Cloudpath
Enrollment System

Release Notes

Software Release 5.1
June 2017

Summary: This document describes the Cloudpath 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 versions 4.2.2626 through the currently released version.
Document Type: Configuration
Audience: Network Administrator

Cloudpath ES Release Notes

Software Release 5.1

June 2017

Cloudpath Release Notes

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 versions 4.2.2626, through the currently released version.

Release Notes for Update 5.1.3483

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

How to Upgrade to Cloudpath Version 5.1.3483

Upgrading From Cloudpath Version 5.0.3314 or Version 5.1.3461

If you are updating from Cloudpath Version 5.0.3314 to 5.1.3483 or from 5.1.3461 to 5.1.3483, navigate to *Administration > System Updates* to download and install the update.

> **Note >>**
> Before downloading and installing the update from *System Updates* page, you must first download the support file and install it on the *Support > Upload Support File* page.

Upgrading From Cloudpath Version 5.0.3302 or Earlier

To update to from version 5.0.3302 or earlier, you must deploy a new 5.1.3483 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, see the document, *How to Upgrade a Cloudpath System*, which is located on the Support tab of the Admin UI.

Minimum Wizard Version

Cloudpath version 5.1 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 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 & Feel of other Ruckus Wireless software products.

Aside from the new Look & 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 2-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, *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.

+1 303.647.1495 | +44 (01) 161.261.1400 | support@cloudpath.net | www.ruckuswireless.com |

- 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 can 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 5.0.3301 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, *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.

> **Warning >>**
> We recommend using Open Access in a limited, or test environment. 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.

Release Notes for Update 4.3.2895

Version 4.3.2895 is a maintenance update, mostly for migration issues, and was released on June 20, 2016.

Feature Enhancements in 4.3.2895

- Added the ability to download a p12 certificate without the chain. After generating a new certificate, the option is available on the *View Certificates* page.
- Added the ability to use variables as RADIUS attributes.

Bugs Fixed in 4.3.2895

- After an upgrade, a snapshot is successfully created if the device configuration contains no SSIDs or is an empty wired configuration.
- For upgrades, the yum call timeouts for download and install have been extended.
- When setting up a new onboard database user, the notification email sends the correct username.
- Wired network configuration information is not included in the Android configuration, as Android does not support wired 802.1x.
- If HTTPS is disabled prior to an upgrade, the administrator is no longer prevented from logging in after the upgrade completes.
- After an upgrade, the trust store is correctly rebuilt to avoid errors when using SMTP for outbound email or Twilio for outbound SMS notifications.

- Unused vouchers that show a value of '0' Uses prior to an upgrade will display '0 of 1' Uses after the upgrade.
- When using multiple MAC registration lists with the same SSID, the system will process the enrollment based on the latest MAC registration list.
- On a system using a shared database, the firewall requirements page lists the correct client IP address.
- Added options for Ubuntu version 16.04, and Fedora version 23 to the OS Settings for Linux. Previously, these versions were supported through the 'next version' flag.
- MAC Registration configurations using the pre-defined config shortcuts, and the POST setting checked (the default), retain this setting with a Save.
- When using the onboard user database, the check box for 'Include Admin Accounts' retains its setting with a Save.
- The OU is now included in the identity information in the enrollment record. Previously, the requested information was not returned.
- The DPSK is now included in the mobileconfig file.
- New account activation code links can be opened using the Internet Explorer browser. Previously, this browser displayed an invalid activation code error.
- When editing an authentication server configuration, the Name field cannot be left blank.
- The *Length of Access* field has been removed from the Cloudpath DPSK configuration. This value is set in the controller and cannot be overwritten. Because of this issue, you are limited to one policy per SSID.

System Updates in 4.3.2895

The scheduled backup and restore commands have been restructured to use the xtrabackup package. Use the following configuration utility commands:

```
# maintenance scheduled-backup mount remove
# maintenance scheduled-backup mount setup <adminuser> <adminpassword>
<pathtomount> <directoryname>  cifs
# maintenance scheduled-backup mount restore
```

Note >>
If you suspect that the <adminpassword> value to be incorrect, check the JBoss logs.

