

Cloudpath

Enrollment System

Command Reference

Software Release 5.1

April 2017

Summary: This document describes the command line interface commands available for Cloudpath from the VMware client console or an SSH login, and the specifications for logging into the command line interface. Each command table provides a description, parameters, if needed, and an example command.

Document Type: Reference

Audience: Network Administrator



Cloudpath Command Reference

Software Release 5.1

December 2017

Copyright © 2017 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2017 Ruckus Wireless, Inc. All rights reserved.

Cloudpath Command Reference

Overview

This document describes the commands that are available to manage a Cloudpath system.

After the initial setup, an administrator can log into the system using SSH on port 8022 and use the command line interface to execute Cloudpath service commands.

Note >>

You need a service password to access the command line interface. The service password is set during the initial configuration of the system.

The following sections describe the command, syntax, parameter, and provides examples for using the Cloudpath command line interface.

Cloudpath Commands

You can access the Cloudpath command line interface using SSH on port 8022 or 22. Log in to the service account (*cpn_service*) and enter the service password.

Tip >>

The default SSH port number is 8022, but can be changed to port 22 on the Cloudpath *Administration > System > System Services* page.

After a successful login to the service account, the command-line configuration utility prompt (#) displays. Enter ? to view the list of available commands.

Tip >>

From the command-line configuration utility, enter the **console** command to access the Linux shell. From the Linux shell, enter the **config** command to access the command-line configuration utility.

Command List

config commands

console command

diag commands

maintenance commands
 replication commands
 show commands
 support commands
 system commands

config commands

The **config** commands allow you to change the configuration of the system.

TABLE 1. **config** commands

Command	Description	Parameters and Examples
config	From the Linux shell, this command provides access to the command line configuration utility.	No parameters. <code>[<serviceacctlogin@<hostname>]\$ config</code>
config admin-access allow-all	Clears restrictions to the administrative functionality so that an administrator can access the Cloudpath Admin UI from any IP address.	No parameters. <code>config admin-access allow-all</code>
config admin-access restrict	Restricts which IP addresses have administrative access to the Cloudpath Admin UI.	[Comma separated list of IP addresses/CIDR] <code>config admin-access restrict 172.16.4.20, 172.16.5.18</code> or <code>config admin-access restrict 172.16.4.20/24</code>
config fips-crypto	Enable or disable use of FIPS 140-2 cryptography.	[Enable or Disable] [Requires the service password] <code># config fips-crypto enable [sudo] password for cpn_service: enterservicepwd</code>
config fips-crypto state	Display whether FIPS 140-2 cryptography is enabled.	No parameters. <code>config fips-crypto state</code>

TABLE 1. **config commands**

Command	Description	Parameters and Examples
config hostname	Sets the hostname.	[This system's network name (FQDN)] <code>config hostname</code> <code>test22.company.net</code>
config hostname-restricted allow-all	Request by IP address are not blocked.	No parameters <code>config hostname-restricted</code> <code>allow-all</code>
config hostname-restricted restrict	Requests that do not match the hostname are blocked.	No parameters <code>config hostname-restricted</code> <code>restrict</code>
config https enable	Sets whether the Apache server should be run as HTTP or HTTPS.	[The HTTPs port to use] <code>config https enable 55</code>
config https disable	Sets whether the Apache server should be run as HTTP or HTTPS.	No parameters <code>config https disable</code>
config https-servername default	Uses the system's hostname (FQDN).	No parameters <code>config https-servername default</code>
config https-servername override	Set the HTTPS server name. This is typically used when operating behind a load balancer.	[This system's network name] <code>config https-servername</code> <code>test22.company.net</code>
config network DHCP	Configures whether you want DHCP to assign network IP addresses.	[<i>true</i> to use DHCP, <i>false</i> to use STATIC IP addresses] <code>config network DHCP true</code> This command causes the system to toggle the eth0 and loopback interfaces.
config network restart	Restarts the network after making configuration changes to DHCP settings.	No parameters. <code>config network restart</code>
config network STATIC dns	Configures the STATIC IP addresses for the DNS server.	[IP address of the DNS server] <code>config network STATIC dns</code> <code>172.16.4.202</code>

TABLE 1. **config commands**

Command	Description	Parameters and Examples
config network STATIC ip	Configures the STATIC IP addresses for the system's eth0 interface, subnet mask, and gateway.	[IP address, subnet mask, and gateway for the eth0 interface] <code>config network STATIC ip 172.16.6.35 255.255.252.0 172.16.4.1</code>
config ntp	Sets the NTP server	[IP address of the NTP server] <code>config ntp 172.16.2.106</code>
config ntp sync-now	Forces an ntpdate to the configured NTP server.	[hostname for shared db] <code>config ntp sync-now</code>
config proxy set	Sets the HTTP proxy. Requires a reboot. The HTTP port and HTTPS port must be the same. This is the port number for the HTTP proxy tunnel. The [proxy-bypass-hosts] parameter (optional) is a comma-separated list of hosts that should bypass the proxy. Use <i>config clear-proxy</i> to remove the configuration.	[HTTP hostname] [HTTP port] [HTTPS hostname] [HTTPS port] [proxy-bypass-hosts] <code>config proxy hostA 80 hostB 80 hostC,hostD</code>
config proxy remove	Removes the HTTP proxy	No parameters <code>config proxy remove</code>
config ssh enable	Enables SSH access. The default port is 8022, or you can select port 22.	[SSH port] <code>config ssh enable</code> or <code>config ssh enable 22</code>
config ssh disable	Disables SSH access.	[SSH port] <code>config ssh disable</code>
config sslv3 allow	Permits SSLv3 protocol on HTTPS connections.	No parameters <code>config sslv3 allow</code>

