CONFIGURATION GUIDE

Cloudpath Enrollment System Ruckus External Dynamic Pre-Shared Key (eDPSK) Configuration Guide, 5.6R2

Supporting Cloudpath Software Release 5.6

Part Number: 800-72622-001 Rev A
Publication Date: 09 March 2020

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

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

Contents

Preface

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

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

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.

- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Introduction to External DPSK (eDPSK)

Ruckus eDPSK is one of several encryption methods you can use with Cloudpath.

An advantage to using external DPSKs for Cloudpath encryption as opposed to internal ("legacy") DPSKs is that the Cloudpath administrator has control over the eDPSKs. eDPSKs are generated by Cloudpath as opposed to being generated by a controller (thus, they are "external" to the controller).

The Cloudpath administrator can create multiple DPSK "pools," with each pool containing its own DPSKs to be associated with an onboarding device. The pools and DPSKs can be managed however the Cloudpath administrator sees fit. A number of smaller pools, each one associated with one or more external DPSK WLANs created on a Ruckus SmartZone controller, can be organized to comfortably manage your network.

A SmartZone Controller version 5.1 or later is required.

As a Cloudpath administrator, you can manually generate DPSKs, then provide them to users and give them the information they need to log in to an external DPSK SSID that you have configured on the controller. Such information would also include the VLAN ID that they might be prompted to enter.

You also have the option of creating an enrollment workflow that will generate DPSKs for the enrolling user. In this case, you need to inform your users which workflow branches to follow during their enrollment.

You can follow these topics in order to use eDPSK encryption in your Cloudpath system:

1. Configuring an External DPSK WLAN on a Ruckus SmartZone Controller on page 7 - You need to configure one or more SSIDs that you will associate with DPSK pools.
2. Creating an eDPSK Pool for Use With External DPSK on page 11 - You need to create one or more DPSK pools, and assign your SSIDs to these pools in a manner that makes your network operations as effective as possible.
3. Creating a PSK in an Existing eDPSK Pool on page 14 or Setting up an eDPSK Workflow on page 21 - You can manually generate DPSKs and provide them to your users, or you can create a workflow to have DPSKs automatically generated during enrollment, or you can do a combination of both.

Also, be sure to refer to Managing eDPSK Pools and DPSKs on page 17 for additional information.

Configuring an External DPSK WLAN on a Ruckus SmartZone Controller

You can configure multiple eDPSK WLANs on a Ruckus Wireless SmartZone controller so that you can then use eDPSK as the encryption method for devices used to onboard users to Cloudpath.

Follow these steps to configure an eDPSK WLAN on a SmartZone controller.

NOTE
The procedure shown here is based on the user interface of a SmartZone controller version 5.1. Different versions of SmartZone may have minor differences in terms of which configuration options appear in what sections of a screen. However, you must be running SmartZone 5.1 or greater.

1. Log in to your SmartZone controller.
2. Click the **Wireless LANS** tab.

   The following screen appears:

FIGURE 1 Wireless LANs Screen

3. On the Wireless LANs screen, highlight the desired zone, then click the **+ Create** button.

   NOTE
   Unless otherwise specified in the remaining steps, you do not have to change default values. The procedure described here is specific to Cloudpath; for information about any fields that are not described here, refer to your controller documentation.

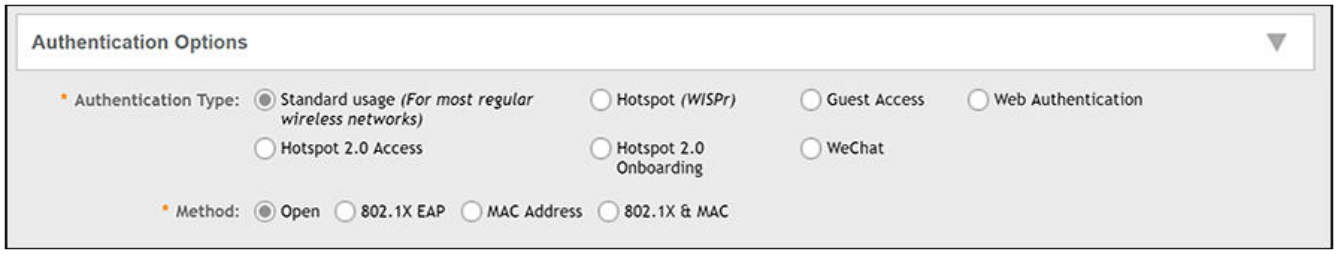
4. The Create WLAN Configuration screen appears; example data of the General Options portion of the screen is shown below:

FIGURE 2 Create WLAN Configuration Screen - General Options

- Name: Enter a meaningful name for the eDPSK WLAN you are creating.
- SSID: When you click in this field, the name you entered above also appears in this field.
- Zone: From the drop-down list, select the zone in which the eDPSK WLAN will reside. This can be the default zone.

5. In the Authentication Options section of the screen, use the settings shown in the following screen.

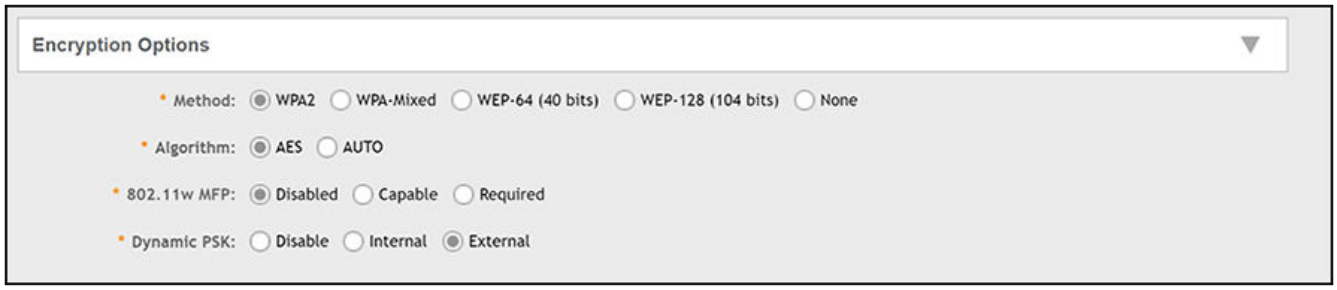
FIGURE 3 Create WLAN Configuration Screen - Authentication Options



- Authentication Type: Standard Usage
- Method: Open

6. In the Encryptions Options section of the screen, select the options shown in the following screen.

FIGURE 4 Create WLAN Configuration Screen - Encryption Options



- Method: WPA2

  NOTE
  Once you select WPA2, the other options you need become visible.

