ADMINISTRATION GUIDE

Cloudpath Enrollment System Operations Guide, 5.5

Supporting Cloudpath Software Release 5.5

Part Number: 800-72415-001 Rev A
Publication Date: 28 August 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview

This document describes how to access and manage the Cloudpath Enrollment System (ES) servers within your network. Basic operations are described in the following sections:

- System Information
- General Maintenance
- Logs
- General System Administration
- How to Import the Database From An Existing System
- Snapshots
- VM Maintenance
- Upgrades
- Reports
- Support
- Command Reference

System Information

This section provides placeholders for referencing the IP addresses and DNS information for each server in the system, as well as login information for each system.

TABLE 1 System Information

Name	IP Address	DNS
<ES1>		
<ES2>		
<ES3>		
<ES4>		

Administrative Access

Administrators can manage the system from any Cloudpath server. Web traffic (enduser, API, and OCSP) is distributed across the systems via an external load balancer.

Use the following information to log into the Cloudpath Admin UI or access the system using the console.

Interface	Login	Password
Admin UI		
Console/SSH	cpn_service	

NOTE
Use of strong passwords is recommended.

Administrator Roles

Administrator Roles

- CA Administrator - Allows full configuration access to the Administrative UI. This administrator role can manage all administrative users.
- Administrator - Allows full configuration access to the Administrative UI, except for Certificate Authorities. This administrator can manage Administrator and Viewer administrative users.
- Viewer - Allows view-only access to Enrollment, User, and Certificate records on the Dashboard, the enrollment Workflow, and the Documentation and Licensing pages. This administrator cannot manage other administrative users.

General Maintenance

SSH

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. A service password is required to access the command line interface. See Admin Access Information for details.

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

Command Reference

The Cloudpath command line uses **klish** commands under the **config** menu and **common Cent OS** commands while in the **console** menu (Linux shell).

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

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

Common Commands

When running klish commands on the system, be aware of the difference between similar commands.

For example:

- **system reboot** - Reboots the system (virtual machine).
- **system restart** - Restarts the web server (JBoss).
- **system shutdown** - Shuts down the system. **Note**: This requires VM access to boot.

Refer to the *Cloudpath Enrollment System Command Reference* for more information.

Testing Network Connectivity

The availability of the system can be monitored at various layers. At the lowest layer, the system responds to ICMP pings.

Positive Testing

The availability and responsiveness of the web server within the system may be monitored using the following URLs:

- https://HOSTNAME/enroll/ping

  This tests the enrollment portal portion of the system, and should return a 200 status.

- http://HOSTNAME/ocsp/ping OR https://HOSTNAME/admin/ocsp/ping

  This tests the admin, API, and OCSP portions of the system and should return a 200 status.

  NOTE
  The path is different for HTTPS and HTTP.

Negative Testing

The following URL may be used for negative testing:

- https://HOSTNAME/ocsp/pingFail

  This should return a 404 error.

Scripts

Use the shell script to install a given application or to perform other tasks from the Linux shell. Scripts can contain commands to be executed sequentially or can use a more complex flow of execution.

Location of script files

You can access Cloudpath scripts from the Linux shell. Scripts are located in the `/opt/cloudpath/ scripts/` directory.

Cleanup Operations

Data Cleanup

The Cloudpath system is designed to clean up old data and log files. The **Data Cleanup** page (**Administration** > **Data Cleanup**) provides the ability to schedule automatic cleanup thresholds. In most environments, the default settings for cleanup operations are adequate.

Additionally, you can clean up items using the Cleanup section at the bottom of the associated page. For example, remove authentication server data using the **Cleanup** section at the bottom of the **Modify Authentication Server** page, or clean up workflows using the **Cleanup** section at the bottom of the **Configuration** > **Workflows**, **Advanced** tab.

Welcome Page Todo Items

When you first log into the Cloudpath Admin UI, the Welcome page displays. On this page, a **Todo** Items list may exist. The Todo Items indicates system or configuration issues that should be addressed.

NOTE
Configuration and Upgrade issues should be addressed by the System Administrator.

If the Todo Item message indicates that the disk partition is almost full, you might consider removing some old wizard versions that are saved.

