RELEASE NOTES

Cloudpath ES Release Notes for Update 5.2.3918

Supporting Software Release 5.2

Part Number: 800-71992-001 Rev A
Publication Date: 20 July 2018

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

Contents

Preface **4**
- Document Conventions 4
- Command Syntax Conventions 4
- Document Feedback 5
- Ruckus Product Documentation Resources 5
- Online Training Resources 5
- Contacting Ruckus Customer Services and Support 5

About This Document **6**

Release Notes for Update 5.2.3918 ..... **6**
- How to Upgrade to Cloudpath Version 5.2.3918 6
- New Feature in 5.2.3918 7
- Bugs Fixed in 5.2.3918 8
- 8

Release Notes for Update 5.2.3847 ..... **8**
- How to Upgrade to Cloudpath Version 5.2.3847 8
- System Changes in 5.2.3847 9
- Bugs Fixed in 5.2.3847 9
- 10

Release Notes for Update 5.2.3761 ..... **10**
- How to Upgrade to Cloudpath Version 5.2.3761 10
- Bugs Fixed in 5.2.3761 10

Release Notes for Update 5.2.3585 ..... **11**
- New Features in 5.2.3585 11
- System Changes in 5.2.3585 11
- Feature Enhancements in 5.2.3585 11
- Bugs Fixed in 5.2.3585 12

Release Notes for Update 5.1.3483 ..... **13**
- New Features in 5.1.3483 13
- Feature Enhancements in 5.1.3483 14
- Bugs Fixed in 5.1.3483 15

Release Notes for Update 5.1.3461 ..... **16**

Release Notes for Update 5.0.3314 ..... **17**
- How to Upgrade to Cloudpath Version 5.0.3314 17
- Bugs Fixed in 5.0.3314 17

Release Notes for Update 5.0.3302 ..... **18**
- What to Expect During an Upgrade to Cloudpath Version 5.0.3302 18
- Changes in Supported OS Versions in Cloudpath Version 5.0.3302 19
- New Features in Cloudpath Version 5.0.3302 19
- Feature Enhancements in Cloudpath Version 5.0.3302 20
- System Changes in Cloudpath Version 5.0.3302 21
- Bugs Fixed in Cloudpath Version 5.0.3302 21

Preface

Document Conventions

The following tables list the text and notice 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.

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*...].

Convention	Description
\	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: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)
- For example:
  - Ruckus Small Cell Alarms Guide SC Release 1.3
  - Part number: 800-71306-001
  - Page 88

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 documentation by product or perform a text search. Access to Release Notes requires an active support contract and Ruckus Support Portal user account. Other technical documentation content is available without logging into 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 Networks products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the 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. Request 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, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.

Self-Service Resources

The Support Portal at https://support.ruckuswireless.com/contact-us 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/software
- 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.

Release Notes for Update 5.2.3918

Version 5.2.3918 is a maintenance release with bug fixes for the Cloudpath server. This version was released on July 20, 2018.

How to Upgrade to Cloudpath Version 5.2.3918

Upgrading From Cloudpath Version 5.0.3314 or Later:

If you are updating from Cloudpath Version 5.0.3314 or later, navigate to **Administration > System Updates** to download and install the update.

NOTE
If upgrading from versions 5.0.3314 or 5.1.3461, you must first download the support file and install it on the **Support > Upload Support File** page before downloading and installing the update package.

Upgrading From Cloudpath Version 5.0.3302 or Earlier:

To update to from version 5.0.3302 or earlier, you must deploy a new 5.2.3918 OVA and import the database from the existing system.

From the command-line configuration utility (klish command) of the new OVA system:

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

After the import is finished, you are prompted 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 document titled *How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Minimum Wizard Version:

Cloudpath version 5.2 requires a minimum version of the wizard. When performing a system update from the Admin UI or by using database import, the system will automatically update your Cloudpath wizard to the appropriate version.

Snapshots:

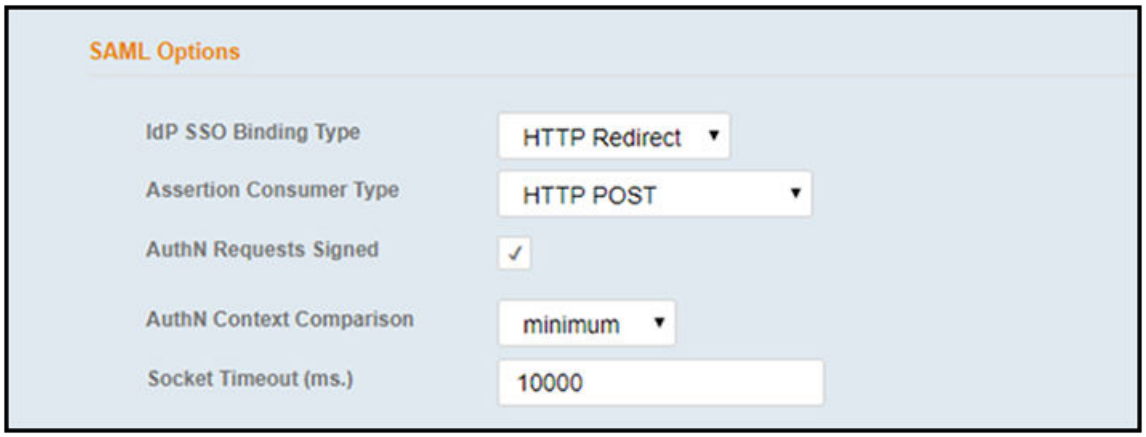
When upgrading your system, all previous snapshots will remain in the system, will be labeled not compatible, and will not be selectable for active snapshots. As part of the upgrade process, a new snapshot is created with the latest wizard build. This automatic snapshot creation allows the system to be fully updated and usable when the upgrade is finished.

