

Cloudpath Enrollment System RUCKUS External Dynamic Pre-Shared Key (eDPSK) Configuration Guide, 6.0

Supporting Cloudpath Software Release 6.0

© 2024 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions.....	5
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
About This Document.....	9
Purpose of This Cloudpath Configuration Guide.....	9
New In This Document.....	9
Introduction to External DPSK (eDPSK).....	11
Supported Controllers.....	11
Basic Steps.....	11
Configuring the Controller.....	13
SmartZone 5.1 or Later or Virtual SmartZone 3.60 or Later.....	13
ZoneDirector 10.4 or Later.....	13
Unleashed 200.8 or Later.....	14
Configuring an External DPSK WLAN on a Ruckus SmartZone Controller.....	15
Configuring Policies.....	21
Creating an eDPSK Pool for Use With External DPSK.....	27
Creating a DPSK in an Existing eDPSK Pool.....	31
Adding Policies to an eDPSK Pool.....	35
Steps to Add Policies.....	35
Policy Rules.....	36
Additional Policy Information.....	39
Testing Policies.....	39
Test Policy Evaluation - Example 1.....	39
Test Policy Evaluation - Example 2.....	41
Test Policy Evaluation - Example 3.....	43
Viewing Policy Information.....	45
Viewing RADIUS Attribute Information.....	47
Managing eDPSK Pools and DPSKs.....	49
Managing DPSK Pools.....	49
Managing DPSKs.....	51
Dashboard Information.....	54
Switching Pre-Release-5.7 DPSK pools to Policy-Assigned Pools.....	55
Setting up an eDPSK Workflow.....	59

Limiting One DPSK per User..... 61

Contact Information, Resources, and Conventions

- [Contacting RUCKUS Customer Services and Support](#)..... 5
- [Document Feedback](#)..... 6
- [RUCKUS Product Documentation Resources](#)..... 6
- [Online Training Resources](#)..... 6
- [Document Conventions](#)..... 7
- [Command Syntax Conventions](#)..... 7

Contacting RUCKUS Customer Services and Support

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

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

What Support Do I Need?

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

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

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

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

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

Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://community.ruckuswireless.com>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- 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.

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.ruckusnetworks.com>.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

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

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
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 .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

Notes, Cautions, and Safety Warnings

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

NOTE

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

ATTENTION

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



CAUTION

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



DANGER

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

Command Syntax Conventions

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

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

About This Document

- Purpose of This Cloudpath Configuration Guide..... 9
- New In This Document..... 9

Purpose of This Cloudpath Configuration Guide

This guide describes the configuration that you perform in the Cloudpath UI to generate eDPSK. It is not intended to cover all aspects of DPSK.

New In This Document

There are no changes in this release.

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 (therefore, they are considered to be 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.

You can also configure an unlimited number of policies to apply to a DPSK pool for the purposes of organizing your users into different categories, but only one policy will be assigned to a user, depending on which criteria that you specify matches a given user trying to connect to Cloudpath. For each policy, you assign a RADIUS attribute group that can contain many attributes including VLAN ID.

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 could 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.

Supported Controllers

The following RUCKUS controllers support eDPSK:

- SmartZone version 5.1 or later
- Virtual SmartZone version 3.60 or later
- ZoneDirector 10.4 or later
- Unleashed AP 200.8 or later

Basic Steps

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

1. [Configuring the Controller](#) on page 13 - You need to configure an EDPSK WLAN on one of the supported RUCKUS controllers.
2. [Creating an eDPSK Pool for Use With External DPSK](#) on page 27 - 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 DPSK in an Existing eDPSK Pool](#) on page 31 or [Setting up an eDPSK Workflow](#) on page 59 - 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.
4. You can create policies ([Configuring Policies](#) on page 21) and then add them to a DPSK pool ([Adding Policies to an eDPSK Pool](#) on page 35).

Also, be sure to refer to [Managing eDPSK Pools and DPSKs](#) on page 49 for additional information.

Configuring the Controller

Create an external DPSK WLAN on one of the supported RUCKUS controllers.

SmartZone 5.1 or Later or Virtual SmartZone 3.60 or Later

Refer to the following table for the settings you need to create the eDPSK WLAN on a SmartZone controller.

NOTE

You can refer also to:

- [Configuring an External DPSK WLAN on a Ruckus SmartZone Controller](#) on page 15
- Your SmartZone controller documentation about how to create a DPSK WLAN.

TABLE 2 Fields/Values to Use for SmartZone eDPSK WLAN

WLAN Configuration Section	Configuration Field and Corresponding Value
General Options	Name: Descriptive name for the eDPSK WLAN you are creating
	SSID: Name of the WLAN you just created
	Zone: Zone in which the eDPSK WLAN will reside
Authentication Options	Authentication Type: Standard Usage
	Method: Open
Encryption options	Method: WPA2
	Algorithm: AES
	802.11w MFP: Disabled
	Dynamic PSK: External
Authentication and Accounting Services	Use controller as proxy: Enable
Authentication Service	Name: Any descriptive name
	Service Protocol: RADIUS
	IP address: 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.
Advanced	Enable Dynamic VLAN (AAA Override) box: Box should be checked.

ZoneDirector 10.4 or Later

Refer to the following table for the settings you need to create the eDPSK WLAN on a ZoneDirector controller.

Configuring the Controller
Unleashed 200.8 or Later

NOTE

For detailed instructions, refer to your *ZoneDirector User Guide*, "Enabling Dynamic Pre-Shared Keys on a WLAN" section, about how to create a DPSK WLAN.

TABLE 3 Fields/Values to Use for ZoneDirector eDPSK WLAN

WLAN Configuration Section	Configuration Field and Corresponding Value
General Options	Name: Descriptive name for the eDPSK WLAN you are creating
	eSSID: Name of the WLAN you just created
WLAN Usages	Type: Standard Usage
Authentication Options	Method: Open
	Dynamic-PSK: External: Use an external AAA (RADIUS) server for client authentication
	DPSK Authentication Server: Drop-down selection for RADIUS server
Encryption Options	Method: WPA2
	Algorithm: AES
	802.11w MFP: Disabled

Unleashed 200.8 or Later

Refer to the following table for the settings you need to create the eDPSK WLAN on an Unleashed controller.

NOTE

For detailed instructions, refer to your Unleashed controller documentation about how to create a DPSK WLAN.

TABLE 4 Fields/Values to Use for Unleashed eDPSK WLAN

WLAN Configuration Field Name or Section	Value
Name	Name of the WLAN you are creating
Usage Type	Standard
Authentication Method	Open
Encryption Method	WPA2
Advanced Options: Zero-IT and DPSK tab	Dynamic PSK: External
	Authentication Server: Click + to add Cloudpath RADIUS authentication server: <ul style="list-style-type: none"> IP address: 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

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.

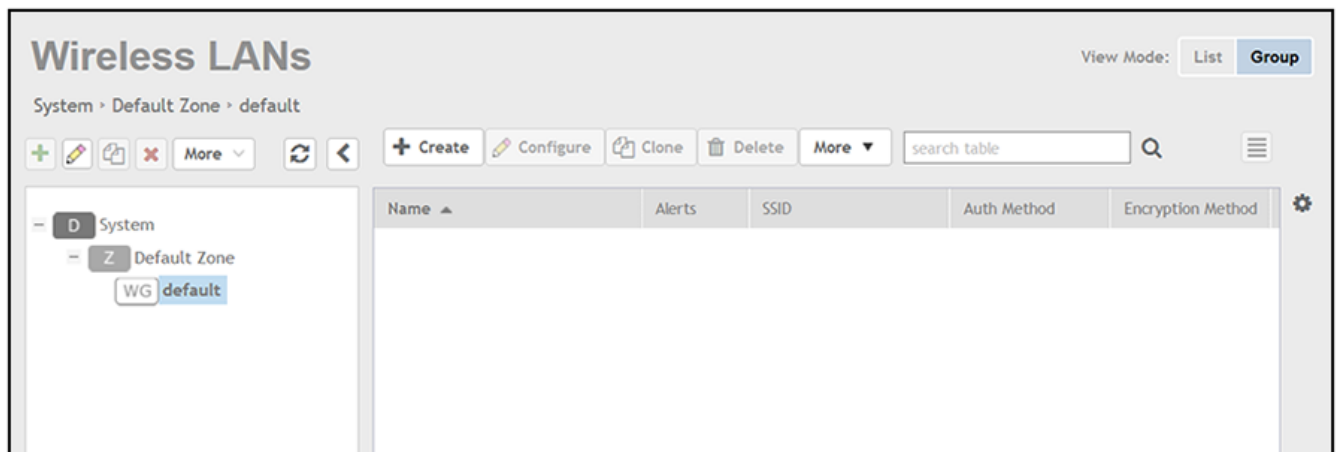
NOTE

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.

- 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

The screenshot shows the 'General Options' section of the configuration interface. It includes the following fields and controls:

- Name:** Text input field containing 'Jeff eDPSK'.
- SSID:** Text input field containing 'Jeff eDPSK'.
- Description:** Empty text input field.
- Zone:** Drop-down menu showing 'Z Default'.
- WLAN Group:** Drop-down menu showing 'default'.
- + Create:** Button to save the configuration.

