

Palo Alto CLI Commands Cheat Sheet(s) PAN-OS v 9.1 and 10.1

Display Format & Command Finder

CLI Display Format (XML is the default)

```
>set cli config-output-format <set json xml default>
```

The **set** format is common for viewing the config in configure mode

XML Format Example:

```
hostname PA-220;
dns-setting {
  servers {
    primary 8.8.8.8;
    secondary 8.8.4.4;
  }
}
```

JSON Format Example:

```
"hostname":
"PA-220",
"dns-setting":
{
  "servers":
  {
    "primary":
"8.8.8.8",
    "secondary":
"8.8.4.4"}
}
```

Set Format Example:

```
set deviceconfig system hostname PA-220
set deviceconfig system dns-setting servers primary 8.8.8.8
set deviceconfig system dns-setting servers secondary 8.8.4.4
```

Find a command via a keyword (works in configure mode)

```
>find command keyword <value>
```

Example: >find command keyword *pbf-policy*

```
#find command keyword <value>
```

Restart & Shutdown

Restart the firewall

```
>request restart system
```

Shutdown the firewall

A shutdown will require a power cycle to power on

```
>request shutdown system
```

Site-to-Site VPN

Show dataplane IPsec-VPN tunnel info

```
>show vpn flow
```

Show IKE Phase 1 security associations (SA)

```
>show vpn ike-sa
```

Show IKE Phase 2 security associations (SA)

```
>show vpn ipsec-sa
```

Show the details of a specific IPsec VPN

x is the ID number shown with "show vpn flow"

```
>show vpn flow tunnel-id x
```

Show details of an active IKE Phase 1 SA (? list)

```
>show vpn ike-sa gateway ?
```

Show details of an active IKE Phase 2 SA (? list)

```
>show vpn ipsec-sa tunnel ?
```

To drop a VPN tunnel (both Phase 1 & 2)

Use ? to list available, then select the desired name

```
>clear vpn ike-sa gateway ?
```

```
>clear vpn ipsec-sa tunnel ?
```

To test (bring up) a VPN tunnel (both Phase 1 & 2)

Use ? to list available, then select the desired name

```
>test vpn ike-sa gateway ?
```

```
>test vpn ipsec-sa tunnel ?
```

Show Active Sessions

Monitor sessions in real-time

```
>show session info
```

Config Mgmt & Commit

To view changes (GUI equiv. to Commit>Preview Changes)

```
>show config diff
```

Validate config (GUI equiv. to Commit>Validate Commit)

```
#validate full
```

Commit config (GUI equiv. to Commit>Commit)

```
#commit
```

System Info - Environment - Resources - Processes - Disk

Show system info (mgmt IP, Uptime, Serial, SW Version)

```
>show system info
```

Display physical environment (Power & Temperature)

```
> show system environmentals
```

Show resource utilization (data plane CPU)

```
>show running resource-monitor
```

Show the running processes

```
>show system software status
```

Show disk space

```
>show system disk-space
```

Restart the server management process

Any admin(s) logged into the GUI or CLI will be disconnected

```
>debug software restart process management-server
```

Networking

Ping a host - default source is the management interface

```
>ping host <ip-address or hostname >
```

Ping from a dataplane interface IP address

```
>ping source <ip-addr-on-dataplane> host <ip-address or hostname>
```

Manually release DHCP IP address (# is interface number)

```
>clear dhcp lease interface ethernet#/# ip <ip-address>
```

Set a static route (example uses the VR named *default*)

```
#set network virtual-router default routing-table ip
static-route #.#.#.#/# nexthop <next-hop-ip-address>
```

Device Setup (The commit command is implied)

Disable ZTP (if supported and ZTP not needed)

```
>request disable-ztp
```

Configure a static IP address on Management interface

```
>configure
```

```
#set deviceconfig system type static
```

```
#set deviceconfig system ip-address x.x.x.x netmask
x.x.x.x default-gateway x.x.x.x
```

Example: #set deviceconfig system ip-address

```
10.0.0.254 netmask 255.255.255.0 default-gateway
```

Note: *default-gateway* is optional

Setup or revert Management interface to DHCP

```
>configure
```

Note: for a successful commit, all options in red are required

```
#set deviceconfig system type dhcp-client accept-dhcp-
domain <yes/no> accept-dhcp-hostname <yes/no> send-
client-id <yes/no> send-hostname <yes/no>
```

```
#request dhcp client management-interface release
```

Palo Alto CLI Commands Cheat Sheet(s) PAN-OS v 9.1 and 10.1

User ID	
User Group(s)	Group
Match specific user to groups > <i>show user user-ids match-user <username></i> > <i>show user user-ids match-user <domain\username></i>	Show members of a group (include " if there are spaces) > <i>show user group name "domain\group_name"</i>
User IP Mapping	Show group list (full OU path) > <i>show user group list</i>
View user to IP mappings > <i>show user ip-user-mapping all</i> > <i>show user ip-user-mapping all option detail</i> > <i>show user ip-user-mapping ip <ip-address></i>	Show a list of groups names local to the firewall. As found in GUI interface locations: Device>User Identification>Group Mapping Settings Device>Local User Database>User Groups
Show user mappings filtered by a username string > <i>show user ip-user-mapping all match <username></i>	> <i>show user group name ?</i>
Manually Sync LDAP Group(s)	View details on a group mapping As found in GUI interface locations: Device>User Identification>Group Mapping Settings
Manually sync all groups > <i>debug user-id refresh group-mapping all</i>	> <i>show user group-mapping state all</i>
List all groups for manual sync > <i>debug user-id refresh group-mapping ?</i>	> <i>show user group-mapping state group_name</i>
Manually sync a specific group > <i>debug user-id refresh group-mapping <group-name></i>	View group mapping statistics (sync times) > <i>show user group-mapping statistics</i>
Clear the User-ID Cache (IP Mapping)	Manually Reset (reconnect) LDAP Group(s)
Manually reset all groups > <i>debug user-id reset group-mapping all</i>	Manually reset all groups > <i>debug user-id reset group-mapping all</i>
Clear the User-ID cache > <i>clear user-cache all</i>	List all groups for manual reset > <i>debug user-id reset group-mapping ?</i>
Clear a User-ID mapping for a specific IP address > <i>clear user-cache ip <ip-address></i>	Manually reset a specific group > <i>debug user-id reset group-mapping <group-name></i>
Clear a User-ID mapping for a network > <i>clear user-cache ip <ip-address/netmask></i>	
SSH to Another Device	Quick Packet Capture of Management Interface
SSH to Another Device (using a specific IP source) > <i>ssh v2 yes source #.#.#.# host username@#.#.#.#</i>	> <i>tcpdump filter "port <port-number>"</i> > <i>tcpdump filter "host <ip-address>"</i>
Above uses SSH v2 and specifies a hostname to use	View the packet capture > <i>view-pcap mgmt-pap mgmt.pcap</i>
Networking	URL Link for more info: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS
Restart routing process (BGP can use <i>test routing bgp</i> command) > <i>debug routing restart</i>	

PAN-OS 9.1 CLI Cheat Sheets

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/cli-cheat-sheets>

CLI Changes in PAN-OS 9.1

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/cli-changes>

PAN-OS 10.1 CLI Cheat Sheets

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/cli-cheat-sheets>

CLI Changes in PAN-OS 10.1

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/cli-changes>

PAN-OS 10.2 CLI Cheat Sheets

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-cheat-sheets>

CLI Changes in PAN-OS 10.2

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/cli-changes>

This document is available at the PacketPassers blog page:

<https://packetpassers.com/palo-alto-networks-cli-cheat-sheet>