

CloudVision Cognitive Unified Edge Container on CV

Table of Contents

Overview of CV-CUE on CV	1
CV-CUE HA Mode Operation	1
Key Features of CV-CUE on CV	2
Capacity of CV-CUE on CV	2
Set Up CV-CUE on CV	2
Set Up CV-CUE on a Standalone CV	2
Set Up CV-CUE on a CV Cluster	3
Enable CV-CUE on Primary Node	4
Set Up CV-CUE on Secondary and Tertiary Nodes	5
Access CV-CUE	5
CLI Access	5
UI Access	6
Key CV-CUE Operations and Directories	8
CVPI Commands for CV-CUE	8
Wifimanager Directories	9
Upgrade CV-CUE on CV	9
CV-CUE Backup and Restore	10
Backup	10
Restore	11
RMA	11
CVP CV-CUE Versions	11
Appendix: Wifimanager CLI Commands	11

CloudVision Cognitive Unified Edge Container on CV

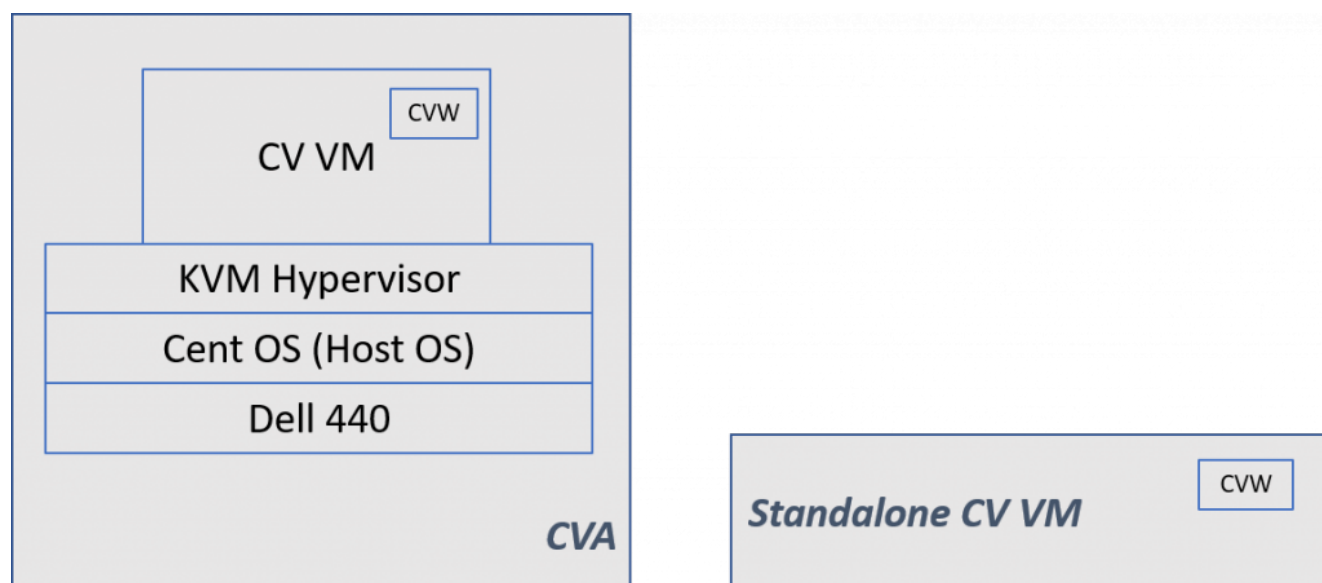
[This site will be decommissioned on October 15, 2024. All content is migrated to Arista Community Central. Visit Arista Community Central for help articles and community engagement discussions on the complete range of Arista products.](#)

The CloudVision Cognitive Unified Edge (CV-CUE) service is available as a container on the Arista CloudVision platform from its 2019.1.0/Grant release. Once you activate the CV-CUE service, you can configure, monitor, troubleshoot, and upgrade Arista Wi-Fi access points using the cognitive CV-CUE UI.

