

Cloudpath Enrollment System Protected Extensible Authentication Protocol (PEAP) Configuration Guide, 5.6

Supporting Cloudpath Software Release 5.6

Copyright, Trademark and Proprietary Rights Information

© 2019 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

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, 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	4
Document Conventions.....	4
Command Syntax Conventions.....	4
Document Feedback.....	5
Ruckus Product Documentation Resources.....	5
Online Training Resources.....	5
Contacting Ruckus Customer Services and Support.....	5
Overview of PEAP Configuration	6
Set up the AAA Authentication Server on the Ruckus ZoneDirector Controller	7
Set up the AAA Authentication Server on the Ruckus SmartZone Controller	9
Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller	10
Conifguring a PEAP WLAN on a Ruckus SmartZone Controller	14
Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller	20
Adding a PEAP Branch to Your Workflow.....	20
Adding a PEAP Device Configuration to Your Workflow.....	23
Configuring Cloudpath to Communicate with the External RADIUS server.....	25
Testing the PEAP User Experience.....	27
Troubleshooting Tips.....	29

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	<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 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.

Convention	Description
<code>x y</code>	A vertical bar separates mutually exclusive elements.
<code>< ></code>	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
<code>...</code>	Repeat the previous element, for example, <code>member[member...]</code> .
<code>\</code>	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.

Overview of PEAP Configuration

Protected Extensible Authentication Protocol (PEAP) is one of several methods available for user authentication in Cloudpath.

PEAP is a username/password-based method of authentication.

NOTE

PEAP requires you to already have an external RADIUS server. This document provides the steps on how to configure your controller and your Cloudpath system to communicate with your external RADIUS server. (The Cloudpath onboard RADIUS server does not support PEAP authentication.)

If you will be using a Ruckus ZoneDirector controller to set up PEAP, follow the procedures in these sections:

1. [Set up the AAA Authentication Server on the Ruckus ZoneDirector Controller](#) on page 7
2. [Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller](#) on page 10
3. [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 20

If you will be using a Ruckus SmartZone controller to set up PEAP, follow the procedures in these sections:

1. [Set up the AAA Authentication Server on the Ruckus SmartZone Controller](#) on page 9
2. [Configuring a PEAP WLAN on a Ruckus SmartZone Controller](#) on page 14
3. [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 20

Set up the AAA Authentication Server on the Ruckus ZoneDirector Controller

You must enter information about your existing external RADIUS server in the controller user interface.

Go to **Configure > AAA Servers** on your ZoneDirector controller. The following screen shows the AAA authentication server configuration.

FIGURE 1 Create AAA Authentication Server on ZoneDirector

Editing (Jeff AAA Auth)	
Name	Jeff AAA Auth
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+
Encryption	<input type="checkbox"/> TLS
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Backup RADIUS	<input type="checkbox"/> Enable Backup RADIUS support
IP Address*	10.176.209.54
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times

OK Cancel

Enter the following values for the authentication server:

- Name = Any descriptive name you wish.
- Type = RADIUS
- Encryption: Leave the TLS box unchecked.
- Auth Method = PAP
- Backup RADIUS: Refer to your controller documentation if you want to use a backup RADIUS server.
- IP address = The IP address of your external RADIUS server.
- Port = 1812
- Shared Secret = The shared secret of your external RADIUS server.

NOTE

Leave the default values for the remaining fields.

Click **OK**.

Proceed to [Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller](#) on page 10.

Set up the AAA Authentication Server on the Ruckus SmartZone Controller

You must enter information about your existing external RADIUS server in the controller user interface.

Go to **System > Services & Profiles > Authentication** on your SmartZone controller. The following screen shows the AAA authentication server configuration.

FIGURE 2 Create AAA Authentication Server on SmartZone

The screenshot shows a configuration window titled "Edit AAA Server: [Jeff AAA Auth vSZ]". It features a "General Options" section with a dropdown menu. Below this, there are input fields for "Name" (filled with "Jeff AAA Auth vSZ"), "Description", and "Type" (with "RADIUS" selected via a radio button). A checkbox for "Backup RADIUS: Enable Secondary Server" is present. A "Primary Server" section contains fields for "IP Address" (10.176.209.54), "Port" (1812), "Shared Secret" (masked with dots), and "Confirm Secret" (masked with dots). At the bottom right, there are "OK" and "Cancel" buttons.

