
Using DPSK with Cloudpath

Best Practices and Design Guide – April 2017

Copyright Notice and Proprietary Information

Table of Contents

Cloudpath Overview **5**
What is the Cloudpath ES **5**
Certificate Management 6
Policy Management 6
Device Enablement 6
Why Use Cloudpath? **6**
Overall Benefits of Cloudpath **6**
Configuration Requirements **6**
DPSK + Headless Devices Overview **8**
What is Ruckus DPSK? **8**
What Are "Headless Devices"? **8**
Using Cloudpath with Ruckus DPSK **8**
Directly registering a device 8
Indirectly registering a device 9
Configuration Procedure 9
Step 1: Configure the DPSK-enabled SSID 9
Step 2: Configure access to the Ruckus WLAN controller for Cloudpath ES 12
Step 3: Configure Cloudpath to distribute DPSKs 16
Congratulations: you are done 21
Displaying the DPSK for a Media Device in the Portal **21**
This message: 22
Produces this result: 23
Branching users by identity and adding Dynamic VLANs to the DPSK assignment **23**
Viewing and Deleting DPSKs in Controllers **28**
ZoneDirector 9.13 28
SmartZone Essentials 3.4 28
SmartZone High Scale 3.4 29
SmartZone 3.5 (Essentials and High Scale) 30
About Ruckus **31**

Intended Audience

This document covers special topics when designing and deploying Cloudpath ES work flows, specifically integration with Ruckus DPSK WLANs. It is written for and intended for use by technical engineers with a background in Wi-Fi design and 802.11/wireless engineering principles in general, and Ruckus Wireless WLA systems in particular. Furthermore, it covers special Cloudpath subjects, and is not an initial deployment guide. For initial deployment, the reader should see the documents listed below on the Ruckus Support Site and it is necessary to have a working Cloudpath ES system, as well as a Ruckus WLAN – either ZoneDirector or SmartZone manged – in order to duplicate the configuration examples.

Cloudpath ES documentation:

- CP_ES 5.0 (GA) Quick Start Guide
- Cloudpath ES 5.0 (GA) Deployment Checklist
- Cloudpath ES 5.0 (GA) Deployment Guide

Best Practices & Design Guide

Using DPSK with Cloudpath

April 2017

Cloudpath Overview

The Cloudpath Enrollment System (ES) is a Security and Policy Management platform that provides a single point-of-entry for devices entering the network environment. The Automated Device Enablement (ADE) approach gives network administrators control over the onboarding of new devices by blending traditional employee-centric capabilities (Active Directory, LDAP, RADIUS, and Integration with Microsoft CA) with guest-centric capabilities (sponsorship, email, SMS, Facebook, and more).

The Cloudpath ES can differentiate the devices by ownership, in addition to just device type, offering the world's first solution to extend secure Set-It-And-Forget-It-Wi-Fi™ to all users, devices, and networks without manual IT involvement.

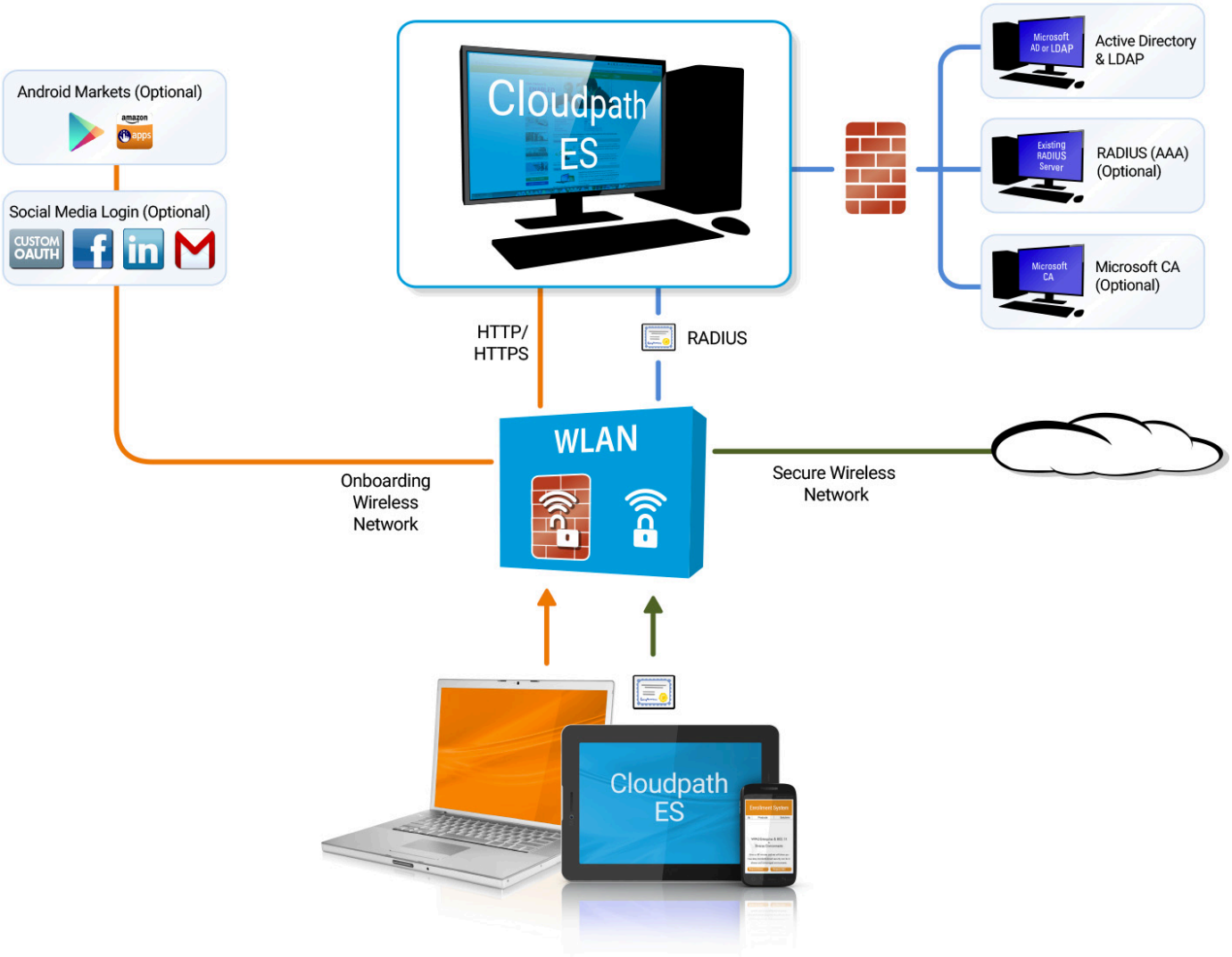

FIGURE 1: CLOUDPATH ES DEPLOYMENT EXAMPLE

What is the Cloudpath ES

Cloudpath Enrollment System is a security management platform with three components: Certificate Management, Policy Management, and Device Enablement. The combination of these capabilities creates a powerful new way to provision, secure and enforce policy on every device connecting to the network, through simple portal based self service for end users. Cloudpath ES is the industry's first Automated Device Enablement (ADE) solution.

Certificate Management

Cloudpath ES software includes a built-in, comprehensive Certificate Authority (CA) that enables any IT department to create and manage its own Public Key Infrastructure (PKI). A built-in RADIUS server and user database greatly simplifies installation and setup and helps in tying policies with certificates. In addition to built-in capabilities, APIs and other mechanisms enable Cloudpath software to easily integrate with existing external CA, RADIUS and user database infrastructures.

Policy Management

Cloudpath ES software provides IT with a simple, workflow-based policy management portal that can be used to establish granular policy-based access control for all users and all devices. The policy engine identifies client and user privileges and applies the correct policies to each user and each device. The software works together with policy enforcement points to ensure policies are properly exercised.

Device Enablement

Cloudpath ES software enables portal-based, self-service onboarding for end users and their devices and further enables pre-boarding for users and devices prior to their arrival at a given location. To ensure the network is properly protected, administrators can control which devices are allowed to join the network and can ensure the requisite on-device enforcement, such as enabling a firewall, installing certain applications, or updating anti-virus software.

Why Use Cloudpath?

The Cloudpath ES provides one portal for automatically onboarding and provisioning authorized devices on the secure network. The process is simple enough to be self-service by end users on an open captive portal, and automated so that the migration to the secure network can be managed without contacting the help desk. Cloudpath achieves this through the use of a dissolvable agent for the initial configuration and provisioning. Cloudpath creates a better Wi-Fi experience by simplifying the network, and implemented in your existing WLAN or wired infrastructure using standards-based security and policy mechanisms.

With user and device authorization, issues with sniffers, snoopers and evil twins are prevented. The reporting capabilities allow user and device visibility and control, so that a network administrator can easily view what is happening on the network.

Overall Benefits of Cloudpath

There are many configuration options and benefits that make Cloudpath a good choice in a variety of environments. These include:

- Reduce manual intervention by IT for network access and device provisioning – end password trouble tickets and end-user device configuration by IT
- Peace of mind – all users, including guests, and devices, including BYOD, are securely connected in a policy-compliant fashion. Network data is more secure because policies keep unauthorized users out
- Quick remediation – devices are associated with users, enabling identity-based policies and rapid remediation of usage violations
- Simplicity – intuitive workflows speed policy configuration. Per user licensing means there's no need to guess device count. Price is all-inclusive. Works with the network you have
- Better end-user experience - provision and configure devices one time and one time only. Same process for all device and device types. Hassle-free roaming across campuses.

Configuration Requirements

This document requires the following:

- Cloudpath ES system (cloud or on premise) pre-configured for basic enrollment service
    - Please see the following documents on the Ruckus Support site (https://support.ruckuswireless.com/documents?filter=89#documents)
        - Cloudpath ES Deployment Checklist
        - Cloudpath ES Quick Start Guide
        - Cloudpath Es Deployment Guide

  - Ruckus offers a "White Glove Service" remote deployment assistance for initially deployment that you may wish to make use of.

- A Ruckus Wi-Fi network, either ZoneDirector or SmartZone managed
- Appropriate user database
- Devices to be onboarded

DPSK + Headless Devices Overview

What is Ruckus DPSK?

When a user asks "what's the Wi-Fi password?", in strict network security terms, they are asking for the Pre-Shared Key, or PSK, of the WLAN. "Pre-shared", because everyone knows it, and "key" because it unlocks the WLAN's privacy encryption. It is perfectly good security for a home WLAN or a small office with a limited number of users, but not good practice in even the smallest of schools. However, Ruckus has a technology that can piggy back on PSK WLANs and give every device a unique encryption key ("Wi-Fi password").

