RELEASE NOTES

Cloudpath Enrollment System Release Notes for Release 5.6.4580

Supporting Cloudpath Software Release 5.6

Part Number: 800-72488-001 Rev A
Publication Date: 15 December 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

Document History

Version	Summary of changes	Publication date
Cloudpath Enrollment System Release 5.6.4580 Version 1	• New features • Enhanced features • Resolved issues	December 16, 2019

Preface

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`
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 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.

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.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

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.ruckuswireless.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://forums.ruckuswireless.com/ruckuswireless/categories
- 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.

About This Document

This document describes the Cloudpath Enrollment System (ES) release notes for all public releases, including new and updated features, system updates, bug fixes, and known issues. This document includes all release notes for all 5.x versions.

NOTE
For the latest versions of Cloudpath manuals, go to: https://support.ruckuswireless.com/

New in This Release

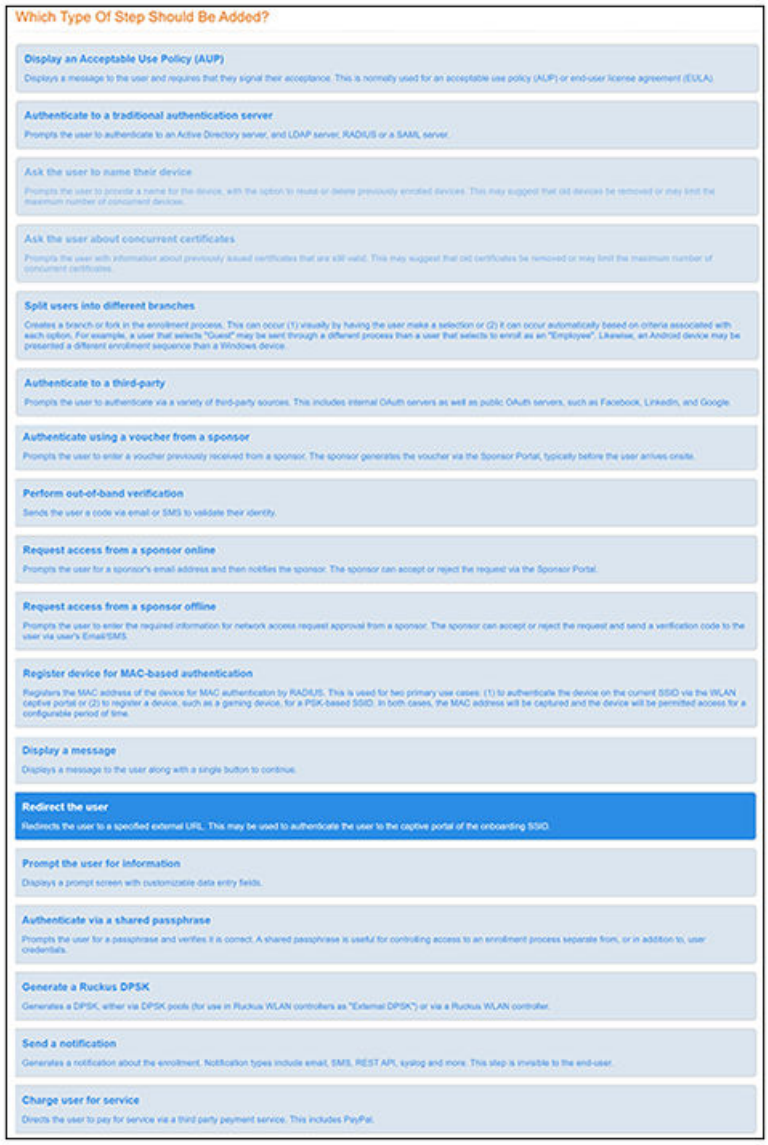
New Features in Release 5.6.4580

- **New workflow plug-in: Request Access From a Sponsor Offline**: This plug-in allows users to request network access from a sponsor, and then, if approved by the sponsor, the activation code is sent to the user via email or text message. This allows the user to remain offline while awaiting approval.

  NOTE
  The plug-in called "Request Access From a Sponsor *Online*" is the same plug-in that was named "Request Access From a Sponsor" in prior releases.

