http/udp/any/1513 http/udp/
any/1514 jabber/tcp/any/any jabber/tcp/any/80 jabber/tcp/any/443 jabber/tcp/
any/5228 jabber/tcp/any/25553 jabber/udp/any/any stun/tcp/any/any stun/tcp/
any/3158 stun/udp/any/any web-browsing/any/any web-browsing/tcp/any/any
web-browsing/tcp/any/80          action allow;
    icmp-unreachable: no
    terminal yes;
}
```

- Test an Authentication policy rule.

Use the **test authentication-policy-match** command to test your Authentication policy. For example, you want to make sure that all users accessing Salesforce are authenticated. You would use the following **test** command to make sure that if users are not identified using any other mechanism, the Authentication policy will force them to authenticate:

```
admin@PA-3060> test authentication-policy-match from trust to untrust source
192.168.201.10 destination 96.43.144.26
```

```
Matched rule: 'salesforce' action: web-form
```

- Test a Decryption policy rule.

Use the **test decryption-policy-match category** command to test whether traffic to a specific destination and URL category will be decrypted according to your policy rules. For example, to verify that your no-decrypt policy for traffic to financial services sites is not being decrypted, you would enter a command similar to the following:

```
admin@PA-3060> test decryption-policy-match category financial-services from
trust source 10.40.14.197 destination 159.45.2.143
```

```
Matched rule: 'test' action: no-decrypt
```

---

# Load Configurations

- [Load Configuration Settings from a Text File](#)
- [Load a Partial Configuration](#)

## Load Configuration Settings from a Text File

In scripting mode, you can copy and paste commands from a text file directly into the CLI. This is a quick and easy way to copy several configuration settings from one Palo Alto Networks device to another.

**STEP 1** | On the device from which you want to copy configuration commands, set the CLI output mode to set:

```
admin@fw1> set cli config-output-format set
```

**STEP 2** | Show the part of the configuration you want to copy. For example, to copy the SNMP configuration you would enter the following command:

```
admin@fw1# show deviceconfig system snmp-setting
set deviceconfig system snmp-setting snmp-system location Headquarters
set deviceconfig system snmp-setting snmp-system contact snmp-
admin@acme.com
set deviceconfig system snmp-setting access-setting version v2c snmp-
community-string public
```



*When pasting commands into the command line, make sure you are entering them in the proper order to avoid errors. Sometimes commands shown in the CLI are not the order in which they must be configured on the device (for example, if you are pasting a configuration from a firewall into Panorama). If you see errors, check whether the command that generated the error is dependent on a later command. In these cases, you can usually just reenter the command. Also make sure you are pasting sections of a configuration in a logical order. For example, you should not copy security policy rules if you have not yet configured the objects the rules rely on, such as zones, security profiles, or address groups.*

**STEP 3** | Copy the commands to a text editor such as Notepad and edit the settings as desired.

**STEP 4** | On the second device, paste the commands into the command line.



*There is a limit to the amount of text that can be copied into the SSH buffer (approximately 20 lines). If you cut-and-paste a large block of text into the CLI, examine the output of the lines you pasted. If you see lines that are truncated or generate errors, you may have to re-paste a smaller section of text, or switch to scripting mode using the `set cli scripting-mode on` operational mode command, which increases the buffer significantly.*

**STEP 5** | [Commit Configuration Changes](#).

## Load a Partial Configuration

Use the **load config partial** command to copy a section of a configuration file in XML. The configuration can be:

- A saved configuration file from a Palo Alto Networks firewall or from Panorama
- A local configuration (for example, running-config.xml or candidate-config.xml)
- An imported configuration file from a firewall or Panorama

To load a partial configuration, you must identify the configuration file you want to copy from and, if it is not local, import it onto the device (see [Use Secure Copy to Import and Export Files](#) for an example of how to import a saved configuration).



*If you are managing more than two or three firewalls, consider using [Panorama](#) for central management and monitoring of your firewalls.*

To specify what part of the configuration to load, you must find the xpath location, which specifies the XML node in the configuration file you are loading from and the node in the local candidate configuration you are loading to.

The format of the command is:

```
admin@PA-3060# load config partial from <filename> from-xpath <source-xpath>
to-xpath <destination-xpath> mode [append|merge|replace]
```

Use the information in the following topics to determine the appropriate Xpath location formats and use them to load a configuration object from one configuration to another:

- [Xpath Location Formats Determined by Device Configuration](#)
- [Load a Partial Configuration into Another Configuration Using Xpath Values](#)

### *Xpath Location Formats Determined by Device Configuration*

You specify the source and destination of the **load partial** command using xpath locations, which specify the XML node in the configuration you are copying from (**from-xpath**) and the XML node in the candidate configuration you are copying to (**to-xpath**). Determining the correct xpath is a critical part of using this command. The following table shows the format for the **from-xpath** and **to-xpath** on different types of devices. Notice that the **from-xpath** begins at devices or shared, whereas the **to-xpath** begins with /config.

Type of Device Configuration	Xpath Formats
Multi-vsyt Firewall	<b>from-xpath</b>
	devices/entry[@name='localhost.localdomain']/vsyt/ entry[@name='vsyt-ID']/<object>
	<b>to-xpath</b>



Type of Device Configuration	Xpath Formats
	<pre>/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys-ID']/&lt;object&gt;</pre>
Single-vsys Firewall	<p><b>from-xpath</b></p> <pre>devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/&lt;object&gt;</pre> <p><b>to-xpath</b></p> <pre>/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/&lt;object&gt;</pre>
Panorama Shared Object	<p><b>from-xpath</b></p> <pre>shared/&lt;object&gt;</pre> <p><b>to-xpath</b></p> <pre>/config/shared/&lt;object&gt;</pre>
Panorama Device Group Object	<p><b>from-xpath</b></p> <pre>devices/entry[@name='localhost.localdomain']/device-group/entry[@name='device-group-name']/&lt;object&gt;</pre> <p><b>to-xpath</b></p> <pre>/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='device-group-name']/&lt;object&gt;</pre>

## Load a Partial Configuration into Another Configuration Using Xpath Values

**STEP 1** | Find the xpath values to use to load the partial configuration.

1. Log in to the web interface on the device and go to the following URL:  
**https://<device-ip-address>/api**
2. Select **Configuration Commands**.
3. Drill down until you find the configuration object you want to load from one configuration to another.

For example, to find the application group xpath on a multi-vsyz firewall, you would select **Configuration Commands > devices > localhost.localdomain > vsys > <vsys-name> > application-group**. After you drill down to the node you want to load, make note of the XPath that is displayed in the text box.

API > Configuration Commands > devices > entry[@name='localhost.localdomain'] > vsys > entry[@name='vsys2'] > application-group

**XPath**

/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys2']/application-group

Submit



You can also find the xpath from the CLI debug mode (use the operational mode command **debug mode on** to enable this), and then enter the configuration mode **show** command that shows the object you are interested in copying. For example, to see the xpath for the application object configuration in vsys1, you would enter the **show vsys vsys1 application** command. Look for the section of the output that begins with `<request cmd="get" obj="`. This signals the beginning of the xpath. In the following example, the highlighted section is the xpath for the application objects in vsys1:

```
admin@PA-3060# show vsys vsys1 application
(container-tag: vsys container-tag: entry key-tag: name value:
vsys1 container-tag: application)
((eol-matched: . #t) (eol-matched: . #t) (eol-
matched: . #t) (xpath-prefix: . /config/devices/
entry[@name='localhost.localdomain'])) (context-inserted-at-end-
p: . #f))
/usr/local/bin/pan_ms_client --config-mode=default --set-
prefix='set vsys vsys1 ' --cookie=2588252477840140 <<'EOF' | /
usr/bin/less -X -E -M
<request cmd="get" obj="/config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
application"></request>
EOF
```

4. After you find the xpath for the node you want to load, identify the appropriate from- and to- [Xpath Location Formats Determined by Device Configuration](#) to load the partial configuration.

**STEP 2 |** Use the **load config partial** command to copy sections of the configuration you just imported. For example, you would use the following command to load the application filters you configured on fw1 from a saved configuration file, fw1-config.xml, you imported from fw1 (a single-vsyz firewall) to vsys3 on fw2. Notice that even though fw1 does not have multiple virtual system support, the xpath still points to the vsys1 (the default vsyz ID on single-vsyz firewalls):