This chapter gives an overview of the CV-CUE containerization on CV and explains how to set up the service. An appendix lists the CLI commands you can run on the CV-CUE service.

Overview of CV-CUE on CV

The figure below shows a conceptual overview of the Arista CV-CUE solution.



As shown in the figure, CV-CUE is containerized within the CV—whether it's CVA (CV on a Dell appliance) or a standalone CV VM. The CV-CUE service runs on both single-node CV and CV cluster. In case of a CV cluster, CV-CUE operates as a single logical instance in HA-mode.

CV-CUE HA Mode Operation

When setting up CV-CUE for the first time, it must be enabled on all the nodes of a cluster. Once CV-CUE is enabled, then at boot time, the CV-CUE service on the primary node automatically becomes the Active instance, and the one on the secondary node becomes the Standby instance. The HA failover and

recovery mechanisms work exactly as expected—if the primary node goes down, the CV-CUE instance on the secondary node becomes active. When the primary node rejoins the cluster, a split-brain recovery kicks in and re-elects the new active and standby containers.

Key Features of CV-CUE on CV

Except for OS and kernel processes, the CV-CUE service on CV runs all the application processes required to manage Arista Wi-Fi and wireless intrusion prevention system (WIPS). Some key features of the CV-CUE service are as follows:

- CV-CUE uses ports 3851 and 161 (both UDP) for all CV communication with external entities. These ports need to be opened in your network.
- CV-CUE consists of two key components:
 - *wifimanager*, the server that manages the Wi-Fi network.
 - *aware*, the cognitive Wi-Fi UI of the server.

Capacity of CV-CUE on CV

The table below shows the number of access points (APs) that a CV-CUE container supports for the given CPU, RAM, and hard disk settings. The CPU and RAM values shown below are the default settings for a DCA-200 device; the actual capacity may vary based on deployment, environment, and load.

Setting	Up to 5000 APs
CPU	8 Core
RAM	32 GB
Hard Disk	250 GB

Set Up CV-CUE on CV

This section describes the process to set up CV-CUE on a standalone CV and on a CV cluster.

Set Up CV-CUE on a Standalone CV

CV-CUE is disabled by default. To enable CV-CUE, perform the following steps:

1. Log in to the CV admin shell via the *cvpadmin* user.
2. Press *e* to edit the settings. The CV configuration wizard is launched.
Note: If you are setting up CV for the first time, you need to enter the values for all the settings (DNS, IP addresses, etc.) in the configuration wizard. Refer to the CV setup for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to step 3.
3. Set the *CloudVision Cognitive Unified Edge Enabled* option to *Yes*, as shown in the figure below.

```

[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>e
common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: aeris_magic_12196
  CloudVision WiFi Enabled: Yes
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
  *hostname (fqdn): cvp101.sjc.aristanetworks.com
  *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
  *IP address of eth0: 172.31.0.220
  *Netmask of eth0: 255.255.0.0
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Using existing settings for new proposed network verification.

```

4. Once the cursor is at the bottom of the configuration wizard, press *a* to apply the configuration changes.

Set Up CV-CUE on a CV Cluster

A few important points about the CV-CUE service in a cluster deployment:

- CV-CUE is disabled by default.
- For a CV cluster, you first need to enable CV-CUE on the primary node and then set up the secondary and tertiary nodes.
Note: The CV-CUE service runs only on the primary and secondary nodes, but you need to apply the configuration changes to all the nodes, including the tertiary node. The CV-CUE service starts on both nodes only after the setup on all the nodes (including the tertiary node) of the cluster has been completed.
- The CV configuration wizard consists of two parts (see the figure in step 3 below):
 - *common configuration*: Settings common to all the nodes in the cluster (e.g. DNS and services such as CV-CUE).
 - *node configuration*: Settings specific to a node (e.g. Hostname and IP settings).