New Feature in 5.2.3918

New SAML Option:

When you select the "Connect to SAML" radio button to configure SAML as an authentication server in Cloudpath, the "SAML Options" section of the ensuing configuration screen includes a new field called "AuthN Context Comparison." The default of this field is "minimum," but you can change the default, if desired, by using the drop-down list. The following figure shows the "SAML Options" section of the screen where this field is located.

FIGURE 1 AuthN Context Comparison Drop-down in SAML Options



Bugs Fixed in 5.2.3918

- The number of kernel packages retained by the system has been reduced to two, removing the installing-package error that occurred when the boot partition needed more space for an upgrade.
- The Windows OS setting "Automatically use my Windows logon name, password" has been restored.
- When sending an SMS via customer Twilio account to a number with a UAE area code, the system was not prepending the **+** sign. This has been corrected.
- An issue where Cloudpath was not installing the full Microsoft CA certificate chain into the network_config.xml file, which was causing Windows 10 to fail, has been fixed
- An "ens32: error fetching interface" error that was not allowing a Hyper-V VM to deploy has been fixed.
- With a DPSK configuration, when the Cloudpath system Timezone value was "UTC," the timeZoneUtcOffset value sent to a virtual SmartZone Controller was not in the correct format, but this issue has been fixed.

Release Notes for Update 5.2.3847

Version 5.2.3847 is a maintenance release with bug fixes for the Cloudpath server. This version was released on May 17, 2018.

How to Upgrade to Cloudpath Version 5.2.3847

Upgrading From Cloudpath Version 5.0.3314 or Later:

If you are updating from Cloudpath Version 5.0.3314 or later, navigate to **Administration > System Updates** to download and install the update.

> **NOTE**
> If upgrading from versions 5.0.3314 or 5.1.3461, you must first download the support file and install it on the **Support > Upload Support File** page before downloading and installing the update package.

Upgrading From Cloudpath Version 5.0.3302 or Earlier:

To update to from version 5.0.3302 or earlier, you must deploy a new 5.2.3847 OVA and import the database from the existing system.

From the command-line configuration utility (klish command) of the new OVA system:

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

After the import is finished, you are prompted 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 document titled *How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Minimum Wizard Version:

Cloudpath version 5.2 requires a minimum version of the wizard. When performing a system update from the Admin UI or by using database import, the system will automatically update 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.

System Changes in 5.2.3847

3DES Cipher Suite Disabled By Default in Future Releases:

In the update for Java JRE 7u181, the default setting for the 3DES cipher suite was changed to disabled. This causes old AD servers (such as Windows 2003) to fail authentications because they depend on the 3DES cipher suite. In this Cloudpath update, this setting was removed to allow 3DES for backward compatibility. However, in future updates, the 3DES cipher suite will remain disabled. Be sure to update your AD server to remain compatible for future releases.

Bugs Fixed in 5.2.3847

- Using the Foundry-CoA-Command RADIUS attribute no longer causes CoA to fail with an unknown attribute.
- VLAN information is correctly changed and sent during the RADIUS Reply attribute for accounts on Cloudpath-hosted systems.
- The number of kernel packages retained by the system has been reduced to two, removing the installing-package error that occurred when the boot partition needed more space for an upgrade.
- When configuring DPSK, the Virtual SmartZone (vSZ) version is selectable, which allows the correct public API version to be sent in the API request for DPSK integration.
- When uploading a private key and public key for the RADIUS server, the system verifies that they match, and displays an error message if they do not match.
- The Windows OS setting 'Automatically use my Windows logon name, password' has been restored.
- For setting up MAC registration, shortcut buttons have been added for configuring Ruckus ICX and Cisco Meraki switches.
- The default setting for Connection Tracking has been changed to disabled to overcome a JBoss performance issue that was causing some RADIUS authentication failures.
- When using a Microsoft CA instead of the onboard CA, the system does not write the OCSP URL, but allows the connection. The logs provide a warning message that there is no OCSP URL in certificate.
- Adding a sponsor to a voucher list, or logging into a sponsorship portal, no longer displays the system-starting message for accounts on a hosted server.
- An issue existed for some hosted accounts where the enrollment URL incorrectly had a double slash where the account name should be located. The missing account name caused the application loader to fail for Windows and Mac OS. This issue has been corrected.