The *Full* backup should contain these files:

- backup-my.cnf
- ib_logfile0
- ib_logfile1

- ibdata1
- xtrabackup_binary
- xtrabackup_binlog_info
- xtrabackup_checkpoints
- xtrabackup_logfile

and these folders:

- lost+found/
- mysql/
- performance_schema/
- replication/
- shiro/

The *Incremental* backups should contain these files (in addition to the above listed folders):

- backup-my.cnf
- ibdata1.delta
- ibdata1.meta
- xtrabackup_binary
- xtrabackup_binlog_info
- xtrabackup_checkpoints
- xtrabackup_logfile

Release Notes for Update 4.3.2861

Version 4.3.2861 is a feature release with enhancements, and bug fixes.

This update was released on May 7, 2016.

What to Expect During an Upgrade to Cloudpath ES 4.3

Rebranding from XpressConnect to Cloudpath ES

Product branding has been changed from XpressConnect to Cloudpath ES. In addition to application branding, the executables and log files are also renamed.

Minimum Wizard Version

Because of the branding changes, when upgrading to Cloudpath ES version 4.3, the minimum wizard version must be version 5.0.386 or later, which is the first released Cloudpath-branded wizard.

Snapshots

When upgrading from version 4.2 to 4.3, 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-branded 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. Check the update/install logs on the System Updates page for upgrade status.

For more information, see the document, *How to Upgrade Cloudpath ES*, which is located on the Support tab of the Admin UI.

New Features in 4.3.2861

Support for PEAP on Cloudpath ES

Added the ability to support password-based PEAP authentication on the Cloudpath ES. Previously, PEAP/MSCHAPv2 was supported only with the Cloudpath Wizard product. While we still advocate using certificates instead of password for secure onboarding, the new capability for Cloudpath ES provides a migration path for customers using the Wizard product.

To configure a PEAP device configuration, select the Password (PEAP) Authentication style for the WLAN. The device configuration setup wizard prompts you to upload the RADIUS server certificate for an external RADIUS server.

Other credential prompt settings, such as *Display Behavior*, *Username Formatting*, and *Default Credentials* are set from the device configuration *Credentials* tab.

New Wizard for Mac OS X

The generation 2 wizard code, which was previously only available for the Windows OS, is now available for Mac OS X, version 10.8 and later. The new wizard code provides a smaller download package, it does not use Java, and provides improved monitoring of the network state during authentication.

To use the new Mac OS X wizard code, change the *User Experience* settings for the device configuration in your workflow.

Feature Enhancements in 4.3.2861

Updated Account Activation Process

Starting with the Cloudpath ES 4.3 release, new accounts can be created with activation codes, in addition to legacy Cloudpath License Server credentials.

When creating a new account, a Cloudpath License Server administrator adds an activation code to your account. When you log into the hosted server (or log into your on-premise VM), the Cloudpath ES system is tied to your account with the activation code instead of legacy credentials.

Simplified System Setup

The initial system setup for new Cloudpath accounts (cloud or on-premise) has been simplified to reduce errors made during the setup process. The Onboard CA, and the Onboard RADIUS server are setup by default, but can be changed when setup is finished.

The system creates a root and intermediate CA, and the RADIUS server certificate is created using the hostname and given a 5-year expiration.

Authentication Servers

Added support for Internal database users. This Authentication Server option enables end-users to authenticate to accounts defined within this system. This option is not meant to replace AD or LDAP system in a production environment, but is useful for trial and demo accounts because, with onboard database accounts, there is no need to open firewall ports for testing. It also allows you to create policies based on group information.

Navigate to *Configuration > Advanced > Authentication Servers*, click *Add Server,* and select *Use Onboard Database Server*. To add users, expand the onboard database server in the list and click *Add User*.