Enable CV-CUE on Primary Node

To enable CV-CUE on the primary node, perform the following steps:

1. Log in to the CV admin shell via the *cvpadmin* user.
2. Press *e* to edit the settings. The CV configuration wizard is launched.
Note: If you are setting up CV for the first time, you need to enter the values for all the settings (those belonging to the *common configuration* as well as the *node configuration*). Refer to the CV setup for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to step 3.
3. You can optionally assign a *CloudVision Cognitive Unified Edge HA Cluster IP*, as shown in the figure below. The CV-CUE HA Cluster IP is a virtual IP address mapped at any given time to the active CV-CUE instance in the HA cluster. It allows external entities (access points and UI consoles, for example) to access all CV-CUE Wi-Fi services using a single IP address.

```
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>e
CVP service is configured and may be running,
reconfigure may be limited to certain parameters
common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: aeris_magic_18062
  CloudVision WiFi Enabled: yes
  CloudVision WiFi HA cluster IP: 172.31.4.96
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
  *hostname (fqdn): cvp150.sjc.aristanetworks.com
  *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
  *IP address of eth0: 172.31.4.115
  *Netmask of eth0: 255.255.0.0
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Using existing settings for new proposed network verification.
```

4. Set the *CloudVision Cognitive Unified Edge Enabled* option to *Yes*, as shown in the figure above
Note:

- The CloudVision Cognitive Unified Edge HA Cluster IP must be in the same subnet as the Device Interface IPs of the primary and secondary nodes.
- The CloudVision Cognitive Unified Edge HA Cluster IP must be different from the IP addresses of the actual device and cluster interfaces.
- In absence of an HA cluster IP address, two IP addresses—those of the Primary and Secondary CV nodes—must be configured on the access points (APs) so that they may connect to the server.
- For details on how to point APs to the server, see the Access Point Configuration Guide . You can also use DHCP Options 43 and 60 to configure APs. For details on how to do that, see the DHCP Option 43 60 app note on the support portal.

5. Press *a* to apply changes.

Set Up CV-CUE on Secondary and Tertiary Nodes

To set up CV-CUE on the secondary and tertiary nodes, perform the following steps on the respective nodes:

1. Log in to the CV admin shell via the *cvpadmin* user.
2. Press *e* to edit the settings. The CV configuration wizard is launched.
Note: The *common configuration* settings are not editable on the secondary and tertiary nodes. If you are setting up CV for the first time, you need to enter the values for all the *node configuration* settings. Refer to the CV setup for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to step 3.
3. Press *Enter* until the cursor reaches the bottom of the configuration wizard, past all the settings.
4. Once the cursor is at the bottom of the configuration wizard, press *a* to apply the configuration changes.
Note: Whether *CloudVision Cognitive Unified Edge Enabled* is set to *Yes* or *No*, applying the configuration changes will cause the secondary and tertiary nodes to update their settings based on the primary node. This, in turn, will start the CV-CUE service on the primary and secondary nodes.

Access CV-CUE

You can access the CV-CUE service via the CLI or via the UI.

CLI Access

To log in to the wifimanager container using CLI, run the following command on the primary or the secondary node:

```
/cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null
```

You can then run wifimanager commands. See the Appendix for a list of wifimanager CLI commands and their descriptions.

```
[root@cvp245 ~]# /cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null
Last login: Sat Jun 29 10:30:57 UTC 2019 on pts/0

Welcome to the Server Config Shell.
Type "help" to list available commands in this shell.

Note: Bash style tabbed command completion, command
history and command line editing are supported by this
shell. This shell works best when used in full screen
mode

To configure backspace, use the 'set erase' command.
[config]$ get status
Server Mode: [Standalone]
Server Integrity Check: [PASSED]
Server Check: [OK]
Server Status: [OFF]
Database Server Status: [ON]
Web Server Status: [ON]
SSH Status: [ON]
Server Up Time: [1:07hrs]
FIPS mode: [OFF]
Full Security Mode: [OFF]
Scheduled DB Backup: [OFF]

TLS version(s) supported by Web Server: [TLSv1.2]

[config]$
```

UI Access

The URL to directly access the wifimanager UI is [http\(s\)://CVP-IP/wifi/wifimanager](http(s)://CVP-IP/wifi/wifimanager)

where CVP-IP refers to the actual CloudVision Portal (CVP) IP/domain name.