Release Notes for Update 5.2.3761

Version 5.2.3761 is a maintenance release with bug fixes for the Cloudpath server. This version was released on March 16, 2018.

How to Upgrade to Cloudpath Version 5.2.3761

Upgrading From Cloudpath Version 5.0.3314 or Later:

If you are updating from Cloudpath Version 5.0.3314 or later, navigate to **Administration > System Updates** to download and install the update.

> **NOTE**
> If upgrading from versions 5.0.3314 or 5.1.3461, you must first download the support file and install it on the **Support > Upload Support File** page before downloading and installing the update package.

Upgrading From Cloudpath Version 5.0.3302 or Earlier:

To update to from version 5.0.3302 or earlier, you must deploy a new 5.2.3761 OVA and import the database from the existing system.

From the command-line configuration utility (klish command) of the new OVA system:

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

After the import is finished, you are prompted 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 document titled*How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Minimum Wizard Version:

Cloudpath version 5.2 requires a minimum version of the wizard. When performing a system update from the Admin UI or by using database import, the system will automatically update 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.

Bugs Fixed in 5.2.3761

- Added validation to the Windows identity privacy setting. Incorrect formats display.
- Added the ability to configure KeyUsage for certificate templates and apply them when certificates are issued.
- Changed the naming format of the db export file to include the filename.
- If the sponsor email regex is left blank, it is processed as a wildcard.
- When using custom logos with the proper 7:1 ratio, the logos show up correctly.
- When importing a large db, using the maintenance cannibalize command, MySQL is no longer restarted while the tar command is still running.

- The serial numbers assigned from a Microsoft CA are unique and the correct certificates can be verified for the corresponding users.
- The random shared secret generator no longer issues a shared secret with a space, double quote, or single quote.
- The enrollment variable ${IDENTITY.FIRST_NAME} correctly displays in the email notification for a DPSK configuration.
- When generating a certificate from a template with 4096 bits, the downloaded p12 displays 4096 bits in the certificate details.
- The MAC registration table no longer displays some records with a blank MAC address.
- Added the ability to display the IP Address as a variable for a custom HTML message on the enrollment portal.
- When filtering to report Expired MAC registrations, the exported file contains the expired MAC registrations.
- The RADIUS log displays correctly in the Admin UI. Previously, this only displayed in the command line interface.
- Certificate template notifications that are sent immediately are sent from the server that processed the event, and not just from the primary server in a replicated system.
- Added the ability to enter custom success messages in the device configuration for each operating system.
- The system no longer displays an error message about a missing default workflow when errant data is passed the enrollment URL.

Release Notes for Update 5.2.3585

Version 5.2.3585 is a maintenance release with bug fixes for the Cloudpath server. For the Cloudpath client, this release introduces a new UI for the Windows, Mac, Linux, and Android OSes, and includes client bug fixes. This version was released on September 22, 2017.

New Features in 5.2.3585

New Look for the Client UI:

The client application user interface for Windows, Mac, Linux, and Android operating systems has been updated. The user interface is consistent across the operating systems that use the application, provides a new style menu, and has updated animation.

The client UI can still be customized with logo, background color, and foreground color (button text).

System Changes in 5.2.3585

- Added support for the following client operating systems: Android 7.1 and 8.0, Mac OS X 10.13, Fedora 26, Ubuntu 17.10, and iOS 11.
- Removed automatic configuration support for Windows XP, Mac OS X 10.7, Ubuntu 12.04, Android 4.0.3. These devices can be configured manually, if needed.
- FreeRADIUS was updated version 3.0.15.
- The internal database was updated to MariaDB 5.5.57.
- The shared database feature has been restored in version 5.2.

Feature Enhancements in 5.2.3585

- Added the ability to support more than one web server certificate for Passpoint R2.