Dynamic Pre-Shared Key (DPSK) is a patented technology that can provide robust, secure wireless access, with a specific key for each network connected device, including devices that only accept PSK level security. Dynamic PSK creates a unique encryption key (up to 63 bytes) for each device accessing a PSK WLAN. There is a master PSK for the WLAN, however there is no need to share it (it can be used if needed by IT personnel). With Ruckus DPSK, devices that do not support 802.1X and certificates can still be uniquely registered and tracked on the network with a record of the registering owner. Or, if there a full certificate PKI is not desirable, DPSK can be used with all WLAN connected devices.

VLAN tagging with DPSK

VLAN tags can be set as part of DPSK creation. This can be used in a number of ways in conjunction with Cloudpath ES to enforce network policies. Headless devices could be assigned to particular VLANs or even matched to VLANs that align with 802.1X-based asignemnts by user identity.

What Are "Headless Devices"?

Unlike a laptop, smartphone or tablet, headless devices typically lack a traditional monitor and have a limited input. Examples include WebTV devices (Roku, AppleTV, Chromecast), interactive whiteboards, printers, possibly game stations, etc. Typically, such devices do not support 802.1X security and are limited to PSK or open WLANs. They are generally marketed for home use, and the designers, not unreasonably, expect them to use home networks which typically do not rely on full blown RADIUS based PKI certificates.

Nevertheless, these devices are often useful in the classroom, even if the original design has not accounted for robust network security. However, Cloudpath ES can utilize another Ruckus technology, Dynamic Pre-Shared Key (DPSK) to enable simple onboarding and robust security of these devices.

Using Cloudpath with Ruckus DPSK

Cloudpath ES can be a key element in enforcing virtually any network policy, but there are two basic approaches to using DPSK with Cloudpath ES:

1) Directly register a device to use a DPSK WLAN and install the DPSK profile to the device immediately
2) Indirectly register another device, manually keying the DPSK into that device, possibly at a later time

Directly registering a device

To use the Cloudpath ES captive portal, a device must have a browser and support TLS encryption and certificates. That is nearly universal for laptops, tablets and smart phones, so for such devices, Cloudpath is generally used for certificate based 802.1X WLAN. However, it can just as easily be used for a DPSK based WLAN. You may have a situation where certificates would be overkill, or intimidating to end users, but the power of individualized encryption possible with DPSK is desirable. In that case, The Cloudpath ES workflow can be nearly identical to that of an 802.1X WLAN. The difference is that the final device configuration is the profile for a DPSK WLAN and includes the DPSK for the device accessing the registration portal.

This combination can be very powerful. Because the key is imbedded in the profile, the end user will not have to key in the DPSK and the full 62-byte option is practical. A 62 byte PSK is not crackable; it's uniquely tied to a single device and can be individually deleted. It is nearly as effective as 802.1X.

Indirectly registering a device

Headless devices, as discussed, are devices that lack features needed to support 802.1X certificates. Often they are home or consumer devices that the designers never intended for Enterprise deployments and Enterprise Class security. In this case, the end user would access the Cloudpath ES portal from a device that they would not want to finish registration and download a profile. We must design the workflow to deliver the DPSK to the screen or via email or SMS and the user will later (or right then) key it in to the Headless devices' interface. In this case, we will build the workflow to *not* download a profile and to *not* assign a device configuration. We also want to configure our DPSK for a manageable size, perhaps 8-12 characters instead of the full 62.

Depending on our policy needs, we can add a branch to the Cloudpath ES workflow for the user to "register a headless device" – or other language that will make sense to your users. Cloudpath can then be configured to check the user's credentials and, if accepted, communicate with the Ruckus Controller to generate a DPSK and keep a record of the registering user. The DPSK is sent to the user, and can be typed into the device like a normal "wi-fi password", at which point the DPSK is locked to that one device (bound to it's MAC address), and is already registered to the particular user.

Configuration Procedure

The following steps are required to configure Cloudpath with Ruckus DPSK.

1. Configure Ruckus controller (ZoneDirector or SmartZone) with a DPSK-enabled SSID
2. Configure the access to the Ruckus WLAN controller for Cloudpath ES
    - Enable the Northbound Interface for ZoneDirector
    - Create a username/password identity on SmartZone
3. Configure the Cloudpath ES workflow and deploy

Step 1: Configure the DPSK-enabled SSID

Keep in mind you can have multiple WLANs, including multiple DPSK WLANs. If you want ALL devices to use DPSK, you could put the direct registration devices on a 62-byte DPSK WLAN, and the headless devices on an 8-byte DPSK WLAN.

ZoneDirector DPSK WLAN Configuration

Use these steps to configure a WLAN with DPSK enabled on ZoneDirector controllers. You will create a standard PSK WLAN and then check the necessary options to enable DPSK. Note that, for historical reasons, we will need to enable Zero-IT to configure DPSK. However, we will not otherwise use Zero-IT (a precursor to Cloudpath ES). Also, we will add a "master" PSK to this WLAN. Keep in mind, this is a normal PSK ("Wi-Fi password") for the WLAN, and will work for any device or even any number of devices. Unlike the typical PSK WLAN, only the WLAN administrator should know this PSK. Ideally, no device should use this key because the point of DPSK is for each device to have a unique key. ALL devices that access the WLAN should be registered via Cloudpath ES and all should use a unique DPSK.

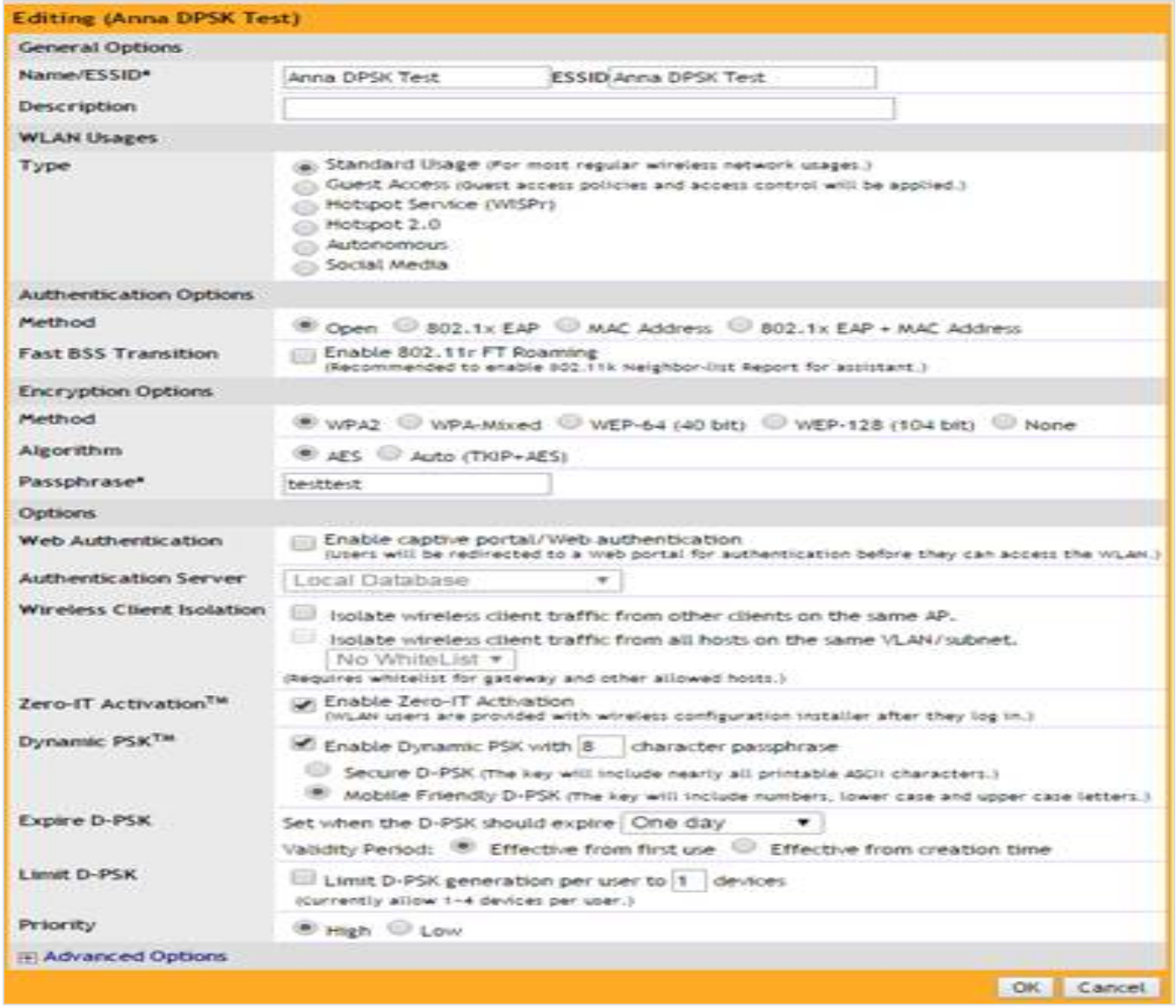

FIGURE 2: RUCKUS ZONEDIRECTOR WLAN CONFIG

1. Go to **Configure > WLANs**
2. Either **Edit** an existing WLAN or **Create New** to open the WLAN configuration form.
3. Under Type, select **Standard Usage**.
4. Under Authentication Options: Method, select **MAC Address** or **Open**.
5. Under Encryption Options: Method, select **WPA2** (*not* WPA-Mixed, as selecting WPA-Mixed will disable the Zero-IT activation option).
6. Under *Encryption Options: Algorithm*, select **AES** (not Auto, as selecting Auto will disable the Zero-IT activation option).
7. If using MAC Address authentication, choose an Authentication Server to authenticate clients against--either **Local Database** or **RADIUS Server**.
8. Ensure that the **Zero-IT Activation** check box is enabled.
9. Next to Dynamic PSK, enable the check box next to **Enable Dynamic PSK**. Select a DPSK passphrase length
    - If intended for direct device registration, we recommend the full 62 bytes and all ASCII characters options. If intended for a headless device requiring manual keying, the range of 8-12 is typical and the "Mobile Friendly" option is recommended.

10. Expire DPSK: Set when the DPSK should expire. In Validity period, choose whether the DPSK expiration period will start from first use or creation time.
11. *Limit* DPSK: By default each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs each user can generate (1-4).
12. Click **OK** to save your settings.

