

# Cloudpath Enrollment System Release Notes for Release 5.12 R6 (5.12.5584)

**Supporting Cloudpath Software Release 5.12R6**

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## 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](http://www.cs-pat.com).

# Contents

---

<b>Document History</b> .....	<b>5</b>
<b>Contact Information, Resources, and Conventions</b> .....	<b>7</b>
Contacting RUCKUS Customer Services and Support.....	7
What Support Do I Need?.....	7
Open a Case.....	7
Self-Service Resources.....	8
Document Feedback.....	8
RUCKUS Product Documentation Resources.....	8
Online Training Resources.....	8
Document Conventions.....	9
Notes, Cautions, and Safety Warnings.....	9
Command Syntax Conventions.....	9
<b>About This Document</b> .....	<b>11</b>
<b>New Features</b> .....	<b>13</b>
<b>Enhancements</b> .....	<b>15</b>
<b>Resolved Issues</b> .....	<b>17</b>
<b>Known Issues</b> .....	<b>19</b>
<b>Upgrade Information</b> .....	<b>21</b>
How to Upgrade to Cloudpath Version 5.12.5584.....	21
Upgrading From Cloudpath Version 5.7.4732 or Later.....	21
Upgrading From Cloudpath Version 5.6.4652 or 5.6.4580.....	21
Upgrading From Cloudpath Version 5.5.4464.....	21
Upgrading From Cloudpath Version in the Range 5.2.3585 to 5.4.4284.....	22
Upgrading From Cloudpath Version in the Range 5.0.3314 to 5.1.3483.....	22
Upgrading From Cloudpath Version 5.0.3302 or Earlier.....	23
Minimum Wizard Version.....	23
Snapshots.....	23
Upgrading a Cluster to 5.12.5584.....	23
Upgrading a Cluster Containing More than Two Nodes to 5.12.5584 from 5.7.4774 or Later.....	23
Upgrading a Two-Node Cluster to 5.12.5584 from 5.7.4774 or Later.....	24
Upgrading a Cluster to 5.12.5584 from 5.6.4652, 5.6.4580, or 5.5.4464.....	25
Upgrading a Cluster to 5.12.5584 from 5.2 or Earlier.....	27



# Document History

---

Version	Summary of changes	Publication date
Cloudpath Enrollment System Release Notes 5.12.TBD.Revision A	<ul style="list-style-type: none"><li>• New features</li><li>• Resolved issues</li><li>• Enhancements</li></ul>	December 15, 2023



# Contact Information, Resources, and Conventions

---

- [Contacting RUCKUS Customer Services and Support](#)..... 7
- [Document Feedback](#)..... 8
- [RUCKUS Product Documentation Resources](#)..... 8
- [Online Training Resources](#)..... 8
- [Document Conventions](#)..... 9
- [Command Syntax Conventions](#)..... 9

## 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](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](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](mailto:#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	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> 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
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	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, <i>member[member...]</i> .
\	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

---

Following are new features for this release of the product.

- The Onboarding Workflow **Display a Message** step can now display a QR code to help with onboarding mobile devices to a DPSK network.

**NOTE**

Support for consuming Wi-Fi QR codes varies by operating system of the onboarding device.

- For integration with Microsoft Intune, Certificate Template Simple Certificate Enrollment Protocol (SCEP) Keys now support the Intune-specific SCEP challenge password type.



# Enhancements

---

Following are enhancements for this release of the product.

- Certificate Template Notification messages now support variable `${ENROLLMENT_PORTAL_URL}` and the default expiration warning messages make use of new variables.
- Improvements were made to the **Administrators** page in the web interface for administrators assigned the role of **Viewer**.
- SAML IdP authentication servers can be used to authenticate administrator users of Cloudpath. The **group** attribute provided by the SAML IdP assertion can be used to determine which SAML user accounts are allowed Cloudpath administrator access.





# Resolved Issues

---

Following are resolved issues for this release of the product.