  For information about how to use each of these plug-ins, refer to the *Cloudpath Enrollment System Deployment Administration Guide*.
- **REST API v2**: New APIs have been created for use with External DPSK (eDPSK). You can use these APIs to create DPSK pools and individual DPSKs using POST calls, as well as to retrieve information (using GET), edit these resources (using PUT), and delete resources (using DELETE), For more information, refer to the new *Cloudpath Enrollment System REST API v2 User Guide*.
- **Workflow "Plug-In" buttons**: You can now click once to add a particular plug-in to your workflow instead of having to click a radio button and then click "Next." The new plug-in screen and its choices are shown in the figure below:

FIGURE 1 Buttons to Add Workflow Plug-Ins



- **Multiple certificate chains are now allowed on Android** versions that support this feature.
- **The Linux key ring can be used to store passwords**. After the device configuration has been performed, go to **Configuration > Device Configurations**, click the arrow next to the desired device configuration to expand the view, then click the **OS Settings** tab. From there, you can scroll to "Linux Settings," click **Add Settings**, then scroll to "General Settings." From there, you can enable the "Store passwords in the key ring" field.

Enhanced Features in Release 5.6.4580

This release contains the following enhancements:

- **Auto VLAN**:
  - In the UI, you can navigate to **Dashboards > VLAN Assignments** for newly provided information about VLANs available, assigned, users for each VLAN, and so on.
  - Auto VLAN can now be used with eDPSK. For information on how to use Auto VLAN, refer to the "Auto VLAN" chapter of the *Cloudpath Enrollment System Deployment Administration Guide*
- **DPSK "Override Reauthentication" configuration field**: When creating a new DPSK, you can now override the Reauthentication period that is set at the DPSK pool level. For more information, refer to the *Cloudpath Enrollment System eDPSK Configuration Guide*.
- **WPA-3 support**: In addition to WPA2, the following types of network authentication are supported for an SSID:
  - WPA3-Enterprise: This is the WPA3 version of WPA1-Enterprise and WPA2-Enterprise. WPA3-Enterprise uses IEEE 802.1X authentication, such as PEAP or EAP-TLS. The network requirements are the same as for a WPA2 enterprise infrastructure, as listed in the "WPA2-Enterprise Infrastructure" section of the *Cloudpath Enrollment System Deployment Administration Guide*.
  - WPA3-Personal (SAE): This is the WPA3 version of WPA1 and WPA2 PSK. A shared key is used to authenticate to the network. In WPA1 and WPA2, this was also known as WPA1-Personal or WPA2-Personal. If you decide to use WPA3-Personal in this release, be sure that your wireless equipment and devices support WPA3-Personal.
  - WPA3-OWE (Opportunistic Wireless Encryption) This type of WPA3 network is intended to replace an open/unencrypted network.
  - WPA3-Enterprise Preferred, WPA2-Enterprise Acceptable: If the NIC supports WPA3, WPA3-Enterprise is used. Otherwise, WPA-2 Enterprise is used.
  - WPA3-Personal Preferred, WPA2-Personal Acceptable: If the NIC supports WPA3, WPA3-Personal is used. Otherwise, WPA2-Personal is used.

    NOTE
    Some of these options are not available until you have already configured a WPA-2 network. Then, if you want to change to one of the WPA-3 network authentication methods, you need to go to the following location in the UI: **Configuration > Device Configurations**, then click the arrow to expand the desired configuration, then click the **Network(s)** tab, then click the pencil icon next to the name of the already-installed network. Next, when you are presented with the Network Information page, use the Network Authentication drop-down to make your selection, then click **Save**.
    Also, note that, if you change to WPA3, the available encryption options change. Whatever encryption methods you select in the Cloudpath UI also must be configured on the controller or the AP. Additionally, the "802.11" authentication method (not to be confused with the "802.1X/EAP" authentication method) needs to match the values configured in the Cloudpath UI.