The URL to directly access the cognitive Wi-Fi UI is [http\(s\)://CVP-IP/wifi/aware](http(s)://CVP-IP/wifi/aware)

where CVP-IP refers to the actual CVP IP/domain name.

You can access CV-CUE UI by clicking on the WiFi tab in the CVP UI as shown in the figure below, or you can access it directly using one of the URLs mentioned above.

ARISTA

Devices

Events

Provisioning

Metrics

CloudTracer

Topology

Wi-Fi

All Devices > Inventory

Inventory

Compliance

Q

Device name, ID, or software version

Showing all 17 devices


Add Device

Device	Status	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
Bldg1-FLR1-AP1	<div><div></div><div></div></div>	O-105	4.18.11M	1.5.4	163.104.78.197	bf:a6:ca:e6:91:82	SPE00000
Bldg1-FLR1-AP2	<div><div></div><div></div></div>	O-105	4.20.12M	1.6.0	148.28.15.34	52:a7:80:76:15:61	SPE00001
Bldg1-FLR2-AP1	<div><div></div><div></div></div>	W-118	4.18.2F	1.6.0	182.204.107.58	9d:53:fc:ab:2d:d3	SPE00002
Bldg1-FLR2-AP2	<div><div></div><div></div></div>	C-130	4.22.0F	1.5.4	12.84.213.19	56:a0:ae:79:7b:b3	SPE00003
Bldg2-FLR1-AP1	<div><div></div><div></div></div>	O-105	4.21.5F	1.4.1	238.139.38.15	98:3c:de:97:28:91	SPE00004
DC-NY-p1r12-Core1	<div><div></div><div></div><div></div></div>	7050TX-128	4.21.5F	1.4.1	43.76.248.15	c0:84:c9:3f:aa:ff	JPE00004
DC-NY-p2r3-Edge1	<div><div></div><div></div><div></div></div>	7050T-52	4.22.0F	1.6.0	243.176.225.93	59:23:80:0c:0e:d7	JPE00002
DC-NY-p2r4-Edge2	<div><div></div><div></div><div></div></div>	7050T-52	4.21.5F	1.4.1	125.138.247.209	fa:90:4f:68:be:d0	JPE00003
HQ-Firewall	<div><div></div><div></div></div>	PAN-5050	4.22.0F	1.4.1	165.89.53.48	de:02:54:ec:26:51	PT0013
HQ-IDF1-Leaf	<div><div></div><div></div><div></div></div>	7050TX-128	4.18.2F	1.5.2	160.95.192.29	71:12:71:d5:b8:a2	JPE00005
HQ-IDF2-Leaf	<div><div></div><div></div><div></div></div>	7050T-52	4.18.11M	1.5.2	24.12.254.105	22:40:b1:42:86:83	JPE00006
HQ-IDF3-Leaf	<div><div></div><div></div><div></div></div>	7050TX-128	4.20.12M	1.6.0	209.158.19.227	49:ba:a9:e9:06:30	JPE00007
HQ-IDF4-Leaf	<div><div></div><div></div><div></div></div>	7050T-52	4.18.2F	1.5.2	137.49.10.3	d1:04:a8:bf:7a:66	JPE00008
HQ-IDF5-Leaf	<div><div></div><div></div><div></div></div>	7050T-52	4.20.12M	1.4.1	239.197.212.107	b9:4c:c1:d0:2d:70	JPE00009
HQ-MD-Spine1	<div><div></div><div></div><div></div></div>	7050S-64	4.20.12M	1.4.1	100.144.246.234	89:d2:5f:a8:d1:4f	JPE00000
HQ-MD-Spine2	<div><div></div><div></div><div></div></div>	7304	4.21.5F	1.4.1	213.220.40.68	f6:c8:14:02:1d:ad	JPE00001
HQ-OOB-Mgmt-IDF1-lab-access-restricted	<div><div></div><div></div><div></div></div>	7050S-64	4.18.2F	1.6.0	41.209.162.177	81:33:15:fc:4b:bc	JPE00011

Export to CSV

Showing 1 to 17 of 17 rows

When you access the UI for the first time, you need to apply the CV-CUE service license as shown in the figure below.