TABLE 1. **config commands**

Command	Description	Parameters and Examples
config sslv3 block	Prevents SSLv3 protocol on HTTPS connections.	No parameters <code>config sslv3 block</code>
config timezone	Sets the timezone to be used.	[Zone name] <code>config timezone</code> This command displays a list of acceptable timezones. When prompted, enter the desired timezone as shown. <code>America/Denver</code> Alternately, you can enter the correct timezone as part of the command. <code>config timezone America/Denver</code>

console commandTABLE 2. **console command**

Command	Description
console	Provides access to the Linux shell (command line).

diag commands

The **diag** commands provide diagnostic tests for network connectivity.

TABLE 3. **diag commands**

Command	Description	Parameters and Examples
diag arp-table	Displays arp table.	No parameters. <code>diag arp-table</code>
diag dns-lookup	Performs a DNS lookup.	[IP address of the host to resolve] <code>diag dns-lookup 172.16.4.64</code>
diag interfaces	Displays network interfaces.	No parameters. <code>diag interfaces</code>
diag ping	Sends ICMP IPv4 messages to network hosts.	[IP address of the host] <code>diag ping 172.16.2.1</code>

TABLE 3. **diag commands**

Command	Description	Parameters and Examples
diag routing-table	Displays routing table.	No parameters. <code>diag routing-table</code>
diag rpm-version	Displays the current version for the rpms.	No parameters. <code>diag rpm-version</code>
diag schema-version	Displays the status of database updates	No parameters. <code>diag schema-version</code>

maintenance commands

The **maintenance** commands import or export the Cloudpath database.

TABLE 4. **maintenance commands**

Command	Description	Parameters and Examples
maintenance backup create	Create a backup file (zipped tar.gz) of the Cloudpath database and SCP it to a remote server.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] <code>maintenance backup create 172.16.4.20 22 username /home/db/file</code>
maintenance backup restore mount	Restore a backup from a locally mounted drive	No parameters. <code>maintenance backup restore mount</code>
maintenance backup restore scp	Restore a backup file from a remote server via SCP.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] <code>maintenance backup restore scp 172.16.4.20 22 username /home/db/file</code>

TABLE 4. maintenance commands

Command	Description	Parameters and Examples
maintenance backup schedule mount	Creates a recurring backup via a locally mounted drive. Note the different syntax examples for cifs and nfs drive types.	[Username for remote drive] [Path to mount] [Path within mount to backup directory] [Type of drive (cifs or nfs)] [true to merge changes into full backup, false to not merge] Syntax for cifs: <pre># maintenance backup schedule mount admin \\\\\\\\172.128.4.20\\backu p\\test servername-cifs cifs true</pre> Syntax for nfs: <pre># maintenance backup schedule mount ' ' 172.128.4.20:/backup/ servername-nfs nfs true</pre>
maintenance backup schedule scp	Creates a recurring backup via SCP to a remote server	[IP address or hostname of the remote server] [Remote port number] [Remote username] [Path to the remote system to place the backup file] [Pattern for the cron schedule] <pre>maintenance backup schedule scp 172.16.4.20 22 username /path/to /file 0 0 * * 3</pre> (Note the space between minute, hour, day, month schedule parameters.) For more information about cron schedule parameters, refer to Linux documentation.
maintenance backup unschedule mount	Removes the previously set up cron job for copying the system database to a remote server via mounted (CIFS) drive.	No parameters. <pre>maintenance backup unschedule mount</pre>

TABLE 4. maintenance commands

Command	Description	Parameters and Examples
maintenance backup unschedule scp	Removes the previously set up cron job for copying the system database to a remote server via SCP.	No parameters. <code>maintenance backup unscheduled scp</code>
maintenance cannibalize	Extract the configuration from a remote system and overwrite this system. The new system must have the same network settings as the old system, from which the database was exported. The Cloudpath uses the SSH port configured in the new system to transfer the database files.	[IP address or hostname of the remote server] <code>maintenance cannibalize 172.16.4.20</code>

replication commands

The replication commands are designed for members of the support team to use for troubleshooting. Customers would typically not be required to run these commands unless requested by the support team.

Note >>

In most cases, gathering log data through the Cloudpath Admin UI, *Collect Replication Logs* button, is sufficient for troubleshooting purposes.