SmartZone DPSK WLAN Configuration

Use these steps to configure a WLAN with DPSK enabled on physical and virtual SmartZone controllers. You will create a standard PSK WLAN and then check the necessary options to enable DPSK. Also, we will add a "master" PSK to this WLAN. Keep in mind, this is a normal PSK ("password") for the WLAN, and will work for any device or even any number of devices. Unlike the typical PSK WLAN, only the WLAN administrator should know this PSK. Ideally, no device should use this key because the point of DPSK is for each device to have a unique key. ALL devices that access the WLAN should be registered via Cloudpath and all should use a unique DPSK

1. Go to **Configuration > WLANs**
2. In a vSZ-H, you may have to navigate to the correct admistrative domain and Zone before choosing WLAN
3. Either **Edit** an existing WLAN or **Create New** to open the WLAN configuration form.
4. Give it a Name and SSID (by default, it will copy the name to SSID)
5. Under Type, select **Standard Usage**.
6. Under Authentication Options: Method, select **MAC Address** or **Open**.
7. Under Encryption Options: Method, select **WPA2**
8. Under Encryption Options: Algorithm, select **AES**
9. Next to Dynamic PSK, enable the check box next to **Enable Dynamic PSK**. Select a DPSK passphrase
    - If intended for direct device registration, we recommend the full 62 bytes and all ASCII characters options. If intended for a headless device requiring manual keying, the range of 8-12 is typical and the "Mobile Friendly" option is recommended.
    - **Secure DPSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for clients whose keyboards may not contain the entire set of printable ASCII characters.
    - **Mobile Friendly DPSK**: Choose this option if this WLAN will be used for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which makes it easier for users to input the **DPSK** when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the **DPSK** length to 8 characters for the convenience of your mobile client users.)
10. Expire **DPSK**: Set when the **DPSK** should expire. In Validity period, choose whether the **DPSK** expiration period will start from first use or creation time.
11. *Limit* **DPSK**: By default each authenticated user can generate multiple **DPSK**s. Select this option to limit the number of **DPSK** s each user can generate (1-4).
12. Click **OK** to save your settings.
13. This WLAN is now ready to authenticate users using Dynamic Pre-Shared Keys, once Cloudpath ES has verified their credentials and issued a DPSK.

Virtual SmartZone - Essentials (vSZ-E-T

Dashboard | Monitor | Configuration | Report | Administration

WLANs

Access Network: Tunnel WLAN traffic through Ruckus GRE
Authentication Type: * Standard usage *(For most regular wireless networks)*
Hotspot *(WISPr)*
Guest Access
Web Authentication
Hotspot 2.0 Access
Hotspot 2.0 Secure Onboarding *(OSEN)*
WeChat

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: * WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
Algorithm: * AES AUTO (TKIP+AES)
Passphrase: * klaatubaradanikto Show
802.11r Fast Romaing: Enable 802.11r Fast BSS Transition
802.11w MFP: * Disabled Capable Required

Accounting Server

Accounting Server: Use the Controller as Proxy Disable

Options

Wireless Client Isolation: * Disable
Enable *(Isolate wireless client traffic from all hosts on the same VLAN/subnet)*
Priority: * High Low
Dynamic PSK: Enable Dynamic PSK with 12 characters passphrase
DPSK Type: * Secure DPSK (The key will use a mixture of nearly all printable ASCII characters)
Keyboard-Friendly DPSK (The key will use letters and number only and avoid unclear characters)
DPSK Expiration: * 2 years From first use

RADIUS Options

Advanced Options

Apply Cancel

Figure 3: Ruckus SmartZone WLAN config

Step 2: Configure access to the Ruckus WLAN controller for Cloudpath ES

ZoneDirector: Configure the Northbound Interface API

Use these steps to configure a password for the NBI API.

1. Go to Configure->System
2. Scroll down to Network Management and click the plus (+) sign to expand it

3. Tick the box titled Enable northbound portal interface support and add a password
4. Click OK to save your changes

Figure 4: Ruckus Zone Director northbound interface

SmartZone: Configure a DPSK generator user role and login for Cloudpath

Create a user role for DPSK generation in SmartZone v 3.4

5. In vSZ-E or Smartzone-100, navigate to “Administration -> Administrators – >Administrator Roles., or
6. In vSZ-H or “Configuration -> Administrators” and scroll down to “Administrator Roles.
7. Choose Create New
8. Name the new role (Ex. “cloudpath-dpsk”)
9. Deselect everything with the deselect all button (square with no checkmark)
10. Navigate the tree to Configuration -> Wireless Network -> WLANs ->WLAN
11. Under WLAN, check “create” and “new”
12. Click OK in the lower left corner to save the new role