ARISTA

Activate this product by entering the license key below.
Select the license key file and press the "Apply" button.

No file chosen

For the license file, please contact Arista Technical Support at support-wifi@arista.com.

Note: Use the `ifconfig` command on the CV root shell to get the `eth0` MAC addresses of the primary and secondary CV servers (you need not access the `wifimanager` CLI for this). You need to include both these MAC addresses when you email support to request a license. One license is generated for the two (primary and secondary) MAC addresses.

Once you apply the license, you need to log in to the CV-CUE UI using the following default credentials:

Username: admin

Password: admin

You can then change the password and add other users.

Also, you can now connect Arista access points to the server.

Key CV-CUE Operations and Directories

Since CV-CUE is containerized as a service on CV, you can run some of the same CVPI commands for CV-CUE as you would for other services. For a complete list of the wifimanager CLI commands and their descriptions, see the [Appendix](#).

For details on how to configure, monitor, and troubleshoot Wi-Fi using CloudVision Cognitive Unified Edge, see the CloudVision Cognitive Unified Edge User Guide on the [Arista WiFi Support Portal](#). You can access the portal from the **WiFi – Support Portal** tile on your dashboard. For details and credentials to access the portal, contact support-wifi@arista.com.

CVPI Commands for CV-CUE

The table below lists the operations you can perform on wifimanager and the corresponding CVPI commands used.

Operation	CVPI Command
start	cvpi start wifimanager
stop	cvpi stop wifimanager
status	cvpi status wifimanager
restart	cvpi restart wifimanager
reset	cvpi reset wifimanager
backup	cvpi backup wifimanager
restore	cvpi restore wifimanager </path/to/backup/file>
debug	cvpi debug wifimanager

Note: The backup restore fails if the user running the restore command does not have access to the path where the backup file is stored.

The restart command restarts the wifimanager service, whereas the reset command resets wifimanager settings and data to factory default values. The debug command generates a debug bundle containing log files and configuration files that can be used to troubleshoot issues.

The table below lists the operations you can perform on aware and the corresponding CVPI commands

used.

Operation	CVPI Command
start	cvpi start aware
stop	cvpi stop aware
status	cvpi status aware

Wifimanager Directories

CV-CUE stores its data in docker volumes that reside under the `/data/wifimanager` directory on the CV. The table below lists the important wifimanager directories and the information they contain.

Directory on CV	Contains
<code>/data/wifimanager/log/glog</code>	Application logs.
<code>/data/wifimanager/data/conf</code>	Configuration files.
<code>/data/wifimanager/data/data</code>	System data files/directories.
<code>/data/wifimanager/data/instances</code>	Customer data files/directories.
<code>/data/wifimanager/data/pgsql_data</code>	Postgres data.
<code>/data/wifimanager/log/slog</code>	System logs.
<code>/data/wifimanager/backup</code>	On-demand backups.

Upgrade CV-CUE on CV

The CV-CUE service is upgraded as part of a CV upgrade.

In case of a CV upgrade, services go through the following steps:

1. Services or service containers (such as CV-CUE) are stopped.
2. Existing container images are deleted.
3. New component RPMs are installed.
4. The server is rebooted and all services are started again.

A service on CV is upgraded only if its version is different from the pre-upgrade version (CV stores its pre-upgrade state to decide this). The wifimanager component follows a similar process: When CV boots up after an upgrade, wifimanager starts just like other services, and it upgrades only if the CV upgrade has resulted in a new wifimanager version. Two actions precede every wifimanager start operation:

1. *load*: Loads the wifimanager container image into docker when CV boots up for the first time after an upgrade.
2. *init*: Initializes wifimanager before the start. The wifimanager init is versioned—`init-8.8.0-01`, for example. The `init-<version>` handler initiates a wifimanager upgrade if needed. Thus, if the wifimanager version has

not changed after the CV upgrade, the wifimanager upgrade is not invoked. If the wifimanager version has changed, then a wifimanager upgrade is called before its start.