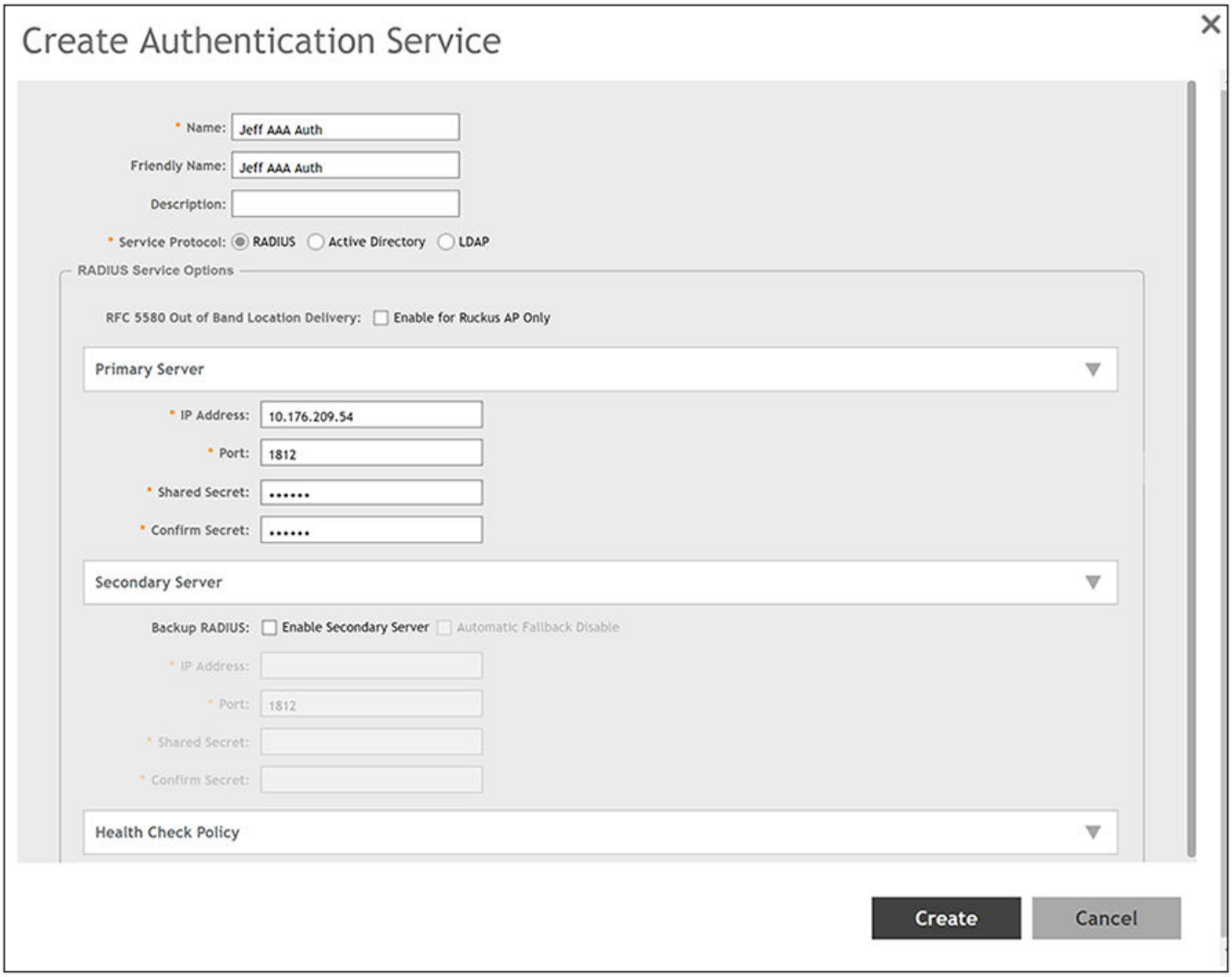
- Algorithm: AES
- 802.11w MFP: Disabled
- Dynamic PSK: External

7. In the Authentication and Accounting Services section, you can use the drop-down list to select an already-configured AAA authentication server, or you can use the **+ Create** button to create one. The "Use the controller as proxy" box must be selected.

FIGURE 5 Create WLAN Configuration Screen - Authentication and Accounting Services

8. If you are creating an AAA authentication server, configure the values as described below the following example screen, and click **Create** when you are done.

FIGURE 6 Creating the AAA Authentication Server



- Name: Any descriptive name you wish.
- Service Protocol: RADIUS
- IP address: The IP address of your external RADIUS server. (This is the IP address of your Cloudpath system.)
- Port: 1812 is typically used and is the default.
- Shared Secret: The shared secret of your external RADIUS server.
- Confirm Secret: Must again enter the shared secret of your external RADIUS server.

NOTE
A backup RADIUS is optional: Refer to your controller documentation if you want to use a backup RADIUS server.

Once this AAA authentication server is created, you can locate its configuration under **Services and Profiles > Authentication**, Proxy tab portion of the controller UI.

9. (Optional) You can create or select an accounting server using the same basic procedure that you used to create or select an authorization server. For an accounting server, port 1813 is the default. (The "Use the controller as proxy" box is not required for the accounting server.)
10. On the Create WLAN Configuration screen, in the Advanced section, be sure that the "Enable Dynamic VLAN (AAA Override)" box is checked. It should be checked by default.
11. On the Create WLAN Configuration screen, click **OK** to create the Wireless LAN with External DPSK enabled.

Creating an eDPSK Pool for Use With External DPSK

You can create eDPSK pools to associate with specific SSIDs in your environment.

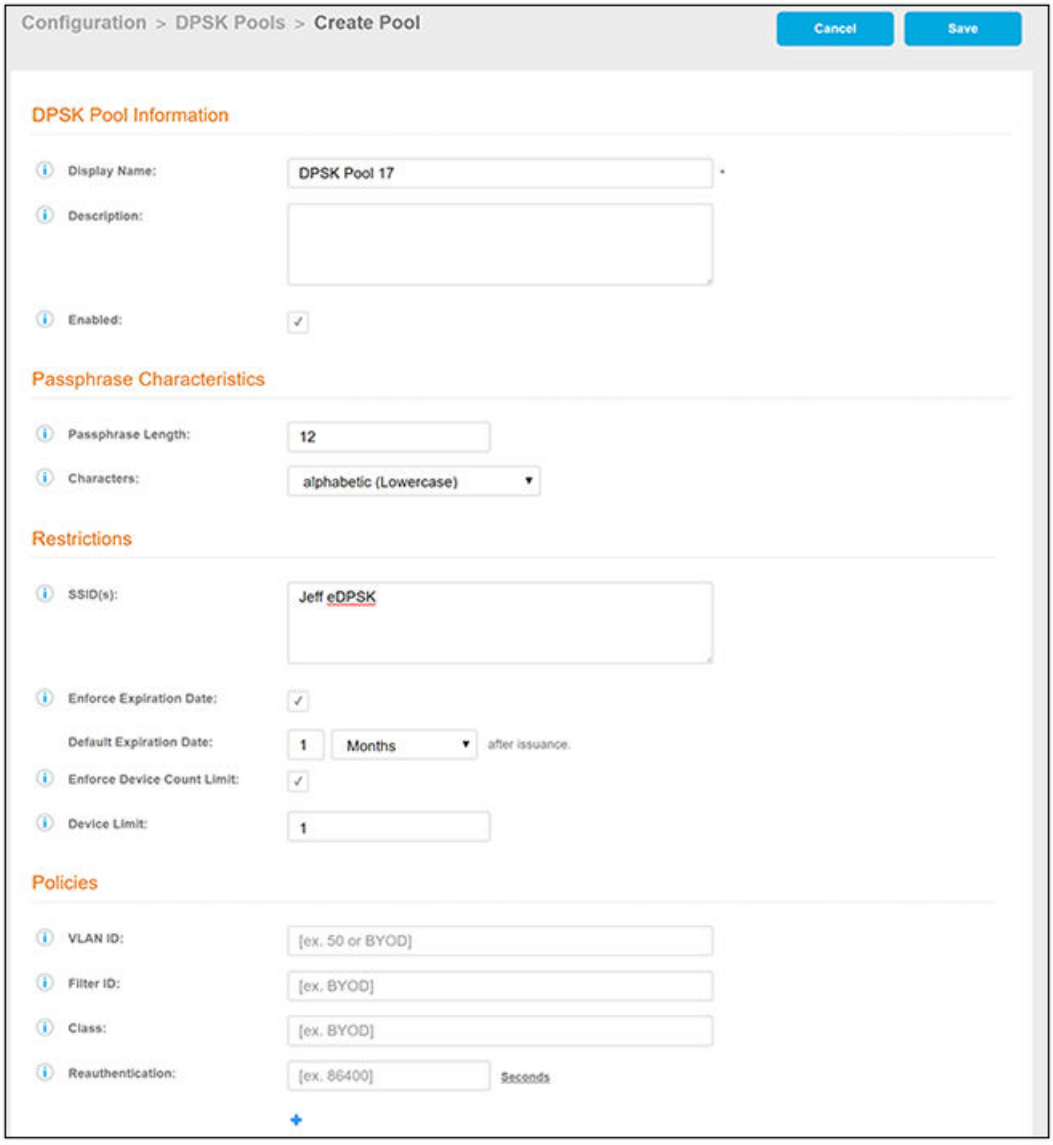
Based on the demands of your network environment, decide how many eDPSK pools you want to create, and how large you want each pool to be. It is recommended to have a number of fairly small pools as opposed to one or two extremely large pools because smaller pools are easier to manage. You can assign as many SSIDs as you want to a pool.