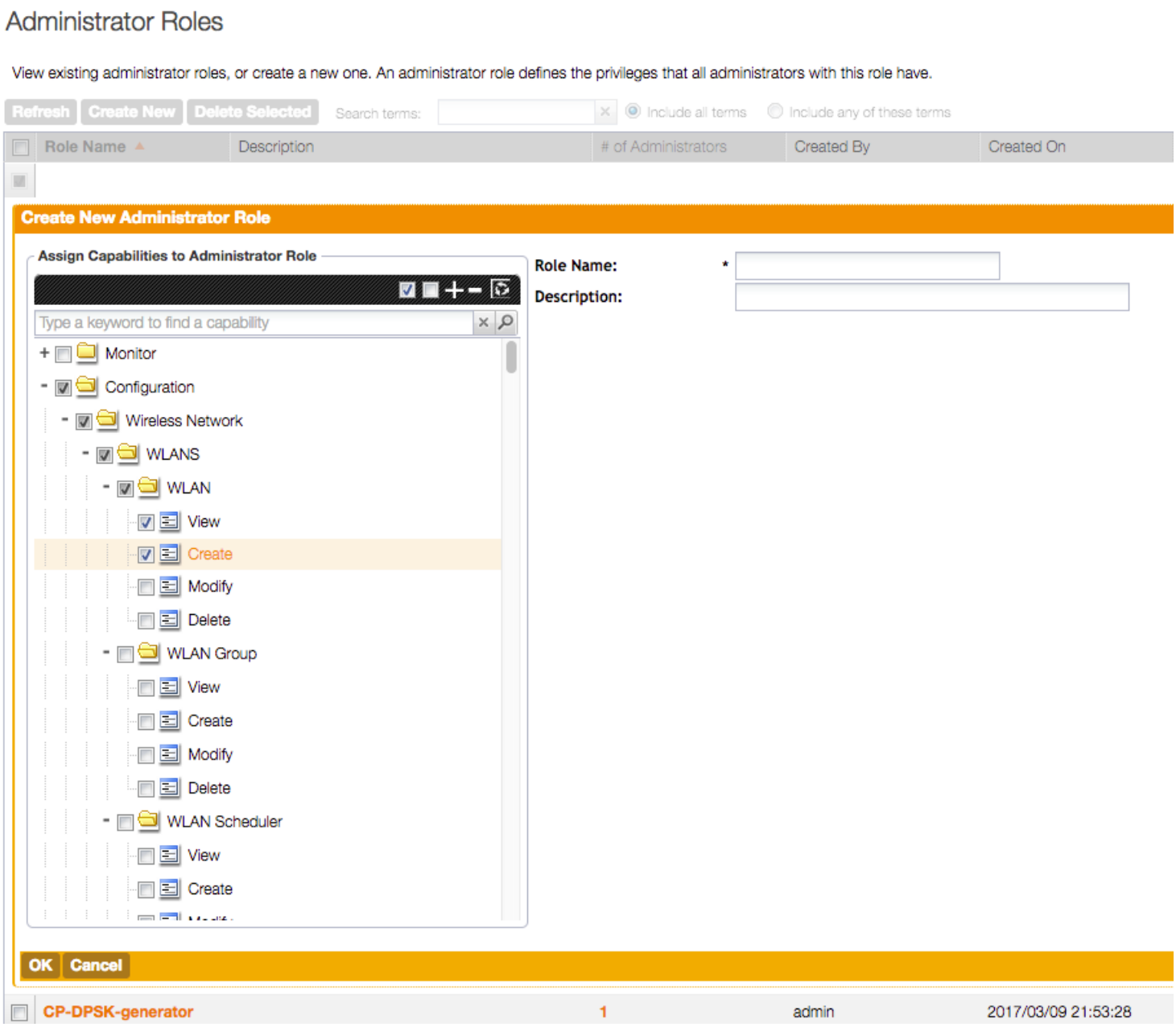

Figure 5: Ruckus SmartZone administrator role config

Create a user role for DPSK generation in SmartZone v 3.5

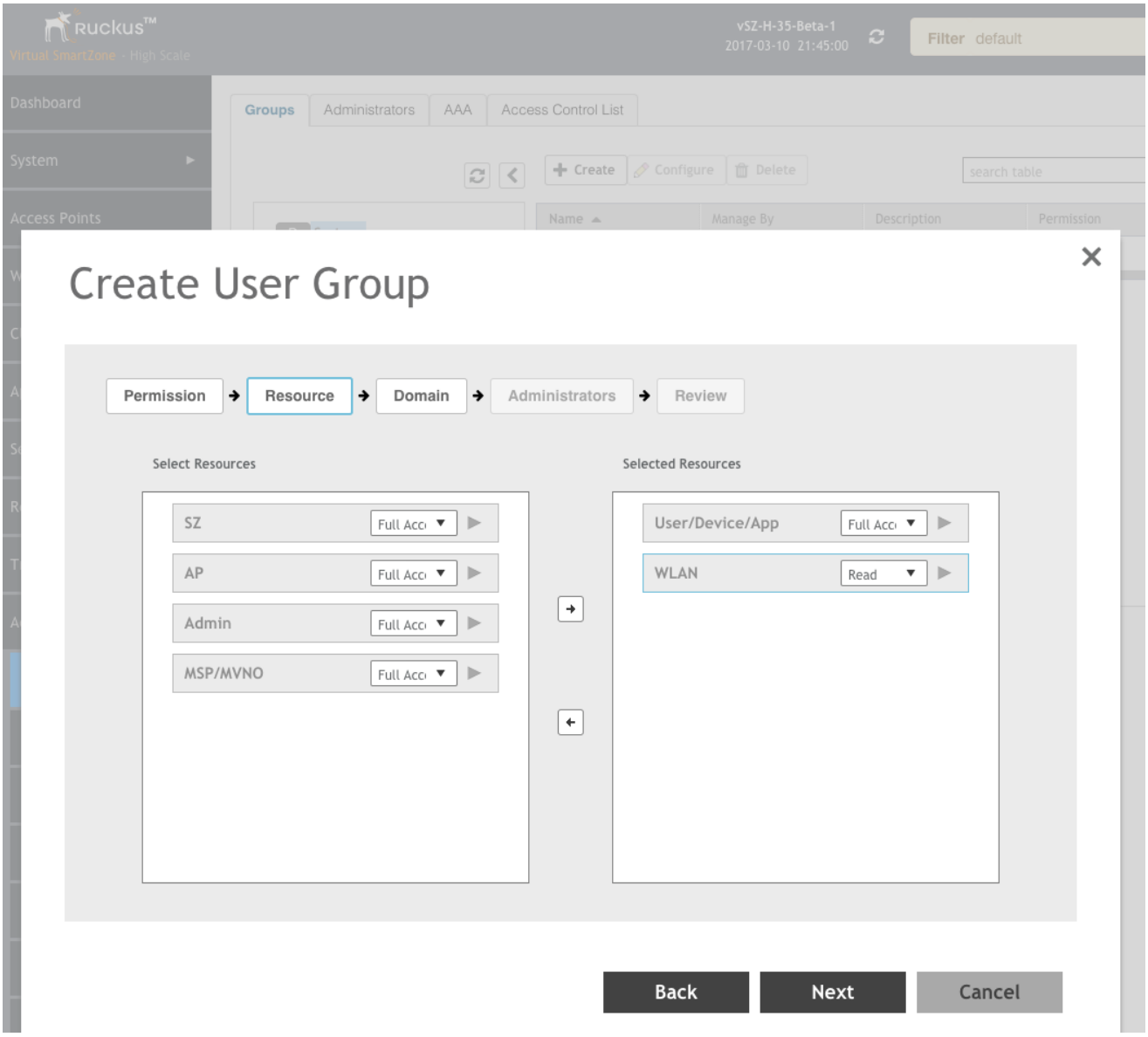

Figure 6: Ruckus SmartZone administrator role config

1. In all SZ variations, navigate to "Administration -> Admins and roles –> Groups.
2. Choose + **Create**
3. Name the new role (Ex. "cloudpath-dpsk")
4. Select "custom" in the permission drop down; click next
5. Select resources by clicking and then using the arrows to move to "selected resources"
6. User/Device/App – choose Full Access in the drop down
7. WLAN – choose Read Only in the drop down
8. Click next
9. In SZ-H, select domain(s), click Next
10. In "Configure User Group", click the plus sign ("+") near "Available users" to Create and Administrator Account
11. Create a login account for the Cloudpath ES; click OK

12. Select the new account by clicking on it, and use the arrows, to move it to "selected users." Click Next
13. Review and if acceptable, click "OK".

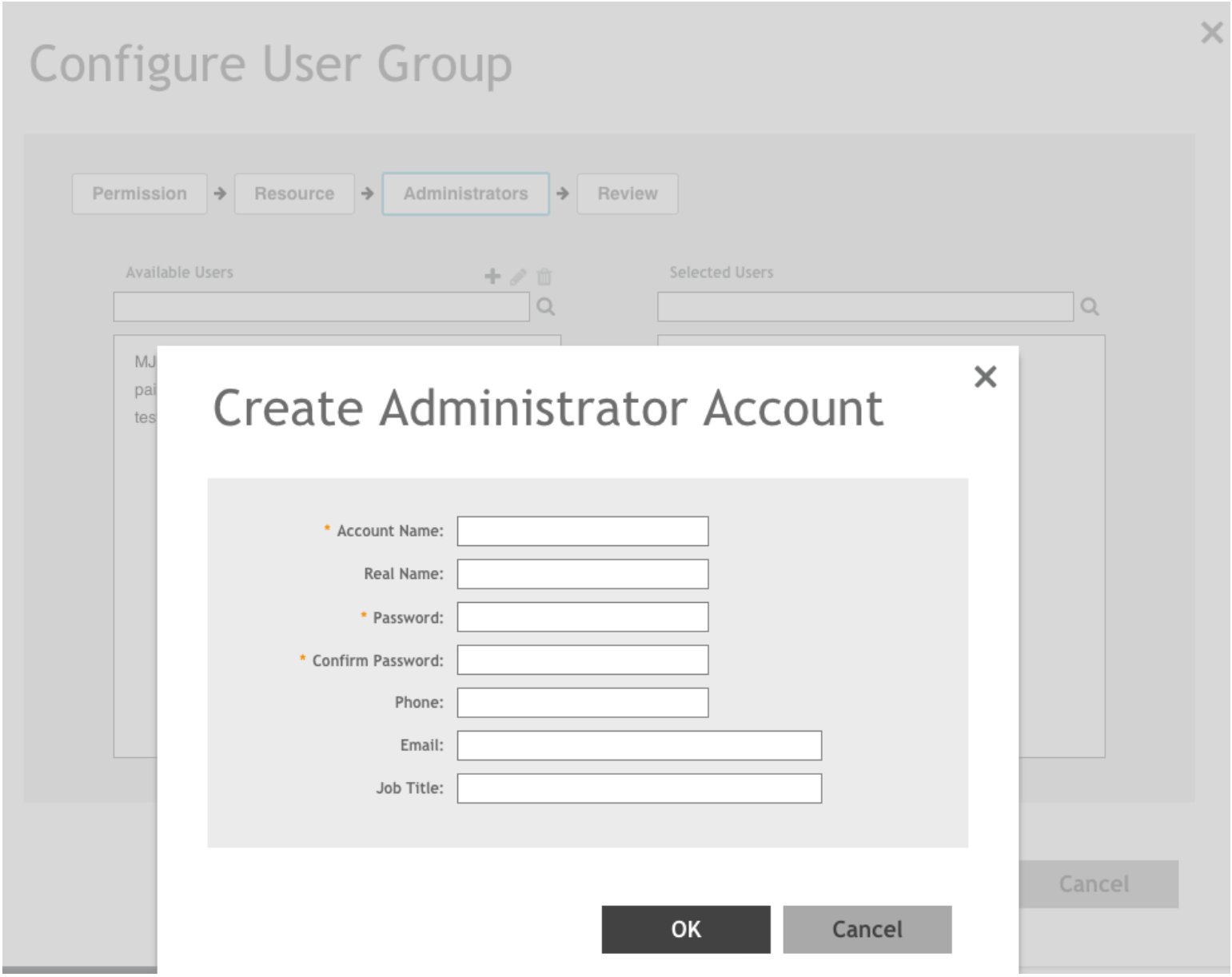

Figure 7: Ruckus SmartZone administrator account config

Step 3: Configure Cloudpath to distribute DPSKs

As previously discussed, there are multiple possible implementations depending on your specific network policy and needs. To provide a baseline, we will add a branch to an existing workflow specifically for headless device, and consider variations afterwards. You should already be familiar with the basics of building a workflow in Cloudpath. If not, please see the "Cloudpath Deployment Guide" and related documentation on the Cloudpath ES server or the Ruckus support site.

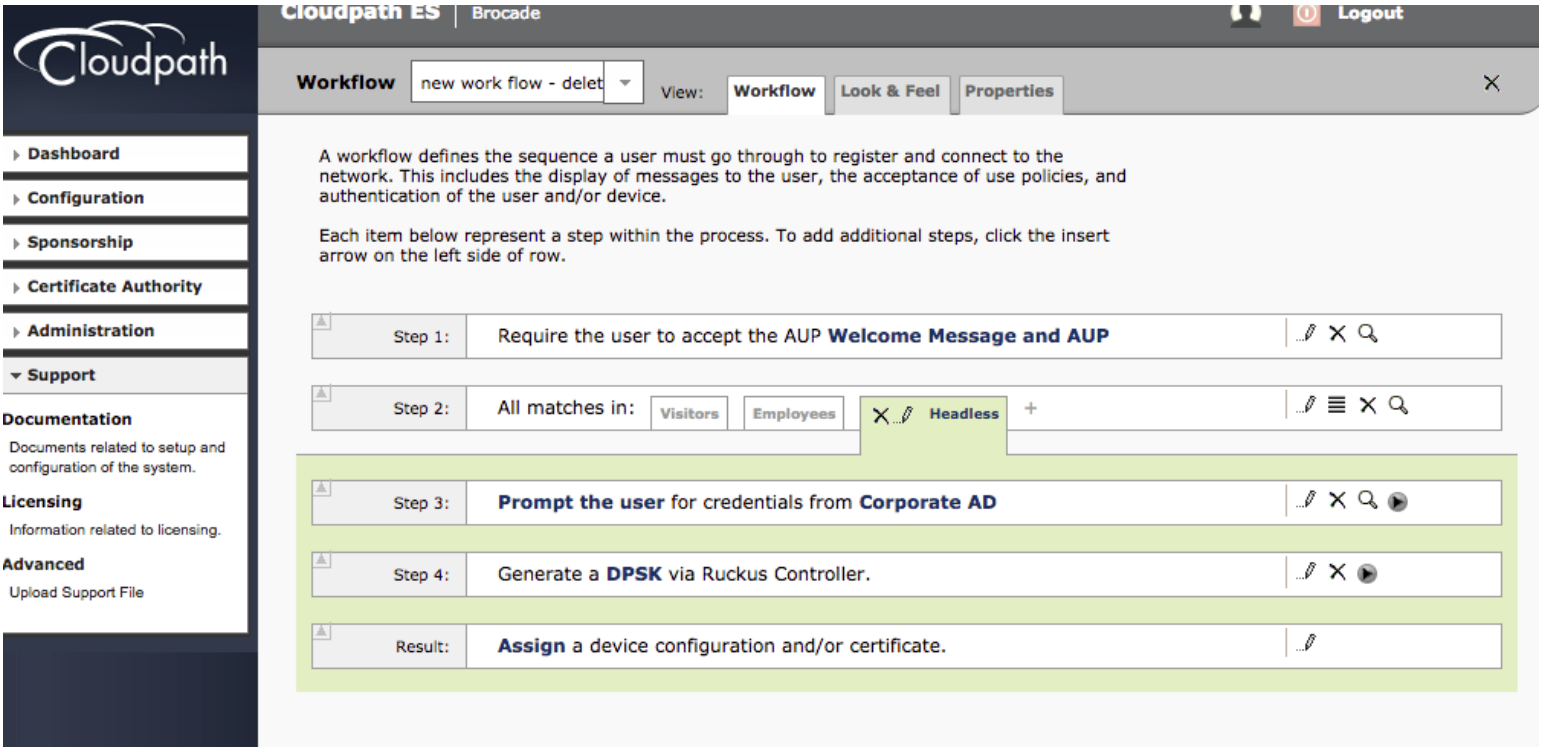

Figure 8: Ruckus SmartZone WLAN config

Basic workflow for DPSK (headless device)

1. Add a branch for headless devices
2. Add User authentication
3. Generate the DPSK – default behavior includes emailing it to user
4. Assign device configuration – this step is required for a workflow, but will be set to "none" since this is registration for another device.