Note that these actions, i.e. load and init, are internal to the wifimanager start operation; they are not run separately.

Because CV-CUE is containerized, no additional steps are required to upgrade the service.

Note: It might take a few minutes for wifimanager to upgrade. As a result, the CV-CUE service might take longer to start than other CV services.

CV-CUE Backup and Restore

We recommend that you back up wifimanager regularly and especially that you perform a backup before any upgrades.

Backup

You can backup wifimanager using the `cvpi backup wifimanager` command, as shown in the figure below.

```
[cvp@cvp101 root]$ cvpi backup wifimanager

Executing command. This may take a few seconds...
Executing command. This may take a few seconds...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
-----
COMPONENT          ACTION          NODE          STATUS
wifimanager-container backup          primary      (E) DONE
Executing command. This may take a few seconds...
[cvp@cvp101 root]$
[cvp@cvp101 root]$ exit
exit
[root@cvp101 ~]# ls -ltr /data/wifimanager/backup/
total 768
-rw-r----- 1 root root  124 Jun  7 12:01 MWM_backup_005056A0F78F_20190607120151.tgz.md5
-rw-r----- 1 root root 386177 Jun  7 12:01 MWM_backup_005056A0F78F_20190607120151.tgz
-rw-r----- 1 root root  124 Jun  7 12:55 MWM_backup_005056A0F78F_20190607125517.tgz.md5
-rw-r----- 1 root root 386171 Jun  7 12:55 MWM_backup_005056A0F78F_20190607125517.tgz
[root@cvp101 ~]#
```

Note: For a CV cluster, you can run the backup on any node but the backup is stored only on the primary node.

Manual backups are stored in the `/data/wifimanager/backup` directory and scheduled backups are stored in the `/data/wifimanager/data/data/backup` directory.

Restore

You can restore wifimanager from a backup using the `cvpi restore wifimanager </path/to/backup/file>` command, as shown in the figure below.

```
[cvp@cvp101 root]$ cvpi restore wifimanager /data/wifimanager/backup/MMM_backup_005056A0F78F_20190607125517.tgz

Executing command. This may take a few seconds...
Executing command. This may take a few seconds...
Executing command. This may take a few seconds...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
-----
COMPONENT      ACTION      NODE      STATUS      ERROR
wifimanager-container  restore    primary   (E) DONE    -
Executing command. This may take a few seconds...
[cvp@cvp101 root]$
```

Note: For a CV cluster, you can run this command only on the primary node.

If no backup was carried out before the upgrade, you can use a scheduled backup under the `/data/wifimanager/data/data/backup` directory to restore wifimanager.

RMA

For RMA or recovery issues, please contact support-wifi@arista.com.

Back up wifimanager on any node before submitting it for an RMA. When the node is re-deployed post-RMA, you can restore earlier wifimanager data from a backup that you have stored elsewhere.

CVP CV-CUE Versions

The table below shows the mapping between CVP version and the supported WM and CV-CUE versions.

CVP Release	WM Build	CV-CUE UI Build
2022.2.0	12.0.1-53	12.0.1-21
2021.3.1	11.0.1-55	11.0.1-55
2021.2.0	10.0.0-124	10.0.0-84

Appendix: Wifimanager CLI Commands

Log in to the CV admin shell via the `cvpadmin` user. To log in to the wifimanager container, run the following command on the primary or the secondary node:

```
/cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null
```

You can then run wifimanager commands.