To create a new eDPSK pool, follow these steps:

1. In the Cloudpath UI, go to **Configuration > DPSK Pools**.
2. Click **Create DPSK Pool**.

3. In the ensuing Create Pool screen, enter the information to create the pool, then click **Save**. The following screen shows an example and describes the fields.

FIGURE 7 New eDPSK Pool Configuration Screen



- Display Name: The name of the eDPSK pool. This should be a descriptive name. It is visible only to Cloudpath administrators.
- Description: Optionally enter a description of this pool. It is visible only to Cloudpath administrators.
- Enabled: This box is checked by default. It must be checked for this DPSK pool to be used.
- Passphrase Length: This is the default length (in number of characters) for the pre-shared keys generated for this pool. The maximum length is 63.
- Characters: From the drop-down, select the types of characters that can be used for the pre-shared keys.
- SSID(s): Enter the specific SSID or SSIDs, separated by semi-colons, for which you want this pool to be used. Wildcard characters are not supported.

- Enforce Expiration Date: If checked, newly generated DPSKs will have an expiration date based on the creation date and the offset that you define in the "Default Expiration Date" popup box.
- Enforce Device Count Limit: If checked, each DPSK will be assigned a maximum device count as specified in the "Device Limit" popup box. If the "Enforce Device Count Limit:" box is un-checked, an unlimited number of devices can use the DPSK.
- VLAN ID: If this field is populated, the VLAN ID is included in the RADIUS reply to the controller for successful authentications. Cloudpath sends Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID. If your network policy is wireless, the Tunnel-Type value is VLAN, the Tunnel-Medium-Type value is 802 (this includes all 802 media plus Ethernet canonical format), and the Tunnel-Private-Group-ID is the integer that represents the VLAN number to which group members will be assigned.

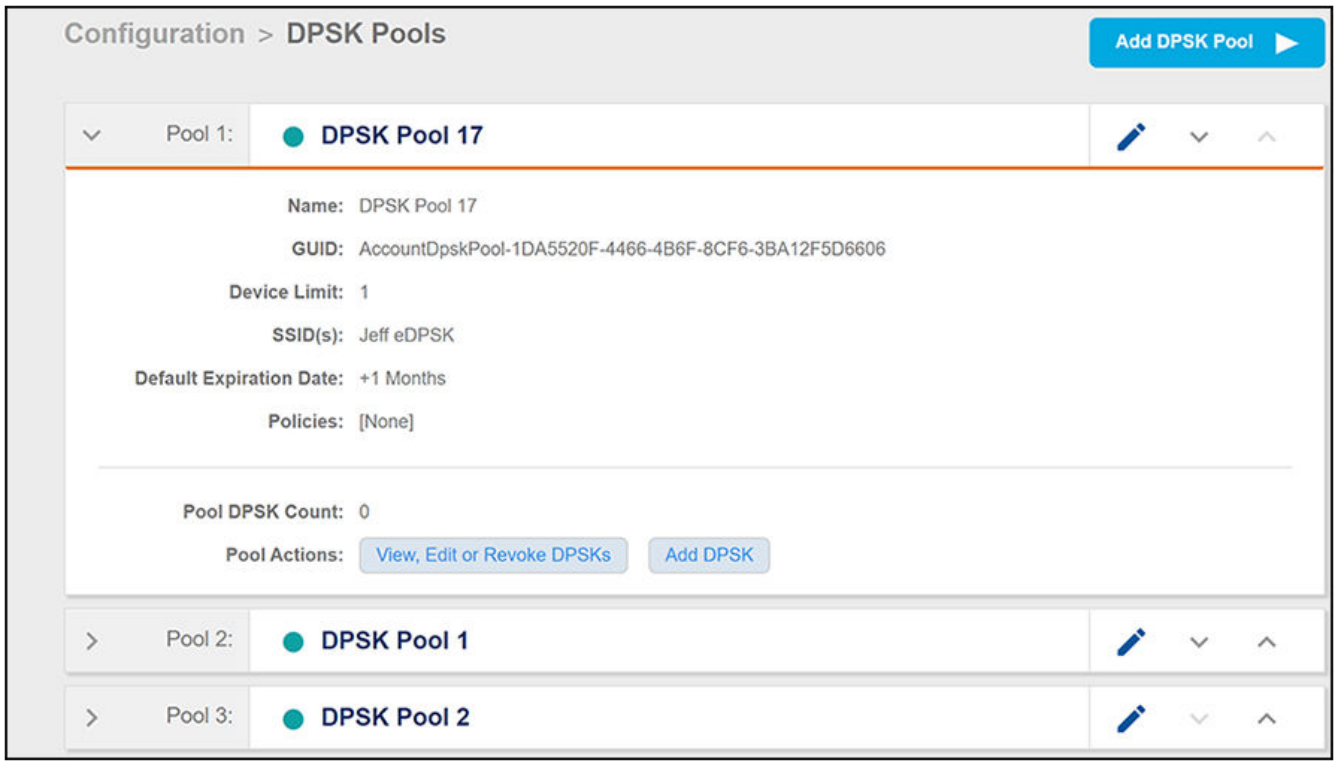
  If the VLAN ID field is left blank, Cloudpath will not return a VLAN ID in the RADIUS reply; therefore the controller assigns the VLAN ID based on its own configuration.

  NOTE
  When you create a workflow to use eDPSK, you can include a step that prompts users to enter their VLAN ID. You can create this step to store the ID in a variable called LOCATION. Then, you would use ${LOCATION} as the default VLAN ID of the pool.

- Filter ID: If this field is populated, the Filter ID is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Filter ID in the RADIUS reply.
- Class: If this field is populated, the Class is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Class in the RADIUS reply.
- Reauthentication: The number of seconds included in the RADIUS reply for successful authentications. If the device stays connected for longer than this period, the WLAN or switch requires that the device be reauthenticated. In wireless devices, this causes the encryption keys to rotate.
- Additional Attributes: You can add other attributes in the "Policies" section of the screen by clicking the **+** button, and selecting the desired fields and values. These attributes will be returned to the controller in an access-accept.

4. After you save your configuration, you are returned to the main eDPSK Pools screen, where you can check the pool you just configured, as shown in the figure below:

FIGURE 8 Newly Created Pool



NOTE
The GUID is auto-generated. You may need this GUID for some API calls.