Configure "Generate a DPSK via Ruckus Controller

1. Add a branch for Headless devices to the work flow
   i.e. – "Teachers, Students, Media devices"
2. Add a user authentication step –
   You can reuse an existing user authentication, such as one for Teachers
3. After user authentication, insert a step, scroll down the list and choose "Generate a Ruckus DPSK. Click Next.
4. Choose a new DPSK configuration, click Next
5. Give it a name and choose "ZoneDirector" or "SmartZone", as appropriate
6. For SmartZone
   a. Use the username and password you created in the previous section
   b. IP/DNS of the Smartzone, SSID and Zone as desired.
   c. VLAN ID is optional. Dynamic VLANs will be addressed in the next section
7. For ZoneDirector
   a. Use the password for the northbound interface you created in the previous section
   b. Chose the key length with the slider bar
   c. VLAN ID is optional. Dynamic VLANs will be addressed in the next section
8. Click Save

Authenticate via a shared passphrase.

Prompts the user for a passphrase and verifies it is correct. A shared passphrase is useful for controlling access to an enrollment process separate from, or in addition to, user credentials.

Generate a Ruckus DPSK.

Generates a DPSK via a Ruckus WLAN controller.

Send a notification

Generates a notification about the enrollment. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user.

Figure 9: Ruckus Cloudpath insert a step

Modify DPSK Cancel Save

Reference Information

Name: vSZ-JimS-DPSK *

Description:

Ruckus Northbound Portal Interface

Controller Type: SmartZone

WLAN IP/DNS: 192.168.85.210 *

Username: admin *

Password: •••••••••• *

Zone Name: Default Zone *

SSID: CP-DPSK-JimS *

VLAN ID: [ex. 90]

Notification

Email Subject: PSK Assignment

Email Template: The following PSK has been assigned to you:

${DPSK}

This PSK is registered to you and usable on only one device. The variable ${DPSK} can be used to represent the DPSK.

Figure 10: Ruckus SmartZone DPSK config

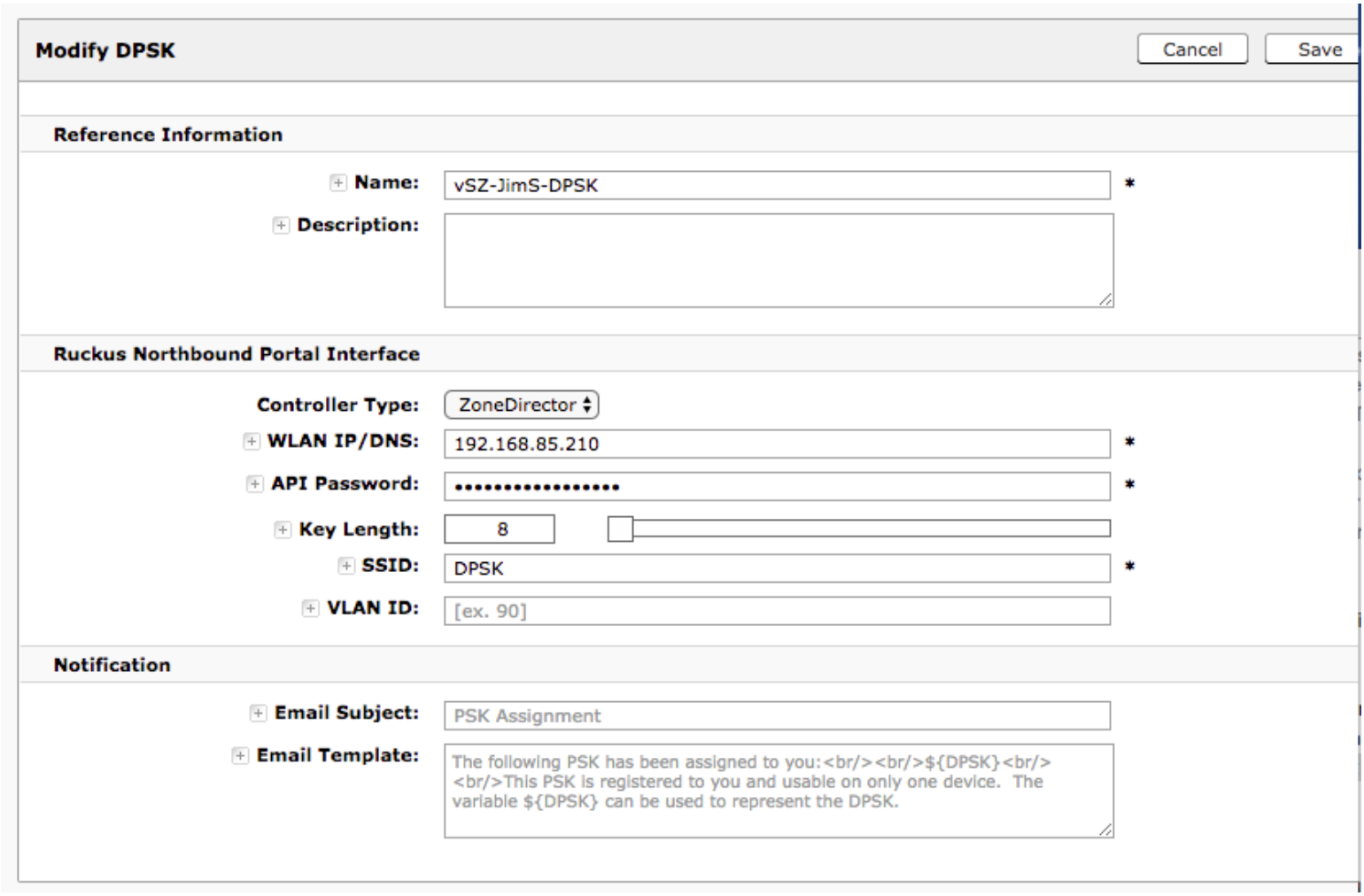

Figure 11: Ruckus ZoneDirector DPSK config

Modify the "assign a device configuration" step

Headless device: DPSK to be manually keyed on another device

Because this DPSK will be entered on another device, there is no need to download a profile unto the device doing the registration

1. At the final workflow step, "Assign a device configuration", click on the pencil icon to Edit
2. Choose "none" and click next
3. Choose 'Do not issue a certificate", click Next

Direct registration: Device is accessing the portal to register itself

When the DPSK WLAN profile should be installed on the access device

1. At the final workflow step, "Assign a device configuration", click on the pencil icon to Edit
2. Choose "a new device configuration" and click 'Next'
3. Name the new device configuration and click 'Next'
4. Fill in the SSID and under "Authentication Style" Choose "Ruckus Dynamic PSK". Click 'Next'
5. Several screens for options not strictly part of this discussion are presented. Accept the defaults for the moment or see other Cloudpath ES documentation
6. On the fourth screen, choose "do not issue a certificate to the user" and click 'Next'

Device Configuration

Add Device Configuration < Back Next >

A single device configuration may support wireless and/or wired connections.

Select the connection method(s) this device configuration supports:

Wireless Connections

The SSID of the wireless network. This value must be entered precisely. It is case sensitive.

SSID: DPSK-config2 *

This setting specifies the authentication used on the SSID.
Client Certificate [Recommended] - The SSID will be configured for WPA2-Enterprise using EAP-TLS.
Password (PEAP) - The SSID will be configured for WPA2-Enterprise using PEAP/MSCHAPv2.
Static Pre-Shared Key - The SSID will be configured for WPA2-Personal using a predefined, static pre-shared key (PSK).
Ruckus Dynamic PSK - The SSID will be configured for WPA2-Personal using a dynamic pre-shared key (DPSK).

Authentication Style: Ruckus Dynamic PSK
Is this SSID Broadcast? Yes, the SSID is broadcast.

Wired 802.1X Connections

Figure 12: Device Configuration settings for Direct Registration

Deploy the workflow to the correct location and test

Don't forget that a workflow must be deployed/published to the web server before an end user can access it. You can use the "User Experience" button for local testing.

