RUCKUS
COMMSCOPE

Cloudpath® Enrollment System Release Notes for Release 6.0R1

Supporting Cloudpath Software Release 6.0R1

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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Document History

Version	Summary of Changes	Publication Date
Cloudpath Enrollment System Release Notes 6.0 Revision A	• Enhancements • Resolved issues	September 2024

Contact Information, Resources, and Conventions

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://community.ruckuswireless.com

- Knowledge Base Articles—https://support.ruckuswireless.com/answers

- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid

- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number

- Document part number (on the cover page)

- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0

- Part number: 800-71850-001 Rev A

- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	device(config)# interface ethernet 1/1/6

TABLE 1 Text Conventions (continued)

Convention	Description	Example
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Document

The *Cloudpath Enrollment System (ES) Release Notes* contain information about new and updated features, system updates, bug fixes, and known issues.

For the latest versions of Cloudpath manuals, go to one of the following sites:

- https://support.ruckuswireless.com/

- https://docs.commscope.com

New Features, Enhancements, and Behavior Changes

This section lists the new features, enhancements, and changed behavior in this release.

New Features and Enhancements

- Increased visibility on usage counts of the Cloudpath provided **Onboard via Cloud** SMS sending service.
- SSH host keys can now be manually regenerated via the command-line interface (CLI) or web-based administrator interface.
- Integrated systems such as Palo Alto Firewalls now support filtering RADIUS Accounting traffic forwarded by the **NAS-ID** RADIUS attribute.
- Workflow "redirects" via HTTP POST now support Enrollment Variable replacements.
- When integrating with Microsoft Intune via SCEP, a new option allows the inclusion of the first user principal name (UPN), uniform resource identifier (URI), email, and DNS subject alternative name (SAN) attributes from the Simple Certificate Enrollment Protocol (SCEP) request to the issued certificate.

Changed Behavior

- The HTTP Strict Transport Security (HSTS) HTTP server header option is now enabled for new installations by default.
- To facilitate mitigation of the Blast-RADIUS vulnerability (CVE-2024-3596), each RADIUS client configuration now supports requiring the **Message-Authenticator** RADIUS attribute.
- The RADIUS Attribute wire format for the **NAS-Filter-Rule** attribute now follows the format defined by **RFC 4849**. Use with non-compliant switches may require switching to a similar vendor-specific **NAS-Filter-Rule** attribute instead.

Resolved Issues

Following are resolved issues for this release of the product.

- DPSK pools now indicate that they cannot be removed when in-use by an enrollment workflow. Previously, attempting remove a pool in this state resulted in non-friendly error.
- Resolved the issue where the "Header Topbar/Ribbon Transparency" option in the Admin UI did not render correctly.
- Resolved the issue where the system SSH host key was insecure.
- Resolved the issue where specific time periods, such as "Weeks Before", certificate expiration email warnings did not function correctly.
- Use of "remove existing certificates" workflow step in conjunction with enrolling users that have large number of "concurrent certificates" can result in extremely high system CPU usage.
- Fixed the issue that if Multi-Factor Authentication (MFA) was enabled for administrators, "SmartZone Network Segmentation" integration became inoperable.
- Resolved issues with getting a "Page not found" message while configuring TACACS.
- Resolved the issue where COA Attributes defined for RADIUS client configuration did not save correctly.
- RADIUS clients now indicate that they cannot be removed when in-use by a Policy. Previously, attempting to remove a RADIUS client in this state resulted in non-friendly error.
- The Cloudpath RADIUS server now supports mitigation of published "Blast-RADIUS" vulnerability (CVE-2024-3596). Please note that the RADIUS Client configuration option "Require Message-Authenticator" must be manually enabled to fully mitigate this potential

vulnerability. This option should be enabled once administrators confirm that the integrated RADIUS infrastructure always includes the Message-Authenticator RADIUS attribute with all authentication requests.

Upgrade Information

Upgrading From Cloudpath Version 5.12.5614 or Earlier

To upgrade from Cloudpath version 5.12.5614 (or earlier) to version 6.0, a new virtual machine image is required. In-place upgrades through the Admin UI are not supported for this transition. However, a utility is provided to streamline the migration of configuration and data from your existing 5.x system to the new 6.x virtual machine.

To update from version 5.12.5614 or earlier, you must perform the following steps:

1. Download the new virtual machine image of Cloudpath ES 6.0.**5816** relevant to your hypervisor (.ova, .qcow2, .vhdx, and so on).

    > **NOTE**
    > Note that a new license key or activation code is not required. The licensing information will be imported from your existing system.

2. Install and deploy the new virtual machine to your hypervisor.

3. In the initial CLI-based setup for the new VM, provide a temporary IP address and network settings that can reach the existing system.

4. Use the following command on the new virtual machine to import information from the existing system to the new system:

    ```
    system:# maintenance cannibalize [existing-system-hostname-or-IP]
    ```

5. The **maintenance cannibalize** command will prompt for SSH credentials for the **cpn_service** account on the existing system and copy and port data from the existing system.

6. At the end of the process, accept the prompt to have the system automatically move the IP address to the new system.

7. The prior existing system will automatically shutdown, the new system will boot and assume the IP address. For more information about how to perform a "cannibalize" import for upgrades, refer to the *Cloudpath Enrollment System Upgrade Guide*.

Minimum Wizard Version

The Cloudpath server requires a minimum version of the wizard.

When performing a system update from the Admin UI or by using database import, the system automatically updates your Cloudpath wizard to the appropriate version.

Snapshots

When upgrading your system, all previous snapshots will remain in the system, will be labeled not compatible, and will not be selectable for active snapshots.

As part of the upgrade process, a new snapshot is created with the latest wizard build. This automatic snapshot creation allows the system to be fully updated and usable when the upgrade is finished.

Upgrading a Cluster to 6.0

To upgrade your cluster to version 6.0, you must deploy new VMs, as follows:

> **NOTE**
> When you first activate a new system, you are presented with a **System Setup** screen that contains the question: "Which Type Of Server is This?" For the node that will serve as your primary node in the cluster, select the **Standard Server (Default)** option. For the node that will serve as your secondary server, select the **Add On Server For Cluster** option.

1. Deploy two new .OVAs as virtual appliances by following the instructions in either the *Deploying Cloudpath as a Virtual Appliance on a VMware™ Server, Release 5.2* or *Cloudpath Enrollment System Deploying Cloudpath as Virtual Appliance using Microsoft Hyper-V, Release 5.2* document, as applicable.

2. Disable the replication service on all current cluster nodes by following the instructions in the *Setting Up Clustering With Cloudpath Servers* guide, 5.2 (or earlier).

3. Import the database from the old primary node to the new primary node using the command-line configuration utility (**klish** command) of the new OVA system:

   ```
   #maintenance cannibalize [oldsystemhostname]
   ```

   > **NOTE**
   > For more information about how to perform a database import for upgrades, refer to the *Cloudpath Enrollment System Upgrade Guide*.

4. After the import is finished, you can accept the prompt to have the system automatically move the IP address to the new system and shut down the old system.

5. Configure the new secondary node to match the network settings of the old secondary node.

6. Once all the nodes have been upgraded, follow the steps in the applicable section of the *Cloudpath Enrollment System Replication Configuration Guide*, Version 5.6 or later, to recreate your cluster:

   > **NOTE**
   > Before you run the **replication setup** command, be sure you have activated both nodes.

   - "Configuring an Active - Standby Replication"
   - "Configuring an Active - Active Replication"