  Operating Systems That Support WPA3:

  - Windows 10 (with WPA3-SAE only) with the following constraints: The wireless card must indicate support for WPA3-SAE networks. Attempting to configure a WPA3-SAE network on a Windows 10 machine that does not have a wireless card and driver that support WPA3-SAE results in a configuration failure.
  - mac OS 10.15 (with WPA3-SAE only) with wireless cards and drivers that support WPA3-SAE.
  - iOS 13 and iPadOS 13 (with WPA3-SAE only) with wireless cards and drivers that support WPA3-SAE.
  - Android 10 (but not yet supported by Cloudpath)

Additional Information for Release 5.6.4580

- **Several Android administrative settings have been removed** from the UI because they are no longer supported on the client. The settings in question are those that are set by navigating to **Configuration > Device Configurations**, clicking the arrow next to an existing device configuration to expand the view, then clicking the **OS Settings** tab. From there, you can scroll to "Android Settings," click **Add Settings**, then scroll to "Behavior Settings." This is where the following options used to exist but have now been removed:
  - Use 'password' to install certificates when a password is needed
  - Failing to get a TLS certificate goes to the failure screen
  - Do not use keystore workarounds
  - Do not use the local keystore
  - Allow devices that can't use certificates
- Android 6.0 devices do not support multiple Root CAs.
- Cloudpath video tutorials are available on youtube for many Cloudpath topics. For more information about what is available, see the *Cloudpath Enrollment System Quick Start Guide*, "Cloudpath Video Tutorials" section.

Known Issues in Release 5.6.4580

There are no known issues in this release.

Resolved Issues in Release 5.6.4580

- An issue where an individual-DPSK VLAN override was not working if there was a VLAN ID in the DPSK pool has been resolved.
-
- Deleting an enrollment that has an associated DPSK is no longer generating an unfounded generic SQL error message.
- An issue has been resolved in which a device was being deleted from a DPSK pool, but the device count was not decrementing nor disassociating from the respective WLAN.
- JBoss/Wildfly is now booting properly even with a restricted outgoing-internet condition.

Upgrade Information

How to Upgrade to Cloudpath Version 5.6.4580

The process you follow to upgrade to version 5.6.4580 depends on which version you are currently running.

Follow the steps in the applicable section(s).

Upgrading From Cloudpath Version 5.4.4284 or Later

If you are updating from Cloudpath Version 5.4.4284 or later, navigate to **Administration > System Updates**, then proceed to download and install the update.

Upgrading From Cloudpath Version in the Range 5.2.3585 to 5.4.4270

If you are updating from Cloudpath Version in the range of 5.2.3585 to 5.4.4270, navigate to **Administration > System Updates**. You must first download the support patch that is displayed on the screen and install the patch on the **Support > Upload Support File** page. After the system reboots, return to **Administration > System Updates** and proceed to download and install the update.

Upgrading From Cloudpath Version in the Range 5.0.3314 to 5.1.3483

To update from versions in the range of 5.0.3314 to 5.1.3483, you can use one of two methods.

The *first* method is to incrementally upgrade to a 5.2 series version, then to subsequently upgrade from 5.2 to 5.6. The incremental upgrade is time consuming and only recommended if deploying a new VM/OVA is not possible in your infrastructure.

1. Upgrade to any 5.2 series version by following the instructions in these release notes for upgrading to the desired 5.2 build.
2. Upgrade to 5.6.4580 by following the instructions in the preceding section called "Upgrading From Cloudpath Version in the Range 5.2.3585 to 5.4.4270."

The *second* method, which is a faster method but requires deploying a new OVA, is to do the following:

1. Deploy a new 5.6.4580 OVA.
2. Import the database from the existing system from the command-line configuration utility (**klish** command) of the new OVA system:

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

3. 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.

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

Upgrading From Cloudpath Version 5.0.3302 or Earlier

To update from version 5.0.3302 or earlier, you must perform the following steps:

1. Deploy a new 5.6.4580 OVA.
2. Import the database from the existing system from the command-line configuration utility (**klish** command) of the new OVA system:

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

3. 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.

For more information about how to perform a database 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 5.6.4580

The process you follow to upgrade your cluster to version 5.6.4580 depends on which version you are currently running and on your infrastructure.