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

FIGURE 3 Create WLAN Configuration Screen - Authentication Options

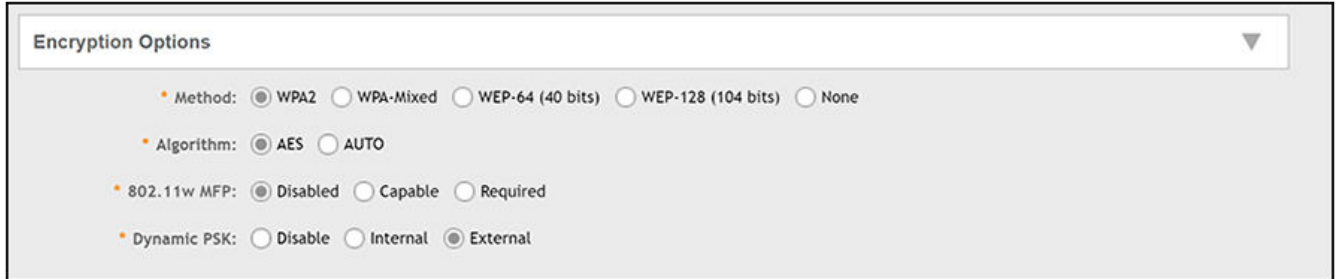
The screenshot shows the 'Authentication Options' section of the configuration interface. It includes the following options:

- Authentication Type:** Radio buttons for:
 - Standard usage (For most regular wireless networks) - **Selected**
 - Hotspot (WISPr)
 - Guest Access
 - Web Authentication
 - Hotspot 2.0 Access
 - Hotspot 2.0 Onboarding
 - WeChat
- Method:** Radio buttons for:
 - Open - **Selected**
 - 802.1X EAP
 - MAC Address
 - 802.1X & MAC

- Authentication Type: Standard Usage
- Method: Open

- 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

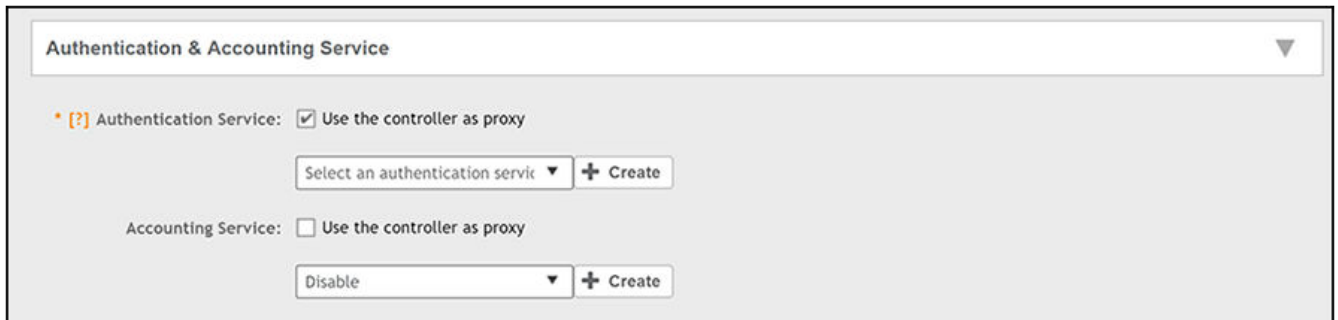
NOTE

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

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

- 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

Create Authentication Service

Name:

Friendly Name:

Description:

Service Protocol: RADIUS Active Directory LDAP

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: Enable for Ruckus AP Only

Primary Server

IP Address:

Port:

Shared Secret:

Confirm Secret:

Secondary Server

Backup RADIUS: Enable Secondary Server Automatic Fallback Disable

IP Address:

Port:

Shared Secret:

Confirm Secret:

Health Check Policy

Create **Cancel**

- 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.

Configuring Policies

Policies allow for mapping incoming successful RADIUS authentication requests to a set of RADIUS response attributes based on dynamic conditions of the request. Each policy has an associated RADIUS attribute group which defines the RADIUS response attributes (such as VLAN ID, filter ID, and class). Each authentication is matched against an assigned list of candidate policies in sequential order. Criteria of a policy can include dynamic conditions such as a user's physical location, username, or the time of day.

As of this release, policies can be used for DPSK pools that are used with External DPSKs.

The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available for selection.

1. In the Cloudpath UI, go to **Configuration > Policies**.
2. Select the **RADIUS Attribute Groups** tab, then click the **Add RADIUS Attribute Group** button.
3. In the ensuing Create Radius Attribute Group screen, enter the information to create the group, then click **Save**.

NOTE

You can configure as many RADIUS Attribute groups as you want. One RADIUS Attribute group will later be assigned to each policy you create.

An example screen and field descriptions follow:

FIGURE 7 Create RADIUS Attribute Screen

- Display Name: The name of the RADIUS attribute group. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this RADIUS attribute group. It is visible only to Cloudpath administrators.
- Assigned Policies: This field lists the names of all the policies that are using this RADIUS attribute group. There will be no policies listed here during the initial configuration of the group.
- Certificate Reply Username: This setting is applied only when the RADIUS attribute group is associated with certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.
- 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 "Attributes" 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 RADIUS server packet.
4. Configure your policies:
 - a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.
 - b. In the ensuing Create Policy screen, enter the information to create the policy, then click **Save**.

NOTE

You can configure as many policies as you want.

An example screen and field descriptions follow:

FIGURE 8 Create Policy Screen

- Display Name: The name of the policy. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this policy. It is visible only to Cloudpath administrators.
- "Conditions": In the Conditions section, use any or all of these fields to create the matching criteria you desire so that the appropriate policy gets applied to each user.

NOTE

You can use the asterisks that appear in some of the Conditions fields, when selected, to denote that any value is acceptable in the place of the asterisk.

- Username Regex: When the user is prompted for credentials, the username specified by the user will be verified against this regular expression for proper format. For example, `^d{8}$` will ensure that the user enters an 8-digit id.

NOTE

Due to the complexity of regular expressions, it is recommended to use this field only if you are experienced with regular expressions. If you need assistance creating a regular expression to match your needs, contact support.

- SSID (regex): A regular expression that lists any Wi-Fi SSID(s) to which you want to limit this policy.
- NAS Identifier: The Network access server (NAS) identifier to limit the policy.

NOTE

If you use this field, and no NAS Identifier is provided in the response, the policy will be "false" and will not get applied to a user.

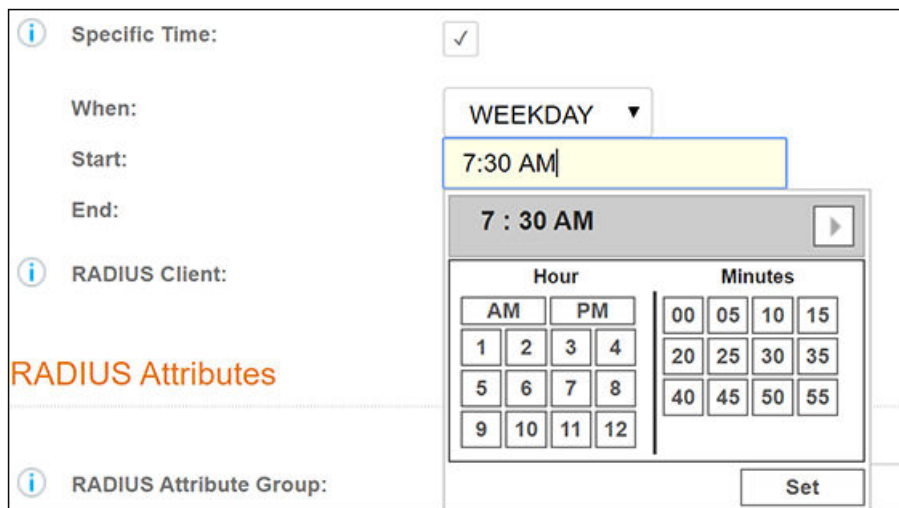
- RADIUS Realm (regex): The RADIUS realm to use in this policy, in the form of @company.com or company.com
- DPSK Reference Name (regex): A regular expression to test against the DPSK Reference Name.

NOTE

This field is applicable only when the policy is applied to a DPSK pool.

- Allow by AD Group: A regular expression that defines the usernames within the Active Directory that this policy allows.
- Specific Time: If checked, drop-downs appear where you can specify the days and times that this policy allows enrollment. Be sure to click the **Set** button to set the desired time (see the following illustration):

FIGURE 9 Setting a Time for a Policy



- RADIUS Client: If you check this box, you are presented with a drop-down where you can then select a RADIUS client if you have already configured this client in the **Configuration > RADIUS Server > Clients** tab. This RADIUS client would then be associated with this policy.
- RADIUS Attribute Group: From this drop-down, select the attribute group that you want associated with this policy.

The following illustration shows the Policies tab after one policy has been added. The information shown in the table represents the policy configuration shown in the example in Figure 8. The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. (The "Certificate Reply Username" applies only to certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.) The RADIUS attribute information shown below comes from the example in Figure 7.