```
admin@fw2# load config partial from fw1-config.xml from-xpath devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application-
filter to-xpath/config/devices/entry[@name='localhost.localdomain']/vsys/
entry[@name='vsys3']/application-filter mode merge
```



The quotation marks around the hostname and the vsyz name (if applicable) must be neutral. The command will fail if there are opened or closed quotation marks.

---

STEP 3 | Commit Configuration Changes.

---

# Use Secure Copy to Import and Export Files

Secure Copy (SCP) is a convenient way to import and export files onto or off of a Palo Alto Networks device. For example, you can use SCP to upload a new OS version to a device that does not have internet access, or you can export a configuration or logs from one device to import on another. The SCP commands require that you have an account (username and password) on the SCP server.



*Because the file for the entire log database is too large for an export or import to be practical on the following models, they do not support the `scp export logdb` or `scp import logdb` commands: Panorama virtual appliance running Panorama 6.0 or later releases, Panorama M-Series appliances (all releases), and PA-7000 Series firewall (all releases).*

- [Export a Saved Configuration from One Firewall and Import it into Another](#)
- [Export and Import a Complete Log Database \(logdb\)](#)

## Export a Saved Configuration from One Firewall and Import it into Another

After you import the saved configuration, you can then [Load a Partial Configuration](#) from the first firewall onto the second firewall.

**STEP 1 |** On the first firewall, save the current configuration to a named configuration snapshot using the `save config to <filename>` command in configuration mode. For example:

```
admin@PA-fw1# save config to fw1-config
```

**STEP 2 |** Export the named configuration snapshot and log database to an SCP-enabled server using the `scp export configuration from <named-config-file> to <username@host:path>` command in operational mode. When prompted, enter the password for your SCP server account.

```
admin@fw1> scp export configuration from <named-config-file>
to <username@host:path>
```

For an SCP server running on Windows, the destination folder/filename path for both the export and import commands requires a drive letter followed by a colon. For example:

```
admin@fw1> scp export configuration from fw1-config.xml to
ccrisp@10.10.10.5:C:/fw-config
```

**STEP 3 |** Log in to the firewall to which you want to copy the configuration and logs, and then import the configuration snapshot and log database. When prompted, enter the password for your SCP server account.

```
admin@fw2> scp import configuration from <username@host:path_to_named-
config-file>
```

For example (on a Windows-based SCP server):

---

```
admin@fw2> scp import configuration from ccrisp@10.10.10.5:c:/fw-configs/fw1-  
config.xml
```

## Export and Import a Complete Log Database (logdb)

**STEP 1** | Export a log database to an SCP-enabled server using the `scp export` command in operational mode. When prompted, enter the password for your SCP server account.

```
admin@fw1> scp export logdb to <username@host:path_to_destination_filename>
```

For an SCP server running on Windows, the destination folder/filename path for both the export and import commands requires a drive letter followed by a colon. For example:

```
admin@fw1> scp export logdb to ccrisp@10.10.10.5:c:/fw-logs/fw1-logdb
```

**STEP 2** | Log in to the firewall on which to import a log database, and then enter the import command. When prompted, enter the password for your SCP server account.

```
admin@fw2> scp import logdb  
from <username@host:path_to_destination_filename>
```

For example (on a Windows-based SCP server):