Licensing Information

The licensing information now includes system utilization statistics for Users, Authentications, MAC Registrations, Certificates, and Notifications. The links, viewable from the Support > Licensing page, add visibility for active concurrent device licensing for guest users.

MAC Registration Enhancements

- MAC Registration Lists can now be sequenced. This is useful because MAC registration filtering is based on first-match.
- To help alleviate common configuration issues with MAC registration, configuration shortcuts have been added for Ruckus Zone Director, Ruckus SmartZone, Cisco, Aruba, and Aerohive controllers.
- Added the ability to filter a workflow split by MAC Registration list.

Certificate Templates

- Added identity options for certificate templates that control whether the certificate's validity is tied to an identity.

  -User + Device - This is the default. The validity of the certificate is based, in part, on the identity of the user (if an identity exists in the enrollment). If the user is blocked, the certificate will be blocked.

-Device-Only - The validity of the certificate does not take into consideration the identity of the user. If the user is blocked, the certificate will not be affected. With this setting, OCSP does not perform a status check.

RADIUS Attributes

- Added support for the Ruckus Zone Director AP group RADIUS attribute.

Scheduled Reports

- Added server information to reports that have been configured as a scheduled task.

Device Configurations

- Added the ability set up a Ruckus Dynamic PSK device configuration.
- Added the ability to turn Hotspot 2.0 settings on or off for Android devices.
- Moved the Android setting, Trusted Root CA for Web Browsers (Machine), to the CA setting list, allowing it to display the correct UI (which allows the cert to be uploaded).
- Added the ability to add a background color on the AD credential prompt response.
- Added the ability to use a PAC URL to set proxy settings on Android OS version 5.0 and later.
- Added the ability to create a WPA2-PSK WLAN profile.
- Added the ability to disable *Connect to networks shared by my contacts (Wi-Fi Sense)* and *Connect to Suggested Open Hotspots* for Windows 10 devices.

Vouchers

- Added the ability to grant different sponsor permissions for bulk voucher creation. These permissions have been updated for onboard sponsors and for permissions granted in the voucher list.

  -*Allow Bulk Creation* controls the ability to create multiple generated vouchers and to upload CSV files.

  -*Allow CSV Upload* controls only the ability to upload CSV files.

Cleanup

- Added the ability to Reset Account or Destroy Account. This is useful for when you want to set up an account for demonstration purposes, or if you have an existing hosted account and are moving to an on-premise account. These destroy actions can be accessed from the *Administration > Advanced > Data Cleanup* page.
- Added a script to remove all snapshots. This is useful as part of the process prior to setting up replication. If there are no configuration snapshots on the system, a user attempting an enrollment receives a message that the system is currently disabled.

System Changes in 4.3.2861

PCAP

- Added the ability to grab a packet capture (pcap) file from the Cloudpath ES. From the Linux console, enter **tcpdump**.

Logging

- The syslog configuration now includes JBoss logs.
- Added the ability to set more than one host for where the syslog is sent.

Web Server Certificate

- Added the ability to upload multiple files when uploading a Web Server certificate.

Bugs Fixed in 4.3.2861

- Entering line breaks in the Verification Code Input Message text box no longer cause javascript errors.
- There is no longer a 4096 character limit when adding a custom CA certificate chain.
- The enrollment completes for an Android device set to use the Turkish locale.
- The CURRENT_SERVER_PK no longer remains cached after rebuilding a cluster.
- The SMS Gateways page has been removed from the Cloudpath Admin UI because they are no longer displayed during enrollment.
- When using an SSL port that is not the default, the Sponsorship portal link now displays the updated port.
- When importing the P12 certificate file, a password is always set. The password is derived from (the first matched of) AD/LDAP password, the last 4 digits of the SMS, the voucher, the user's email address, or the assistance ID.
- RADIUS PAP administrator logins are no longer restricted to 16 characters.
- Snapshot creation no longer fails if the referencing device configuration has zero SSIDs or an empty wired configuration.
- If an LDAP authentication server is configured with strip name enabled and username attribute as a non-existent value, and the user enters a domain\username, the enrollment's username variable is correctly set.
- Enrollment records download correctly to an XLS file.
- The /enroll pages will now by default use the output from hostname (in a cluster) rather than the hostname within the enroll URL.
- When configuring the proxy server in ES for iOS devices and Max OS X devices, the port is correctly passed to the device.