FIGURE 10 Policies Table Example After One Policy Is Configured

The screenshot shows a web interface for configuring policies. At the top, there is a breadcrumb 'Configuration > Policies' and a tab 'RADIUS Attribute Groups'. Below this, there is a section titled 'Policies' with an 'Add Policy' button. A table displays the configured policy. The table has columns for Name, Policy, Attribute Group Name, Attributes, DPSK Rel., Cert.Template Rel., and PEAP Rel. The single row shows a policy named 'Building 1 on weekdays' with a specific NAS Id regex and time range, associated with 'VLAN 1' and specific attributes. Below the table, there are pagination controls showing 'Results 1 - 1 of 1' and a dropdown menu set to '15'.

	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.
+	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	0	0	0

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 **Add DPSK Pool**.

Creating an eDPSK Pool for Use With External DPSK

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 11 Create eDPSK Pool Configuration Screen

Configuration > DPSK Pools > Create Pool

DPSK Pool Information

Display Name: DPSK Pool 17

Description:

Enabled:

Property Count: 0

Generated Passphrase

Passphrase Length: 12

Characters: alphanumeric (Lowercase)

Restrictions

SSID(s): Jeff eDPSK

Enforce Expiration Date:

Enforce Device Count Limit:

Device Limit: 2

RADIUS Policies

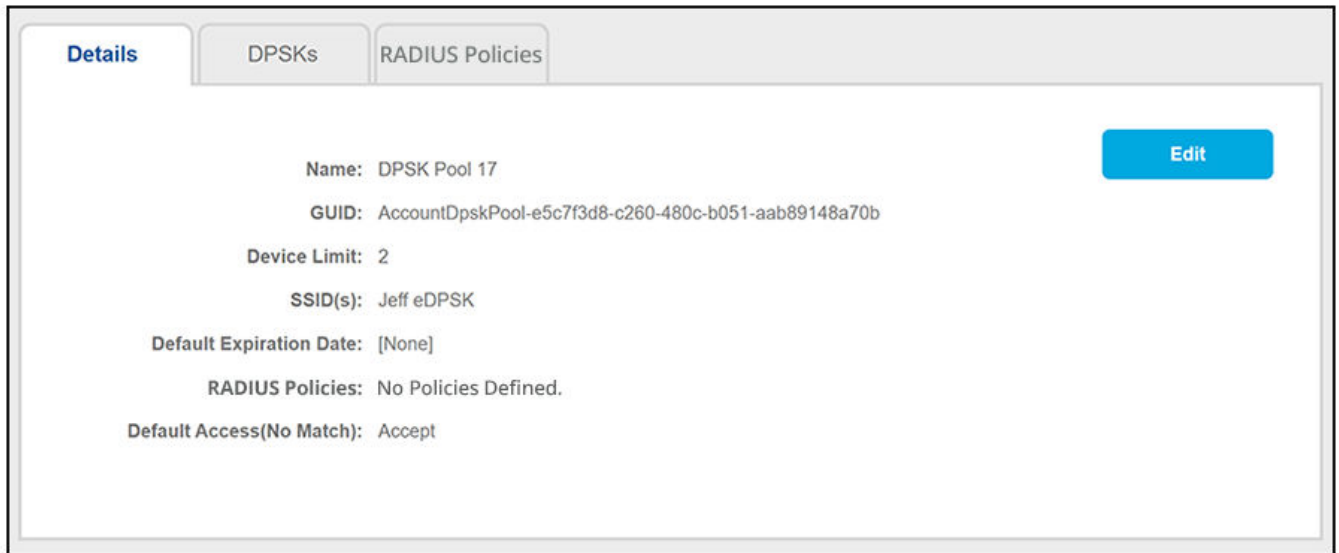
Default Access(No Match): Accept

No policies have been assigned to this pool

- 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.
- Property Count: This field is used for the property management feature. For more information, refer to the *Cloudpath Enrollment System Property Management Configuration Guide*.
- 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.
 - Default Access (No Match): A drop-down where you can select whether to allow a user onto the network even if there is no matching policy for the user.
4. After you save your configuration, you are returned to the following screen, where you can check the pool you just configured:

FIGURE 12 Newly Created Pool



NOTE

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

Creating a DPSK in an Existing eDPSK Pool

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

You can then provide the manually generated DPSKs to users so that, once they log in to a specific SSID, their device gets 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** to view all existing pools.

FIGURE 13 Adding a DPSK to an Existing Pool

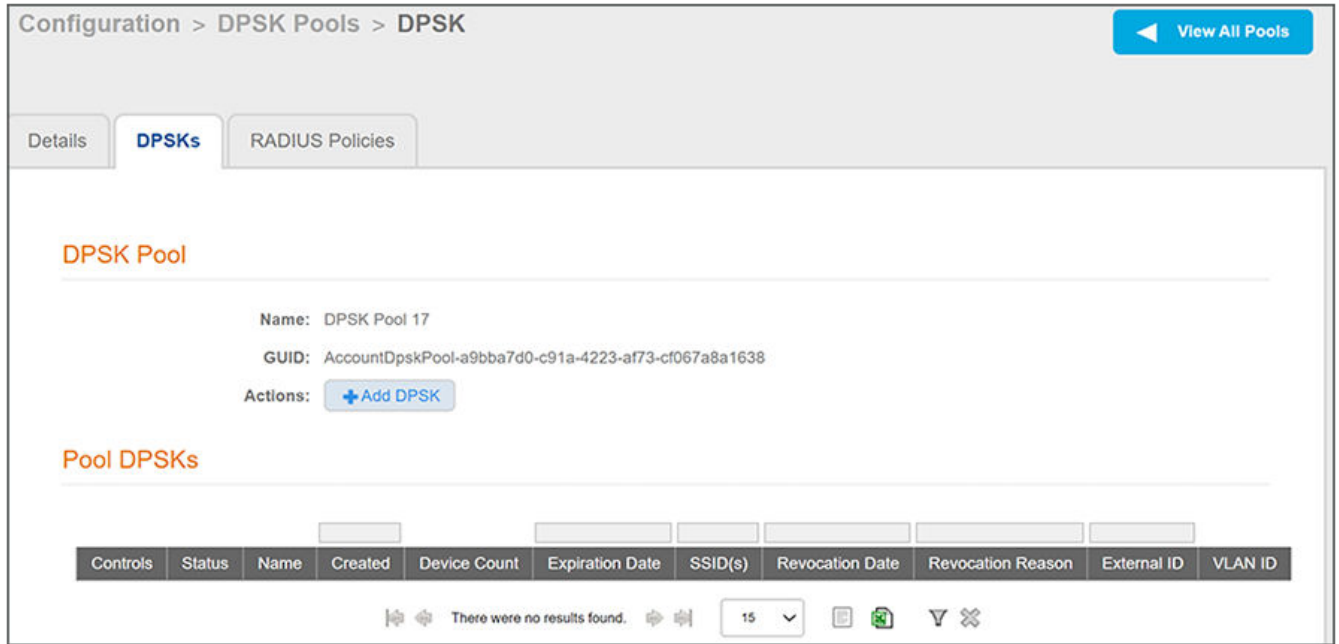
+	Sequence	Status	Name	Description	SSID's	DPSK Count	Policy Count	Default Access
	1	Enabled	DPSK Pool 17		Jeff eDPSK	0	0	ACCEPT
	2	Enabled	DPSK Pool 1		ssid for dpsk pool 1	0	0	ACCEPT
	3	Enabled	DPSK Pool 2		ssid for dpsk pool 2	0	0	ACCEPT

- 2.
3. Click the wrench icon for the desired pool; for example the DPSK Pool 17 entry in the screen above.

Creating a DPSK in an Existing eDPSK Pool

- In the ensuing screen, click the DPSKs tab to bring up the following screen:

FIGURE 14 Button for Adding a DPSK to an Existing DPSK Pool



- Click **Add DPSK**.

- 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 15 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:** If this box is checked, 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, if this box is not checked, the DPSK will not expire. The Expiration Date field does not appear unless the box for Enforce Expiration Date is checked.
- **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.

Creating a DPSK in an Existing eDPSK Pool

- **Override VLAN ID:** By default, this box is unchecked, which means that the DPSK uses the VLAN ID specified in the RADIUS attribute group of the corresponding policy (once you add a policy to the pool). If checked, you can specify a VLAN ID in the popup "VLAN ID" field that will override that VLAN ID. 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 what VLAN ID gets assigned to the pool.
 - **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.
7. 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 16 DPSK Added to Pool

The screenshot shows the configuration page for a DPSK Pool. The breadcrumb navigation is "Configuration > DPSK Pools > DPSK". There is a "View All Pools" button in the top right. The page has three tabs: "Details", "DPSKs", and "RADIUS Policies". The "DPSKs" tab is active.