Enter the following values for the authentication server:

- Name = Any descriptive name you wish.
- Type = RADIUS
- Backup RADIUS: Refer to your controller documentation if you want to use a backup RADIUS server.
- IP address = The IP address of your external RADIUS server.
- Port = 1812
- Shared Secret = The shared secret of your external RADIUS server.

Click **OK**.

Proceed to [Configuring a PEAP WLAN on a Ruckus SmartZone Controller](#) on page 14.

Configuring a PEAP WLAN on a Ruckus ZoneDirector Controller

You can configure a PEAP WLAN on a Ruckus Wireless ZoneDirector controller so that you can then use PEAP as one method of authenticating users to Cloudpath.

Follow these steps to configure a PEAP WLAN on a Ruckus ZoneDirector controller.

NOTE

The procedure shown in this section is based on the user interface of a ZoneDirector controller version 10.0. Different versions of ZoneDirector may have minor differences in terms of which configuration options appear in what sections of a screen.

1. Log in to your Ruckus ZoneDirector controller.
2. Navigate to **Configure > WLANs**.

- Under the WLAN List section, click **Create New**.
The **Create New** section of the screen is displayed.

FIGURE 3 Create New WLAN on ZoneDirector

The screenshot shows the 'Create New' configuration page for a WLAN. It is organized into several sections:

- General Options:** Includes fields for 'Name/ESSID*' (with a 'New Name' input) and 'ESSID' (with a 'New Name' input), and a 'Description' field.
- WLAN Usages:** Contains a 'Type' section with radio buttons for 'Standard Usage' (selected), 'Guest Access', 'Hotspot Service (WISPr)', 'Hotspot 2.0', 'Autonomous', and 'Social Media'.
- Authentication Options:** Includes a 'Method' section with radio buttons for 'Open' (selected), '802.1x EAP', 'MAC Address', and '802.1x EAP + MAC Address'. It also has a 'Fast BSS Transition' section with a checkbox for 'Enable 802.11r FT Roaming'.
- Encryption Options:** Includes a 'Method' section with radio buttons for 'WPA2', 'WPA Mixed', 'WEP-64 (40 bit)', 'WEP-128 (104 bit)', and 'None' (selected).
- Options:** Contains several checkboxes: 'Enable captive portal/Web authentication', 'Isolate wireless client traffic from other clients on the same AP', 'Isolate wireless client traffic from all hosts on the same VLAN/subnet', and 'Enable Zero-IT Activation'. It also includes dropdown menus for 'Authentication Server' (set to 'Local Database') and 'WhiteList' (set to 'No WhiteList').
- Priority:** Includes radio buttons for 'High' (selected) and 'Low'.

At the bottom of the form, there is a link for 'Advanced Options' and 'OK' and 'Cancel' buttons.

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.

- Complete the General Options section:

FIGURE 4 General Options Section of Creating a New WLAN

General Options	
Name/ESSID*	<input type="text" value="eng-PEAP"/> ESSID <input type="text" value="eng-PEAP"/>
Description	<input type="text" value="Jeff AAA RADIUS server for P"/>

- Name: Enter a meaningful name for the PEAP WLAN you are creating.
 - ESSID: When you click in this field, the name you entered in the Name field also appears in this field.
 - Description: You can enter a brief description to indicate that you are creating a RADIUS WLAN for PEAP.
- In the WLAN Usages section, use the default selection of Standard Usage.

FIGURE 5 WLAN Usage section of Creating a New WLAN

WLAN Usages	
Type	<input checked="" type="radio"/> Standard Usage (For most regular wireless network usages.)
	<input type="radio"/> Guest Access (Guest access policies and access control will be applied.)
	<input type="radio"/> Hotspot Service (WISPr)
	<input type="radio"/> Hotspot 2.0
	<input type="radio"/> Autonomous
	<input type="radio"/> Social Media

- In the Authentication Options section, be sure that you select 802.1x EAP.