- When hostname-restricted is enabled, attempting to connect using an IP address the browser correctly shows a Page Not Found message.
- Using a REST API to get an Enrollment record by MAC address works as expected.
- There is no longer an issue extracting the cab file with running an enrollment on Windows 7/8/10 devices with the non-Unicode language set to Chinese/Japanese.
- The Japan +81 country code has been added to the SMS Country list for Twilio.
- When a voucher is created, the date, time, and timezone are displayed for that voucher. Previously, there was a timezone discrepancy for clients enrolling on hosted systems because it displayed the date in UTC.
- If your configuration includes additional CAs, they are now installed correctly in Android OSes 4.0, 4.1, 4.2, and 4.3.

Release Notes for Update 4.2.2630

Version 4.2.2630 is a maintenance release to address 4.2 migration issues.

This update was released on December 23, 2015.

Bugs Fixed in 4.2.2630

- Fixed an upgrade issue wherein snapshot creation after an upgrade may display an error if a Display Message plug-in is used in the workflow.
- Fixed an issue that caused MAC registration to fail if using a Ruckus SmartZone controller with the *encrypt-mac-ip* setting enabled. This setting in the SmartZone controller must be disabled when integrating with Cloudpath ES.
- The Look & Feel custom background colors now render correctly after the upgrade.
- During initial setup, the system did not check for duplicate administrator email addresses on the company information page. This could cause duplicate administrators to be created in the database, which locked the administrator account and prevented logins.

Release Notes for Update 4.2.2626

This update was released on December 10, 2015.

New Features in 4.2.2626

Administrator Roles

This update adds support for different administrator roles:

- A *CA Administrator* has full configuration and view access to the system.

- An *Administrator* has full configuration and view access to the system, except CA certificates and the private key.
- A *Viewer* has view-only privileges, mostly contained to user, device, or enrollment information. The viewer role has no configuration access and is useful for helpdesk administrators.

Feature Enhancements in 4.2.2626

Additional APIs

The following APIs have been added to the Cloudpath system:

- Register MAC address - Registers the MAC address for the specified device to a specified MAC Registration list.
- Device Capabilities Query - Checks for Hotspot 2.0 capabilities.
- Device Authorization - Authorizes a device on the system.
- Change MAC address - Changes MAC address for an enrollment record.
- Get Device Info by Certificate Serial Number - Queries customer account number for a certificate.
- Get Devices For External ID - Returns all devices associated with a customer account number.
- Get Device Info by MAC address - Queries customer account number for a MAC address.
- Revoke By MAC address and External ID - Revokes one or more certificates associated with a customer account number and specified MAC address.
- Revoke By Certificate Serial Number - Clear Device Capability Cache.
- Destroy Enrollments for External ID - For Testing Only.

OS Settings

- An OS Setting has been added to the Android User Experience, which allows you to suppress the *Rate this App* option. When checked, the *Rate this App* button appears after a successful connection. When unchecked, it does not appear.
- Instructions for manually configuring Windows RT and Windows Phone (8+) are now independently configurable within the Device Configuration.
- Fixed an issue with unmanaged Chrome OS when configuring a “manual” web proxy with a static IP and port.

Workflow Plug-Ins

- Added the ability to set a kill session flag in the *Display Message* workflow plug-in. When set, the session is destroyed when the page is loaded.
- The certificate information for Concurrent Certificates has been enhanced, with the end-user devices sequenced by date issued, listing the oldest enrolled device first.
- For enrollment workflows that do not issue certificates, such as those for MAC registration, you can add an event notification URL to be called based on completion of the workflow.