DPSK Pool

Name: DPSK Pool 17
GUID: AccountDpskPool-e5c713d8-c260-480c-b051-aab89148a70b
Actions: [+ Add DPSK](#)

Pool DPSKs

Controls	Status	Name	Created	Device Count	Expiration Date	SSID(s)	Revocation Date	Revocation Reason	External ID	VLAN ID
Search Edit Delete Refresh	Active	Device Group 10	20210118 1917 MST	0 of 2.	[None]	Jeff eDPSK				(Determined by assigned policy)

Results 1 - 1 of 1. 15

Adding Policies to an eDPSK Pool

You can add as many policies as you want. However, only one policy can be associated with a specific user. For a user to successfully connect to the network, the user must be a match for at least one policy (or you can allow users to connect even if they do not match a policy).

Steps to Add Policies

Follow these steps to add a policy:

1. In the Cloudpath UI, go to **Configuration > DPSK Pools** to view all existing pools:

FIGURE 17 DSPK Pools View

	Sequence	Status	Name	Description	SSID's	DPSK Count	Policy Count	Default Access
	1	Enabled	DPSK Pool 17		Jeff eDPSK	1	0	ACCEPT
	2	Enabled	DPSK Pool 1		ssid for dpsk pool 1	0	0	ACCEPT
	3	Enabled	DPSK Pool 2		ssid for dpsk pool 2	0	0	ACCEPT

- 2.
3. Click the wrench icon for the desired pool; for example the DPSK Pool 17 entry in the screen above.
4. In the ensuing screen, click the RADIUS Policies tab, then click **Assign Policy**. The Select Policy Drop-down list appears, as shown in the following example list. The policies that you have already configured are available for you to add:

FIGURE 18 Select Policy Drop-down List

Select Policy

Select the policy to use.

Policy: Building 1 on weekends

- Building 1 on weekends
- Username and RADIUS Realm
- Building 1 on weekdays

Cancel Save

Adding Policies to an eDPSK Pool

Policy Rules

5. Select the policy you wish to add, then click **Save**.
6. Continue to add policies as you desire. If you have added all available policies, you will receive the message: " All Defined Policies have been assigned."

Policy Rules

The following illustration shows an example of how the page appears after three policies have been added:

FIGURE 19 Policies Added to DPSK ePool

DPSK Pool

Name: DPSK Pool 17
GUID: AccountDpskPool-e5c713d8-c260-480c-b051-aab89148a70b

Actions: [+ Assign Policy](#) [Test Policy Evaluation](#) [Reset Counts](#)

Assigned Candidate Policies:

	Name	Description	Policy	Attributes	Usage Count
X ^ v	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
X ^ v	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
X ^ v	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: '10'	0

When none of the policies are matched, the default access will be: Accept

- There may be many policies whose criteria are matched by a user, but the first policy that is a match is the one that gets applied. For example, if you have three policies, as shown above, the order in which you have them listed is the order in which they will be tested for matches with an enrolling user.

NOTE

You can use the arrows in the screen show above to list the policies in the desired order. If you want to remove a policy from being used in a specific DPSK pool, click the X next to the policy, then confirm the removal of the policy when prompted.

- Because the "Building 1 on weekends" policy is listed first, the matching criteria in that policy (listed in the Policy column) will first be checked against an enrolling user. If there is a match, the policy is applied to the user (meaning that the attributes listen in the Attributes column are applied to the user). If there is no match, the next policy ("Building 1 on weekdays") is checked against the enrolling user, and so on.

NOTE

If none of the policies match a specific user, the default access setting (configured when you create a pool) is used to either accept or reject the user. In the example above, at the bottom of the illustration, the default access is to accept the user because that is how the field was set when DPSK Pool 17 (the example pool shown above) was configured.

Additional Policy Information

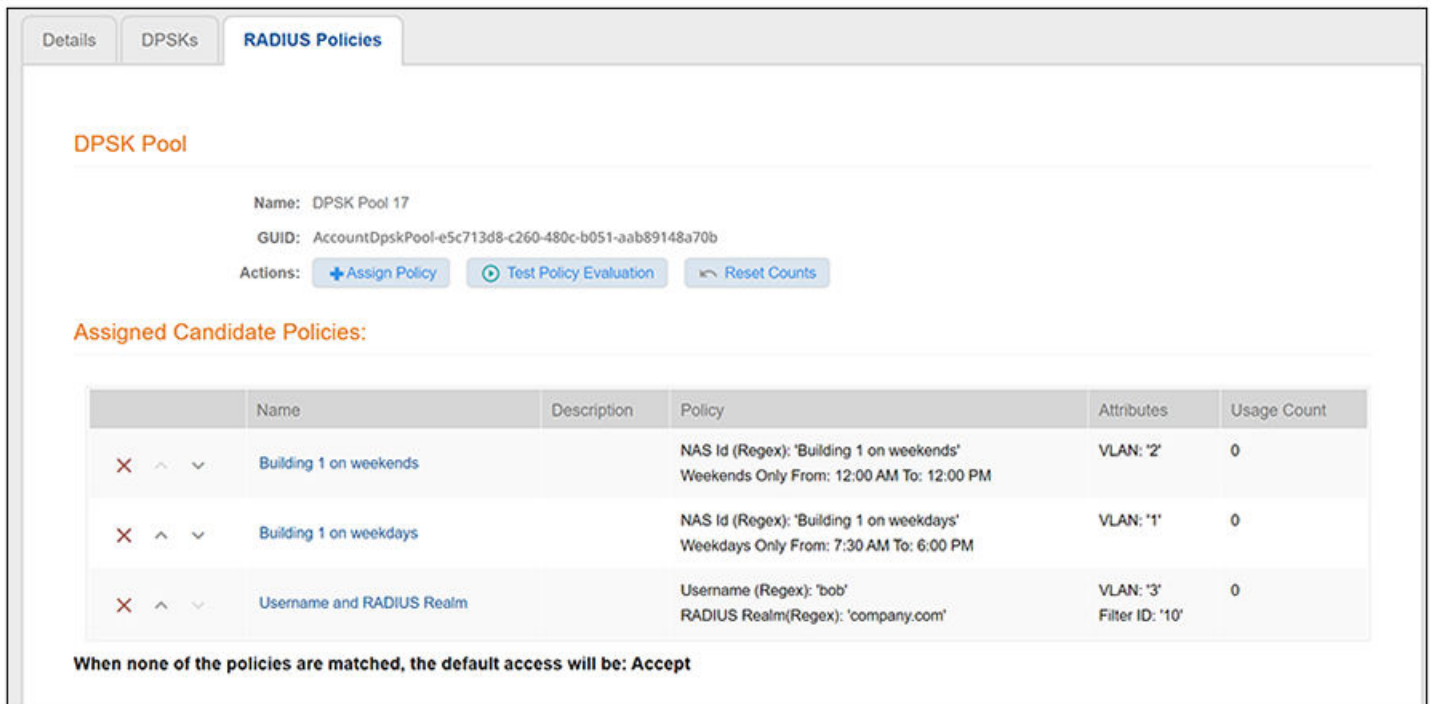
- Testing Policies..... 39
- Viewing Policy Information..... 45
- Viewing RADIUS Attribute Information..... 47

Testing Policies

You can test your policies to be sure they are working as desired before you implement them in a live environment.

The following screen shows an example of three policies that have been added to an eDPSK pool. To get to this screen, go to **Configuration > DPSK Pools**, click the Wrench icon next to the desired pool, then click the **RADIUS Policies** tab.

FIGURE 20 Three-Policy Example



Test Policy Evaluation - Example 1

1. Click the **Test Policy Evaluation** button (see the screen above).
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 21 Test Policy Selection - Example 1 Values

Configuration > DPSK Pools > DPSKs > Test Policy Selection Cancel Apply

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

Username: bob@company.com

SSID: SSID

Authentication Groups: DEMO\domain users DEMO\bob

NAS ID: Building 1 on weekdays

DPSK Reference Name: UserDevice_123

Authentication Date: 20200518

Authentication Time: 5:20 PM

Client Short Name: 0.0.0.0/0

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

The sample values shown above have been entered to test that the "Building 1 on weekdays" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

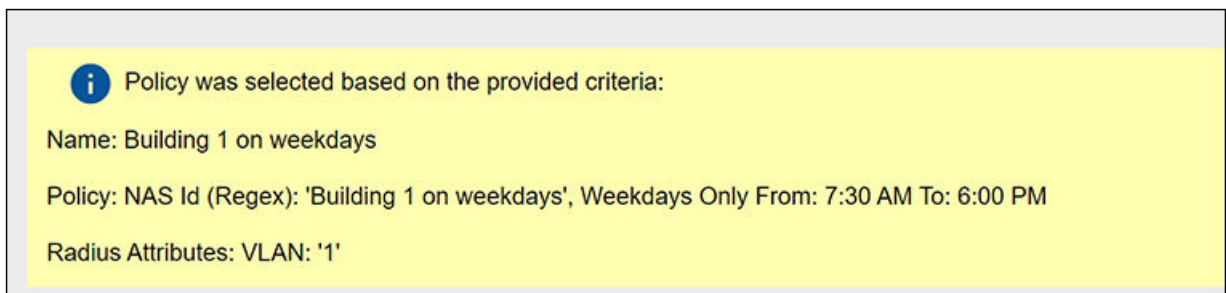
NOTE

The sample values can include fields that are not configured in a policy, and could still be a match for the policy. For example, there could be a value entered in the Client Short Name field in the example above, and it would have no impact on the results of the policy evaluation test because none of the three policies shown above show a value for Client Short Name (as evidenced by the values shown in the Policy column for each policy).