Creating a PSK in an Existing eDPSK Pool

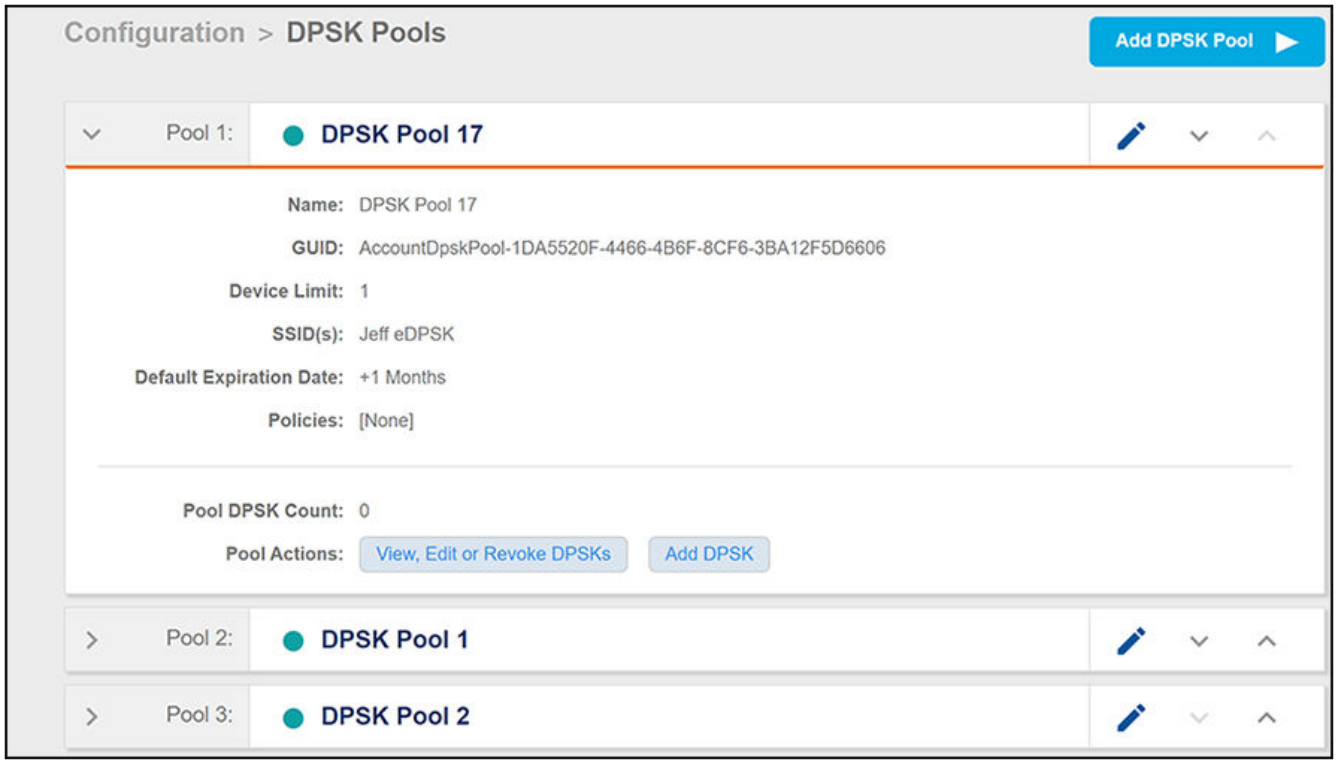
You can manually generate DPSKs from within a configured eDPSK pool.

You can provide manually generated DPSKs to users. Once they log in to a specific SSID, the device they used is then associated with the DPSK.

Follow the steps below to generate a DPSK from within an existing eDPSK pool:

1. In the Cloudpath UI, go to **Configuration > DPSK Pools**, then expand the pool from which you want to generate a DPSK. In this example, the DPSK is called "DPSK Pool 17."

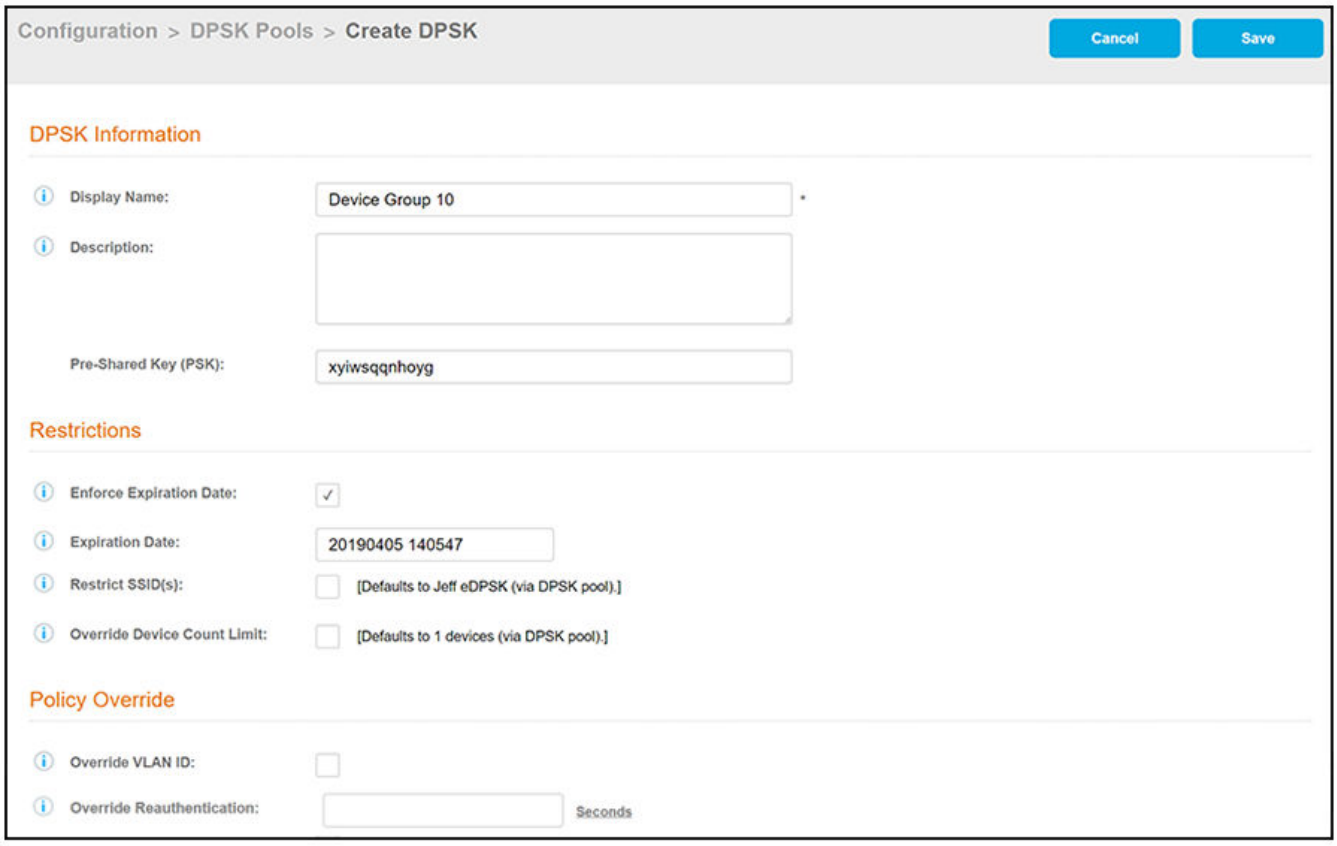
   FIGURE 9 Adding a DPSK to an Existing Pool



2. Click **Add DPSK**.

3. In the ensuing screen, configure the values for the new DPSK, and click **Save** when you are done. The figure below shows sample data, followed by descriptions of the various fields.

FIGURE 10 Configuring a New DPSK



- Display Name: Provide a descriptive name; the name is visible to administrators only.
- Description: Optionally, you can describe the DPSK; for example, you might want to list the device type to which you plan to assign this DPSK.
- Pre-Shared Key: This is the auto-generated key, which adheres to the character limit and character type configured for the pool.