Bugs Fixed in 5.2.3585

- Entering the maximum amount of HTML characters in the OS Settings > User Experience boxes no longer displays an error.
- A sponsor can manually approve an access request from the enrollment record.
- Using a Voucher Code in a workflow with DPSK no longer throws an error.
- Cloudpath supports IP address/port numbers to be set for 2 eduroam RADIUS clients.
- DHCP fingerprinting data can be removed with Data Cleanup.
- Instructions are provided for enabling web CA certificates on iOS 10.3 and later devices.
- Duplicate entries have been removed from the Dashboard > ToDo Items.
- The list of conflicting SSID are not written to the mobileconfig file.
- The date range check has been added to the log files.
- SafeConnect is properly installed with both wired and wireless interfaces.
- A sponsor can create and maintain a Shared passphrase.
- After an upgrade, you can download the mobileconfig file from a generated certificate without errors.
- The Cloudpath Android application can be opened directly from the Google Play store, and will continue with the configuration of the device for Android devices running OS 6.0, or later.Previously, this feature was available for Android OS 5.x devices.
- The client supports the WPA/WPA2 and TKIP/AES modes in Windows.
- A maintenance cannibalize no longer fails when a network configuration software installer is present on the system to be upgraded.
- The Workflow Information table in the Enrollment record no longer displays Unicode characters.
- Updated the messaging for DPSK when it is configured with special characters.
- The device configuration screen sub-tabs work correctly with the Internet Explorer browser.
- The Enable DNS Shortcut feature works correctly for an Enrollment Portal URL.
- The database migration errors have been corrected when upgrading from version 4.3.2895 to 5.1.3461.
- A new server deployment defaults to the /admin page instead of the /enroll page.
- Logging in as a Viewer administrator role no longer displays an error.
- The **support activate-ui-recovery** command cannot be issued by a read-only user.
- The Enrollment Data that is exported from the system is complete.
- When Assertion Consumer Type is set to HTTP POST for a SAML authentication server, an Artifact Resolution URL is not required in the SAML IdP metadata.
- When enabling ActiveSync iOS device config setting, there are now 3 options for Included Credentials: Certificate, Username/Password, Both Certificate & Password.
- Added support for the Airespace-IPv6-ACL-Name RADIUS Attribute.
- The registerMac API works as expected.
- With SAML authentication, if the distinguished name attribute is not mapped to SAML field, the subject name is used for the username.
- Using a wildcard for the Admin Group Regex field no longer denies an AD administrator authentication.
- The system correctly generates a CSR for a 4096 Key Length.
- An LDAP DN now allows a period in the value, for example, o=gavalin.edu.

- The TLS certificates are installed in the correct certificate store on a Windows 10 Creators Edition device.
- The Favicon option has been removed from multi-tenant servers.
- The progress of the Data Cleanup feature can be monitored from a log file.
- The system verifies the value of the URL value for a custom SMS provider.
- When using multiple Microsoft CA certificate templates, the VLAN is correctly assigned.
- Added support for ElasticSearch 5.5.2 schema.

Release Notes for Update 5.1.3483

Version 5.1.3483 was a feature release, with a new look for the Admin UI, with enhancements, and bug fixes. This version was released on June 12, 2017.

New Features in 5.1.3483

New Look for the Admin UI:

The Cloudpath Admin user interface has been improved to more closely align with the look and feel of other Ruckus Wireless software products.

Aside from the new look and feel, the workflow pages have been restructured:

- The workflow configuration is managed from the **Configuration > Workflow > Enrollment Process** tab.
- Snapshots are now managed from the **Configuration > Workflow > Snapshots** tab.
- The Deployment URL is renamed *Enrollment Portal URL* and is now managed from the **Configuration > Workflow** page.
- When configuring a Ruckus controller, the Enrollment Portal URL is used in place of the WLAN Redirect URL.

DHCP Fingerprinting:

The Cloudpath server supports DHCP Fingerprinting, for IPv4, or IPv6, or both. This feature is enabled on the **Administration > System Services > DHCP Fingerprinting** page. Once enabled, the server discovers, via the DHCP packet exchange, information about the devices on your local network and displays it on the on the **Dashboard > DHCP Fingerprints** page. Additional devices can be exposed by enabling the ip helper configuration on the router (example router configuration below).

```
enable
configure terminal
interface type number
ip helper-address address (address is the IP address of the Cloudpath server)
exit
```

Additionally, the DHCP Summary Information, obtained by DHCP fingerprinting and displayed in the enrollment record, can be used as a filter in the workflow. Modify the split option in the workflow and navigate to **Device-Based Filters > DHCP Summary Pattern**.

Support for Hyper-V Deployments:

Cloudpath now supports virtual appliance deployments using a Microsoft Hyper-V Manager.

The Cloudpath virtual appliance can be distributed as a Hyper-V virtual hard disk (vhdx) disk image file, which can be deployed as a virtual machine using Microsoft Hyper-V Manager Cloudpath offers a Non-Production POC, as well as several Production configurations for deployment.

Just like OVA deployments, if you are setting up a Cloudpath account for the first time, you will be sent an activation code in an email notification. For an on-premise deployment, the activation code link allows you to download the Cloudpath VHDX image file, binding your VHDX file with the activation code.

When the download is complete, deploy the image file using the Hyper-V Manager.

Support for Security Assertion Markup Language 2.0 (SAML 2.0):

Cloudpath added support for a SAML (Shibboleth) Identity Provider (IdP) to be configured as an Authentication Server. With traditional authentication server types (LDAP, AD, etc) Cloudpath prompts for the user credentials, which are then verified with the authentication server. With SAML, Cloudpath delegates to the IdP to prompt the user for credentials.