```
admin@fw2> scp import logdb from ccrisp@10.10.10.5:c:/fw-logs/fw1-logdb
```

# CLI Jump Start

The following table provides quick start information for configuring the features of Palo Alto Networks devices from the CLI. Where applicable for firewalls with multiple virtual systems (vsys), the table also shows the location to configure shared settings and vsys-specific settings.

To configure...	Start here...
MGT interface	<pre># set deviceconfig system ip-address</pre>
admin password	<pre># set mgt-config users admin password</pre>
DNS	<pre># set deviceconfig system dns-setting servers</pre>
NTP	<pre># set deviceconfig system ntp-servers</pre>
Interfaces	<pre># set network interface</pre>
System settings	<pre># set deviceconfig system</pre>
Zones	<pre># set zone &lt;name&gt; # set vsys &lt;name&gt; zone &lt;name&gt;</pre>
Security Profiles HIP Objects/Profiles URL Filtering Profiles WildFire Analysis Profiles	<pre># set profiles # set vsys &lt;name&gt; profiles # set shared profiles</pre>
Server Profiles	<pre># set server-profile # set vsys &lt;name&gt; server-profile # set shared server-profile</pre>
Authentication Profiles	<pre># set authentication-profile # set vsys &lt;name&gt; authentication-profile # set shared authentication-profile</pre>

To configure...	Start here...
Certificate Profiles	<pre># set certificate-profile # set vsys &lt;name&gt; certificate-profile # set shared certificate-profile</pre>
Policy	<pre># set rulebase # set vsys vsys1 rulebase</pre>
Log Quotas	<pre># set deviceconfig setting management quota-settings</pre>
User-ID	<pre># set user-id-agent # set vsys &lt;name&gt; user-id-agent # set user-id-collector # set vsys &lt;name&gt; user-id-collector</pre>
HA	<pre># set deviceconfig high-availability</pre>
AutoFocus Settings	<pre># set deviceconfig setting autofocus</pre>
WildFire Settings	<pre># set deviceconfig setting wildfire</pre>
Panorama	<pre># set deviceconfig system panorama-server</pre>
Restart	<pre>&gt; request restart system</pre>





# ***CLI Cheat Sheets***

- > CLI Cheat Sheet: Device Management
- > CLI Cheat Sheet: User-ID
- > CLI Cheat Sheet: Networking
- > CLI Cheat Sheet: VSYS
- > CLI Cheat Sheet: Panorama



# CLI Cheat Sheet: Device Management

Use the following table to quickly locate commands for common device management tasks:

If you want to...	Use...
<ul style="list-style-type: none"><li>• Show general system health information.</li></ul>	<pre>&gt; show system info</pre>
<ul style="list-style-type: none"><li>• Show percent usage of disk partitions. Include the optional <code>files</code> parameter to show information about inodes, which track file storage.</li></ul>	<pre>&gt; show system disk-space files</pre>
<ul style="list-style-type: none"><li>• Show the maximum log file size.</li></ul>	<pre>&gt; show system logdb-quota</pre>
<ul style="list-style-type: none"><li>• Show running processes.</li></ul>	<pre>&gt; show system software status</pre>
<ul style="list-style-type: none"><li>• Show processes running in the management plane.</li></ul>	<pre>&gt; show system resources</pre>
<ul style="list-style-type: none"><li>• Show resource utilization in the dataplane.</li></ul>	<pre>&gt; show running resource-monitor</pre>
<ul style="list-style-type: none"><li>• Show the licenses installed on the device.</li></ul>	<pre>&gt; request license info</pre>
<ul style="list-style-type: none"><li>• Show when commits, downloads, and/or upgrades are completed.</li></ul>	<pre>&gt; show jobs processed</pre>
<ul style="list-style-type: none"><li>• Show session information.</li></ul>	<pre>&gt; show session info</pre>
<ul style="list-style-type: none"><li>• Show information about a specific session.</li></ul>	<pre>&gt; show session id &lt;session-id&gt;</pre>
<ul style="list-style-type: none"><li>• Show the running security policy.</li></ul>	<pre>&gt; show running security-policy</pre>
<ul style="list-style-type: none"><li>• Show the authentication logs.</li></ul>	<pre>&gt; less mp-log authd.log</pre>

If you want to...	Use...
<ul style="list-style-type: none"> <li>Restart the device.</li> </ul>	<pre>&gt; request restart system</pre>
<ul style="list-style-type: none"> <li>Show the administrators who are currently logged in to the web interface, CLI, or API.</li> </ul>	<pre>&gt; show admins</pre>
<ul style="list-style-type: none"> <li>Show the administrators who can access the web interface, CLI, or API, regardless of whether those administrators are currently logged in.</li> </ul> <p>When you run this command on the firewall, the output includes both local administrators and those pushed from a Panorama template.</p>	<pre>&gt; show admins all</pre>
<ul style="list-style-type: none"> <li>Configure the management interface as a DHCP client.</li> </ul> <p>For a successful commit, you must include each of the parameters: <b>accept-dhcp-domain</b>, <b>accept-dhcp-hostname</b>, <b>send-client-id</b>, and <b>send-hostname</b>.</p>	<pre># set deviceconfig system type dhcp-client accept-dhcp-domain &lt;yes no&gt; accept-dhcp-hostname &lt;yes no&gt; send-client-id &lt;yes no&gt; send-hostname &lt;yes no&gt;</pre>

---

# CLI Cheat Sheet: User-ID

Use the following commands to perform common [User-ID](#) configuration and monitoring tasks.



*To see more comprehensive logging information enable debug mode on the agent using the `debug user-id log-ip-user-mapping yes` command. When you are done troubleshooting, disable debug mode using `debug user-id log-ip-user-mapping no`.*

## CLI Cheat Sheet: User-ID

View all User-ID agents configured to send user mappings to the Palo Alto Networks device:

- To see all configured Windows-based agents:

```
> show user user-id-agent state all
```

- To see if the PAN-OS-integrated agent is configured:

```
> show user server-monitor state all
```

View how many log messages came in from syslog senders and how many entries the User-ID agent successfully mapped:

```
> show user server-monitor statistics
```

View the configuration of a User-ID agent from the Palo Alto Networks device:

```
> show user user-id-agent config name <agent-name>
```

View group mapping information:

```
> show user group-mapping statistics
> show user group-mapping state all
> show user group list
> show user group name <group-name>
```

View all user mappings on the Palo Alto Networks device:

```
> show user ip-user-mapping all
```

Show user mappings filtered by a username string (if the string includes the domain name, use two backslashes before the username):

```
> show user ip-user-mapping all | match <domain>\\<username-string>
```

Show user mappings for a specific IP address:

---

## CLI Cheat Sheet: User-ID

```
> show user ip-user-mapping ip <ip-address>
```

Show usernames:

```
> show user user-ids
```

---

View the most recent addresses learned from a particular User-ID agent:

```
> show log userid datasourcename equal <agent-name> direction equal backward
```

---

View mappings from a particular type of authentication service:

```
> show log userid datasourcetype equal <authentication-service>
```

where *<authentication-service>* can be **authenticate**, **client-cert**, **directory-server**, **exchange-server**, **globalprotect**, **kerberos**, **netbios-probing**, **ntlm**, **unknown**, **vpn-client**, or **wmi-probing**.

For example, to view all user mappings from the Kerberos server, you would enter the following command:

```
> show log userid datasourcetype equal kerberos
```

---

View mappings learned using a particular type of user mapping:

```
> show log userid datasource equal <datasource>
```

where *<datasource>* can be **agent**, **captive-portal**, **event-log**, **ha**, **probing**, **server-session-monitor**, **ts-agent**, **unknown**, **vpn-client**, or **xml-api**.

For example, to view all user mappings from the XML API, you would enter the following command:

```
> show log userid datasourcetype equal xml-api
```

---

Find a user mapping based on an email address:

```
> show user email-lookup
+ base                Default base distinguished name (DN) to use for
  searches
+ bind-dn             bind distinguished name
+ bind-password       bind password
+ domain              Domain name to be used for username
+ group-object         group object class(comma-separated)
+ name-attribute       name attribute
+ proxy-agent          agent ip or host name.
+ proxy-agent-port     user-id agent listening port, default is 5007
+ use-ssl              use-ssl
* email               email address
> mail-attribute       mail attribute
```

---

## CLI Cheat Sheet: User-ID

```
> server ldap server ip or host name.  
> server-port ldap server listening port
```

For example:

```
> show user email-lookup base "DC=lab,DC=sg,DC=acme,DC=local" bind-dn  
"CN=Administrator,CN=Users,DC=lab,DC=sg,DC=acme,DC=local" bind-password  
acme use-ssl no email user1@lab.sg.acme.local mail-attribute mail server  
10.1.1.1 server-port 389 labsg\user1
```

---

Clear the User-ID cache:

```
clear user-cache all
```

Clear a User-ID mapping for a specific IP address:

```
clear user-cache ip <ip-address/netmask>
```

---

# CLI Cheat Sheet: Networking

Use the following table to quickly locate commands for common networking tasks:

If you want to . . .	Use . . .
<b>General Routing Commands</b>	
<ul style="list-style-type: none"><li>• Display the routing table</li></ul>	<pre>&gt; show routing route</pre>
<ul style="list-style-type: none"><li>• Look at routes for a specific destination</li></ul>	<pre>&gt; show routing fib virtual-router &lt;name&gt;   match &lt;x.x.x.x/Y&gt;</pre>
<ul style="list-style-type: none"><li>• Change the ARP cache timeout setting from the default of 1800 seconds.</li></ul>	<pre>&gt; set system setting arp-cache- timeout &lt;60-65536&gt;</pre>
<ul style="list-style-type: none"><li>• View the ARP cache timeout setting.</li></ul>	<pre>&gt; show system setting arp-cache-timeout</pre>
<b>NAT</b>	
<ul style="list-style-type: none"><li>• Show the NAT policy table</li></ul>	<pre>&gt; show running nat-policy</pre>
<ul style="list-style-type: none"><li>• Test the NAT policy</li></ul>	<pre>&gt; test nat-policy-match</pre>
<ul style="list-style-type: none"><li>• Show NAT pool utilization</li></ul>	<pre>&gt; show running ippool &gt; show running global-ippool</pre>
<b>IPSec</b>	
<ul style="list-style-type: none"><li>• Show IPSec counters</li></ul>	<pre>&gt; show vpn flow</pre>
<ul style="list-style-type: none"><li>• Show a list of all IPSec gateways and their configurations</li></ul>	<pre>&gt; show vpn gateway</pre>
<ul style="list-style-type: none"><li>• Show IKE phase 1 SAs</li></ul>	<pre>&gt; show vpn ike-sa</pre>




If you want to . . .	Use . . .
<ul style="list-style-type: none"> <li>Show IKE phase 2 SAs</li> </ul>	<pre>&gt; show vpn ipsec-sa</pre>
<ul style="list-style-type: none"> <li>Show a list of auto-key IPsec tunnel configurations</li> </ul>	<pre>&gt; show vpn tunnel</pre>
<b>BFD</b>	
<ul style="list-style-type: none"> <li>Show BFD profiles</li> </ul>	<pre>&gt; show routing bfd active-profile [&lt;name&gt;]</pre>
<ul style="list-style-type: none"> <li>Show BFD details</li> </ul>	<pre>&gt; show routing bfd details [interface &lt;name&gt;] [local-ip &lt;ip&gt;] [multihop][peer-ip &lt;ip&gt;] [session-id] [virtual-router &lt;name&gt;]</pre>
<ul style="list-style-type: none"> <li>Show BFD statistics on dropped sessions</li> </ul>	<pre>&gt; show routing bfd drop-counters session-id &lt;session-id&gt;</pre>
<ul style="list-style-type: none"> <li>Show counters of transmitted, received, and dropped BFD packets</li> </ul>	<pre>&gt; show counter global   match bfd</pre>
<ul style="list-style-type: none"> <li>Clear counters of transmitted, received, and dropped BFD packets</li> </ul>	<pre>&gt; clear routing bfd counters session-id all   &lt;1-1024&gt;</pre>
<ul style="list-style-type: none"> <li>Clear BFD sessions for debugging purposes</li> </ul>	<pre>&gt; clear routing bfd session-state session-id all   &lt;1-1024&gt;</pre>
<b>PVST+</b>	
<ul style="list-style-type: none"> <li>Set the native VLAN ID</li> </ul>	<pre>&gt; set session pvst-native-vlan-id &lt;vid&gt;</pre>
<ul style="list-style-type: none"> <li>Drop all STP BPDU packets</li> </ul>	<pre>&gt; set session drop-stp-packet</pre>
<ul style="list-style-type: none"> <li>Verify PVST+ BPDU rewrite configuration, native VLAN ID, and STP BPDU packet drop</li> </ul>	<pre>&gt; show vlan all</pre>
<ul style="list-style-type: none"> <li>Show counter of times the 802.1Q tag and PVID fields in a PVST+ BPDU packet do not match</li> </ul>	<pre>&gt; show counter global</pre>

If you want to . . .	Use . . .
	Look at the <code>flow_pvid_inconsistent</code> counter.
<b>Troubleshooting</b>	
<ul style="list-style-type: none"> <li>• Ping from the management (MGT) interface to a destination IP address</li> </ul>	<pre>&gt; ping host &lt;destination-ip-address&gt;</pre>
<ul style="list-style-type: none"> <li>• Ping from a dataplane interface to a destination IP address</li> </ul>	<pre>&gt; ping source &lt;ip-address-on-dataplane&gt;   host &lt;destination-ip-address&gt;</pre>
<ul style="list-style-type: none"> <li>• Show network statistics</li> </ul>	<pre>&gt; show netstat statistics yes</pre>

# CLI Cheat Sheet: VSYS

Use the following commands to administer a Palo Alto Networks firewall with multiple [virtual system](#) (multi-vsys) capability. You must have superuser, superuser (read-only), device administrator, or device administrator (read-only) access to use these commands. These commands are not available for virtual system administrator or virtual system administrator (read-only) roles.