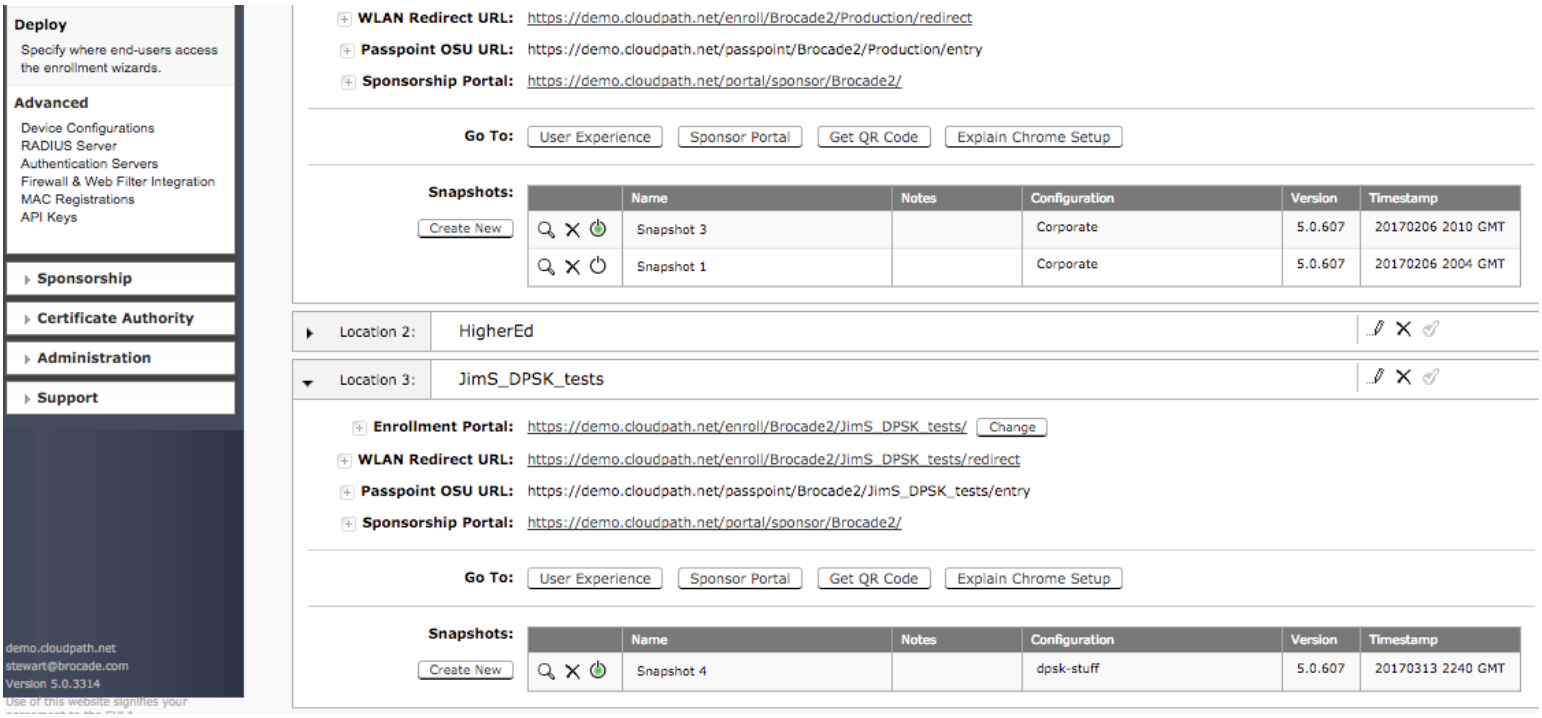

Figure 13: Cloudpath Workflow deployment screen

Congratulations: you are done

You have configured a DPSK WLAN and a Cloudpath ES registration portal for DPSK device registration. However, Cloudpath ES is almost infinitely configurable, and some special topics are discussed below.

Other Configuration options

Displaying the DPSK for a Media Device in the Portal

By default, the DPSK is emailed to the user. You can add a message that displays it to the screen.

1. Insert a step in the workflow after the DPSK generation
2. Choose "Display a message"
3. Click Next
4. Choose "A New Message from a Standard Template"
5. Name and modify the template to display the DPSK and an appropriate message
    a. Note that the template accepts HTML
    b. The DPSK itself can be represented as a variable with ${DPSK}

This message:

Modify Message

Reference Information

Reference Name: DPSK display *

Description:

Webpage Display Information

Page Source: Standard Template

HTML Title: The password (DPSK) for your device is...

HTML Message:

```
${DPSK}
<br><br>
It is a unique password, specific to one device, and will be locked to the
first device that uses it to access the network.  Be sure to use it on the
```

Bottom Label: this is the bottom label; don't forget to test "kill session"

Continue Button Label: Continue >

Show Continue Button: ☑

Show Back Button: ☑

Kill Session: ☐

Figure 14: Cloudpath message display config

Produces this result:

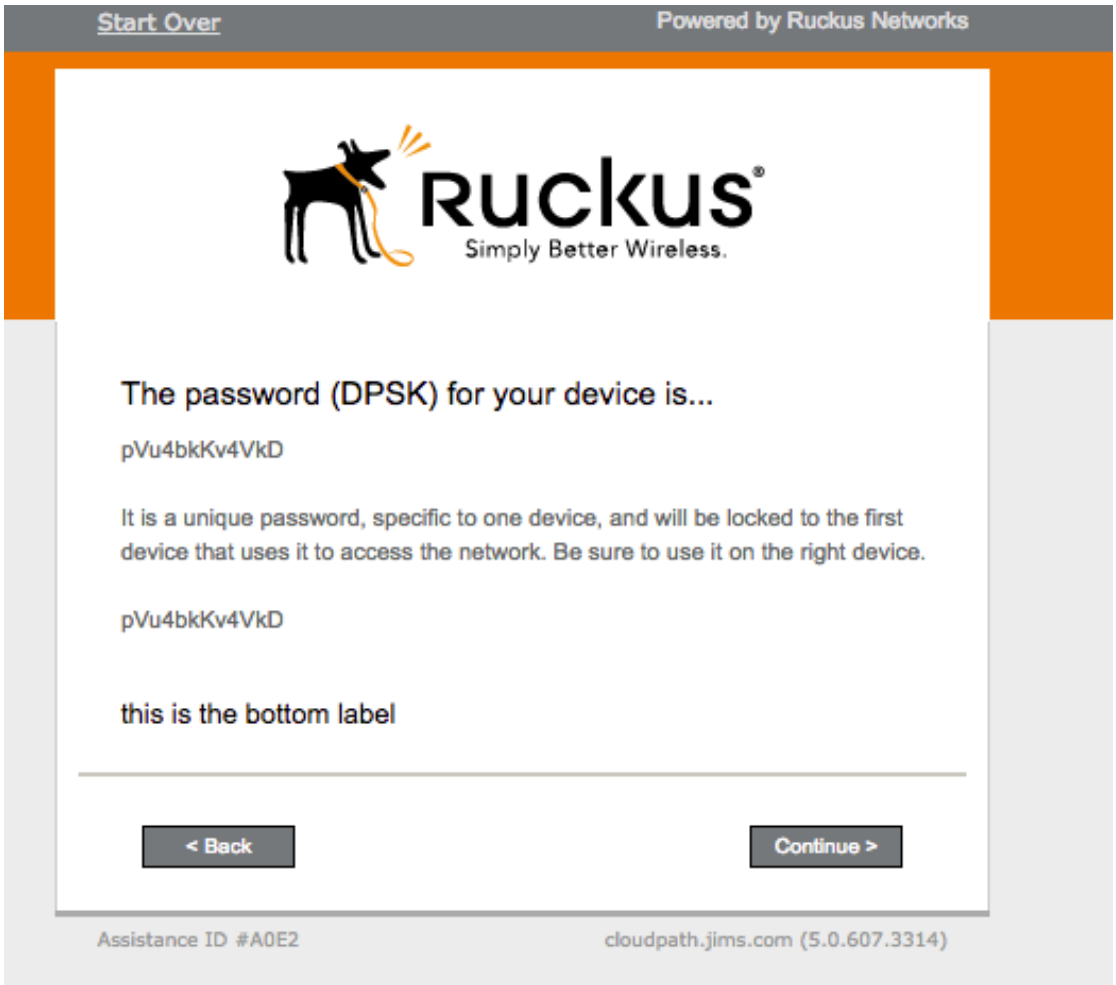

Figure 15: Cloudpath message display screen result

Branching users by identity and adding Dynamic VLANs to the DPSK assignment

Up to this point, we have assigned all DPSK devices to the same VLAN, whether tagged or native. That is, all DPSK devices are assigned to the same SSID and VLAN. However, VLANs and other options can be assigned based on user in put or credentials. For instance multiple DPSK devices can use the same WLAN/SSID but be VLAN tagged differently.

Please take note: this section is assuming that you are already applying user or user group based network Policy in your AAA servers. It is unlikely that this would make sense for headless devices other wise. This is intended to supplement an 802.1X based policy for supporting end user devices with a similar policy application for their headless devices. It usually does not make sense if the former is not in place, although network goals are infinitely variable. 802.1X policy is covered in the basic Cloudpath deployment documentation.

Configure WLAN controllers for Dynamic VLANs

1. SmartZones automatically include Dynamic VLANs with any DPSK WLANs. No changes are necessary
2. ZoneDirectors – in the edit screen for the DPSK WLAN, expand 'advanced options' and insure that the Enable Dynamic VLAN box is checked.

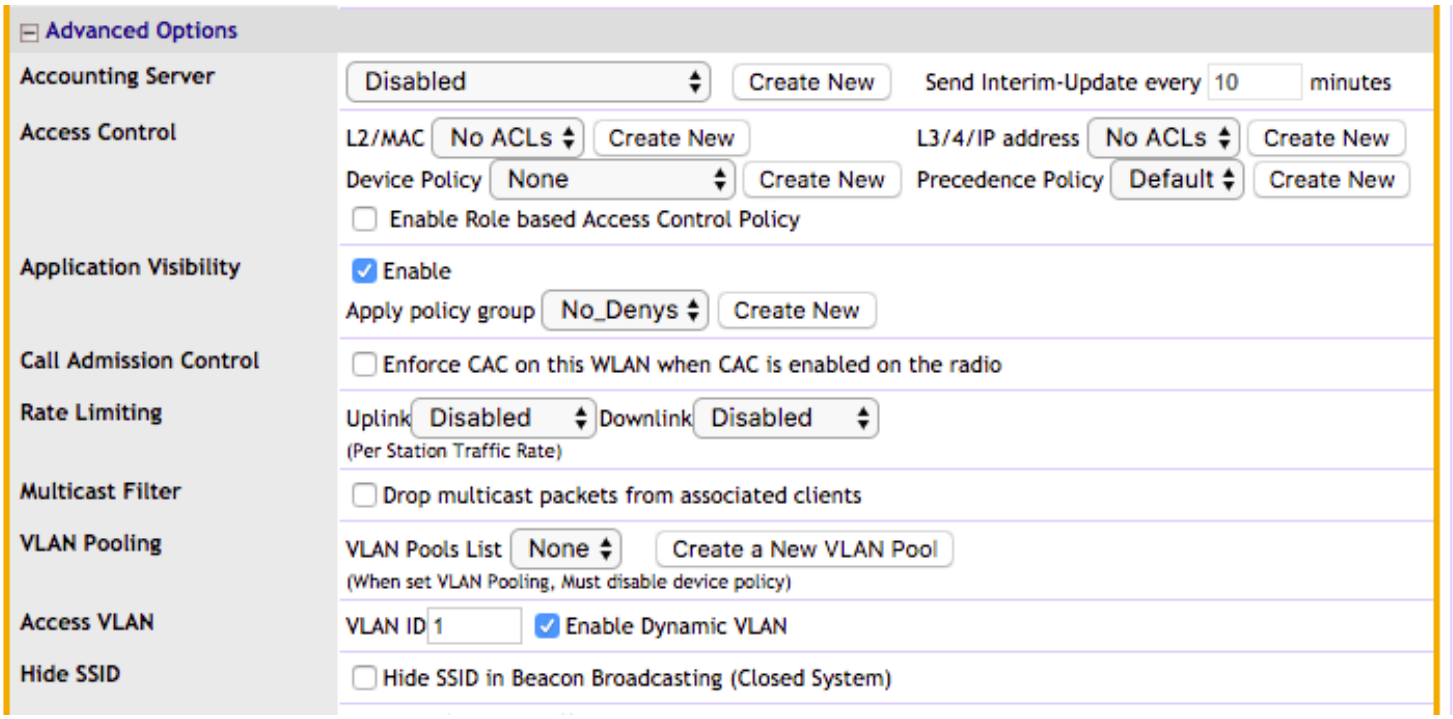

Figure 16: ZoneDirector enable dynamic VLANs

Create a group value in your user database for VLAN assignment

This will vary depending on your database. For Active Directory, this will normally involve creating a network policy group. For simplicity's sake, we are using the Cloudpath onboard DB to illustrate this the process. Note that we have included group assignments of VLANs