Create and manage SAML authentication servers from the **Configuration > Authentication Servers** page. To establish trust between Cloudpath and a SAML IdP configuration is required on both Cloudpath and at the IdP itself.

Feature Enhancements in 5.1.3483

Enhancements for Android:

Starting in the 5.1 release, the Cloudpath Android application can be opened directly from the Google Play store, and will continue with the configuration of the device.

> **NOTE**
> If you have customized the Android Instructions HTML in the device configuration OS Settings, you must reapply your changes after the upgrade.

Android versions 4.4 and earlier will continue to use the two-step process.

Notification Enhancements:

Added support for setting up Change of Authorization (CoA) disconnects as a notification, as part of the certificate template configuration, or as a Notification workflow plug-in.

Workflow Enhancements:

- Added support for using a language regex as a filter for a workflow split.
- Added the ability to specify a variable for the VLAN ID in the DPSK plug-in.

API Enhancements:

Added support for an API that will revoke all MAC registrations.

Support Enhancements:

- Added the ability to upload a wizard binary via a support file.
- Added a Contact Sales link on the **Support > Licensing** page, to assist with licensing issues.

MAC Registration Enhancements:

- Added checks for duplicate MAC addresses, both for the MAC Registration list and for the MAC Import list.
- Clarified the *Behavior* selections when configuring a MAC Registration plug-in.
- Streamlined imports of large MAC Registration lists.
- Added support for additional Date formats on MAC Registration lists.

RADIUS Enhancements:

- Added support for the Foundry RADIUS attributes; *Foundry-RADIUS-COA-Command* and *Foundry- Voice-Phone-Config*.
- Added support on the RADIUS client for additional formats for the MAC address delimiters.

System Updates:

- Added the OCSP URL for the web server certificate to the Firewall Requirements page.
- If you change the Account URL Name, the Workflow URL Name, switch to HTTP/HTTPS, or change the web server name via config https-servername override, the Snapshot tab indicates the change and a new *Publish* will use the updated name.
- Added support for Ubuntu 17.04.
- Added the ability to provide OVAs signed with SHA-1, SHA-256, or SHA-512 algorithms. VMware version 6.5 requires a SHA-2 signed OVA.

Multi-tenant Enhancements:

Enhanced licensing for MSP Multi-tenant (MT) customers:

- Added the ability to create a MT server using a special activation code.
- Added the ability for MSP MT customers to add their own new or trial accounts to the Cloudpath license server from the MSP MT root account.
- Added the ability to link a tenant account to a parent account on the Cloudpath license server.

Replication Enhancements:

- Added support for replication with or without a load balancer:
  - If setting up replication behind a load balancer, the hostname of the load balancer is added in the replication configuration.
  - If setting up replication without a load balancer, the hostname of the primary server becomes the load balancer DNS.
- Added a mechanism to preserve replication setup values to reduce errors during system upgrades.
- Added the all RADIUS server IP addresses (both for master-master, and all for star) to the Replication Setup page.
- Removed the ability to manage the cluster from the non-primary system.

Bugs Fixed in 5.1.3483

- Using IE 11 browser during enrollment, the system correctly refreshes after a request from a sponsor is approved.
- If the web server certificate does not contain OCSP (for example, it is from Microsoft and OCSP has not been enabled), the Apache server will start.
- Added the following attributes to the OAuth2 integration: first_name, last_name, company, and email.
- The settings for optionally installing SafeConnect displays a skip button if there is an error during installation.
- A custom application logo correctly displays on the Mac client app.
- The *Rate this app* dialog window has been restored.
- If a connection attempt fails, the system does not go back and recheck the clock before a retry.
- SecureW2 version 3.5.15 has been added to the list of versions in the Wizard Setting Configuration.
- The connection pooling configuration has been adjusted to reduce the max connection log messages on Cloudpath-hosted servers.
- Installing a trusted root CA from the iOS device configuration OS Settings correctly installs the certificate on the device.
- Setting up an LDAPs server with a self-signed certificate logs a message, but completes, and no longer displays a blank page.
- The generateMobileconfig API no longer fails if the password is left blank.

- Timezone identifiers with multiple slashes (America/Kentucky/Monticello) are correctly parsed during setup and system restart.
- The MAC_APPLET_DOWNLOAD_ZIP file no longer causes an issue during database migration.
- A certificate template notification, configured for Start of Hour, On Certificate Revocation, no longer causes an error.
- If a customer fails to remove the cluster configuration before updating the Cloudpath servers, a support file is needed to correctly clear the tables in the database.
- When changing SSH ports from the Admin UI, the system correctly disables SSH, then enables with the new SSH port.
- The Syslog settings are retained after a database migration.
- A multi-tenant server blocks duplicate administrator accounts with the same email address.
- Favicon files can be uploaded without errors.
- Using forward and back slashes in Certificate Template fields no longer prevents RADIUS from restarting.
- The ability to use AD credentials for administrator logins has been removed from multi-tenant servers.
- Changes to the Enrollment Portal URL are correctly transferred to the Sponsorship Portal URL.
- The system correctly identifies a Windows Phone that is projecting a false user-agent.
- Updated the messaging when uploading a voucher list, and improved the default templates.
- If attempting to enroll devices before the database migration is complete, the system no longer displays errors, instead the log entries show the migration is still in progress.
- When configuring a Palo Alto firewall, if the Get Key windows is canceled on a blank page, this no longer displays an alert popup message.
- Allow PEAP fast reconnect to be disabled on Windows by setting a value in the configuration file.

