System Administration via CLI

Though spare in appearance, Asset Manager's command-line interface (CLI) is a powerful tool with many of the same capabilities as Asset Manager's GUI. It also provides some functionality not yet available in Asset Manager's GUI. This section introduces the basic CLI syntax and provides the procedures you are most likely to use.

CLI Menu Structure

CLI commands are organized in tiered menus. Below are the commands available on the primary and secondary tiers.

Primary Tier of CLI

Top

Command	Purpose
authentication	Manage licenses, SSL certificates and authentication
certificate	Manage licenses and SSL certificates
collector	View and edit collectors
connections	View and connect to Asset Manager systems
exit	Logout of the current CLI session
help	Display an overview of the CLI syntax
history	Display the current session's command line history
log	View and edit system log settings
logout	Logout of the current CLI session
organization	View and edit organizations
role	View and edit roles
support	Tools for FireMon Customer Support
system	View, edit system parameters; shutdown/reboot system
top	Exit sub-command mode and return to top level
user	View and edit users
zone	View and edit zones

Secondary Tiers of CLI

authentication

Command	Purpose
ad	Show or set the user authentication mechanism
exit	Logout of the current CLI session
help	Display an overview of the CLI syntax
history	Display the current session's command line history
ldap	Configure authentication via LDAP
logout	Logout of the current CLI session
pki	Manage client-side authentication
radius	Configure authentication via RADIUS
top	Exit sub-command mode and return to top level

certificate		
	Command	**Purpose**
	ca	Install or remove a new CA certificate
	crl	Install or remove the Certificate Revocation List
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	license	Install a new Asset Manager license certificate
	logout	Logout of the current CLI session
	ocsp	Configure OCSP settings
	server	Install or remove a new SSL server certificate
	top	Exit sub-command mode and return to top level

connections		
	Command	**Purpose**
	connect	Connect command center to scout or portal
	delete	Delete scout from command center
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	list	List Asset Manager command centers and scouts
	logout	Logout of the current CLI session
	top	Exit sub-command mode and return to top level
	upgrade-scout	Upgrade scout to a new version of Asset Manager

> ⓘ Previous to 4.7, this menu was named "lumeta"

exit	Will close and logout of the current CLI session

help	CONTEXT SENSITIVE HELP
	[?] - Display either a list of possible command completions with summaries,
	    or the full syntax of the current command. A subsequent repeat of this
	    key, when a command has been resolved, will display a detailed
	reference.
	
	AUTO-COMPLETION
	The following keys perform auto-completion for the current command line.
	If the command prefix is not unique then the bell will ring and a subsequent
	repeat of the key will display possible completions.
	
	[enter] - Auto-completes, syntax-checks then executes a command.
	[space] - Auto-completes, or if the command is already resolved inserts a
	space.
	[tab] - Like [space], but can complete some variable data as well.
	
	MOVEMENT KEYS
	[^A] / [^E] - Move to the start/end of the line
	[up] / [down] - Move to the previous/next command line held in history.
	[left] / [right] - Move the insertion point left/right one character.
	
	DELETION KEYS
	[^C] - Delete and abort the current line
	[^D] / [^H] - Delete the character to the right/left of the insertion point.
	[^K] / [^U] - Delete all characters to the right/left of the insertion point.

history	Will display the current session's command line history

log	Command	Purpose
	cefserver	Show CEF syslog server settings or set CEF syslog server
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	level	Set or get the logging levels for FAM services
	logout	Logout of the current CLI session
	server	Show syslog server settings or set local or remote syslog server
	services	Show the defined log services
	show	View log data
	top	Exit sub-command mode and return to top level

logout	Will close the SSH connection

organization	Command	Purpose
	delete	Delete an organization
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	list	Display information about organizations
	logout	Logout of the current CLI session
	new	Add new organization
	top	Exit sub-command mode and return to top level

role	Command	Purpose
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	list	Display all role names or, given a role, display its permissions
	logout	Logout of the current CLI session
	top	Exit sub-command mode and return to top level
	users	Change role's users

support	Command	Purpose
	!	Run a Linux command
	bash	Run an interactive bash subshell
	db	Tools for database monitoring
	details	Display Linux system & process details
	diagnostics	Export a zip file containing system logs and diagnostic data
	dnslookup	Query a DNS name server
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	logout	Logout of the current CLI session
	ls	List files in a directory
	ping	Send ICMP ping packets to another device
	ps	Give details of current processes
	queries	Display currently running database queries
	resize	Extend LVM paritions
	root-ssh	Enable or disable ssh to root
	service	Start, stop or get status of FAM and system services
	snmp	Display the status of an SNMP agent or perform an SNMP walk
	top	Exit sub-command mode and return to top level
	traceroute	Print the route that packets trace to get to network host

