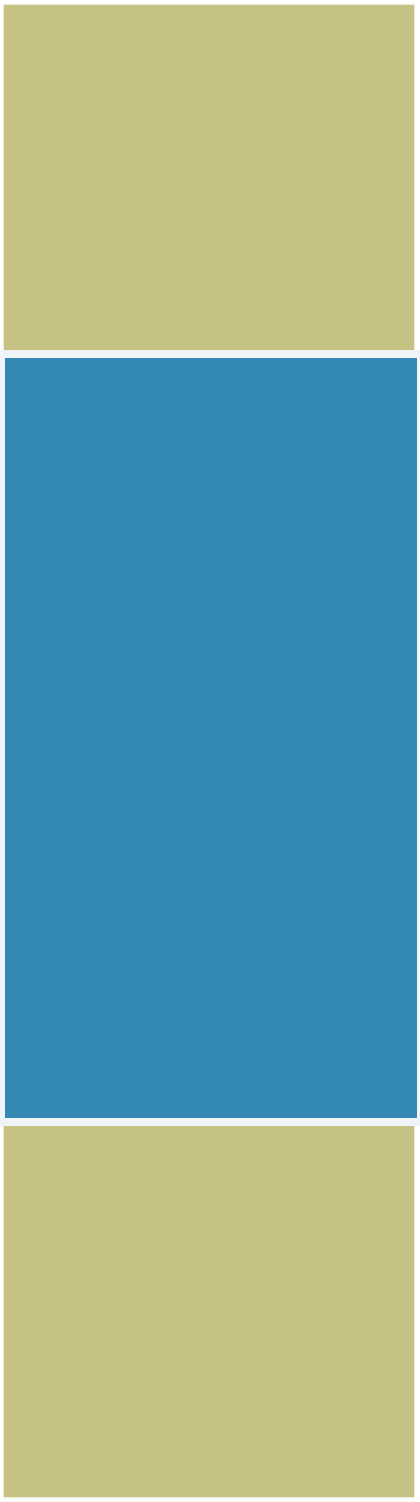

CLI Cheat Sheets

Palo Alto Networks

PAN-OS® CLI Quick Start
Version 7.0

Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-us

About this Guide

This guide shows you how to get started with the PAN-OS Command Line Interface (CLI) and shows you how to find a command and get help on using the command. This guide replaces the CLI Reference Guide. For additional documentation on our products, refer to the following resources:

- For information on the additional capabilities and for instructions on configuring the features of Palo Alto Networks devices, refer to https://www.paloaltonetworks.com/documentation.
- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS 7.0 release notes, go to https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes.html.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: February 3, 2016

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

If you want to...	Use...
• Show general system health information.	`> show system info`
• Show percent usage of disk partitions.	`> show system disk-space`
• Show the maximum log file size.	`> show system logdb-quota`
• Show running processes.	`> show system software status`
• Show processes running in the management plane.	`> show system resources`
• Show resource utilization in the dataplane.	`> show running resource-monitor`
• Show the licenses installed on the device.	`> request license info`
• Show when commits, downloads, and/or upgrades are completed.	`> show jobs processed`
• Show session information.	`> show session info`
• Show information about a specific session.	`> show session id <session-id>`
• Show the running security policy.	`> show running security-policy`
• Show the authentication logs.	`> less mp-log authd.log`
• Restart the device.	`> request restart system`
• Show the administrators who are currently logged in to the web interface, CLI, or API.	`> show admins`
• Show the administrators who can access the web interface, CLI, or API, regardless of whether those administrators are currently logged in. When you run this command on the firewall, the output includes both local administrators and those pushed from a Panorama template.	`> show admins all`

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 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:
`> 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 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`

CLI Cheat Sheet: User-ID

View mappings learned using a particular type of user mapping:

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

where `<datasource>` can be be `agent`, `captive-portal`, `event-log`, `ha`, `probing`, `server-session-monitor`, `ts-agent`, `unknown`, `vpn-client`, `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
> 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