Release Notes for Update 5.1.3461

Version 5.1.3461 is a feature release, with a new look for the Admin UI, with enhancements, and bug fixes. This version was released on May 25, 2017.

Version 5.1.3461 was pulled shortly after release due to the following issues, which have been fixed in version 5.1.3483.

- When a device configuration is not specified in the result step, the enrollment prompt correctly displays the certificate download and provides password information.
- If an account on a MT system did not have a default workflow prior to upgrade, this condition is corrected, and the Enrollment Portal URLs are correctly updated after the upgrade.
- If an account on a MT system used the default Enrollment URL prior to an upgrade, an error condition no longer occurs when using the default Enrollment Portal URL after the upgrade.
- After an upgrade, the logrotate permissions allow a MT system to effectively manage the logs and prevent them from affecting the performance of the system.

Release Notes for Update 5.0.3314

Version 5.0.3314 is a maintenance update, released on January 31, 2017.

How to Upgrade to Cloudpath Version 5.0.3314

Requires Database Import:

This version cannot be updated using the normal Admin UI system updates from a previous version. To update to version 5.0.3314, you must deploy a new 5.0 OVA and import the database from the existing system.

For more information about how to perform a database import for upgrades, see the document titles *How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Bugs Fixed in 5.0.3314

- The Maximum Certificates threshold retains the correct value for the Concurrent Certificates workflow plug-in.
- The certificate CN uses the Enrollment GUID string and cannot be modified.
- When a device configuration contains a chained network, the device is migrated to the first network in the list, and is configured for the second network.
- Added the ability to delete an authentication server. Use the Cleanup section on the bottom of the Modify Authentication Server page.
- Added a lockout for excessive incorrect logins to the Admin UI, after which, the administrator receives an email notification to reset the password.
- The show icon in the system settings tray works correctly.
- A Nokia phone is registered correctly as a Windows phone in the enrollment table.
- When using a self-signed certificate, or a root CA certificate, the system displays the appropriate error message.
- When adding a new deployment location, the base URL is no longer available for the enrollment port URL. If an end-user only enters the base URL, they will receive the Default enrollment portal.
- The pre-shared key is correctly saved when configuring a PSK device configuration.
- When editing a workflow in two different windows, the workflow names are not duplicated or overwritten.
- The Regex custom field requirements have been corrected on the Active Directory credentials prompt.
- The Certificate Generator does not activate when enrolling with a PEAP configuration using a Chromebook.
- When creating Sponsored Logins with Text Entry, the Default Sponsor Email is no longer a required field.
- Certificate notifications using the Minutes After parameter now sends out the email notification.
- If the User table contains user identity records that are not associated to any enrollment or device, they are removed during Data Cleanup.
- Email notifications are no longer sent for enrollments with revoked certificates.
- Users authentication via RADIUS PAP now correctly display the Username field of the Users table.
- The scheduled backups cron backup file supports the format xpressconnect-date-tar.gz.
- The notification email for new accounts has been updated. Previously, the instructions were directed toward standalone wizard customers.
- The Change button for the RADIUS shared secret has been renamed New Random, to help clarify the difference between setting a shared secret and having the system generate a new one.

- The web server Strict Transport Security setting is now correctly enabled, when set.
- When you change the SSID Regex field for a MAC Registration configuration, this SSID Regex change correctly saved.
- RADIUS debug has been disabled for customers on Cloudpath-hosted servers, and can only be enabled from the root account, or with the help of customer support.
- The System Updates page no longer shows the upgrade instructions when you are already at the latest version.
- Added the ability to turn off RADIUS Accounting Status Check for external firewalls. On the Modify Firewall & Web Filter Integration page, set the Status Interval to zero.
- The system correctly processes support files.
- If an account is added to a Cloudpath-hosted systems, the RADIUS port for the account is correctly added to the database.
- When enrolling using an Android device, the Configure link has been updated to reduce dependency on the Alternate Option link.
- When the Request Access from a Sponsor workflow plug-in is configured for a Static drop-down list, the UI now allows 4096 characters in the entry field.
- The Sponsorship Portal URL is now correctly updated after changing hostname or HTTPS server name.
- The system no longer locks up when exporting an xls or csv file for a table with 60k+ enrollments or connections.
- There is no longer an OCSP stapling error when you open the Admin UI with the Firefox browser.
- Added the ability to configure and outer identity for PEAP device configurations on Mac OS X, Linux, and Android.
- Added an optional field for socket timeout when creating/editing a workflow step to a traditional Authentication Server of type RADIUS.
- Custom RADIUS attributes are now included in the RADIUS response.
- Replication can be set up using port 22.
- The email notification queue has been enhanced to manage situations where the queue gets backed up for an extended period of time.
- The system status command in the command-line configuration utility now displays the correct output.