- Username (required): Must be a valid username that your Cloudpath system will accept when this user attempts enrollment.
- SSID: Matches the Wi-Fi SSID name for the connecting device. If this field is populated, this will match only the Wi-Fi based connections.

- Authentication Groups (required): The list of groups returned from a user (as configured in your authorization server; you need a workflow step that requires authentication to an authorization server for the user to have groups).
 - NAS ID: The NAS ID that is expected to be returned from the controller. In the example above, the value "Building 1 on weekdays" is entered because it matches the NAS ID of the "Building 1 on weekdays" policy.
 - Authentication Date: The date on which the user would attempt to authenticate. In the example above, the date is on a weekday because the "Building 1 on weekdays" policy specifies weekdays only for authentication.
 - Authentication Time: The time when the user would attempt to authenticate. In the example above, the time is 5:10 p.m., which falls in the range of 7:30 a.m. to 6 p.m. that the policy specifies for authentication.
 - Client Short Name: RADIUS Client-Shortname expected to be returned from the controller.
3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
- a. The values entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy.
 - b. The values entered are next compared to the second policy in the list, which is the "Building 1 on weekdays" policy. You can see that the values entered for testing all *do* match those listed for this policy. Therefore, the expected behavior is that, when you click the **Apply** button, the "Building 1 on weekdays" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
 - c. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 22 Test Policy Selection - Example 1 Results



Test Policy Evaluation - Example 2

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 23 Test Policy Selection - Example 2 Values

Configuration > DPSK Pools > DPSKs > Test Policy Selection
Cancel ▶ Apply ▶

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

i Username:

i SSID:

i Authentication Groups:

i NAS ID:

i DPSK Reference Name:

i Authentication Date:

i Authentication Time:

i Client Short Name:

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

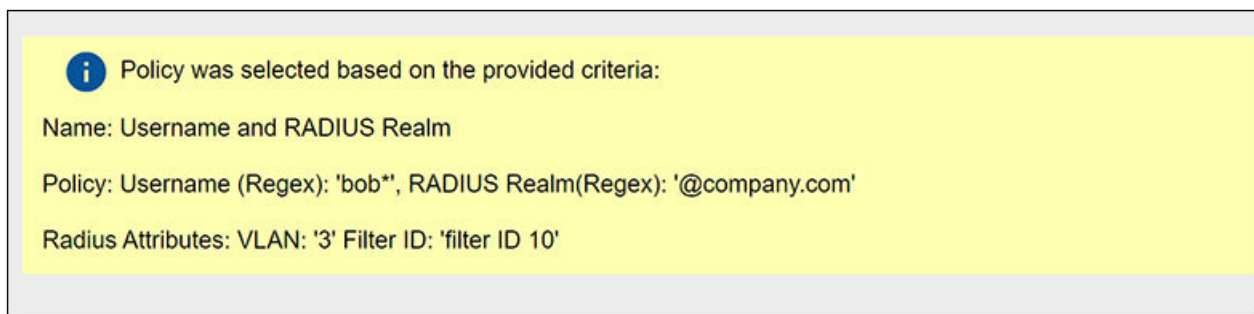
The sample values shown above have been entered to test that the "Username and RADIUS Realm" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
 - a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
 - b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on

weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

- c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the values entered for testing all *do* match the conditions listed for this policy: A username in the form of bob* (where the * can be replaced with any value) and a RADIUS realm (in the username field for the sample test values) in the form of company.com. Therefore, the expected behavior is that, when you click the **Apply** button, the "Username and RADIUS Realm" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 24 Test Policy Selection - Example 2 Results



Test Policy Evaluation - Example 3

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 25 Test Policy Selection - Example 3 Values

Configuration > DPSK Pools > DPSKs > Test Policy Selection
Cancel Apply ▶

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

i Username:

i SSID:

i Authentication Groups:

i NAS ID:

i DPSK Reference Name:

i Authentication Date:

i Authentication Time:

i Client Short Name:

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: 'filter ID 10'

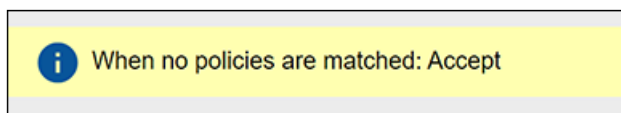
The sample values shown above have been entered to test that no policy will be applied to users who do not match the criteria defined by any of the policies belonging to the pool (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
 - a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.
 - b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on

weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, eliminating any chance of a match to this policy.

- c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the username does not match the conditions listed for this policy, eliminating any chance of a match to this policy. Therefore, the expected behavior is that, when you click the **Apply** button, you should receive a message indicating that no policies matched, but that the user is still accepted onto the network. provided that the " Default Access (No Match)" field was configured to "Accept" a user if there was no policy match. You can confirm this is true for the example pool called DPSK Pool 17 by checking [Figure 20](#).
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 26 Test Policy Selection - Example 3 Results



Viewing Policy Information

To view your currently configured policies, go to **Configuration > Policies** in the UI, and be sure to highlight the Policies tab.

The following table shows you an example of what a policy table looks like after three different policies have been created and assigned to DPSK pools, certificate templates, or PEAP.

FIGURE 27 Policy Table Example

	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.
+	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	1	0	0
+	Building 1 on weekends	NAS Id (Regex): 'Building 1 on weekends', Weekends Only From: 12:00 AM To: 12:00 PM	VLAN 2	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	1	0	0
+	Username and RADIUS Realm	Username (Regex): 'bob', RADIUS Realm(Regex): 'company.com'	VLAN 3 and Filter ID	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	1	0	0

You can use the policy table as follows:

TABLE 5 Description of Policy Table

Column Title	Description
+	<ul style="list-style-type: none"> • You can view details of the policy by clicking on the magnifying glass icon (for an example of the Policy Information screen that gets invoked, see Figure 28). • You can edit the policy by clicking on the pencil icon. • If the policy has not yet been assigned (such as to PEAP or a DPSK pool), there will be a X next to the policy name. Clicking that X deletes the policy. However, in the example above, all three policies are in use; therefore the - sign denotes that you cannot delete the policy as long as it remains in use. You would first need to remove the policy from where it is being used before you can delete the policy from the table shown above.

Additional Policy Information

Viewing Policy Information

TABLE 5 Description of Policy Table (continued)

Column Title	Description
Name	The name of the policy as configured in the Display Name field in the Policy configuration screen, an example of which is shown in Figure 8 on page 24. .
Policy	All the conditions that you set when you created the policy are listed in this column. For example, the "Building 1 on weekdays" policy conditions are the ones that were configured in the example shown in Figure 8 on page 24.
Attribute Group Name	The name of the group that has been selected in the RADIUS Attribute Group drop-down when the policy was created. For the "Building 1 on weekdays" policy shown in this example, the group name VLAN 1 matches the selection that was shown in the example in Figure 8 on page 24.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 7 on page 22. NOTE The "Reply Username" attribute applies only to certificate templates.
DPSK Rel, Cert Template Rel, and PEAP Rel	The number of times that a policy has been assigned to each category of authentication.

FIGURE 28 Policy Information Screen Example

The screenshot displays the 'Policy Information' screen. At the top, the policy name is 'Building 1 on weekdays'. Below it, the 'Description' field is empty. The 'Conditions' section lists 'NAS Id (Regex): 'Building 1 on weekdays'', 'Weekdays Only From: 7:30 AM To: 6:00 PM', and 'RADIUS Attribute Group: Reply Username: 'Certificate Common Name (Default)', VLAN: '1''. The 'Relationships' section contains a table with three rows: PEAP (Location: PEAP, Usage Count: 0), DPSK (Location: DPSK Pool 17, Usage Count: 0), and CERTIFICATE (Location: username@byod.company.com, Usage Count: 0).

Type	Location	Usage Count
PEAP	PEAP	0
DPSK	DPSK Pool 17	0
CERTIFICATE	username@byod.company.com	0

The screen above indicates that the policy is currently being used by PEAP, one DPSK pool, and one certificate. The "Location" column of this screen in the UI provides live links to the specific configuration areas where the policy is used.

The Usage column will be incremented each time a device is assigned to the policy in question. Also, If a device then gets assigned to a different policy and later gets reassigned to its original policy, the usage count of the original policy will be incremented.

Viewing RADIUS Attribute Information

To view your currently configured RADIUS attribute groups, go to **Configuration > Policies** in the UI, and be sure to select the RADIUS Attribute Groups tab.

The following table shows you an example of what a RADIUS Attribute Groups table looks like after three different RADIUS attribute groups have been created.