If you want to . . .	Use . . .
General Routing Commands	
• Display the routing table	`> show routing route`
• Look at routes for a specific destination	`> show routing fib virtual-router <name> | match <x.x.x.x/Y>`
NAT	
• Show the NAT policy table	`> show running nat-policy`
• Test the NAT policy	`> test nat-policy-match`
• Show NAT pool utilization	`> show running ippool` `> show running global-ippool`
IPSec	
• Show IPSec counters	`> show vpn flow`
• Show a list of all IPSec gateways and their configurations	`> show vpn gateway`
• Show IKE phase 1 SAs	`> show vpn ike-sa`
• Show IKE phase 2 SAs	`> show vpn ipsec-sa`
• Show a list of auto-key IPSec tunnel configurations	`> show vpn tunnel`
Troubleshooting	
• Ping from the management (MGT) interface to a destination IP address	`> ping host <destination-ip-address>`
• Ping from a dataplane interface to a destination IP address	`> ping source <ip-address-on-dataplane> host <destination-ip-address>`
• Show network statistics	`> netstat all yes`

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 . . .
• Find out if the firewall is in multi-vsys mode	`admin@PA> show system info | match vsys` `  multi-vsys: on`

• View a list of virtual systems configured on the firewall	`admin@PA> set system setting target-vsys ?`
	`  none  none`
	`  vsys1  vsys1`
	`  vsys2  vsys2`
	`  <value>  <value>`

• Switch to a particular vsys so that you can issue commands and view data specific to that vsys	`admin@PA> set system setting target-vsys <vsys-name>`
	For example, use the following command to switch to vsys2; note that the vsys name is case sensitive:
	`> set system setting target-vsys vsys2`
	`Session target vsys changed to vsys2`
	`admin@PA-vsys2>`
	Notice that the command prompt now shows the name of the vsys you are now administering.

• View the User-ID mappings in the vsys	`admin@PA-vsys2> show user ip-user-mapping all`
• Return to configuring the firewall globally	`admin@PA-vsys2> set system setting target-vsys none` `>admin@PA>`

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 . . .
M-Series Appliance Mode of Operation (Panorama, Log Collector, or PAN-DB Private Cloud Mode)	
 Switching the mode reboots the M-Series appliance, deletes any existing log data, and deletes all configurations except the management access settings.	
• Display the current operational mode.	`> show system info | match system-mode`
• Switch from Panorama mode to Log Collector mode.	`> request system system-mode logger`
• Switch from Panorama mode to PAN-DB private cloud mode (M-500 appliance only).	`> request system system-mode panurldb`
• Switch from Log Collector mode or PAN-DB private cloud mode (M-500 appliance only) to Panorama mode.	`> request system system-mode panorama`
Panorama Management Server	

• Change the output for **show** commands to a format that you can run as CLI commands.	`> set cli config-output-mode set`
	The following is an example of the output for the **show device-group** command after setting the output format:
	`# show device-group branch-offices`
	`set device-group branch-offices devices`
	`set device-group branch-offices pre-rulebase`
	`...`

• Enable or disable the connection between a firewall and Panorama. You must enter this command from the firewall CLI.	`> set panorama [off | on]`
• Synchronize the configuration of M-Series appliance high availability (HA) peers.	`> request high-availability sync-to-remote [running-config | candidate-config]`
• Reboot multiple firewalls or Dedicated Log Collectors.	`> request batch reboot [devices | log-collectors] <serial-number>`

If you want to . . .	Use . . .
Device Groups and Templates	
• Show the history of device group commits, status of the connection to Panorama, and other information for the firewalls assigned to a device group.	`> show devicegroups name <device-group-name>`
• Show the history of template commits, status of the connection to Panorama, and other information for the firewalls assigned to a template.	`> show templates name <template-name>`
• Show all the policy rules and objects pushed from Panorama to a firewall. You must enter this command from the firewall CLI.	`> show config pushed-shared-policy`
• Show all the network and device settings pushed from Panorama to a firewall. You must enter this command from the firewall CLI.	`> show config pushed-template`
Log Collection	
• Show the current rate at which the Panorama management server or a Dedicated Log Collector receives firewall logs.	`> debug log-collector log-collection-stats show incoming-logs`
• Show status information for log forwarding to the Panorama management server or a Dedicated Log Collector from a particular firewall (for example, the last received and generated log of each type). When you run this command at the firewall CLI (skip the `device <firewall-serial-number>` argument), the output also shows how many logs the firewall has forwarded.	`> show logging-status device <firewall-serial-number>`
• Clear logs by type. 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.	`> clear log [acc | alarm | config | hipmatch | system | threat | traffic]`