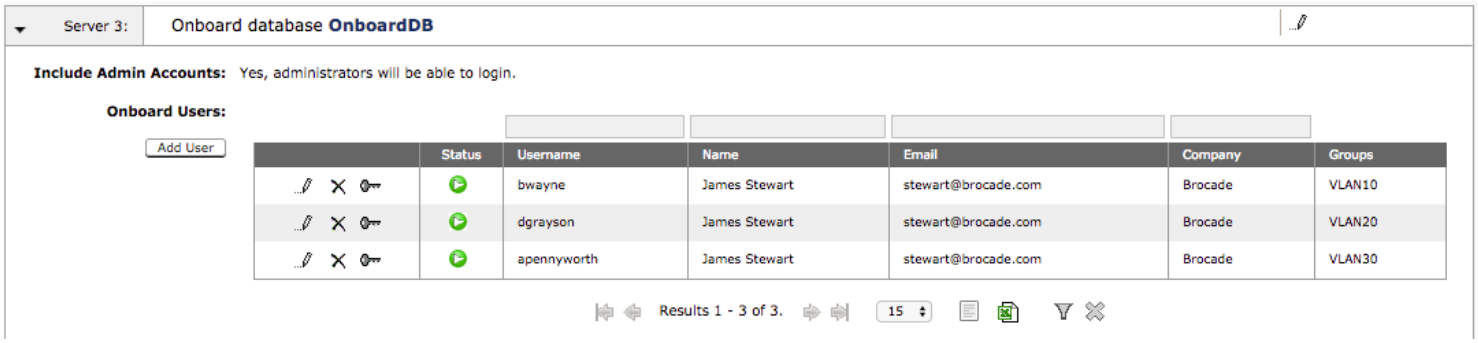

Figure 17: Cloudpath onboard DB example

Modify the Cloudpath workflow

3. In the Cloudpath Workflow, insert a step after "Prompt the user for credentials"
4. Choose "Split users into different branches"
5. Choose "use a new split"

What type of step should be added to the workflow? Cancel Next >

Display an Acceptable Use Policy (AUP).

Displays a message to the user and requires that they signal their acceptance. This is normally used for an acceptable use policy (AUP) or end-user license agreement (EULA).

Authenticate to a traditional authentication server.

Prompts the user to authenticate to an Active Directory server, and LDAP server, or a RADIUS server.

Ask the user about concurrent certificates.

Prompts the user with information about previously issued certificates that are still valid. This may suggest that old certificates be removed or may limit the maximum number of concurrent certificates.

Split users into different branches.

Creates a branch or fork in the enrollment process. This can occur (1) visually by having the user make a selection or (2) it can occur automatically based on criteria associated with each option. For example, a user that selects "Guest" may be sent through a different process than a user that selects to enroll as an "Employee". Likewise, an Android device may be presented a different enrollment sequence than a Windows device.

Figure 18: Cloudpath user split/branch config

Create Split Cancel < Back Save

Reference Information

Name: VLAN assignment split for headless DPSK *

Description:

Match Behavior: Use All Options That Match

Options

The following settings will setup initial options for this split. To add additional options or to tune the option, use the options icon (3 horizontal lines) on the previous screen.

Note: Steps currently existing in the workflow below the point of insertion will be assigned to the Option 1 branch.

Step 2: Split users by: Option 1 Option 2 Option 3 Option 4

Option 1: VLAN 10

Option 2: VLAN 20

Option 3: VLAN 30

Option 4: VLAN 40

Figure 19: Cloudpath split/branch config, cont.

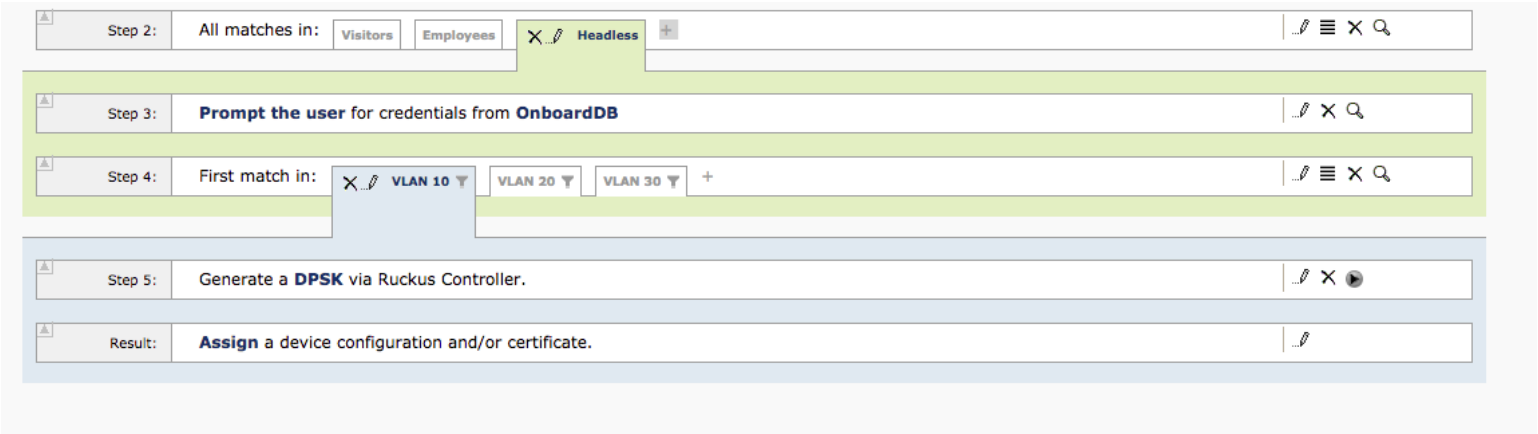

Figure 20: Cloudpath user split/branch result

6. Give the split a name and name the desired options
7. In a split like this, whether the options are displayed to the end user depends on what they are. If, as in this case, the options are automatic, they will not be displayed to the end user

Edit each branch of the split

8. Click the pencil at the top of a branch (by "VLAN 10" in the example)
9. Expand the "Filters & Restrictions" section
10. Enter an appropriate filter value, such as a group ID
11. Click "save" at the top

Webpage Display Information

Short Name: VLAN 10
Display Title: VLAN 10
Display Text:
Enabled: ☑
Icon File: Default: Using default file. Upload: Choose File No file chosen

Filters & Restrictions

The following settings control which users will have access to this option. If nothing is specified below, all users will have access to this option. If criteria below, only users meeting the criteria will have access to this option.

User-Based Filters

A regular expression that controls which user groups are allowed to access this branch. To filter against multiple AD groups, use a vertical pipe (|) separator between AD groups. For example, mygroup1|mygroup2.

Group Name Pattern:	Matches	VLAN10
Username Pattern:	Matches	[ex. bob]
User DN Pattern:	Matches	[ex. .*ou=IT,.*]
Email Pattern:	Matches	[ex. .*@company.com$]

Figure 21: Cloudpath filter config

12. add or edit a "generate a DPSK" step
13. This time, include the VLAN ID that you want to map to your filter condition
14. Click Save

Ruckus Northbound Portal Interface

Controller Type:	SmartZone	
WLAN IP/DNS:	192.168.85.210	*
Username:	admin	*
Password:	••••••••••	*
Zone Name:	Default Zone	*
SSID:	CP-DPSK-JimS	*
VLAN ID:	10	

Notification

Figure 22: DPSK with VLAN ID

15. Check that the "assign a device configuration" step leads to "none" and "Do not assign a device configuration"
16. Repeat for the other branches.

Filters are a powerful tool in Cloudpath, and can be used for a wide variety of branching and configuration options.