FIGURE 29 RADIUS Attribute Groups Example

	Name	Description	Policy Count	Attributes	Timestamp
+ [pencil] [X]	VLAN 1		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	20210118 1509 MST
[pencil] [X]	VLAN 2		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	20210118 2024 MST
[pencil] [X]	VLAN 3 and Filter ID		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	20210118 2025 MST

You can use the RADIUS Attribute Groups table as follows:

TABLE 6 Description of RADIUS Attribute Groups Table

Column Title	Description
+	<ul style="list-style-type: none"> You can edit the RADIUS attribute group by clicking on the pencil icon. If the RADIUS attribute group has not yet been assigned to any policy, there will be a X next to the name. Clicking that X deletes the group. However, in the example screen shown above, all the groups have already been assigned to at least one policy; therefore the X is not selectable, which denotes that you cannot delete the group as long as it remains in use by one or more policies. You would have to edit the policy itself to remove the RADIUS attribute from the policy if you then want to delete the RADIUS attribute.
Name	The name of the RADIUS attribute group as configured in the Display Name field in the RADIUS Attribute Group configuration screen, an example of which is shown in Figure 7 on page 22.
Description	Any optional description that was entered in the configuration of the RADIUS attribute group.
Policy Count	The number of policies that the RADIUS attribute group is currently assigned to.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 7 on page 22. NOTE The "Reply Username" attribute applies to certificate authentications only.
Timestamp	Time that the RADIUS attribute group was created.

Managing eDPSK Pools and DPSKs

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

Refer to:

- [Managing DPSK Pools](#)
- [Managing DPSKs](#)
- [Dashboard Information](#)

Managing DPSK Pools

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

FIGURE 30 Configured List of eDPSK Pools - Searched From Top Down

	Sequence	Status	Name	Description	SSID's	DPSK Count	Policy Count	Default Access
⚙️ ⌵ ⌶	1	Enabled	DPSK Pool 17		Jeff eDPSK	2	3	ACCEPT
⚙️ ⌵ ⌶	2	Enabled	DPSK Pool 1		ssid for dpsk pool 1	0	0	ACCEPT
⚙️ ⌵ ⌶	3	Enabled	DPSK Pool 2		ssid for dpsk pool 2	0	0	ACCEPT

Here are some actions you can take:

- **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/viewing the configuration settings:** To edit (or view) the settings of a pool, click the Wrench icon to the left of the pool name. In the ensuing screen, with the "Details" tab selected, click **Edit**. The configuration screen for that pool is invoked, and you can make any changes you want. The following is an example of a screen that gets invoked when you want to edit an existing pool:

FIGURE 31 DSPK Pool in Edit Mode

Configuration > DPSK Pools > Modify Pool

DPSK Pool Information

Display Name: DPSK Pool 17

Description:

Enabled:

Property Count: 0

Generated Passphrase

Passphrase Length: 12

Characters: alphanumeric (Lowercase)

Restrictions

SSID(s): Jeff eDPSK

Enforce Expiration Date:

Enforce Device Count Limit:

Device Limit: 2

Policies

Default Access(No Match): Accept

Name	Description	Policy	Attributes	Usage Count
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: 'filter ID 10'	0

> Cleanup

- **Cleanup options:** From within edit mode, 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.

- **Other actions after using Wrench icon:** When you click the Wrench icon for a DPSK pool (refer to Figure 30), then ensuing screen contains the "DPSKs" and "RADIUS Policies" tabs in addition to the "Details" tab described previously.
 - DPSKs tab: Refer to [Managing DPSKs](#).
 - Policies tab: Shows you the policies associated with the pool, as in the following example screen:

DPSK Pool

Name: DPSK Pool 17
 GUID: AccountDpskPool-e5c713d8-c260-480c-b051-aab89148a70b

Actions: [+ Assign Policy](#) [Test Policy Evaluation](#) [Reset Counts](#)

Assigned Candidate Policies:

	Name	Description	Policy	Attributes	Usage Count
X ^ v	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
X ^ v	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
X ^ v	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: '10'	0

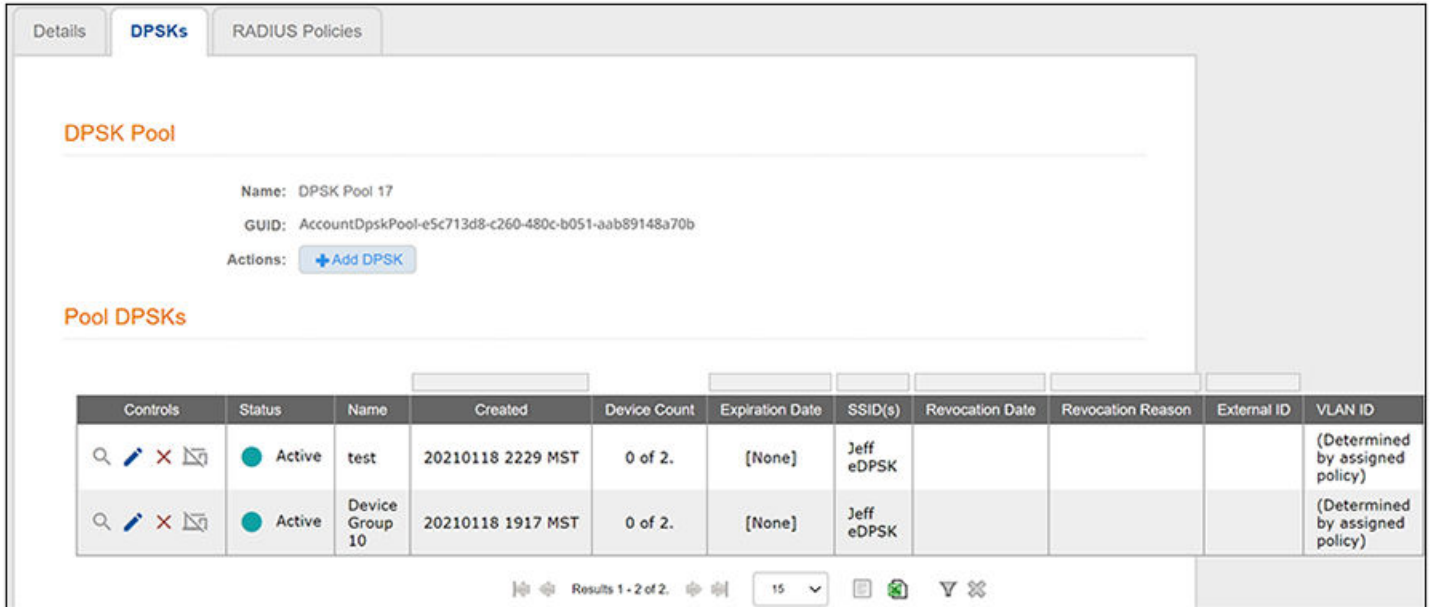
When none of the policies are matched, the default access will be: Accept

- › To add a policy to the pool, click **Assign Policy**. For more information, see [Adding Policies to an eDPSK Pool](#) on page 35.
- › To test the policies, click **Test Policy Evaluation**. For more information, see [Testing Policies](#) on page 39.
- › To remove a policy from the pool, click the X next to the policy name.
- › To re-order the policies in the list, use the up and down arrows.

Managing DPSKs

If you go to **Configuration > DPSK Pools** and click the Wrench icon for a DPSK pool (refer to [Figure 30](#)), you can then click the "DPSKs" tab on the ensuing screen to view all the DPSKs that have been generated for that pool. The screen below shows the DPSKs for a pool called "DPSK Pool 17."

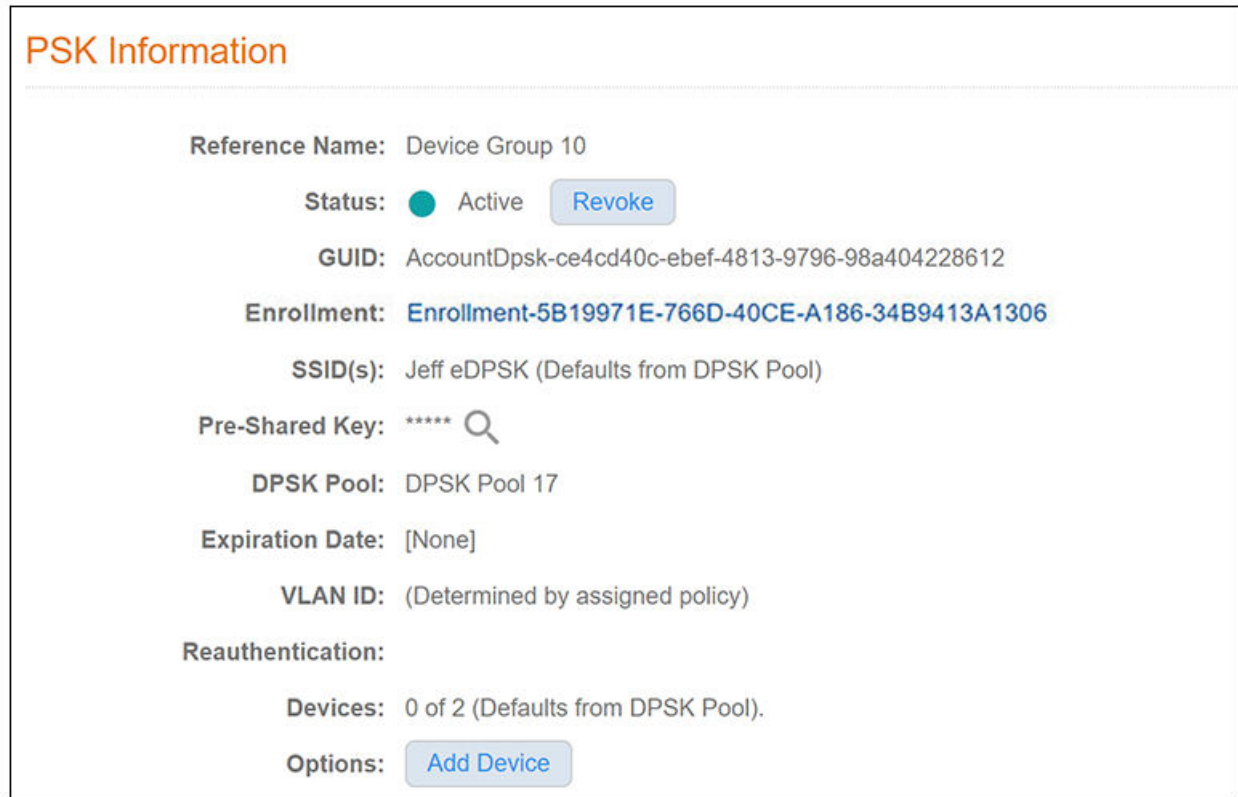
FIGURE 32 List of DPSKs Within a Specific Pool - Actions You Can Take