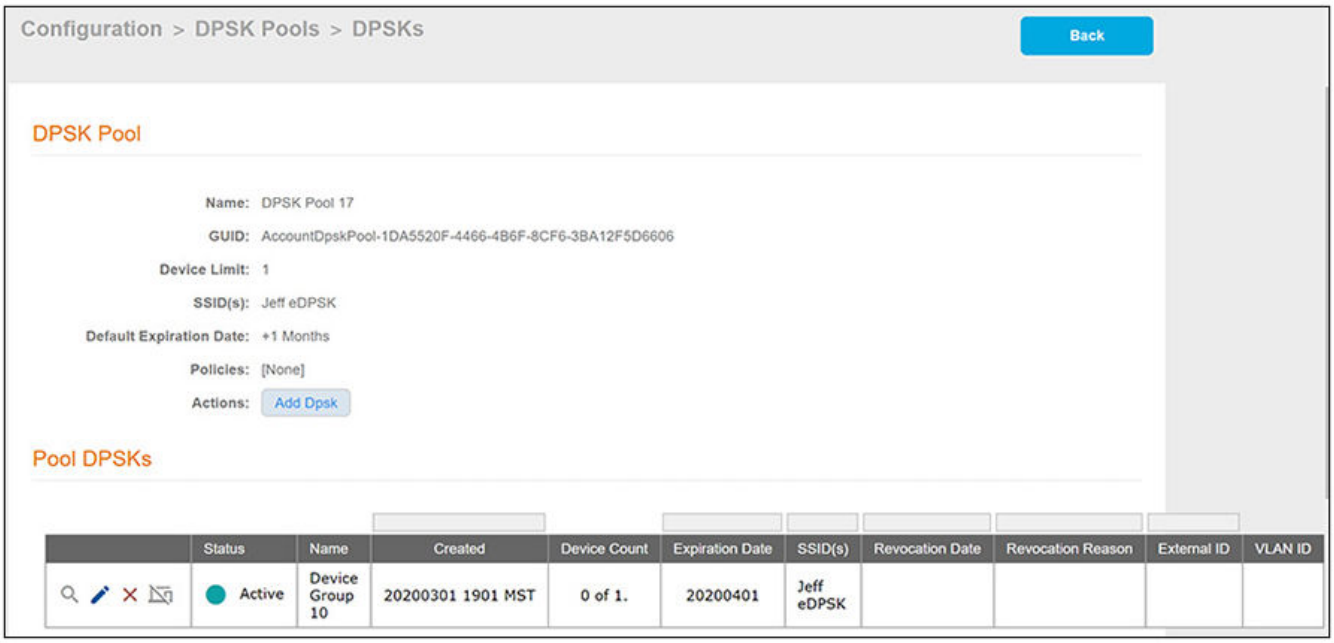
  NOTE
  Should you choose to manually specify a pre-shared key, the key must be unique to the pool and between 8-63 characters in length.

- Enforce Expiration Date: This field is checked by default. This means that the DPSK will expire on the date shown in the "Expiration Date" field, which is determined by the configuration for the corresponding eDPSK pool. However, you can un-check this box, which means that the DPSK will not expire.
- Restrict SSID(s): This field is unchecked by default, which means that the allowable SSIDs for this DPSK are the same as the SSIDs configured for the corresponding pool. However, you can further restrict this SSID list for the DPSK by checking this field, then entering a subset of the eDPSK pool's SSIDs into the "SSID(s)" popup box.

- Override Device Count Limit: By default, this box is unchecked, which means that the DPSK uses the device count limit specified within the eDPSK pool. If checked, however, this DPSK can have its own device count limit that you specify in the popup "Device Count Limit" box.
- Override VLAN ID: By default, this box is unchecked, which means that the DPSK uses the VLAN ID specified within the eDPSK pool. If checked, you can specify a VLAN ID in the popup "VLAN ID" field that will override the VLAN ID specified within the eDPSK pool. For example, if you specify an Override VLAN ID of 10, the RADIUS reply (access-accept) for the DPSK will contain the attributes (tunnel-type, tunnel-medium-type, private-tunnel-group-id) to set the VLAN to 10, regardless of whether the VLAN ID field for the pool is populated or empty.
- Override Reauthentication: If you enter a value in this field, that value becomes the reauthentication timeout for this DPSK and overrides the Reauthentication period specified within the DPSK pool.

4. After you have saved the DPSK, the newly added DPSK is shown as part of the pool. Check that the information for the DPSK is what you want. An example is shown below, where a DPSK named "Device Group 10" has been added to DPSK Pool 17:

FIGURE 11 DPSK Added to Pool



Managing eDPSK Pools and DPSKs

Once you have created eDPSK pools and have generated DPSKs, you can manage them in many ways.

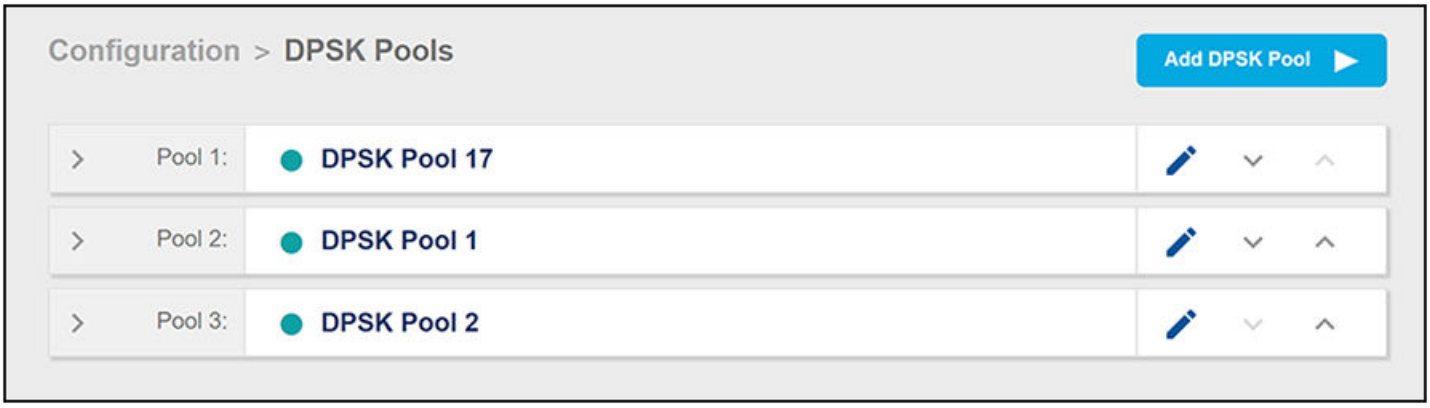
Refer to:

- DPSK Pools
- DPSKs
- Dashboard Information

DPSK Pools

If you go to **Configuration > DPSK Pools**, you can view the pools that have been created:

FIGURE 12 Configured List of eDPSK Pools - Searched From Top Down



Here are a few things you can do:

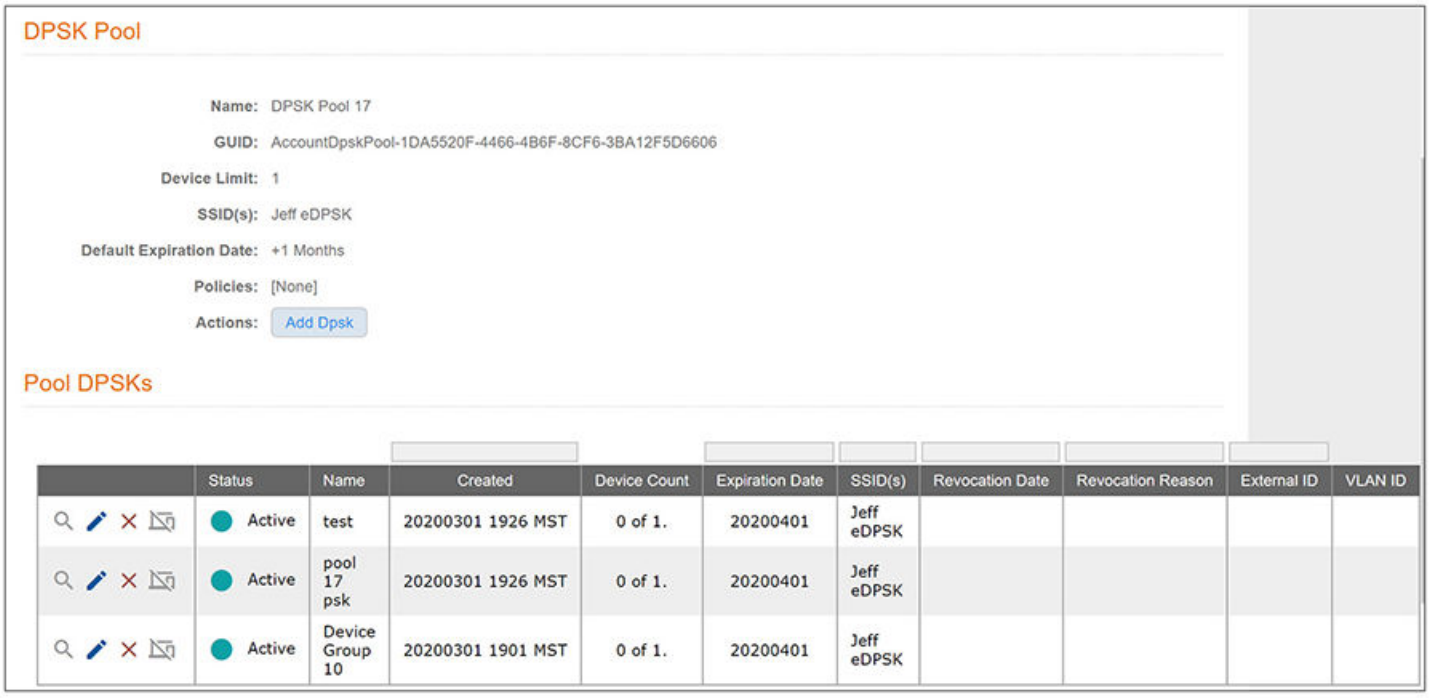
- **Reorder the list**: Each time you create a new pool, this pool goes to the top of the list. Pools are searched from top to bottom when a match for an SSID is being looked up. If you wish to reorder the pools, use the arrows to the right of the pool you wish to move up or down.
- **Editing the configuration settings**: To edit the settings of a pool, click the pencil icon to the right of the pool name. The configuration screen for that pool is invoked, and you can make any changes you want.
- **Cleanup options**: If you wish to delete all DPSKs belonging to a pool, scroll to the bottom of the configuration screen, and expand "Cleanup." You then have the options of deleting all the DPSKs belonging to the pool but leaving the pool itself in tact, or deleting the DPSKs and destroying the pool.

  NOTE
  If you choose either option, be sure that is what you really want to do before confirming the popup warning that appears if you try to take either action.

DPSKs

If you go to **Configuration > DPSK Pools** and expand a pool, then click **View, Edit or Revoke DPSKs** (refer to Figure 9 on page 15) you can view all the DPSKs that have been generated for that pool. The screen below shows the DPSKs for a pool called "DPSK Pool 17."

FIGURE 13 List of DPSKs Within a Specific Pool - Actions You Can Take



Some of the things you can do include:

- **Add a device to an existing DPSK**: If this DPSK has not reached a configurable limit of supported devices, you can add more devices by clicking the magnifying glass icon in the far-left column for the corresponding DPSK. The PSK Information screen for that DPSK appears, an example of which is shown below:

  FIGURE 14 PSK Information Screen

Click **Add Device**, then in the popup screen that appears, enter the MAC address of the device, the SSID to which it will be allowed to connect, then click **Done**.

- **View the pre-shared key**: Click the magnifying glass in the Pre-Shared Key field on the PSK Information screen, shown in Figure 14.
- **Revoke the DPSK**: You can click **Revoke DPSK** from the PSK Information screen (shown above), or you can click the Revoke DPSK icon (to the right of the **X** icon) on the DPSK Pools screen (with expanded list of DPSKs), shown in Figure 13.

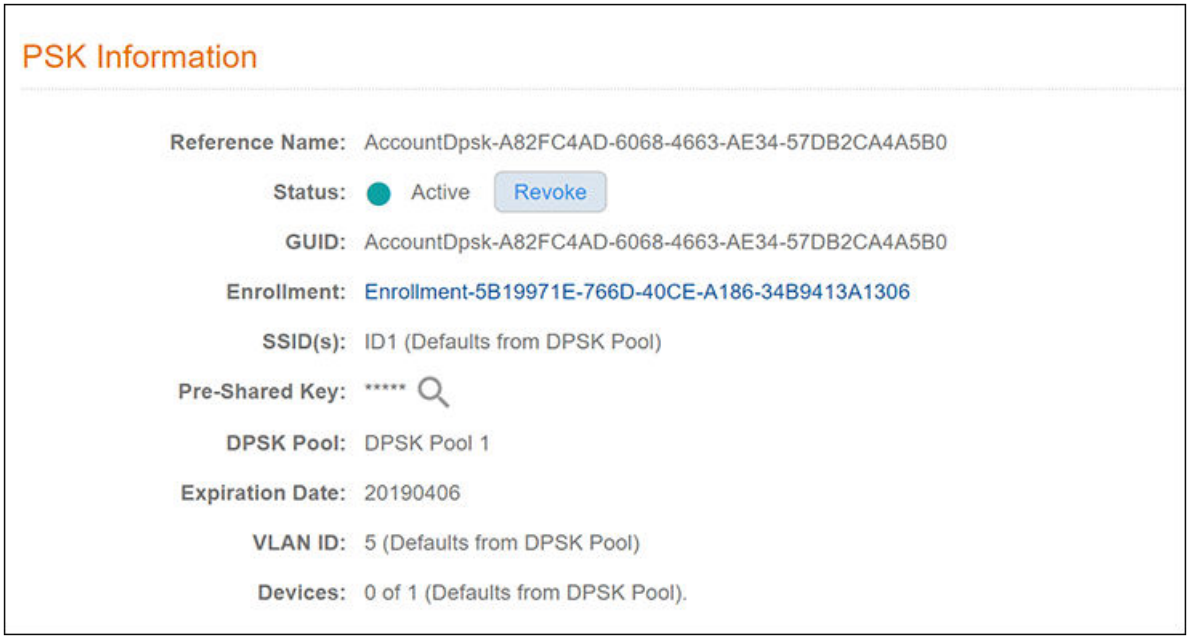
  NOTE
  Revoking a DPSK leaves its records in the database for auditing purposes, and allows you to unrevoke it if you ever need to.

- **Delete DPSK from pool**: To delete the DPSK from its pool, click the **X** icon to the left of the corresponding DPSK.

  NOTE
  Deleting a DPSK removes any record that it existed.