FIGURE 6 Authentication Options section of Creating a New WLAN

Authentication Options	
Method	<input type="radio"/> Open <input checked="" type="radio"/> 802.1x EAP <input type="radio"/> MAC Address <input type="radio"/> 802.1x EAP + MAC Address
Fast BSS Transition	<input type="checkbox"/> Enable 802.11r FT Roaming <small>(Recommended to enable 802.11k Neighbor-list Report for assistant.)</small>

- In the Encryption Options section, choose WPA2 for the Method. When you choose WPA2, the Encryption Options section appears as shown below:

FIGURE 7 Encryptions Options section after choosing WPA2 as the Method

Encryption Options	
Method	<input checked="" type="radio"/> WPA2 <input type="radio"/> WPA-Mixed <input type="radio"/> WEP-64 (40 bit) <input type="radio"/> WEP-128 (104 bit) <input type="radio"/> None
Algorithm	<input checked="" type="radio"/> AES <input type="radio"/> Auto (TKIP+AES)
802.11w MFP	<input checked="" type="radio"/> Disabled <input type="radio"/> Optional <input type="radio"/> Required

- Algorithm: Be sure that the default value of AES is selected.
 - 802.11w MFP: Be sure the default value of Disabled is selected.
- In the Options section, select the authentication server that you configured in [Set up the AAA Authentication Server on the Ruckus ZoneDirector Controller](#) on page 7 from the drop-down list.

FIGURE 8 Options Section After Authentication Server is Selected

Options	
Authentication Server	Jeff AAA Auth <input type="button" value="Create New"/>
Wireless Client Isolation	<input type="checkbox"/> Isolate wireless client traffic from other clients on the same AP. <input type="checkbox"/> Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList <input type="button" value="Create New"/> (Requires whitelist for gateway and other allowed hosts.)
Zero-IT Activation™	<input type="checkbox"/> Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	<input checked="" type="radio"/> High <input type="radio"/> Low

NOTE

Do not configure an accounting server for PEAP.

- In the Advanced Options section, there are many fields (not shown here), but you can also use all the default values.

10. Click **OK** to complete the PEAP WLAN configuration.

Your newly created PEAP WLAN should now appear in the WLAN List, "eng-PEAP" in this example:

FIGURE 9 Newly Created WLAN Appears in WLAN List

<input type="checkbox"/>	Name	ESSID	Description	Authentication	Encryption	Actions
<input type="checkbox"/>	dpsk test	dpsk test		Open	WPA2	Edit Clone
<input type="checkbox"/>	eng-PEAP	eng-PEAP	Jeff AAA RADIUS server for PEAP	802.1x EAP	WPA2	Edit Clone
<input type="checkbox"/>	HQ1-Jeff	HQ1-Jeff	HQ1-Jeff	802.1x EAP	WPA2	Edit Clone
<input type="checkbox"/>	Jeff PSK	Jeff PSK		Open	WPA2	Edit Clone

To review the completed configuration or to make any configuration changes, click the **Edit** button.

Proceed to [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 20.

Configuring a PEAP WLAN on a Ruckus SmartZone Controller

You can configure a PEAP WLAN on a Ruckus Wireless SmartZone controller so that you can then use PEAP as one method of authenticating users to Cloudpath.

Follow these steps to configure a PEAP WLAN on a Ruckus SmartZone controller.