If you want to ...	Use ...								
<ul style="list-style-type: none"><li>Find out if the firewall is in multi-vsys mode</li></ul>	<pre>admin@PA&gt; show system info   match vsys multi-vsys: on</pre>								
<ul style="list-style-type: none"><li>View a list of virtual systems configured on the firewall</li></ul>	<pre>admin@PA&gt; set system setting target-vsys ? none      none vsys1     vsys1 vsys2     vsys2 &lt;value&gt;   &lt;value&gt;</pre>								
<ul style="list-style-type: none"><li>Switch to a particular vsys so that you can issue commands and view data specific to that vsys</li></ul>	<pre>admin@PA&gt; set system setting target- vsys &lt;vsys-name&gt;</pre> <p>For example, use the following command to switch to vsys2; note that the vsys name is case sensitive:</p> <pre>&gt; set system setting target-vsys vsys2 Session target vsys changed to vsys2 admin@PA-vsys2&gt;</pre> <p>Notice that the command prompt now shows the name of the vsys you are now administering.</p>								
<ul style="list-style-type: none"><li>View the maximum number of sessions allowed, in use, and throttled</li></ul>	<pre>admin@PA&gt; show session meter</pre> <p>Example output:</p> <table><tr><th>VSYS</th><th>Maximum</th><th>Current</th><th>Throttled</th></tr><tr><td>1</td><td>10</td><td>30</td><td>1587</td></tr></table> <p>Maximum indicates the maximum number of sessions allowed per dataplane, Current indicates the number of sessions being used by the virtual system, and Throttled indicates the number of sessions denied for the virtual system because the sessions exceeded the Maximum number multiplied by the number of dataplanes in the system.</p>	VSYS	Maximum	Current	Throttled	1	10	30	1587
VSYS	Maximum	Current	Throttled						
1	10	30	1587						

If you want to . . .	Use . . .
	 <p><i>As shown in this example, on a PA-5200 Series or PA-7000 Series firewall, the Current number of sessions being used can be greater than the Maximum configured for Sessions Limit (Device &gt; Virtual Systems &gt; Resource) because there are multiple dataplanes per virtual system. The Sessions Limit you configure on a PA-5200 or PA-7000 Series firewall is per dataplane, and will result in a higher maximum per virtual system.</i></p>
<ul style="list-style-type: none"> <li>View the User-ID mappings in the vsys</li> </ul>	<pre>admin@PA-vsyz2&gt; show user ip-user-mapping all</pre>
<ul style="list-style-type: none"> <li>Return to configuring the firewall globally</li> </ul>	<pre>admin@PA-vsyz2&gt; set system setting target- vsyz none admin@PA&gt;</pre>


# CLI Cheat Sheet: Panorama

Use the following commands on [Panorama](#) to perform common configuration and monitoring tasks for the Panorama management server (M-Series appliance in Panorama mode), Dedicated Log Collectors (M-Series appliances in Log Collector mode), and managed firewalls.



To view system information about a Panorama virtual appliance or M-Series appliance (for example, job history, system resources, system health, or logged-in administrators), see [CLI Cheat Sheet: Device Management](#).

A Dedicated Log Collector mode has no web interface for administrative access, only a command line interface (CLI).

If you want to . . .	Use . . .
<b>M-Series Appliance Mode of Operation (Panorama, Log Collector, or PAN-DB Private Cloud Mode)</b>	
 Switching the mode reboots the M-Series appliance, deletes any existing log data, and deletes all configurations except the management access settings.	
<ul style="list-style-type: none"><li>Display the current operational mode.</li></ul>	<pre>&gt; show system info   match system-mode</pre>
<ul style="list-style-type: none"><li>Switch from Panorama mode to Log Collector mode.</li></ul>	<pre>&gt; request system system-mode logger</pre>
<ul style="list-style-type: none"><li>Switch from Panorama mode to PAN-DB private cloud mode (M-500 appliance only).</li></ul>	<pre>&gt; request system system-mode panurldb</pre>
<ul style="list-style-type: none"><li>Switch an M-Series appliance from Log Collector mode or PAN-DB private cloud mode (M-500 appliance only) to Panorama mode.</li></ul>	<pre>&gt; request system system-mode panorama</pre>
<ul style="list-style-type: none"><li>Switch the Panorama virtual appliance from Legacy mode to Panorama mode.</li></ul>	<pre>&gt; request system system-mode panorama</pre>