- **Editing the DPSK**: To make changes to the current settings for this DPSK, click the pencil icon for that DPSK. The configuration screen for the DPSK is invoked, and you can make any changes you want.
- **View enrollment data**: Once a DPSK has been used to enroll a device, the PSK Information screen for the device will contain an Enrollment link that you click. An example is shown in the following figure:

FIGURE 15 PSK Information Screen With Link to Enrollment Data

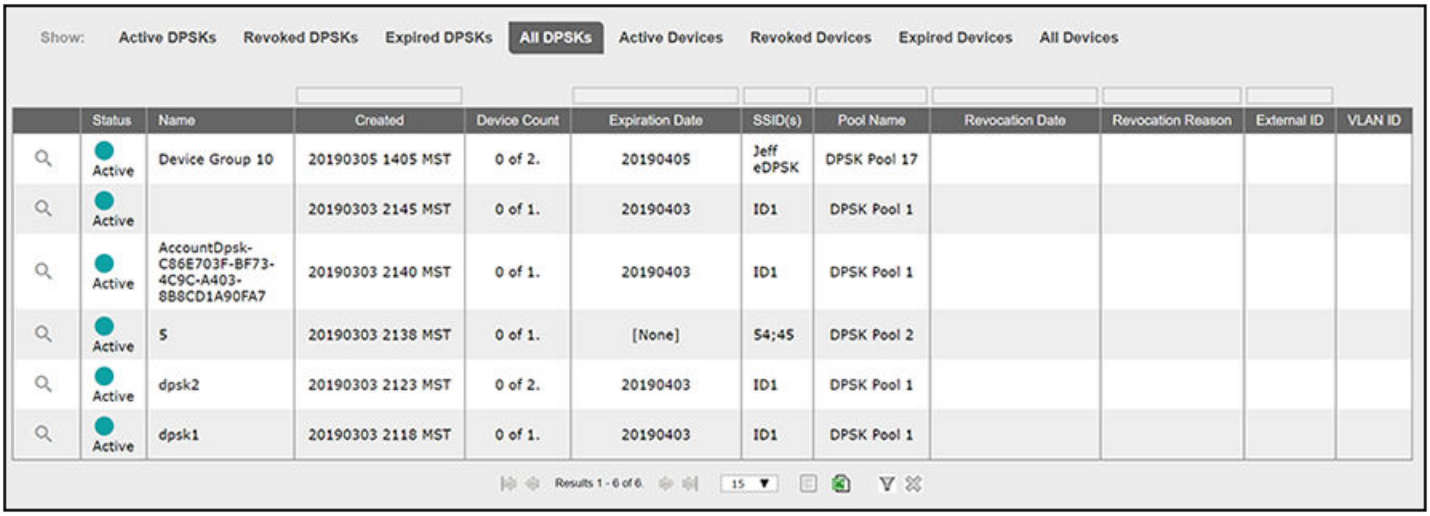


This link brings you to a page that contains many categories of information about the enrollment, including device, workflow, and notification data.

Dashboard Information

For a listing of all DPSKs, go to **Dashboard > DPSKs**, as shown in the following example figure:

FIGURE 16 DPSKs Listed in the Dashboard



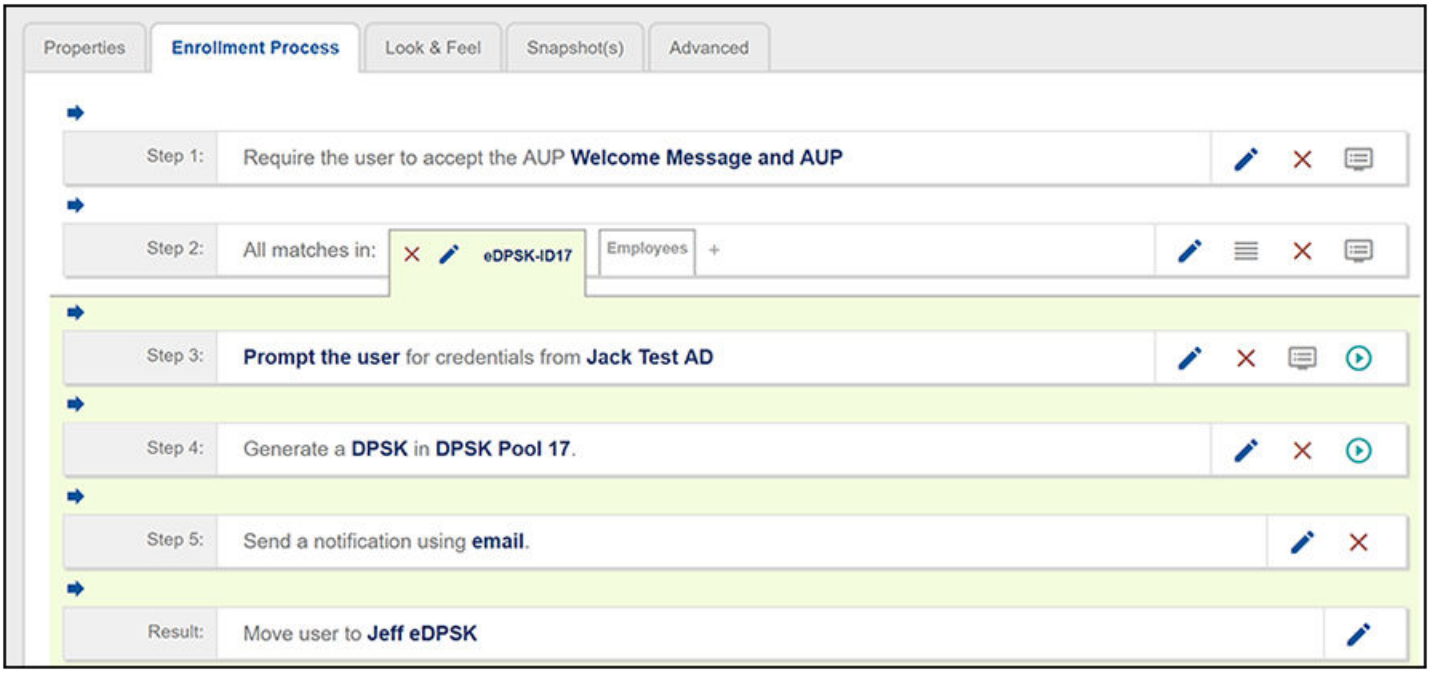
To view all DPSKs created in the system, highlight the **All DPSKs** tab. Use the other tabs as desired. To view information about a specific DPSK, click the magnifying glass icon.

Setting up an eDPSK Workflow

You can create a workflow that includes a DPSK pool step from the pools you have already created, or you can create a pool at the same time you create the workflow.

The figure below shows a simple workflow example that incorporates eDPSK:

FIGURE 17 Sample eDPSK Workflow



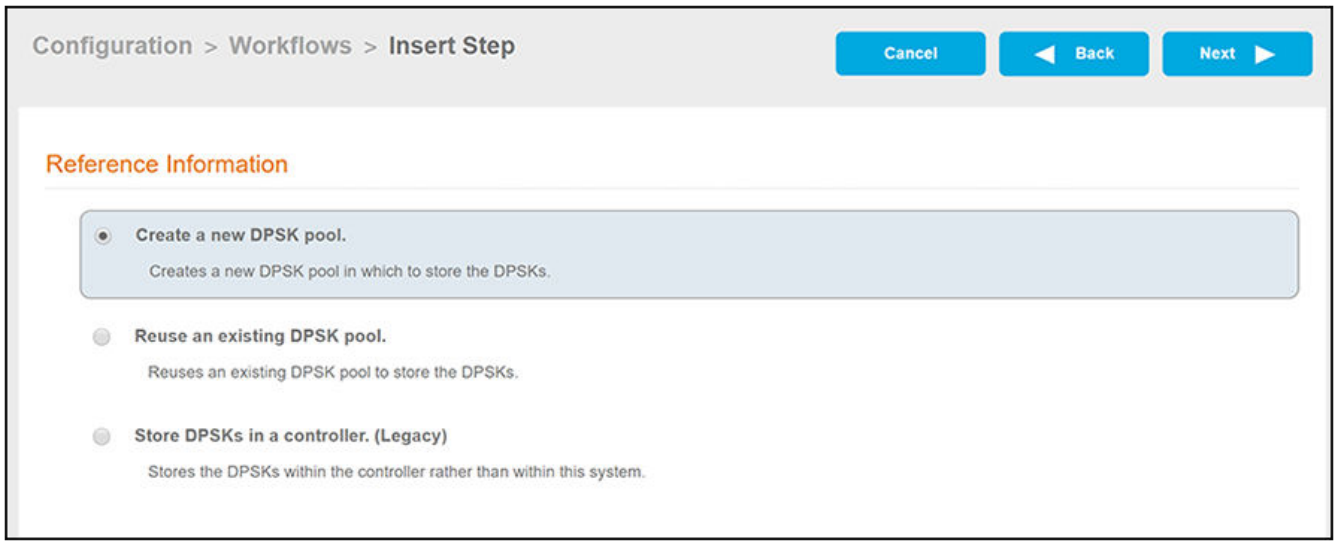
The concept of workflows and how to create one is described in detail in the *Cloudpath Enrollment System Administration Guide* and the *Cloudpath Enrollment System Quick Start Guide*. Therefore, the purpose of the procedure in this section is to demonstrate how to add the eDPSK step to a workflow.