Viewing and Deleting DPSKs in Controllers

ZoneDirector 9.13

Monitor -> Generatred PSK/Certs

Note that user name, VLAN, MAC Address and creation date are all captured

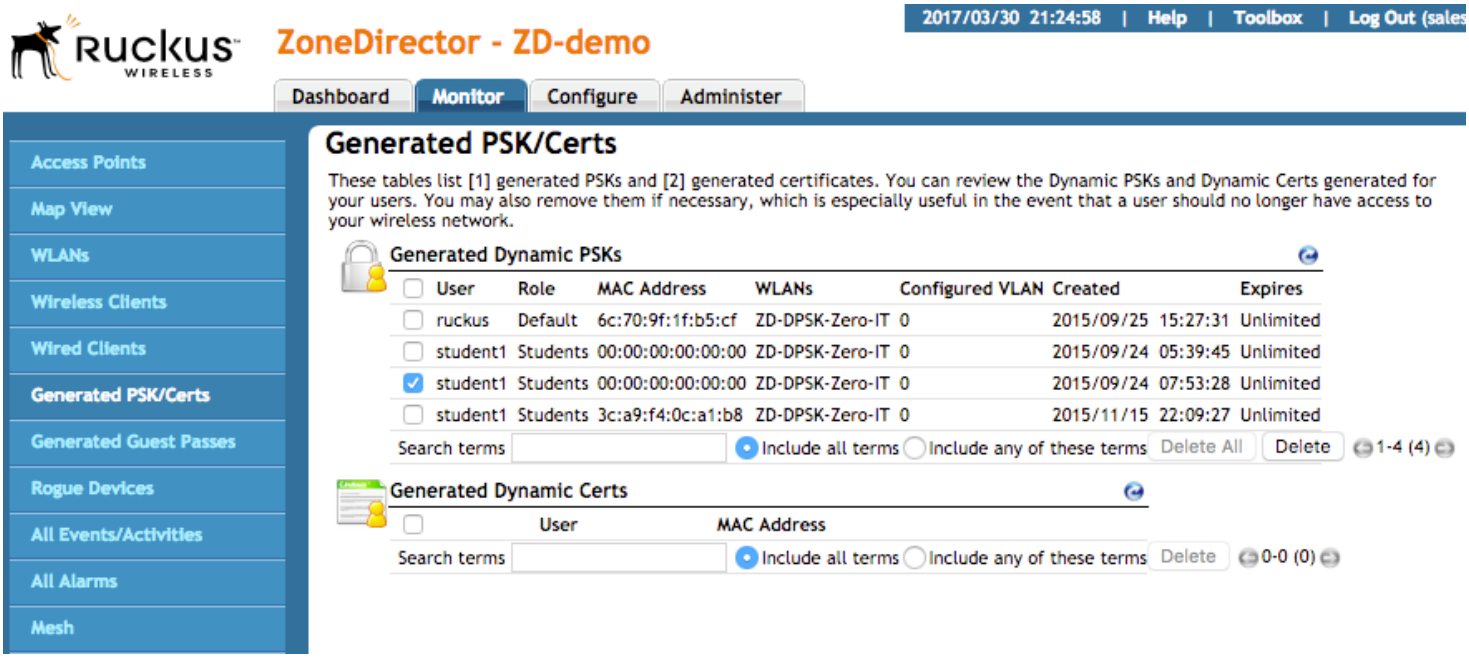

Figure 23: ZoneDirector DPSK

SmartZone Essentials 3.4

Configuration -> Identity -> Dynamic PSK

Note that user name, VLAN, MAC Address and creation date are all captured

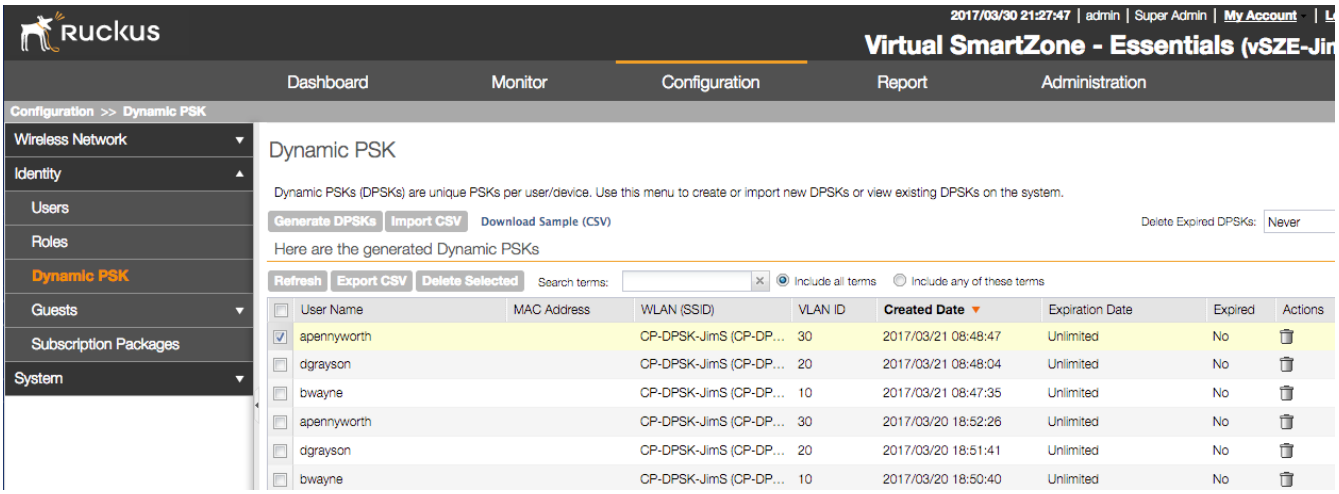

Figure 24: vSZ-E DPSK

SmartZone High Scale 3.4

Configuration -> AP zones -> AP Zone list ->Identity -> {specific zone} ->Dynamic PSK

Note that user name, VLAN, MAC Address and creation date are all captured

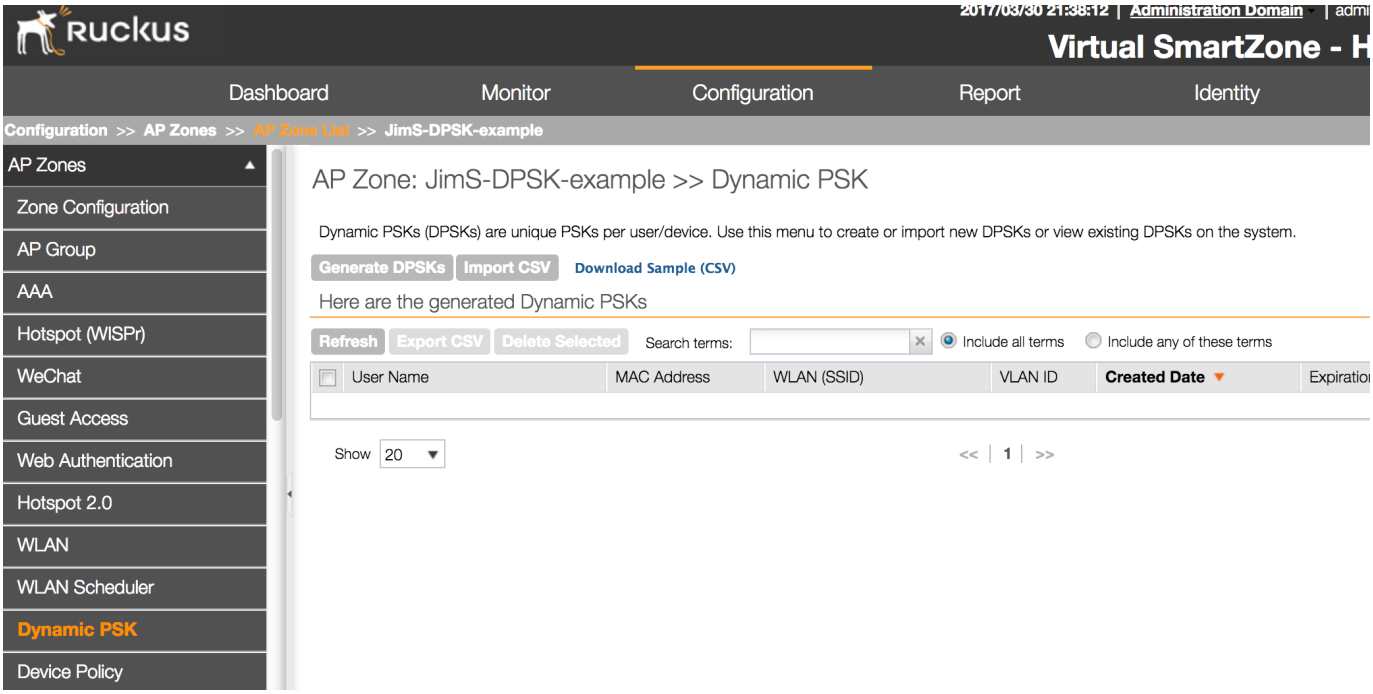

Figure 25: vSZ-H DPSK

SmartZone 3.5 (Essentials and High Scale)

Clients -> Dynamic PSK

Note that user name, VLAN, MAC Address and creation date are all captured

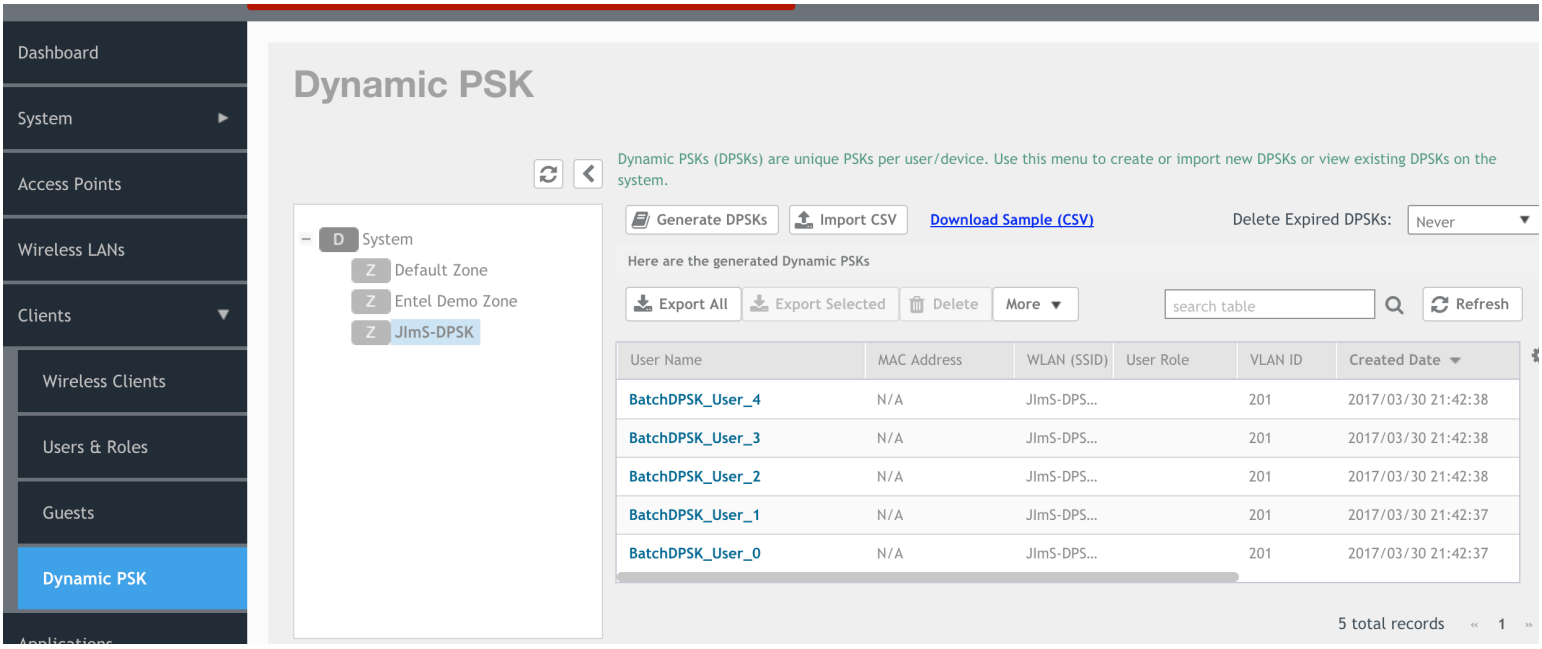

Figure 26: vSZ-H DPSK

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor "Smart Wi-Fi" products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit http://www.ruckuswireless.com.