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 33 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.
- **Revoke the DPSK:** You can click **Revoke** 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 32](#).

NOTE

Revoking a DPSK leaves its records in the database for auditing purposes, and allows you to un revoke 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 to go 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 34 DPSKs Listed in the Dashboard

	Status	Name	Created	Device Count	Expiration Date	SSID(s)	Pool Name	External ID	VLAN ID
	Active	test	20200519 0009 MDT	0 of 2.	[None]	Jeff eDPSK	DPSK Pool 17		(Determined by assigned policy)
	Active	Device Group 10	20200518 2144 MDT	0 of 2.	[None]	Jeff eDPSK	DPSK Pool 17		(Determined by assigned policy)

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.

Switching Pre-Release-5.7 DPSK pools to Policy-Assigned Pools

DPSK pools are created differently in Release 5.7 and later from prior releases. If you have older pools in your system, you can continue to use them the same way in 5.7 or later, or you can convert them to the policy-type DPSK pools that are created in Release 5.7 and later. Once you switch an old pool to the new policy-type format, you cannot revert back to the pre-5.7 pool configuration.

The figure below shows an example of a DPSK pool configured from a release prior to 5.7:

FIGURE 35 Modify Pool Configuration Screen: Pre-Release 5.7 DPSK Pool

The screenshot shows the 'Modify Pool' configuration screen for a Pre-Release 5.7 DPSK Pool. The breadcrumb navigation at the top reads 'Configuration > DPSK Pools > Modify Pool'. There are 'Cancel' and 'Save' buttons in the top right corner. The form is organized into four sections:

- DPSK Pool Information:** Includes 'Display Name' (Pre-57 pool), 'Description' (empty text area), and 'Enabled' (checked checkbox).
- Passphrase Characteristics:** Includes 'Passphrase Length' (12) and 'Characters' (alphanumeric (Lowercase)).
- Restrictions:** Includes 'SSID(s)' (pre57_ssid), 'Enforce Expiration Date' (checked), 'Default Expiration Date' (3 Months after issuance), 'Enforce Device Count Limit' (checked), and 'Device Limit' (1).
- RADIUS Attributes:** Includes 'Switch Pool to Policies' (unchecked checkbox), 'VLAN ID' (1), 'Filter ID' (filter3), 'Class' ([ex. BYOD]), and 'Reauthentication' ([ex. 86400] Seconds).

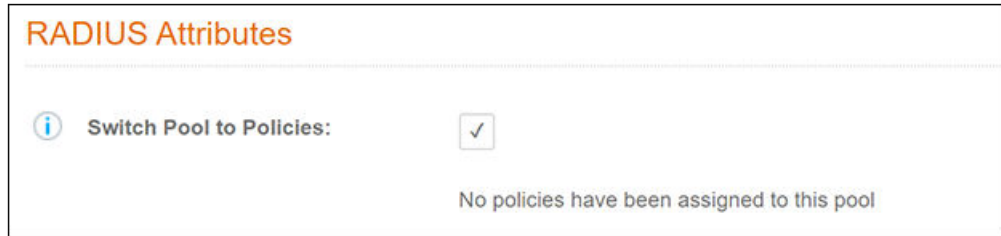
A blue plus sign is located at the bottom of the RADIUS Attributes section.

NOTE

Under RADIUS Attributes, the one new field called "Switch Pool to Policies" is how you change the pool to a policy-assigned pool.

If you want to proceed with switching to the policy model, follow these steps:

1. Check the "Switch Pool to Policies" box. You will receive the following message:

FIGURE 36 Message Displayed After Selecting Checkbox to Switch Pool to Policies

2. Click **Save** on the Modify Pool Configuration screen. The DPSK Pool is now converted to the new format, as shown in the following example:

FIGURE 37 Old Pool Now in Policy Format

3. Select the **RADIUS Policies** tab and add any desired policies. For instructions on adding policies, see [Adding Policies to an eDPSK Pool](#) on page 35.

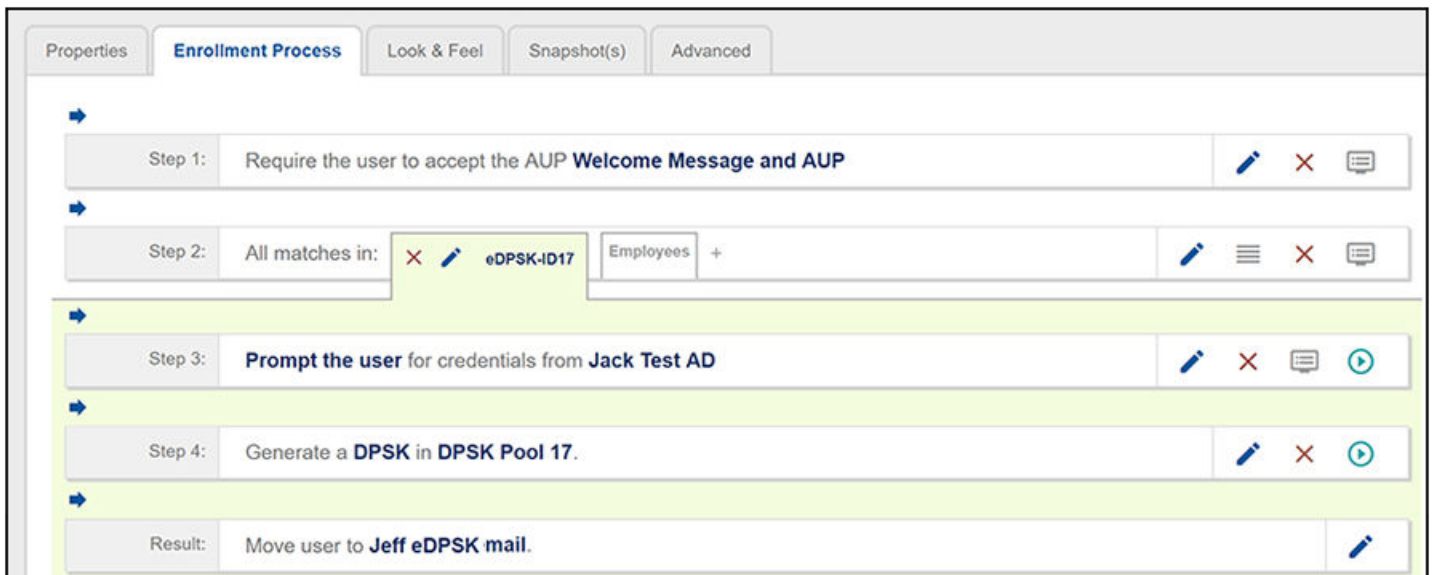
Setting up an eDPSK Workflow

- Limiting One DPSK per User..... 61

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 38 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.