	Command	Purpose
system	audit	View or change system auditing
	backup	Generate a system backup
	banner	Set or display the login banner text
	configuration	Export/import system configuration data
	database-auditing	View or change the database auditing policy
	device-persistence-policy	View or change the device persistence policy
	dns	View or change the DNS name servers
	exit	Logout of the current CLI session
	expire-data-interval	View or change time period to remove old data
	feed	Get or set threat feed configuration
	fips	View or change FIPS mode
	hardware-id	Get the system hardware identifier (UUID)
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	hostname	View or change system hostname
	interface	Information about network interface card(s).
	logout	Logout of the current CLI session
	ntp	View or change the NTP name servers
	password-controls	View or change password-controls state
	password-parameters	View or change customized password parameters
	reboot	Restart the FAM appliance
	reinit	Re-run post-install setup program
	shutdown	Power off the FAM appliance
	snmpd	Configure the server SNMP agent
	ssh	Set or get the incoming SSH port
	timeout	View or change session timeout
	top	Exit sub-command mode and return to top level
	type	Is this system a command center or a scout?
	upgrade	Upgrade to a new version of FAM
	version	Show the versions of FAM, Linux and packages
top	Exit sub-command mode and return to top level	

user	Command	Purpose
	delete	Delete user
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	key	Fetch or remove user API key
	list	Display all user names or, given a user, display details
	logout	Logout of the current CLI session
	new	Add new user
	password	Change user password
	roles	Modify roles assigned to a user
	superuser	Set or take away superuser privileges
	top	Exit sub-command mode and return to top level

zone	Command	Purpose
	customattributes	Specify IP/CIDR, Label and Value
	delete	Delete a zone
	discoveryspaces	Specify CIDR blocks
	exit	Logout of the current CLI session
	help	Display an overview of the CLI syntax
	history	Display the current session's command line history
	list	Show available zones or details of one zone
	logout	Logout of the current CLI session
	new	Add new zone
	organization	Change zone's organization
	top	Exit sub-command mode and return to top level

> ⊘ **CLI Syntax Tips**
>
> To see what's next and display syntax tips while working in it, press **?** after a partial command for possible completions plus brief descriptions of the command's purpose and syntax.
>
> If you press **??** after a command completes, an expanded description will display.
>
> You can navigate down through each menu tier by pressing ⏎ after entering a single command at that tier (e.g., system ⏎ hardware-id ⏎) or you can include the full command, separating each tier's command with a space. Press ⏎ at the end of the line (e.g., system hardware-id ⏎). Enclose values that have spaces in them such as "Finance Department" in quotation marks (e.g., admin@Organization1> zone new "Finance Department" Organization1).

Enabling NetFlow Capture

To enable NetFlow capture from the command-line interface:

1. Log in to the CLI.
2. At the command-line prompt, enter **support service packetcapture start**

3. Exit the CLI.

Retrieving Your System's Hardware ID/ Identifying your UUID

The *hardware-id* command is useful as it displays the information you'll need to supply FireMon Support to generate a license. You can also access your hardware ID via the
Asset Manager GUI.

1. Log in to the CLI.
2. At the command-line prompt, enter **system hardware-id**
   The hardware ID displays.

Installing and Activating a License

The *certificate license* command in the CLI enables you to activate a license or find out the activation date of your current license. Licenses, however, are more frequently activated via the browser interface.

If you have a term license that entitles you to use the system for a limited time, the system will prompt you to install its key the first time you log in via the CLI. The license counter will begin at that point. You can use the CLI as much as you like; it does not decrement the license counter.

> ⓘ If a command requires a file upload, you have two choices. You can put the file on an SSH server or you can use an SFTP tool like PSFTP or FileZilla to copy the file to Asset Manager first.
>
> If the file is on an SSH server, then you can refer to it with this syntax: **userid@sshserver:/path/to/file**. For example if the file is on a server called "xenon" and you have an account on xenon with the name "alice" and the file is in your home directory and called "license.p12", you can use "alice@xenon:/home/alice/license.p12".
>
> ```
> certificate license install alice@xenon:/home/alice/license.p12
> ```
>
> If the file is not on an SSH server, then use SFTP and your Asset Manager credentials to copy the file to the /tmp directory. Then you would use this syntax:
>
> ```
> certificate license install /tmp/license.p12
> ```

1. Log in to the CLI.
2. If you have a term license, type **certificate license install *<loginname@IPaddress:/directory/license_filename>*** at the command prompt and press **Enter** (for example, certificate asset manager install junebug@10.246.246.159:/users/junebug/Downloads/license.p12.)
3. The license installs and you are returned to the command prompt.
4. Copy and paste the UUID to an email message and send it to our support team at support@firemon.com. In response, Support will send you a message containing your license key.
5. Put the license file you receive from Support in a location that can be accessed by SSH.