Remove Old Wizard Versions

A system with multiple updates may contain unused wizard versions. The **Wizard Versions on Disk** section on the **Data Cleanup** page allows you to delete extraneous wizard versions. When you delete a version from the admin UI, it removes both the tar.gz and the extracted wizard files from the `/opt/ cloudpath/work/admin/versions` directory.

Other Cleanup Operations

The Cloudpath system provides additional cleanup commands, if needed. For example:

The **support system clean-disk** command cleans up the JBoss server log.

Refer to the *Cloudpath Enrollment System Command Reference* for more information.

Firewall Settings

The Cloudpath Admin UI provides a table (**Administration** > **Firewall Requirements**) that lists the inbound and outbound traffic of your Cloudpath ES. This information is dynamically generated based on the current system configuration and can changes as the system configuration is modified.

Logs

Each system contains rolling logs, which can be reviewed for troubleshooting purposes.

Syslog

The ES web servers are configured to use a syslog as a central repository for VM and other server log messages. To view the syslog configuration, navigate to **Administration** > **System Services**, and expand the **Logs** service. The Syslog Status displays the syslog configuration information.

Other Logs

View or download additional logs from the **Logs** component. All logs can be run in **Normal** (default) or **Debug** (finer, or verbose) mode.

- **General** - The General log is the JBoss server log file, which are web application log files.
- **SCEP** - Logs related to Simple Certificate Enrollment Protocol (SCEP). The system provides an outward-facing SCEP server interface that allows SCEP clients, such as iOS, to pull certificates via SCEP.
- **OCSP** - Logs related to Online Certificate Status Protocol (OCSP), which is used for obtaining the revocation status of an X.509 digital certificate.

Additional logs are located in the `/var/log` directory from the Linux shell.

Event Logs

The Events log (**Dashboard** > **Notifications** > **Events**) displays all system events, such as account logins, enrollments, acceptance of AUPs, registrations, certificate issuance, errors, account updates, and snapshot creation.

Web Server

The Cloudpath web server is an Apache server and provides both and HTTP Access Log and an HTTP Error log. Navigate to **Administration** > **System Services**, and expand the **Logs** service.

Audit Logs

The system logs all administrative activity initiated from the Admin UI or the console. Audit log files are located in the `/var/log/jboss/admin_audit.log` directory from the Linux shell.

Network Diagnostics

The Cloudpath system logs all network activity to and from individual components of the system, including protocols used, whitelists, and packet information. Navigate to **Administration** > **System Services**, and expand the **Network** service to view or download the **Network Diagnostic** logs.

General System Administration

The ES web server **Administration** tab provides access to system-related operations.

- **Administrators** - During the initial account setup, the Cloudpath ES system sets up an administrator account using the **Company Information** provided during the setup. By default, there is also an **Administrator Group**, which allows administrative access to the Admin UI using credentials from the configured authentication server. This allows users that belong to a specific group to access the system.
- **Company Information** - Used within the URL for enrollments and sponsorships, and included in the onboard CAs.
- **System Services** - Start, stop, and restart servers, view or download log files, manage server certificates, manage SSH, open a support tunnel, and manage SMS and email services.
- **System Updates** - View and manage the Cloudpath build versions.
- **Data Cleanup** - Manage database cleanup thresholds for enrollment records, abandoned certificates, vouchers, notifications, manage wizard versions, and other system events.
- **Firewall Requirements** - Displays inbound and outbound traffic from Cloudpath to assist with firewall configuration.

How to Import the Database From An Existing System

The import database command can be used for recovery or for upgrading the system.

1. On your existing system, shut down the web service for your deployment URL to temporarily discontinue new enrollments.

   Use this command from the Linux shell:

   ```
   [ServiceAccount@AccountName ~]$ sudo /sbin/service httpd stop
   ```

2. Log into the system with the new OVA (via SSH or vCenter console) and import the database from the existing system.

3. Use the following command from the new system configuration utility:

```
# maintenance cannibalize [IP address or hostname of existing system]
```

NOTE
The new system must use the same SSH port that is configured in the old system to transfer database files.

For example:

```
# maintenance cannibalize 172.16.4.20
```

You must restart the server after you import the database.

Snapshots

In this guide we refer to snapshots as one version of the different aspects of the system. There are two kinds of snapshots that you need to become familiar with:

- Configuration snapshots, which are snapshots of the Cloudpath workflow configuration.
- VMware snapshots, which preserves the state and data of a virtual machine at a specific point in time.