Release Notes for Update 5.0.3302

Version 5.0.3302 is a major feature release with enhancements, and bug fixes. This update was released on January 6, 2017.

What to Expect During an Upgrade to Cloudpath Version 5.0.3302

Database Import:

The Cloudpath 5.0 operating system has been updated to Cent OS 7. This change in the operating system does not allow normal Admin UI system updates from version 4.3, and earlier. To update to version 5.0, you must deploy a new 5.0 OVA and import the database from the older system.

Changes to Database Import Process:

The database import process has been enhanced in this release, with these main improvements:

- You are no longer required to log into the Admin UI and bind the system before you perform the database import.
- The command-line configuration utility (klish command) has changed to:

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

- Improved logging shows the progress of the database tables being imported.
- After the import is finished, you are prompted to have the system automatically move the IP address to the new system and shut down the old system.

Minimum Wizard Version:

Because of the operating system update for Cloudpath version 5.0, the minimum wizard version must be version 5.0.586, or later. When performing a database import, the system will automatically update your Cloudpath wizard to the appropriate version.

Snapshots:

When upgrading from version 4.3 or earlier, all previous snapshots will remain in the system, but 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 Cloudpath wizard build. This automatic snapshot creation allows the system to be fully updated and usable when the upgrade is finished.

> **NOTE**
> Do not reboot the system during the upgrade. The system will reboot itself when the process is complete.

For more information about how to perform a database import for upgrades, see the document titled *How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Changes in Supported OS Versions in Cloudpath Version 5.0.3302

The list of OS versions for user devices was truncated in this release. Cloudpath version 5.0 supports the following OSes for automated configuration:

- Mac OS X version 10.7 and later
- Windows XP, and later
- iOS version 6, and later
- Android versions 4.0.3, and later
- Fedora version 18, and later
- Ubuntu version 12.04, and later

All previous OS versions are supported for manual configuration only.

New Features in Cloudpath Version 5.0.3302

Change of Authorization (CoA) Disconnect Messages:

Enable CoA to send Change of Authorization disconnect messages (DMs) from Cloudpath on port 3799 to the switch or wireless LAN controller. You can send disconnects manually from the **Dashboard > Connections** page, or via an enrollment *Revoke*.

CoA is enabled by default with Cloudpath new 5.0 OVA systems, but after database update from a previous version (4.2 or 4.3), you must enable CoA on the RADIUS server Status tab. CoA attributes are configured on the RADIUS server Client tab.

Refer to the *Cloudpath Onboard RADIUS Server Change of Authorization (CoA)* guide on the Support tab for configuration details.

Hotspot 2.0 Release 2 and Online Sign-up (OSU):

Hotspot 2.0 (HS 2.0), often referred to as Wi-Fi Certified Passpoint, is the new standard for Wi-Fi public access that automates and secures the connection.

In Release 2, mobile devices use Online Sign-Up (OSU) to accomplish registration and credential provisioning to obtain secure network access. Each Service Provider network has an OSU Server, an AAA Server, and access to a certificate authority (CA). The CA is known by two attributes: its name and its public key. An OSU server certificate should be obtained from any of the CAs authorized by Wi- Fi Alliance.

Refer to the *Configuring Cloudpath to Support Hotspot 2.0 Release 2 (Passpoint)* guide for details on the Support tab for details about how to configure a Ruckus SmartZone controller and Cloudpath for Passpoint.

Connection Tracking:

Connection Tracking displays the current device connections on the **Dashboard > Connections** page. RADIUS Accounting must be enabled on your wireless LAN controller. Connection Tracking is enabled by default with Cloudpath new 5.0 OVA systems, but after database update from a previous version (4.2 or 4.3), you must enable Connection Tracking on the RADIUS server Status tab.

RADIUS Accounting:

If your wireless LAN controller is configured to support RADIUS accounting, and if Connection Tracking is enabled, the Accounting tab displays RADIUS accounting packets local to the Cloudpath server. View RADIUS accounting packets on the RADIUS server Accounting tab.

See the *Integration with Ruckus Controllers* guide on the Support tab for complete configuration information.

Time-Based Access (Open Access):

Configure short-term time-based access for a specific SSID, for a specified time-period for short-term usage from the RADIUS server Open Access tab.

The onboard RADIUS server accepts all connections (via MAC authentication). New connections are granted access for the defined period of time. After this period is exceeded, the connection is blocked.

> **NOTE**
> You should use Open Access in a limited or test environment only. SSIDs configured for Open Access are not secure.