The following illustrates the syntax to install an Asset Manager license via the CLI.

1. Provide the location of your license file. In the following screen capture, `admin` is the username, `connections-command-center:Desktop/` is the location of the license file, and `license.p12` is the filename of the license. For example: `connections install admin@10.9.0.240:Desktop/license.p12`
2. Type **yes** when prompted to continue. The license file loads and a confirmation message displays.

Enable/Disable Data Retention Policy

- At the CLI command-line prompt, enter **system device-persistence-policy** for the status.
- At the CLI command-line prompt, enter **system device-persistence-policy enable** to turn it on.
- At the CLI command-line prompt, enter **system device-persistence-policy disable** to turn it off

Connecting and Disconnecting Scouts

- At the CLI command-line prompt, enter **connections connect** to connect a Command Center to a Scout
- At the CLI command-line prompt, enter **connections delete** to delete a Scout connected to the Command Center

Upgrading via CLI

To upgrade to a new version of Asset Manager, or to upgrade your Scouts, use the System Upgrade

command, the syntax of which is *user@host:path/to/local/file*

- At the CLI command-line prompt, enter **certificate license install *<user@host:path/to/local /file>***
- At the CLI command-line prompt, enter **certificate license install *admin@10.9.0.240:Desktop /upgrade5443.tgz***
  Open the file you receive to execute the upgrade.

Identifying Your Installed Version

The **system version Lumeta** command is especially useful when working with Support to Identify your release.

Installing Self-Signed Certificates

If a company uses its own certificates, they'll need to make use of the `certificate ssl install` command:
certificate ssl install friendlyName admin@10.9.0.240:Desktop/copyCert.pem

Identifying Your System ID

To retrieve the full name of a Scout such as spectre32Scout:eth1, which is useful if you don't remember the full name, or want to see the IP address of your system, enter . . .

1. **system interface list**
2. Press the **Tab** key.
   The system name and interface ID displays.

Enable/Disable BGP

- collector bgp <collector name> enabled [true | false]
- collector bgp <collector name> peer new <ipaddr> [enable | disable] <password> <remote AS>
- collector bgp <collector name> peer delete <ipaddr>

Exporting Support Diagnostics

To run the /api/rest/management/system/diagnostic/export API, use the CLI command: support diagnostics file

This command will return a zip file containing:

- system configuration (same as configuration export command)
- contents of /var/log
- system "specs" file (name, uuid, Lumeta version, os version, interface config)

Adding a Superuser

Only a superuser can add or remove another user's superuser status. Multiple superusers are allowed. The last one cannot be deleted.

user superuser <userid> [true | false]

Exporting the System Configuration

This command (`system configuration export`) exports all configuration data to a remote file. To export the configuration and save the file remotely, run:
system configuration export username@hostname:<path to file>

Importing a System Configuration

This command (`system configuration import`) imports configuration data from a file you've stored locally. To import configuration from the local system, run:
system configuration import <path to file>

Using Special Characters in Names

Most symbols can be entered without any special quoting. If you want to include spaces or double quotes as part of a name, however, care must be taken. To use double quotes, enclose the entire string in double quotes and put a backslash in front of each double quote you wish to be part of the name:

- admin@cc> collector new "before\"after" Zone1 cc:eth0
- admin@cc> collector list
- before"after

To use spaces, you have two choices. Either use a backslash before each space, or enclose the entire name in double quotes:

- admin@cc> collector new with\ space Zone1 cc:eth0
- admin@cc> collector new "two words" Zone1 cc:eth0
- admin@cc> collector list
- two words
- with space

The above is true for passwords, zone names, and organization names, and with the exception of user names, anywhere you enter a free-form string. **User names cannot have special characters.**

Connecting Asset Manager Components

Use the Interface parameter in the third position to indicate the Asset Manager component to which you intend to connect (command-center, portal or scout). In addition, when you connect a command center and portal, you need to supply location information for Command Center and can optionally enter a label and icon (avatar).

From Command Center:
connections connect portal *portal_name_or_ip portal cc_lat cc_long* [*cc_label* [*user@host:path/to /cc_icon/file.png*]]
connections connect scout *scout_name_or_ip*

From Scout:
connections connect command-center *cc_name_or_ip* { **command-center** | **scout** }
 (where the final parameter is the connection initiator)

Disabling FIPS

To disable FIPS:

- system fips disable
- system reboot