Command	Description
db backup	Backs up the database to the specified remote server.
db clean	Cleans up resources without disrupting services.
db restore	Restores the database from a previous backup on a remote server.
db reset	Resets the database to factory defaults but maintains network settings.
get cert	Generates a self-signed certificate.
get openconfig mode	Displays current OpenConfig mode.
get cors	Displays the current status of CORS support.
get certreq	Generates a Certificate Signing Request.
get db backup info	Displays scheduled DB backup information.
get debug	Creates a debug information tarball file. This file can be used for debugging.
get debug verbose	Creates a basic debug information tarball.
get debug ondemand	Displays the debug information.
get device upgrade bundles	Displays information about device upgrade bundles available in the local repository.
get device repo config	Displays configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.
get idle timeout	Displays the current idle timeout value. A value of 0 indicates no timeout.
get integrity status	Checks the integrity of critical server components.
get ha	Displays High Availability (HA) Pair configuration and service status.
get lldp	Displays the LLDP configuration.
get remote logging	Displays the remote logging configuration.
get log config	Displays the logger configuration.
get log level gui	Displays log levels of GUI modules.
get log level aruba	Displays the log level of Aruba Mobility Controller Adapter module.
get log level wlc	Displays the log level of the Cisco WLC Adapter module.
get log level msmcontroller	Displays the log level of HP MSM Controller Integration.
get msmcontroller cert	Generates a self-signed certificate for HP Adapter.

get msmcontroller certreq	Generates a Certificate Signing Request for HP Adapter.
get access address	Shows access IP Address/Hostname of this server.
get server config	Displays complete server configuration.
get server cert	Uploads server certificate to a remote host.
get server check	Runs a server consistency check and displays results. If any fatal item fails, a failure result is recorded.
get server tag	Displays the custom tag set by the user.
get serverid	Displays the server ID.
get sensor debug logs	Uploads AP debug logs to the specified upload URL.
get sensor list	Displays the list of APs.
get sensor reset button	Displays the state of the AP's pinhole reset button.
get status	Displays the status of server processes.
get ssh	Displays the SSH server status.
get version	Displays the version and build of all the server components.
get packet capture	Captures packets on Public and HA/Management network interface(s).
set scan config	Modify AP background scanning parameters.
set openconfig mode	Enable/disable OpenConfig mode.
set cert	Installs a signed SSL certificate.
set cors	Enables or disables CORS support.
set dbserver	Starts/stops database server.
set db backup info	Sets scheduled DB backup information.
set device capability	Updates the device capability information.
set device upgrade bundles	Upload/delete device upgrade bundles in the local repository.
set device repo config	Sets configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.
set erase	Configures the backspace key.
set ha dead time	Changes the Dead Time of High Availability (HA) service.
set ha link timeout	Sets the timeout in seconds to signal Data Sync Link failure.
set idle timeout <timeout-in-minutes>	Sets the idle timeout for the command shell. A value of 0 disables the idle timeout.
set lldp	Sets LLDP configuration.
set remote logging	Sets remote logging configuration.

set log config	Sets the configuration of the logger.
set log level gui	Sets log levels of GUI modules.
set log level aruba	Sets the log level of Aruba Mobility Controller Adapter Module.
set log level wlc	Sets log level of Cisco WLC Adapter Module.
set log level msmcontroller	Sets log level of HP MSM Controller Integration.
set msmcontroller cert	Installs a signed SSL certificate for HP Adapter.
set loginid case sensitivity	Toggles login ID case sensitivity.
set server	Starts/stops application server.
set server discovery	Changes server discovery settings on given AP(s).
set server tag	Configure a custom tag for files generated by this server.
set access address	Sets access IP Address/Hostname of the server.
set serverid	Sets server ID.
set ssh	Starts/stops SSH access to the server.
set communication passphrase	Sets the communication passphrase used for AP-server authentication and to encrypt the communication between APs and the server.
set communication key	Sets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.
set communication key default	Resets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.
set sensor legacy authentication	This allows/disallows APs running on versions lower than 6.2 to connect to the server.
set sensor reset button	Sets the state of the AP's pinhole reset button (select AP models only).
set smart device oui	Add, remove MAC OUI's for specific smart device type IDs.
set webserver	Starts/stops web server.
set wlc mapper	Manage Cisco WLC Custom Mapper file.
exit	Exits the config shell session.
ping <Hostname/IP Address>	Ping a host.
reset locked gui	Unlocks Graphical User Interface (GUI) account for the "admin" user.
reset password gui	Sets Graphical User Interface (GUI) password for the "admin" user to factory default value.
upload db backup	Uploads successful DB backup(s) to an external server.
application signature update	Updates app visibility signature.