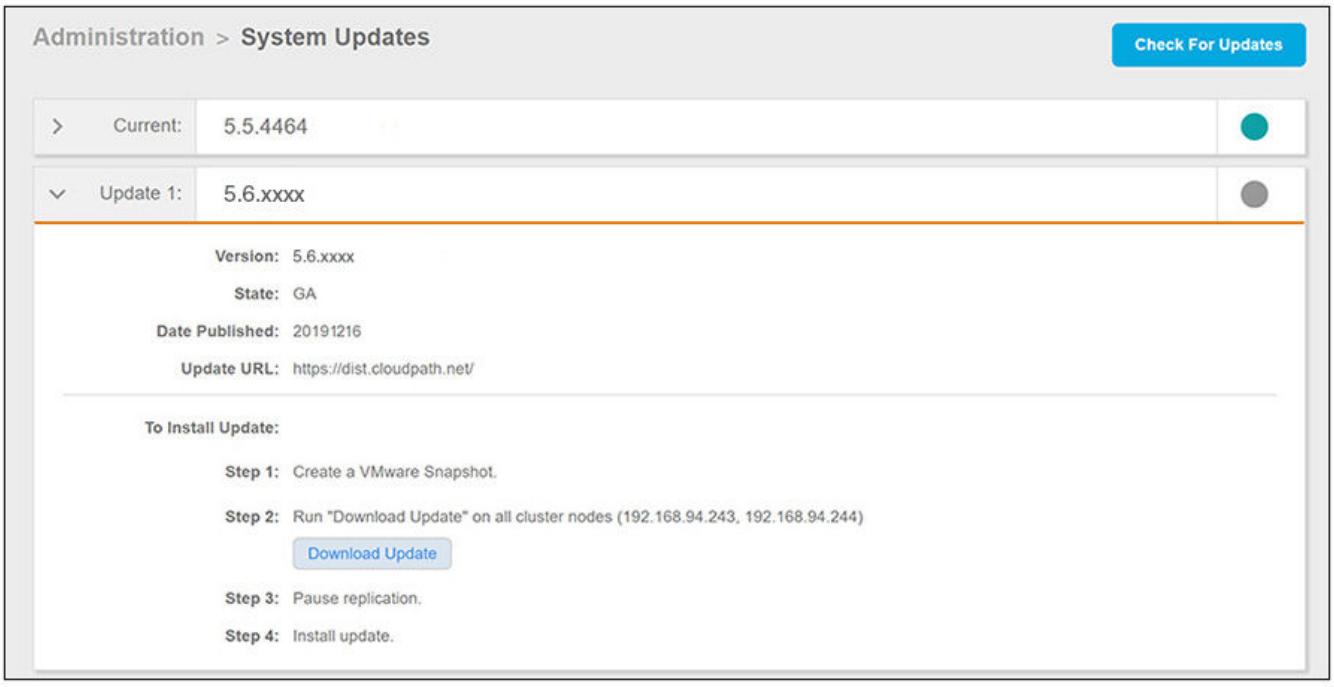
Follow the steps in the applicable section(s).

Upgrading a Cluster to 5.6.4580 from 5.5.4464

If your cluster is already running 5.5.4464, follow the steps below to upgrade the cluster to 5.6.4580:

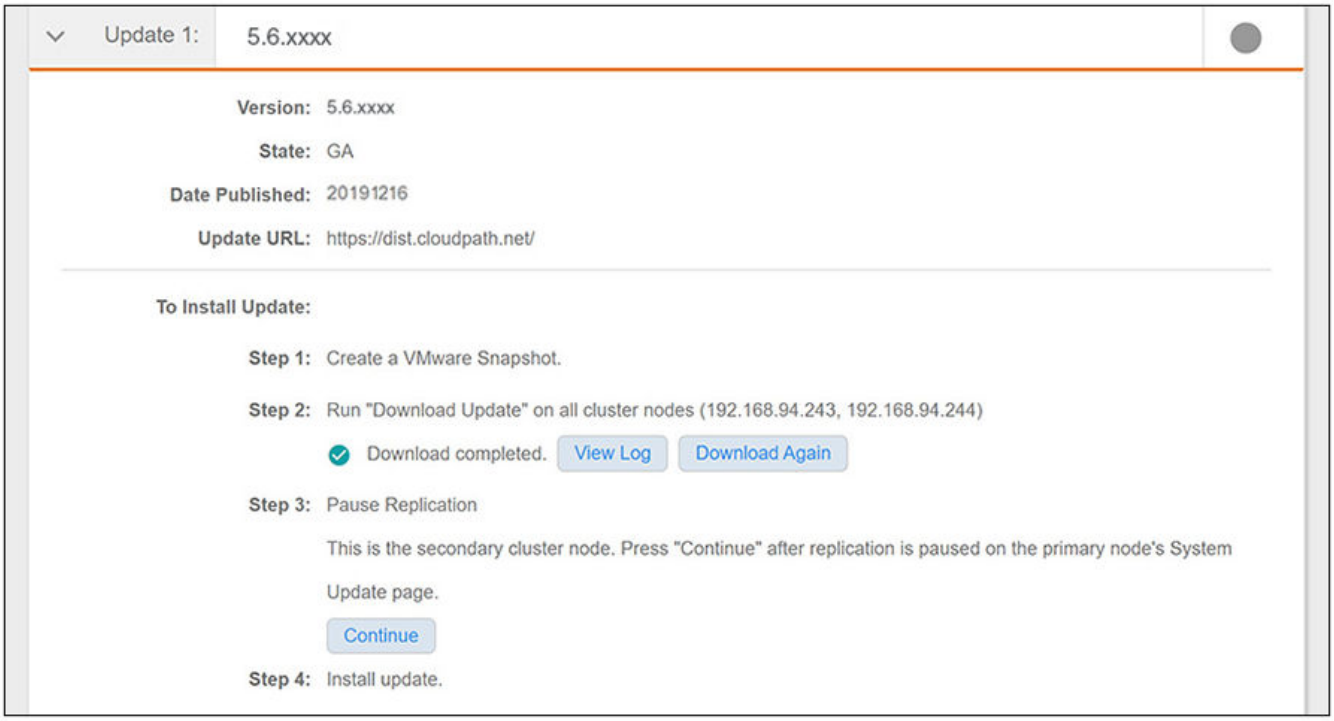
1. From the Cloudpath UI on the primary node in your cluster, navigate to **Administration > System Updates**. A screen such as the following indicates that there is a newer build (the build number is xxxx only for the purpose of the illustration) to which you can upgrade your cluster:

   FIGURE 2 System Updates Screen for Upgrading a Cluster From 5.5.4464 to 5.6.4580



2. Create a VMWare Snapshot of the primary node.
3. Click the **Download Update** button on the primary node.
4. From the Cloudpath UI on the secondary node in your cluster, navigate to **Administration > System Updates**.
5. Create a VMWare Snapshot of the secondary node.
6. Click the **Download Update** button on the secondary node.
7. Return to the UI on the primary node, and pause replication.
8. On the secondary node, click **Continue** (see Step 3 in the following screen):

FIGURE 3 Secondary Node Updates Screen Before Pressing "Continue" Button



NOTE
Proceed with the cluster system updates in the following order: Secondary node *must be updated first*, then the primary node.

9. On the secondary node, click **Install Update**.

   NOTE
   The Admin UI on the secondary node is unavailable during the upgrade. However, you can use the Klish commands (refer to the *Cloudpath Enrollment System Command Reference, 5.6*) to determine when the secondary node reboot is complete. Then, proceed with the system update on the primary node.

10. On the primary node, click **Install Update**. The system will be unavailable for several minutes during the upgrade.

    NOTE
    Once the primary node completes the upgrade, both cluster nodes are accessible through the Admin UI. You can log in to the Admin UI on both systems to verify the system upgrades.

Upgrading a Cluster to 5.6.4580 from 5.2 or Earlier

NOTE
As of release 5.5.4464, two-node clusters are supported.

Two upgrade procedures are provided in this section to upgrade your cluster from 5.2 or earlier to 5.6.4580:

- Upgrading by deploying two new virtual machines. This is the recommended method, as long as you do not have constraints on the number of VMs in your environment.
- Upgrading without creating new virtual machines.

Upgrading Cluster by deploying new VMs:

> **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 VMWare or Hyper-V deployment guides, 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 from 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, 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"

Upgrading Cluster Without Deploying New VMs:

> **NOTE**
> This method is more complex and creates more system downtime than the preferred method described above where you deploy new VMs.

1. 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).
2. Upgrade each node to the new version via the **Administration > System Updates** page by following the instructions given on that page.

   > **NOTE**
   > If your current version is older than 5.2, you first need to upgrade all nodes to any 5.2.xxxx version by following the instructions in these release notes for upgrading to the desired 5.2 build.

3. 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, to recreate your cluster:
    - "Configuring an Active - Standby Replication"
    - "Configuring an Active - Active Replication"

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