Firewall and Web Filter Integration:

Cloudpath can be configured to integrate with Palo Alto Firewalls and other Web Filter applications, such as LIghtspeed Systems and iBoss Web Security Gateway from the **Configuration > Advanced > Firewall & Web Filter Integration** link. You can also configure a custom RADIUS Accounting server.

Cloudpath supplements data already captured by these applications by adding mappings of the IP address to a UserId, which allows the captured traffic to be identifiable. When the user joins the network via Cloudpath, the firewall or web filter application is notified of the user's login. Similarly, when a user is known to have left the network, the application is notified of the logout.

See the *Cloudpath Integration with Palo Alto Firewalls* guide on the Support tab for more information.

Feature Enhancements in Cloudpath Version 5.0.3302

Authentication Servers:

Updated the settings and labeling information on the OAuth configuration pages to reflect updates and changes in the Facebook, LinkedIn and Google developer pages.

MAC Registration:

Added the ability to delete or reset MAC registrations lists.

Admin UI:

Added the information about the administrator that is currently logged into the Admin UI. This information can be seen if you hover over the administrator icon in the top right corner of the Admin UI (next to Logout).

DPSK Support for Ruckus SmartZone Controllers:

Cloudpath has added support for DPSK configured on Ruckus SmartZone controllers. When adding a new DPSK configuration to the workflow, specify the Controller Type in the Ruckus Northbound Interface configuration.

System Changes in Cloudpath Version 5.0.3302

System Updates:

The following applications have been updated in the Cloudpath system:

- The Red Hat Enterprise Linux (RHEL) distribution was updated to Cent OS 7.
- The onboard RADIUS server was updated to FreeRADIUS version 3.0.11-2.e17.
- Apache web server was updated to version 2.4.
- Internal database was updated to MariaDB 5.5.44.

APIs:

API changes in this release:

- The *destroy* parameter was added to external/revokeByMacAndExternalID
- The *external/destroyByEnrollmentGuid* API was added.

FIPS 140-2:

The *haveged* rpm was added to the Cloudpath system to increase the entropy to 1000-2500 bits, in compliance with FIPS 140-2.

To list the current entropy, enter this command from the Linux shell:

```
[root@servername cpn_service]# cat /proc/sys/kernel/random/entropy_avail
```

The following FIPS commands have been added to the command-line configuration utility:

```
# config fips-crypto enable/disable

# config fips-crypto state
```

Wizard Loader

The Cloudpath Wizard loader for Windows is signed with MD5 hash algorithm.

Command Reference:

Several of the Cloudpath command-line configuration utility commands (config and support commands) have been restructured with this release. See the *Cloudpath Command Reference* for the complete listing of commands and their usage.

Bugs Fixed in Cloudpath Version 5.0.3302

- Removed support for the Facebook scope user_groups because Facebook deprecated this API call.
- If support for Mac OS X is disabled in the device configuration, it affects only the specified OS X version.
- The failure to download error no longer occurs when using new client code on a Windows device that has non-Unicode language setting.
- Support files are successfully generated in the correct location with the new Mac OS X client code.
- The old PEAP profile is removed when onboarding to a TLS network with a Mac OS X device using the new client code.

- The ${MAC_ADDRESS} variable displays correctly with the Display Message workflow plug-in if the MAC_ADDRESS is available.
- The cryllic characters display correctly on the download screen for iPhone and Windows devices.
- The period(.) has been removed from the end of the password in the DEFAULT e-mail notification for new onboard database users.
- The username displays correctly in the email notification for new onboard database users.
- The Cloudpath system accepts multiple, comma separated entries, IP only, or CIDR notation for entries in the Admin UI Allowed IP/CIDR field for the Web Server.
- If an enrollment record is blocked, the Mac Registration page displays the correct status.
- When a concurrent certificate workflow step is removed, the associated certificate template is also cleaned up. Previously this caused the error: "Cannot delete or update a parent row: a foreign key constraint fails."
- With 'support next version' flag set, the Mac OS X 10.12 opens the correct download tab.
- The system limits the administrator to one process per HTTP session to avoid leaving multiple processes running.
- MAC Registrations configured to expire on a specified date will expire as set.
- Java heap space memory error no longer prevents customers from downloading RADIUS log on Cloudpath-hosted servers.
- Profiles with empty names, which might occur with Korean characters, no longer causes an error on Windows devices
- The mobileconfig file is correctly extracted from the network_config.jar.
- The application no longer throws an error when searching for the configuration file on Mac OS X.
- The Mac OS X client no longer fails when the Root CA has no Common Name.
- The credential prompt screen displays the user name suffix correctly after clicking out of the user name edit box on Mac OS X and Windows.
- Mobileconfig validation no longer fails when Cloudpath is using HTTP instead of HTTPS.
- The MAC Registration import list with a date format MM.DD.YYYY displays the correct expiration date.
- A PEAP configuration now supports IDENTITY_PRIVACY. This is enabled by default.

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