<ul style="list-style-type: none"><li>Switch the Panorama virtual appliance from Panorama mode to Legacy mode.</li></ul>	<pre>&gt; request system system-mode legacy</pre>
<b>Panorama Management Server</b>	
<ul style="list-style-type: none"><li>Change the output for <b>show</b> commands to a format that you can run as CLI commands.</li></ul>	<pre>&gt; set cli config-output-mode set</pre>

If you want to . . .	Use . . .
	<p>The following is an example of the output for the <b>show device-group</b> command after setting the output format:</p> <pre># show device-group branch-offices set device-group branch-offices devices set device-group branch-offices pre-rulebase ...</pre>
<ul style="list-style-type: none"> <li>• Enable or disable the connection between a firewall and Panorama. You must enter this command from the firewall CLI.</li> </ul>	<pre>&gt; set panorama [off   on]</pre>
<ul style="list-style-type: none"> <li>• Synchronize the configuration of M-Series appliance high availability (HA) peers.</li> </ul>	<pre>&gt; request high-availability sync-to-remote [running-config   candidate-config]</pre>
<ul style="list-style-type: none"> <li>• Reboot multiple firewalls or Dedicated Log Collectors.</li> </ul>	<pre>&gt; request batch reboot [devices   log-collectors] &lt;serial-number&gt;</pre>
<ul style="list-style-type: none"> <li>• Change the interval in seconds (default is 10; range is 5 to 60) at which Panorama polls devices (firewalls and Log Collectors) to determine the progress of software or content updates. Panorama displays the progress when you deploy the updates to devices. Decreasing the interval makes the progress report more accurate but increases traffic between Panorama and the devices.</li> </ul>	<pre>&gt; set dlsrvr poll-interval &lt;5-60&gt;</pre>
<b>Device Groups and Templates</b>	
<ul style="list-style-type: none"> <li>• Show the history of device group commits, status of the connection to Panorama, and other information for the firewalls assigned to a device group.</li> </ul>	<pre>&gt; show devicegroups name &lt;device-group-name&gt;</pre>
<ul style="list-style-type: none"> <li>• Show the history of template commits, status of the connection to Panorama, and other information for the firewalls assigned to a template.</li> </ul>	<pre>&gt; show templates name &lt;template-name&gt;</pre>
<ul style="list-style-type: none"> <li>• Show all the policy rules and objects pushed from Panorama to a firewall. You must enter this command from the firewall CLI.</li> </ul>	<pre>&gt; show config pushed-shared-policy</pre>

If you want to . . .	Use . . .
<ul style="list-style-type: none"> <li>Show all the network and device settings pushed from Panorama to a firewall. You must enter this command from the firewall CLI.</li> </ul>	<pre>&gt; show config pushed-template</pre>
<b>Log Collection</b>	
<ul style="list-style-type: none"> <li>Show the current rate at which the Panorama management server or a Dedicated Log Collector receives firewall logs.</li> </ul>	<pre>&gt; debug log-collector log-collection-stats show incoming-logs</pre>
<ul style="list-style-type: none"> <li>Show the quantity and status of logs that Panorama or a Dedicated Log Collector forwarded to external servers (such as syslog servers) as well as the auto-tagging status of the logs. Tracking dropped logs helps you troubleshoot connectivity issues.</li> </ul>	<pre>&gt; debug log-collector log- collection-stats show log- forwarding-stats</pre>
<ul style="list-style-type: none"> <li>Show status information for log forwarding to the Panorama management server or a Dedicated Log Collector from a particular firewall (such as the last received and generated log of each type).</li> </ul> <p>When you run this command at the firewall CLI (skip the <b>device &lt;firewall-serial-number&gt;</b> argument), the output also shows how many logs the firewall has forwarded.</p>	<pre>&gt; show logging-status device &lt;firewall-serial- number&gt;</pre>
<ul style="list-style-type: none"> <li>Clear logs by type.</li> </ul> <p>Running this command on the Panorama management server clears logs that Panorama and Dedicated Log Collectors generated, as well as any firewall logs that the Panorama management server collected. Running this command on a Dedicated Log Collector clears the logs that it collected from firewalls.</p>	<pre>&gt; clear log [acc   alarm   config   hipmatch   system   threat   traffic]</pre>