TABLE 5. replication commands

Command	Description	Parameters and Examples
replication force- cleanup	Forces the removal of the replication setup.	No parameters. <code>replication force-cleanup</code>
replication replicator	Perform an operation on the replication server.	[start][stop][restart][status][offline][on line] <code>replication replicator restart or replication replicator status</code>
replication show- cluster	Displays the state of the cluster.	No parameters. <code>replication show-cluster</code>

TABLE 5. replication commands

Command	Description	Parameters and Examples
replication show-log	Show log.	No parameters. <code>replication show-log</code>
replication trepctl	Performs an operation on a service (ex. alpha, bravo, charlie).	[FQDN of the server node][service name][status/online/offline] <code>replication trepctl test23.company.net alpha status</code> or <code>replication trepctl test23.company.net bravo offline</code>
replication validate-cluster	Displays whether replication can be set up on this server. Note: This command should only be used before replication is set up.	No parameters. <code>replication validate-cluster</code>

show commands

The **show** commands display the current configuration.

TABLE 6. show commands

Command	Description
show config	Shows currently operating configuration.
show date	Shows current date.
show logs	Shows application and server logs.
show logs apache-access	Shows contents of Apache server access logs.
show logs apache-error	Shows contents of Apache server error logs.
show logs application	Shows contents of JBoss logs.
show logs config	Shows contents of config log.
show proxy	Shows HTTP proxy information.
show timezone	Shows currently configured timezone.

support commands

The **support** commands enable or disable the support tunnel.

TABLE 7. **support commands**

Command	Description
support activate-ui-recovery	Activates a temporary password, which allows you to log into the Cloudpath Admin UI with the <i>recovery</i> username. This command requires the <i>service</i> password. The recovery user credentials are only valid for 5 minutes.
support database login	Allows you to log into the database. The password for this command is only available to support staff.
support database reset-schema	Resets the status of the last database schema version.
support database schema-version	Lists the database schema version.
support database shrink	Depending on the size of the database, this operation may take some time to complete.
support database view-size	Displays the amount of data in the database.
support https restore certificate	Resets HTTPS to self-signed certificate.
support https restore ciphers-and-protocols	Resets https to default SSL ciphers and protocol.
support support-tunnel enable	Start support tunnel on port 8022.
support support-tunnel disable	Stop support tunnel.
support system apply-patches	Applies patches for the current version. The system will reboot.
support system benchmark	Perform CPU and disk IO tests.
support system clean-disk	The Cloudpath runs a clean-disk script on a schedule. This command allows an administrator to clean up the <i>jboss.log</i> manually.

system commands

The **system** commands control system operations

Note >>

If the boot password requirement has been set, you must enter a password to complete these commands.

TABLE 8. system commands

Command	Description
system reboot	Reboots system.
system restart	Restarts the JBoss and Apache servers.
system shutdown	Shuts down the system. This command requires VMware access to boot the system.
system status	Lists the status of key services (web server, firewall, NTP, RADIUS, etc.)

Recovery

Administrative UI Recovery

If you are locked out of the Cloudpath Admin UI, log in via SSH and use the **activate-ui-recovery** command from the service account. This activates a temporary password for a short time period, which allows you to log into the Cloudpath Admin UI and set up a new Administrator account, or reset a password for an existing account.

Service Account Recovery

If you are locked out of the service account, you can log in via SSH to a *Recovery* account.

Note >>

You must contact Cloudpath Networks *Support* to obtain a recovery password.

To receive a recovery password for the service account, you must provide the *System Identifier* and current *Version* on your system.

1. Log into the Cloudpath Admin UI.
2. Go to *Support > Licensing*.

- The *System Identifier* is listed in the *License Server* section.

FIGURE 1. System Identifier

The screenshot shows the 'Support > Licensing' page. It is divided into several sections: License Information, System Utilization, License Server, and Notices. The 'License Server' section contains the following information:

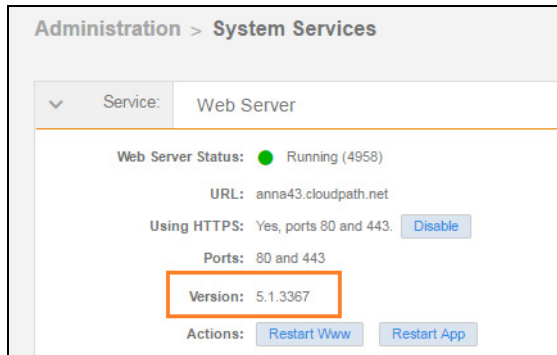
License Server:	https://bvt.cloudpath.net
Link Established:	Yes, since 20170324 1047 MDT Advanced
Customer GUID:	{e651219dd6993e2bb68afd95ddf019e39e9e433}
System Identifier:	{000000-115030E4-BF8D-389B-C7EA-4FE942A30ABC-2134023F-F668-BA8F-C237}

The 'System Identifier' field is highlighted with an orange border. The 'Notices' section includes Open Source Notices, Patent Notice, and Copyright Notice.

How To Find Your Current Cloudpath Version

The Cloudpath version is displayed in two locations.

- Go to *Administration > System Services > Web Server* service. The current build is listed in the *Version* field.

FIGURE 2. Current Cloudpath Version System Services

2. The Cloudpath version is displayed in the lower left corner of the Admin UI, and is visible on all pages.

FIGURE 3. Current Cloudpath Version Lower Left