- Resolved an issue where DPSK pools previously referenced by workflows could not be deleted.
- Resolved an issue where duplicated DPSK device records were created if a single end-user device alternated between using or reusing two or more DPSKs.
- Resolved an issue in Managed Access, Property Management and Tenant Portal interfaces that allows generating a new passphrase for a unit. Prior, the automatically generated DPSK passphrase did not conform to the format and length defined by the DPSK Pool.

## NOTE

Unit DPSK can be set manually only by the unit owner through the tenant portal.

- Resolved an issue where default Chromebook ONC installation instructions presented to the onboarding end-user was outdated.
- Resolved an issue with DPSK authentication incorrectly being rejected when **Override Device Count Limit** was set for a specific DPSK in the past but was subsequently disabled.
- Resolved an issue in the **Dashboard > Enrollments** page. When viewing an enrollment that uses a **Request access from a sponsor** workflow step and the request is pending sponsor approval, an administrator clicking the **Approve** or **Reject** buttons received an error message.



# Known Issues

---

- For mobileconfig-based Mac OS X enrollments to be disconnected upon profile installation, the "WLAN Profile Type" must be set to "Machine." To locate this setting in the UI for a completed device configuration, go to **Configuration > Device Configurations**, then click the arrow to expand the device configuration. Next, click the **OS Settings** tab, then click the pencil icon to edit the field called "Configuration from the Network(s) and Trust tabs" under the **Mac OS X Settings** area. In the Advanced Settings area, see "WLAN Profile Type." For more information, refer to the "Device Configuration and Client Certificate" section in the *Cloudpath Enrollment System Deployment Administration Guide*.
- For the property management feature, if the DPSK pool associated with a property contains more than one SSID, then a tenant must access the wi-fi network by performing the following steps (the wi-fi QRCode will not currently provide access in the two-SSID scenario):
  1. Select the appropriate SSID on their device.
  2. Manually enter the dynamic pre-shared key (DPSK). This is the "Wi-Fi Passphrase" on the Tenant Portal home page. (The property manager can also simply provide this key to the tenant.)
- With the use of Rest APIs, policies with a start time of 0:00 or an end time of 23:59 will fail on attempts to apply them to an eDPSK pool. All other timeframes work properly.
- When configuring a SmartZone integrated system in the Cloudpath UI (**Configuration > Integrated Systems**) for network segmentation, using the IP address of the vSmartZone controller can throw a "Hostname verification failed" exception. Perform one of the following two methods to allow for successful self-signed SmartZone integration with Cloudpath:
  - To prevent the exception, before you add the integrated system, manually upload the SmartZone self-signed server certificate to the Cloudpath truststore (**Configuration > Truststore**). Once this certificate exists in the Cloudpath truststore, you can use either the SmartZone IP address or its hostname to integrate with Cloudpath.
  - You can auto-pin the SmartZone self-signed server certificate. With this method, Cloudpath retrieves and verifies the remote self-signed certificate. The default verification matches the hostname with the subject alternative name of the certificate, as specified in the exception. If you used the vSmartZone IP address to add the integrated system, navigate to **Configuration > Truststore > Server Status** and click the **fixing** button.

## NOTE

Network segmentation requires a vSmartZone 6.1 controller. For more information about network segmentation, refer to the *RUCKUS SmartZone and Cloudpath Network Segmentation Configuration Guide*, available with the release of vSmartZone 6.1.

- **Device Configuration, Web Browser Trust option when used with MacOS 13+ (Ventura+) requires manual user trust acceptance:** For Device Configurations that specify "Web Browser Trust, Install additional CAs", the resulting SSL certificates installed on enrolled devices now require manual user acceptance steps on MacOS Ventura, and newer, for them to be fully trusted by the device.

MacOS Ventura (version 13.x.x) has added heightened security measures when adding a root CA certificate via Profiles. When root CA certificates are installed on MacOS devices running MacOS Ventura or newer via a Profile, the certificates installed to the device are no longer marked as "Always Trust" for SSL (web) automatically. As such, to fully trust these certificates for SSL usage the user must manually mark them as trusted. To fully trust these certificates, the user must:

1. Visit the resulting certificate entry in the MacOS application Keychain Access. It is recommended to use the search box and enter words from the name of the certificate.
2. Expand the "Trust" section/settings of the certificate.
3. For the dropdown for "Secure Socket Layer (SSL)" select "Always Trust".