Step 3 in the workflow example shows an authentication step that you might want to have. Then, to create Step 4, which is the DPSK pool step, you would do the following:

1. Click the arrow underneath Step 3 above to insert a step. You are presented with a screen that has the text: "Which type of step should be added?"
2. Scroll down and click the "Generate a Ruckus DPSK" button.
3. You are presented with the following options next:

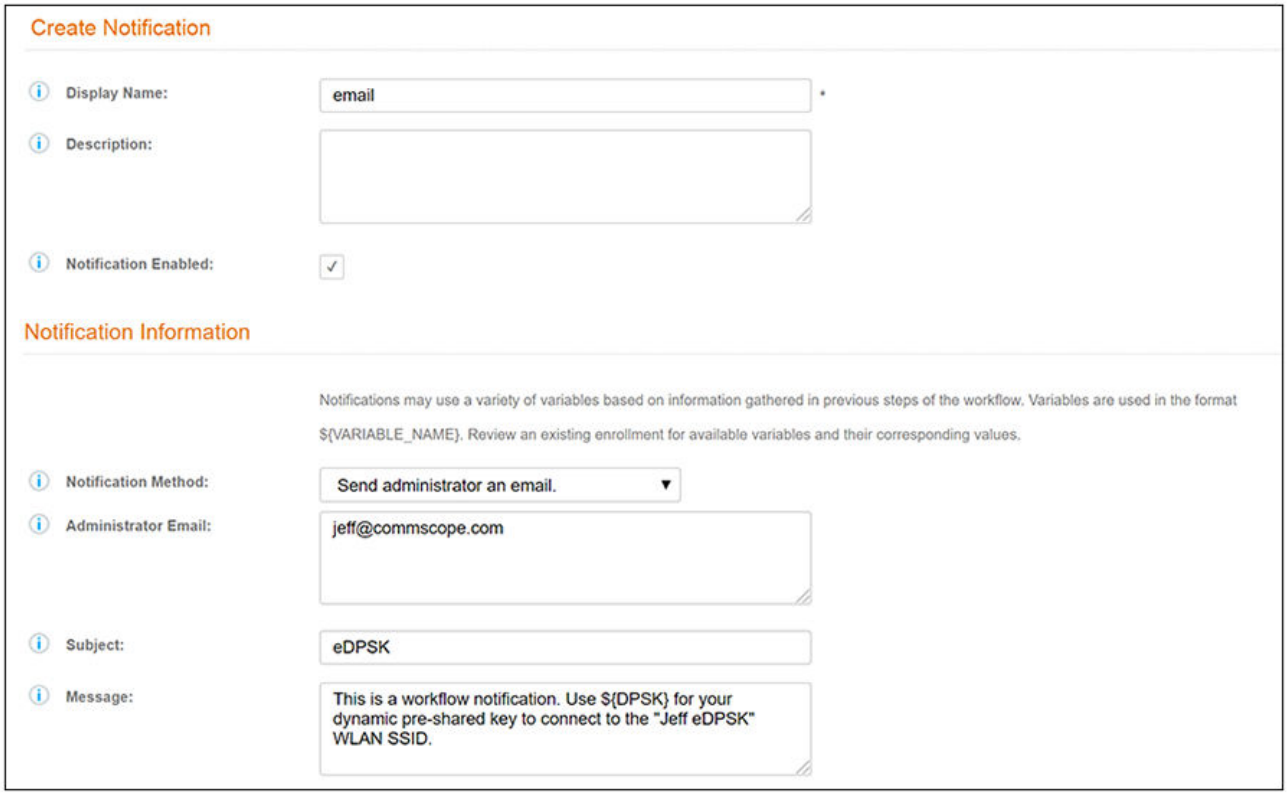
> **NOTE**
> The "Reuse an existing DPSK pool" option appears only if you have already configured one or more DPSK pools.

FIGURE 18 Continuing With an eDPSK Workflow Step



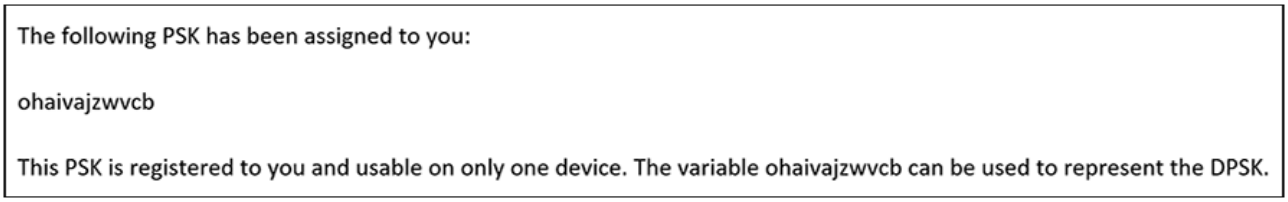
4. You could choose either of the DPSK "pool options." If you choose to create a new DPSK pool and click **Next**, you are then taken to the DPSK Pool configuration screen (which is described in Creating an eDPSK Pool for Use With External DPSK on page 11. If you choose to reuse an existing pool and click **Next**, you are taken to a screen that has a drop-down menu to choose the pool you wish to add to this workflow.
5. Once you have completed the DPSK pool step, you can add a Notification step, as shown in Figure 17. The importance of adding a notification step is to send the DPSK that was just generated in the previous step either directly to the user or to the system administrator, who can then inform the user. This is done by using a variable called **${DPSK}**:
   a. To insert a Notification step in the workflow, scroll down to select the "Send a notification" plugin step, then click **Next**.
   b. On the ensuing screen, choose a new notification, then click **Next**.
   c. Configure the Create Notification screen. An example is shown below. The most important field is the "Message" field because this is where you enter the **${DPSK}** variable. In this example, the notification of the DPSK will be sent by email to the administrator because that option has been selected from the "Notification Method" drop-down list.

FIGURE 19 Using the ${DPSK} Variable in a Notification Workflow Step



As the user goes through the enrollment process, the email notification that gets sent to the administrator will appear as follows:

FIGURE 20 Email Notification Sent to Administrator Showing the PSK Assigned to User



The administrator can send then inform the user of the pre-shared key.

NOTE
Another option of providing the DPSK to the user is by adding a workflow step called "Display a message." Again, the key element if you use this step is to include the **${DPSK}** variable in the HTML Message field.

6. For the Result step, create a device configuration where you select one of the External DPSK SSIDs that you have configured on the controller (refer to Configuring an External DPSK WLAN on a Ruckus SmartZone Controller on page 7) that has been configured as one of the SSIDs in the DPSK pool used in this workflow.

Once the user enrolls, the device used for enrollment contains the pre-shared key for the network. The pre-shared key is assigned to the enrolled user, and will continue to be in use until its configured expiration date. The pre-shared key can be used only of the enrollment device. As administrator, you can obtain information about the newly created DPSK by referring to Managing eDPSK Pools and DPSKs on page 17.

COMMSCOPE®
RUCKUS®

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