- Added the ability to enforce a CAPTCHA on the login page for Active Directory and LDAP.
- Added the ability for a branch in the workflow to contain more than 16 options.

Vouchers

- Added the ability for an SMS/email voucher prompt in the workflow to accept vouchers from multiple voucher lists. This, for example, allows a sponsor-created voucher to be submitted on the same screen used for SMS-based authorization.
- Added the ability to use a single voucher code to enroll multiple devices. With this setting, which is controlled in the voucher list, you can specify the number of times a voucher can be reused, or you can suppress this setting for sponsors.

Dashboard

- Added certificate template notifications to the Workflow Information table in the Enrollment record.
- Updated the method for displaying the username in the Enrollments table, to include information gathered from a Data Prompt.
- Added URLs for remote monitoring.

  -/constant/ping.html - tests the web server

  -/admin/ping - tests the application server

  -/enroll/ping - tests the enrollment portal

Certificate Templates

- Added the Start of Half and End of Half settings to the certificate template Start Date and Expiration Dates to allow certificate validity period to be based on a semester schedule.
- Added the ability to include Airespace and Ruckus WISPr VSAs to the RADIUS policy. These VSAs can be added via the certificate template.

System Changes in 4.2.2626

Code-Signing Certificate

- By default, the ES uses the web server certificate as the code-signing certificate to allow iOS devices to display the green “Verified” label, and the System Services page has been updated to reflect this change. A separate code-signing certificate can be uploaded, if desired, but is not normally necessary.

Command-Line Utility

- The restructured the **maintenance scheduled-backup** commands to allow backup via SCP or a mounted (CIFS) drive. New commands include:

  -maintenance scheduled-backup mount setup

-maintenance scheduled-backup mount remove

-maintenance scheduled-backup scp setup

-maintenance scheduled-backup scp remove

Web Server Certificate

- Added the capability to specify one or more Subject Alternative Names (SAN) when generating the CSR for a web server or RADIUS server certificate.

Data Cleanup

- Added the ability to remove old wizard builds and resources on the *Administration > Advanced > Data Cleanup* page.

Bugs Fixed in 4.2.2626

- The system no longer throws an error when the workflow does not capture a username but contains a split with a regex based on username.
- If only the root and intermediate CA are uploaded to a device configuration, and the RADIUS server certificate name is blank, the Connect to Servers flag in the Windows configuration is no longer set by the system.
- If an invalid CSR is detected, the system returns the correct error string.
- The Chrome extension ID for the *XpressConnect Certificate Generator* has been added to the Managed Chromebook Setup Instructions.
- Certificate notifications by 'Specified Date' are correctly sent by the system.
- An error is no longer generated when using the exclamation point character in an SSID name.
- The device configuration description is only visible to administrators and no longer displays to end-users in the profile description.
- The link for the XpressConnect application in the Amazon Appstore has been updated.
- If you include an additional (web) CA in your device configuration, the ONC file for an unmanaged Chromebook shows this CA as trusted.
- Scheduled Reports are now correctly sent by the system. Previously, the scheduler could stop under certain conditions and not process scheduled reports until restarted.
- Documentation links on the *Support > Documentation* page open up in a new tab, rather than in the same window.
- Fixed a thread lock issue that could impact the performance of the system on loads exceeding 450 enrollments per minute for 24 hours.
- Updated the SHA1-to-SHA2 conversion to reuse the serial number by default.
- When Microsoft CA template displays warning that configuration is out of sync, it will not specify the local and remote values.

- Enhanced the upgrade UI and process to provide better feedback on completion status. This will take effect when upgrading from this version.
- Prevent the OCSP accounting threads from shutting down if an exception occurs.
- When reviewing a table of data, the query-by-example lines now support wildcards anywhere, allowing queries like bob@*cloudpath.net.