# Upgrade Information

---

- [How to Upgrade to Cloudpath Version 5.12.5584](#)..... 21
- [Minimum Wizard Version](#)..... 23
- [Snapshots](#)..... 23
- [Upgrading a Cluster to 5.12.5584](#)..... 23

## How to Upgrade to Cloudpath Version 5.12.5584

The process you follow to upgrade to version 5.12.5584 depends on which version you are currently running.

Follow the steps in the applicable section(s).

### Upgrading From Cloudpath Version 5.7.4732 or Later

If you are updating from Cloudpath Version 5.7.4732 or later, navigate to **Administration > System Updates**, then proceed to download and install the update.

### Upgrading From Cloudpath Version 5.6.4652 or 5.6.4580

To update from Cloudpath Version 5.6.4652 or 5.6.4580, you can use one of two methods.

The *first* method is to upgrade to 5.9.5324, then to subsequently upgrade from 5.9.5324 to the current release. The incremental upgrade is time consuming and only recommended if deploying a new VM/OVA is not possible in your infrastructure.

1. Upgrade to 5.9.5324 by following the instructions in your Cloudpath 5.9.5324 release notes for upgrading to 5.9.5324.
2. Upgrade to 5.12.5584 by following the instructions in the preceding section called "Upgrading From Cloudpath Version 5.7.4732 or Later."

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

1. Deploy a new 5.12.5584 OVA.
2. Import the database using 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 5.5.4464

To update from Cloudpath Version 5.5.4464, you can use one of two methods.

The *first* method is to upgrade to 5.8.5012, then to subsequently upgrade from 5.8.5012 to the current release. The incremental upgrade is time consuming and only recommended if deploying a new VM/OVA is not possible in your infrastructure.

1. Upgrade to 5.8.5012 by following the instructions in the *Cloudpath Enrollment System Release Notes for Release 5.8.5012*.
2. Upgrade to 5.12.5584 by following the instructions in the earlier section called [Upgrading From Cloudpath Version 5.7.4732 or Later](#).

## Upgrade Information

### How to Upgrade to Cloudpath Version 5.12.5584

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

1. Deploy a new 5.12.5584 OVA.
2. Import the database using 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 in the Range 5.2.3585 to 5.4.4284

To update from versions in the range of 5.2.3585 to 5.4.4284, you can use one of two methods.

The *first* method is to incrementally upgrade to 5.7.4774, then to subsequently upgrade from 5.7.4774 to the current release. The incremental upgrade is time consuming and only recommended if deploying a new VM/OVA is not possible in your infrastructure.

1. Upgrade to 5.7.4774 by following the instructions in the *Cloudpath Enrollment System Release Notes for Release 5.7.4774*.
2. Upgrade to 5.12.5584 by following the instructions in the preceding section called [Upgrading From Cloudpath Version 5.7.4732 or Later](#).

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

1. Deploy a new 5.12.5584 OVA.
2. Import the database using 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 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 the current release. 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 the *Cloudpath Enrollment System Release Notes for Release 5.2*.
2. Upgrade to 5.12.5584 by following the instructions in the earlier section called [Upgrading From Cloudpath Version in the Range 5.2.3585 to 5.4.4284](#).

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

1. Deploy a new 5.12.5584 OVA.
2. Import the database using 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 5.12.5584 OVA.
2. Import the database using 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 5.12.5584

The process you follow to upgrade your cluster to version 5.12.5584 depends on which version you are currently running and on your infrastructure.

Follow the steps in the applicable section(s).