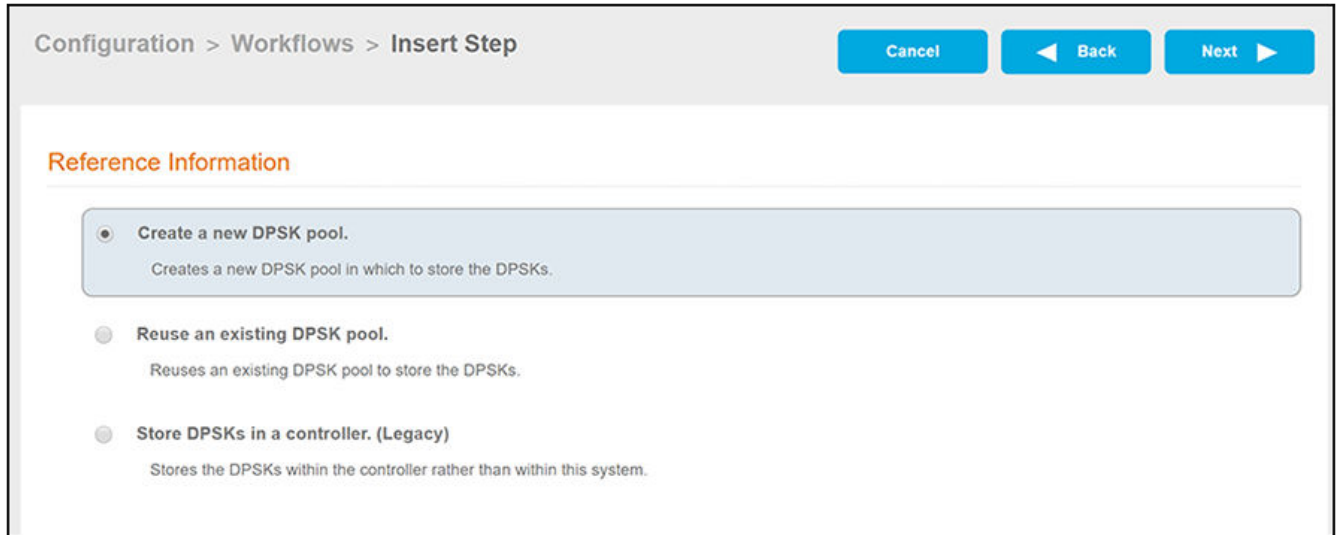
Step 3 in the workflow example shows an authentication step that you might want to have. Then, to create Step 4, which is the DPSK pool step, you would do the following:

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 39 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 27). 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 edit the plugin to have the pre-shared key emailed to the user:
 - a. Click the pencil icon to the right of the DPSK Pool plugin (step 4 in [Figure 38](#)).
 - b. On the ensuing screen, check the "Send Email" checkbox (see the Notifications area of the screen below). This box is unchecked by default.
 - c. Optionally, you can also edit the Email Subject and Email Template fields.

FIGURE 40 Sending an Email to the User With Pre-Shared Key (PSK)

- d. Click **Save** when you are done.

As the user goes through the enrollment process, an email notification gets sent to the user, as shown in the following example:

FIGURE 41 Email Notification Sent to User Showing Assigned PSK

The following PSK has been assigned to you:

ohaivajzwvcb

- 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 15) 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 on the enrollment device. As administrator, you can obtain information about the newly created DPSK by referring to [Managing eDPSK Pools and DPSKs](#) on page 49.

Limiting One DPSK per User

You can restrict users from creating multiple DPSKs from multiple enrollments.

If the user already has multiple DPSKs, during the enrollment process, the system prompts the user to choose one DPSK and revokes the other DPSKs. To perform this action, the user must have an identity.

Setting up an eDPSK Workflow

Limiting One DPSK per User

NOTE

Limiting one DPSK per user is applied only to the DPSKs created from Cloudpath DPSK pool. The restriction rule is not applied to the DPSKs created from SmartZone or Zone Director.

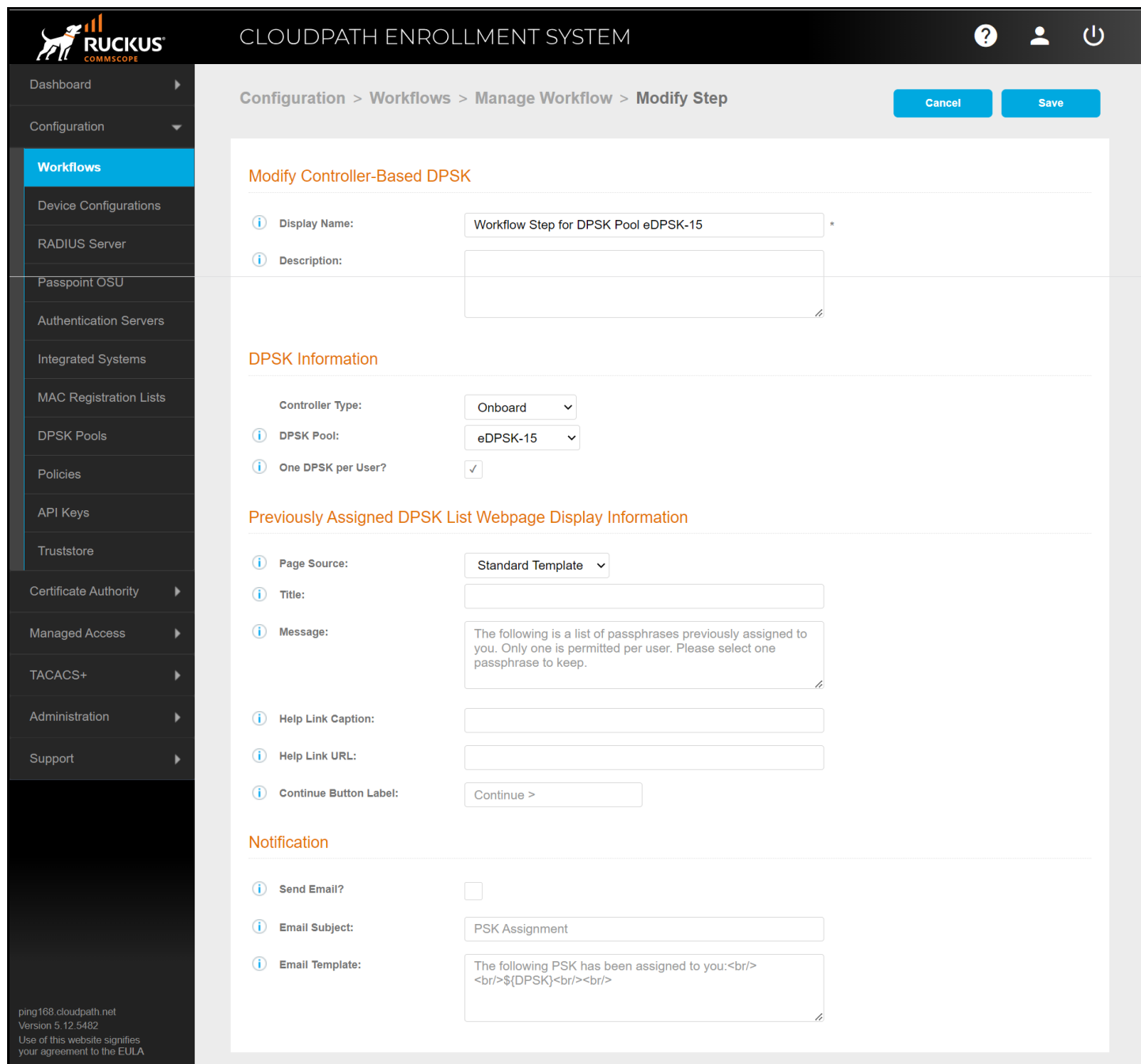
To limit one DPSK per user, perform the following:

One DPSK per User option is added to the existing **Generate a Ruckus DPSK** plugin. The checkbox is available when controller type is configured as Onboard. After selecting the **One DPSK per user?** checkbox, a new section **Previously Assigned DPSK List Webpage Display Information** is displayed. Enter the details in the section, as shown in the figure below.

- **Page Source** - By default the system displays **Standard Template**. However, user can click on the drop-down arrow to choose **Upload HTML File** and upload the HTML file as source of the display page.
- **Title** - Enter a title for the content area.
- **Message** - Enter the main message to be displayed in the content area.
- **Help Caption** - Enter the text to be used as the help link.
- **Help Link** - Enter the help link URL.
- **Continue Button Label** - Enter a label that displays on the continue button.

Click **Save**.

FIGURE 42 Limiting One DPSK per User



There are 3 scenarios associated to **One DPSK per user** during an enrollment process.

1. Scenario 1 - If the user has multiple DPSKs, the system prompts the user to choose one permanent DPSK to keep.
2. Scenario 2 - If the user is enrolling for the first time, the system generates a DPSK for the user.
3. Scenario 3 - If the user already has one DPSK, the system assigns the same DPSK to the user.

Setting up an eDPSK Workflow

Limiting One DPSK per User

The purpose of **Previously Assigned DPSK List Webpage Display Information** is to administer a user prompt page for the users in Scenario 1, to allow such users to choose one DPSK to keep. There are no user prompts for the users in Scenarios 2 and 3. One example of the user prompt (in Scenario 1) is shown in the figure below.

FIGURE 43 Choose One DPSK



The following is a list of passphrases previously assigned to you. Only one is permitted per user. Please select one passphrase to keep.

- Passphrase: wmlgvktrtdct**
Expiration Date: 20230730 113454
unlimited devices
- Passphrase: rnieynbbeidx**
Expiration Date: 20230725 203910
unlimited devices
aabbccddeeff
- Passphrase: uivtooikldtc**
Expiration Date: 20230722 102109
unlimited devices

< Back Continue >



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>