Configuration Snapshots

A configuration snapshot is a version of a workflow configuration. You can create and maintain multiple versions of each configuration. However, only one snapshot can be active at a time for each deployment location.

NOTE
Each time the workflow configuration changes, you must create another workflow snapshot.

1. Create a configuration snapshot from the Cloudpath Admin UI, **Configuration** > **Workflow** > , **Snapshots** tab.
2. Click the **Publish** button.

VM Maintenance

Cloudpath supports both VMware and Hyper-V deployments. See the appropriate sections below for tips on VM and Hyper-V maintenance.

VMware Snapshots

A VMware snapshot is a version of a VM at a specific point in time. As a best practice, it is recommended that you take a VM snapshot of your deployment before making any changes to the system.

To create a VMware snapshot:

1. From the virtualization software client (VMware vSphere Client), select your virtual image, right click and select **Snapshot** > **Take Snapshot**.
2. Enter the **Name** and **Description** of the snapshot. Provide enough details in the **Description** so that other administrators can understand what is in each snapshot.
3. Select **Snapshot machine's virtual memory**.

4. (Optional) If VMware Tools is installed, you can also select **Quiesce guest file system** to pause running processes before you take a snapshot.

How to Increase the Virtual Appliance Memory on VMware

Use these instructions to change the memory configuration of a virtual machine's hardware. The VM must be powered off to edit memory settings.

1. From the vCenter client, power off the virtual appliance.
2. Select the VM, and right-click to **Edit Settings**.
3. With the **Hardware** tab selected, select **Memory**.
4. On the right window pane, increase the **Memory Size**.
5. Click **OK**.
6. Power on and reboot the VM.

How to Expand the MySQL Partition Size

Use these instructions to expand size of the partition used for MySQL database operations.

From the vCenter Client:

1. With the VM running, select the VM and right-click to **Edit Settings**.
2. With the **Hardware** tab selected, select **Hard disk 2**.
3. On the right pane, in the **Disk Provisioning** section, increase the **Provisioned Size** to the desired size and click **OK**.

   If the **Provisioned Size** cannot be selected, try restarting the server using the **sudo halt** command.

Hyper-V Checkpoints

A Hyper-V checkpoint is a version of a VM at a specific point in time. As a best practice, it is recommended that you create a VM checkpoint of your deployment before making any changes to the system.

To create a Hyper-V checkpoint:

1. From the Hyper-V Manager, select your virtual machine, right click and select **Checkpoint**.
2. The Hyper-V Manager creates a checkpoint with the current timestamp.
3. Use the bottom right menu to rename, export, or revert checkpoints.

How to Increase the VM memory on Hyper-V

Use these instructions to change the memory configuration of a virtual machine's hardware. The VM must be powered off to edit memory settings.

1. From the Hyper-V Manager, select your virtual machine, right click and select **Settings**.
2. Select **Memory** from the **Hardware** section on the left pane.
3. Increase the RAM, as needed.
4. Click **OK**.
5. Power on and reboot the VM.

Upgrades

NOTE
Under normal conditions, upgrades are not a part of daily operations. Please contact the network administrator or the Cloudpath support team before attempting to upgrade your system.

Upgrade for Local Deployment

NOTE
Certain upgrades, such as those with major operating system changes, require a database import instead of a System Update. Refer to the release notes for your upgrade version for instructions.

There are two methods for upgrading your Cloudpath ES virtual appliance.

- Update your existing system from the ES Admin UI (**Administration** > **System Updates**).
- Set up a virtual appliance using the new OVA and import the database from the existing system.

NOTE
For upgrade instructions, refer to the *Cloudpath Enrollment System Upgrade Guide*.

Reports

Records Export

Enrollment and User data can be can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

Use the CSV Export icon  or XLS Export icon  located at the bottom of any table in the Dashboard.

The Enrollment and User export files are designed to be a quick view of the activity since midnight. To export only certain items in the table, for a specific date and time, or to export items for a longer time period, see Scheduled Reports.

Scheduled Reports

The scheduled report feature allows you to schedule a task to export enrollment record data, by date, or schedule a recurring export. For example, you might schedule an enrollment data report to occur on a weekly, or daily basis. This report can be emailed to one or multiple email addresses.