## Upgrading a Cluster Containing More than Two Nodes to 5.12.5584 from 5.7.4774 or Later

If you have a cluster of more than two nodes running 5.7.4774 or later, follow the steps below to upgrade to 5.12.5584:

1. Remove all APP-only nodes from the cluster. Retain two DB nodes in the cluster. For instructions, refer to the *Cloudpath Enrollment System Replication Configuration Guide*, 5.7R2.
2. Individually upgrade all APP nodes to 5.12.5584. Refer to the [Upgrading From Cloudpath Version 5.7.4732 or Later](#) on page 21 steps in the section [How to Upgrade to Cloudpath Version 5.12.5584](#) on page 21.

## Upgrade Information

### Upgrading a Cluster to 5.12.5584

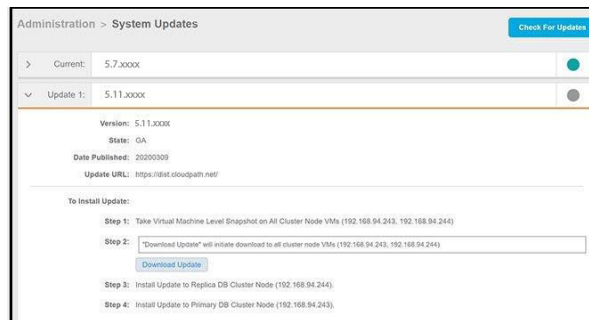
- Upgrade the retained two-node DB cluster by following the steps in section [Upgrading a Cluster Containing More than Two Nodes to 5.12.5584 from 5.7.4774 or Later](#).
- Add all APP nodes back into the cluster. For instructions, refer to the *Cloudpath Enrollment System Replication Configuration Guide*, 5.7R2.

## Upgrading a Two-Node Cluster to 5.12.5584 from 5.7.4774 or Later

If your two-node cluster is running 5.7.4774 or later, follow the steps below to upgrade the cluster to 5.12.5584:

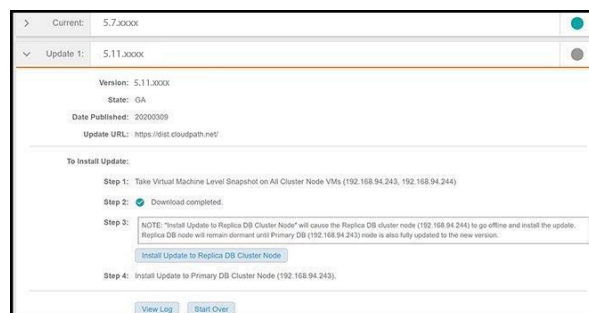
- Using the Cloudpath UI on the primary node in your cluster, navigate to **Administration > System Updates**. A screen such as the following indicates that there is a newer build (the build number is xxxx only for the purpose of the illustration) to which you can upgrade your cluster:

**FIGURE 1** System Updates Screen for Upgrading a Cluster from 5.7.4774 (or Later) to 5.12.5584



- Follow the instructions on the screen under the "To Install Update:" section.
- After the update completes, you should see the following screen:

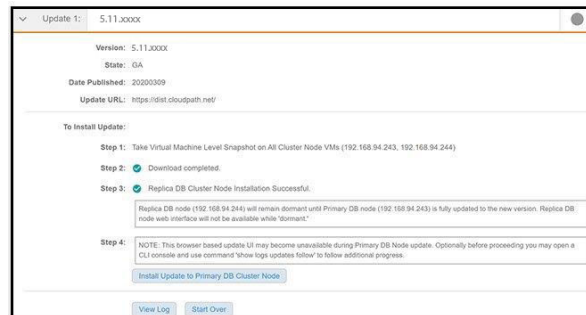
**FIGURE 2** Download Completed for Update



- Continue by clicking **Install Update to Replica DB Cluster Node**.
- After successful replication DB installation, you should see the following screen to indicate that the replica database cluster node installation was successful:



FIGURE 3 Replica DB Installation Successful



6. Continue by clicking **Install Update to Primary DB Cluster Node**.

The system will be unavailable for several minutes during the upgrade.

7. After a few minutes, you can log in to both nodes to verify that they have been successfully upgraded to the new build. Be sure to collapse all navigation bars on the left side of the UI, then check the lower-left corner of the UI for the release and build number.

## Upgrading a Cluster to 5.12.5584 from 5.6.4652, 5.6.4580, or 5.5.4464

If your cluster is running 5.6.4652 to 5.6.4580, you first must upgrade the cluster to 5.9.5324, then upgrade from 5.9.5324 to 5.12.5584.

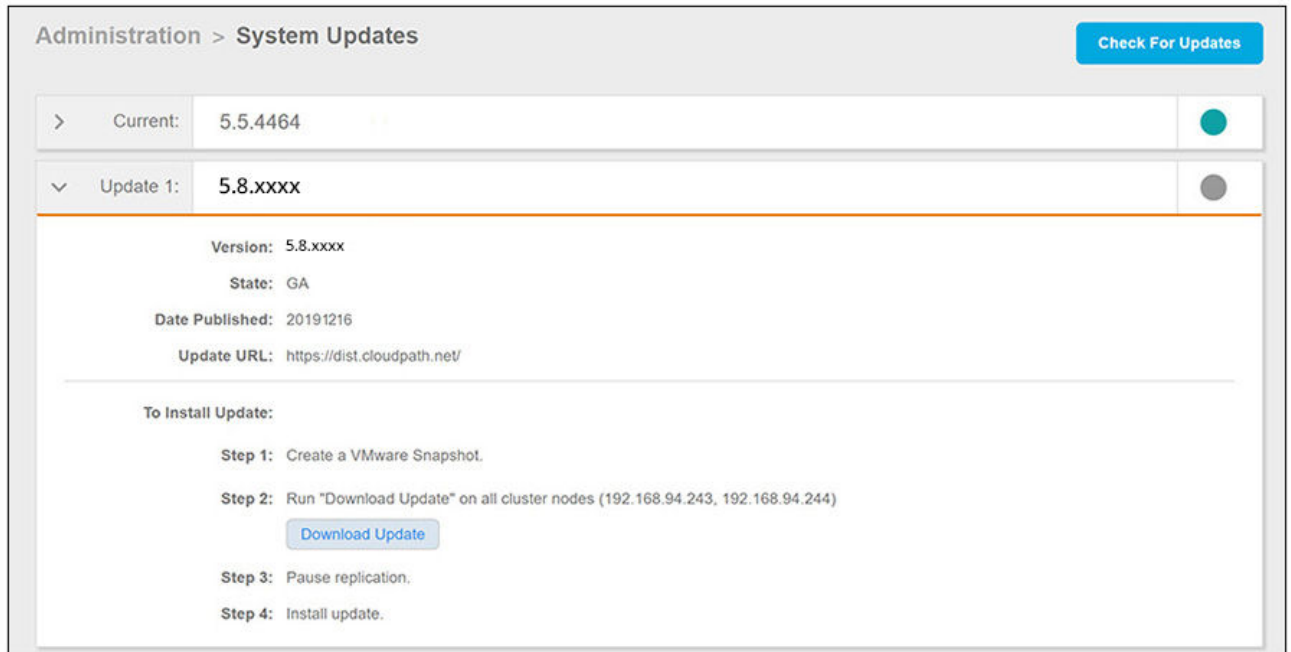
If your cluster is running 5.5.4464, you first must upgrade the cluster to 5.8.5012, then upgrade from 5.8.5012 to 5.12.5584:

1. First, upgrade to either 5.9.5432 or 5.8.5012, depending on your current version:
  - a. Using 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:

## Upgrade Information

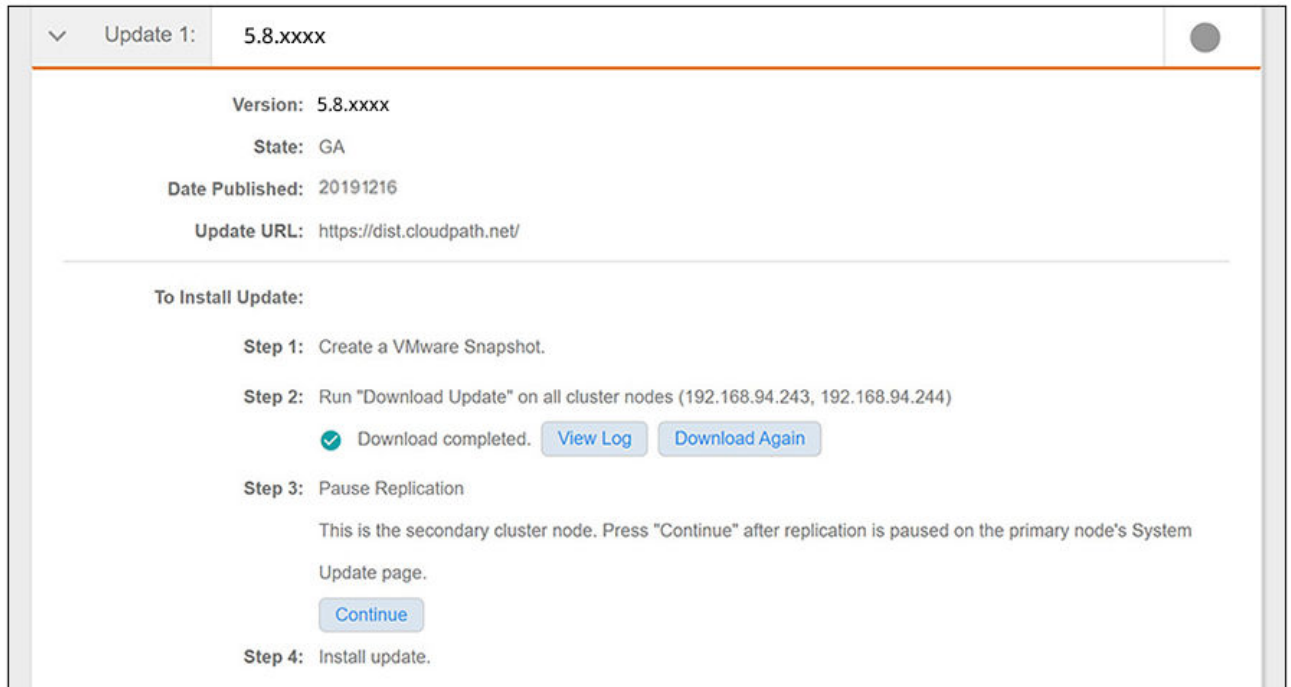
Upgrading a Cluster to 5.12.5584

**FIGURE 4** System Updates Screen Example for Upgrading a Cluster from 5.5.4464 to 5.8.5012



- b. Create a VMWare Snapshot of the primary node.
- c. Click the **Download Update** button on the primary node.
- d. Using the Cloudpath UI on the secondary node in your cluster, navigate to **Administration > System Updates**.
- e. Create a VMWare Snapshot of the secondary node.
- f. Click the **Download Update** button on the secondary node.
- g. Return to the Cloudpath UI on the primary node and pause replication.
- h. On the secondary node, click **Continue** (see Step 3 in the following screen):

FIGURE 5 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.

- i. 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*) to determine when the secondary node reboot is complete. Then, proceed with the system update on the primary node.

- j. 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.

2. Next, upgrade from 5.8.5012 to 5.12.5584 by following the instructions in the section [Upgrading a Cluster Containing More than Two Nodes to 5.12.5584 from 5.7.4774 or Later](#).

## Upgrading a Cluster to 5.12.5584 from 5.2 or Earlier

**NOTE**

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

## Upgrade Information

### Upgrading a Cluster to 5.12.5584

Two upgrade procedures are provided in this section to upgrade your cluster from 5.2 or earlier to 5.9.5324:

- 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 a 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 *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* 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 using 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 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"

#### Upgrading a 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 using the Cloudpath UI **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 the *the Cloudpath Enrollment System Release Notes for Release 5.2*.

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 or later, to recreate your cluster:
  - "Configuring an Active - Standby Replication"
  - "Configuring an Active - Active Replication"



© 2023 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>