You can schedule multiple reports. For example, you can create a report that emails an enrollment record report based on enrollments with revoked certificates, and another based on issued certificates.

To schedule a task, go to **Dashboard** > **Notifications** > **Scheduled Reports**.

The enrollment record data is emailed, as a CSV file, to the specified address, at the scheduled frequency.

You can also download an interim report from this page.

Support

Documentation

Refer to the **Support** > **Documentation** page in the Cloudpath Admin UI for documentation and links that cover all aspects of the system, from setup to configuration and system administration.

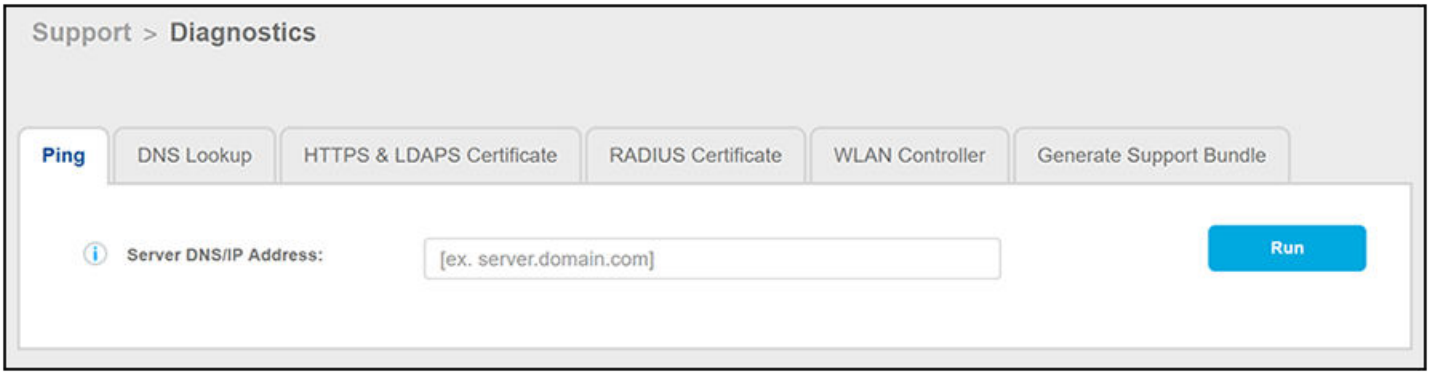
Support Tunnel

The Support Tunnel component allows you to open a support tunnel to help you in diagnosing issues with your application or configuration. If requested by a Support Team member, you might be required to enable a support tunnel from the **Administration** > **System Services** > **Support Tunnel** page.

Diagnostics

The Diagnostics page (**Support > Diagnostics**) provides useful tools for system troubleshooting connectivity issues and for verifying certificate information.

FIGURE 1 Cloudpath Connectivity Diagnostics



The diagnostics include:

- Ping: Ping an IP address or hostname
- DNS Lookup: Provide server information and IP address for a given hostname.
- HTTPS & LDAPS Certificate: Query the server certificate used by a secured server (such as HTTPS or LDAPS) to verify the certificate currently in use by a server.
- RADIUS Certificate: Query the RADIUS server certificate and the chain presented by the RADIUS server. This is useful to verify the certificate currently in use by a RADIUS server. For this test to work, Cloudpath must be able to reach the IP and port, the shared secret must be correct, and Cloudpath must be an approved client for the RADIUS server.
- WLAN Controller: Query the WLAN controller to check if required ports are accessible.
- Generate Support Bundle: Click **Run** from this tab to generate a zip file that contains log files and metrics information to provide to your Ruckus support representative.

Support File

If support has provided a support file, you can upload it from the **Support** > **Upload Support File** page. This will make changes to the system, so be sure to create a VMware snapshot first.

Password Recovery

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

If you are locked out of the service account, you can log in via SSH to a Recovery account. However, you must contact Cloudpath Networks Support to obtain a recovery password.

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

How To Find Your System Identifier

1. Log into the ES Admin UI.
2. Go to **Support** > **Licensing**, **License Server** section for the system identifier.

How To Find Your Current ES Version

1. Go to **Administration** > **System Services** > **Web Server**.
2. Under Web Server Status, the current build is listed in the **Version** field.

Command Reference

For all Cloudpath commands, syntax, and descriptions, see the *Cloudpath Enrollment System Command Reference*.

Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com