NOTE

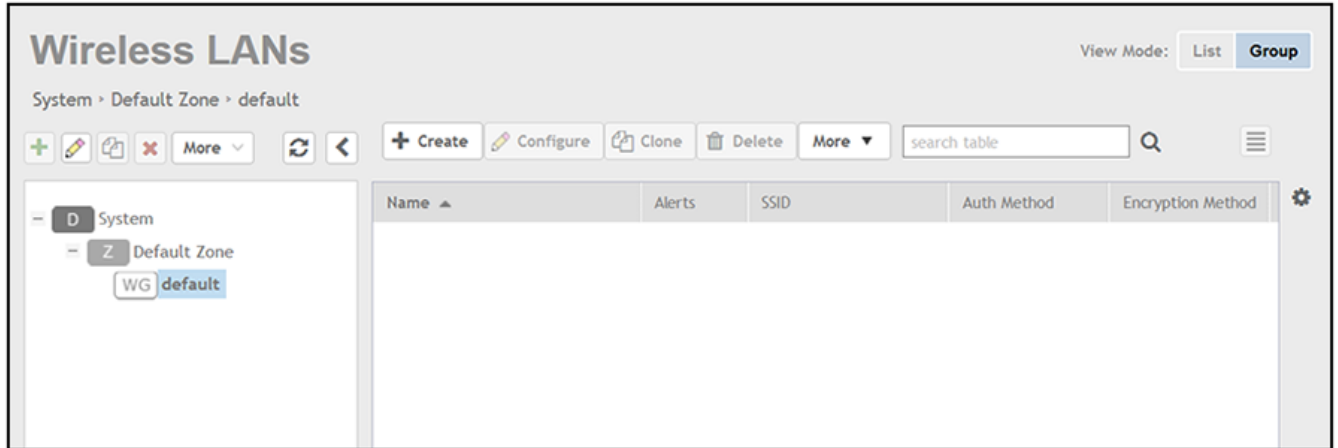
The procedure shown in this section is based on the user interface of a SmartZone controller version 3.5.1. Different versions of SmartZone may have minor differences in terms of which configuration options appear in what sections of a screen.

1. Log in to your Ruckus SmartZone controller.

2. Click the **Wireless LANs** tab.

The following screen appears:

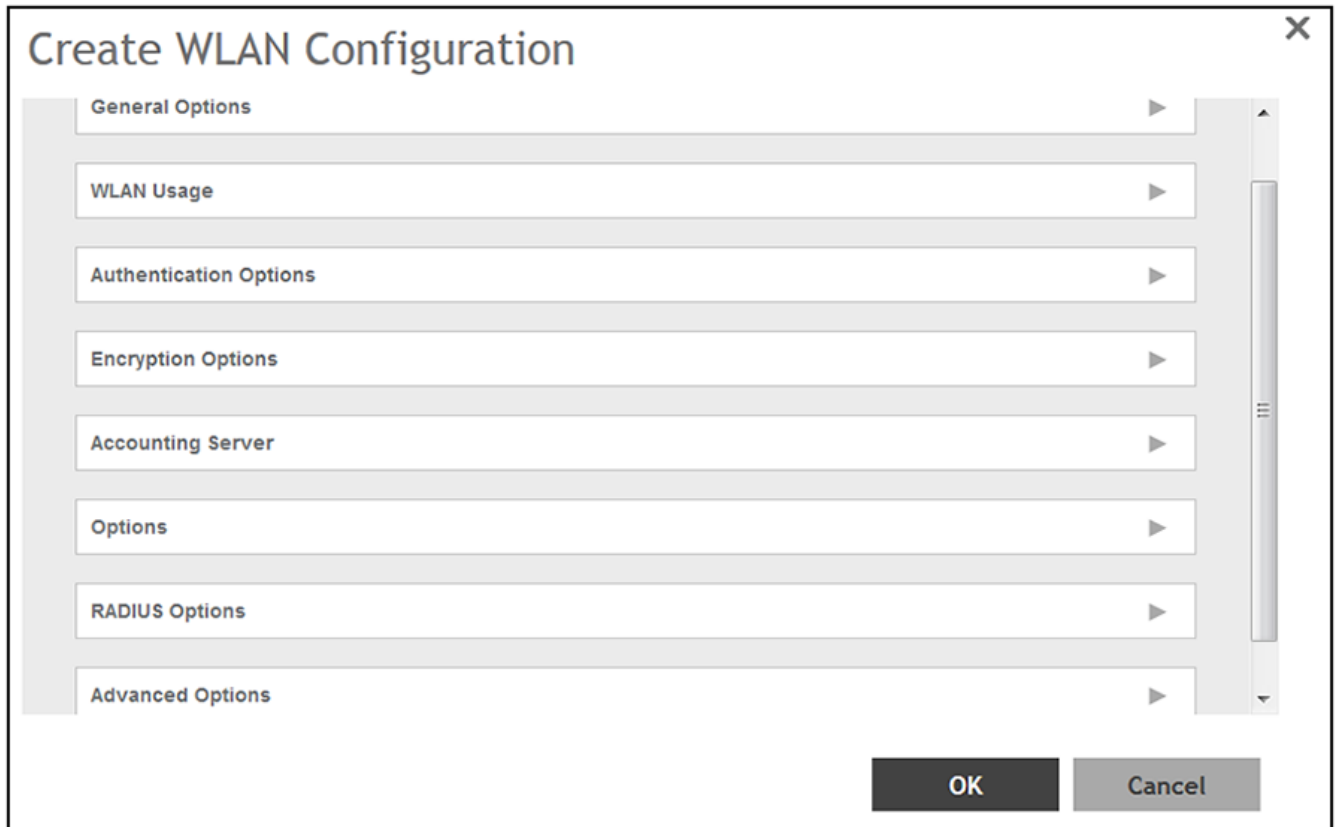
FIGURE 10 Wireless LANs Screen



3. On the Wireless LANs screen, click the + **Create** button.

The Create WLAN Configuration appears. This screen is shown below (with each area of the screen in a collapsed view):

FIGURE 11 Create WLAN Configuration Screen on SmartZone



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.

- Complete the General Options section of the screen:

FIGURE 12 General Options Section of the Create WLAN Configuration Screen

The screenshot shows the 'General Options' section of the configuration screen. It contains the following fields and values:

- Name:** eng-PEAP
- SSID:** eng-PEAP
- Description:** Jeff AAA RADIUS server for PEAP
- Zone:** Z Default Zone
- WLAN Group:** default

A '+ Create' button is located at the bottom right of the form.

- Name: Enter a meaningful name for the PEAP WLAN you are creating.
 - SSID: When you click in this field, the name you entered above also appears in this field.
 - Description: You can enter a brief description to indicate that you are creating a RADIUS WLAN for PEAP.
 - Zone: From the drop-down list, select the zone in which the PEAP WLAN will reside. This can be the default zone.
- In the WLAN Usage section of the screen, use the default selection of Standard usage.

FIGURE 13 WLAN Usage section of the Create WLAN Configuration Screen

The screenshot shows the 'WLAN Usage' section of the configuration screen. It includes the following options:

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

- In the Authentication Options section of the screen, select 802.1x EAP.

FIGURE 14 Authentication Options section of the Create WLAN Configuration Screen

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

- Method:**
 - Open
 - 802.1x EAP
 - MAC Address

- In the Encryptions Options section of the screen, you must select "WPA2," which displays the section as follows:

FIGURE 15 Encryption Options Section After Selecting WPA2 Method

Encryption Options

* Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

* Algorithm: AES AUTO

802.11r Fast Roaming: Enable 802.11r Fast BSS Transition

* 802.11w MFP: Disabled Capable Required

- Algorithm: Be sure that the default value of AES is selected.
 - 802.11w MFP: Be sure the default value of Disabled is selected.
- In the Authentication & Accounting Server section, select the authentication server that you configured in [Set up the AAA Authentication Server on the Ruckus SmartZone Controller](#) on page 9 from the drop-down list.

FIGURE 16 Authentication & Accounting Server Section of the Create WLAN Configuration Screen

Authentication & Accounting Server

* Authentication Server: Use the Controller as Proxy

Accounting Server: Use the Controller as Proxy

NOTE

Do not configure an accounting server for PEAP.

9. In the Options section, you can use the default values, shown below:

FIGURE 17 Options Section of the Create WLAN Configuration Screen

The screenshot shows the 'Options' section of the configuration screen. It includes the following settings:

- Acct Delay Time:** Enable
- Wireless Client Isolation:** Disable Enable (*Isolate wireless client traffic from all hosts on the same VLAN/subnet*)
- Isolation Whitelist:** Gateway Only (Automatic) [Dropdown] + Create [Button]
(The whitelist requires entries for the subnet gateway and other allowed hosts.)
 (The whitelist can only contain wired destinations; wireless clients are not supported on the whitelist.)
- Priority:** High Low

10. In the RADIUS Options section, you can use the default values, shown below:

FIGURE 18 RADIUS Options section

The screenshot shows the 'RADIUS Options' section of the configuration screen. It includes the following settings:

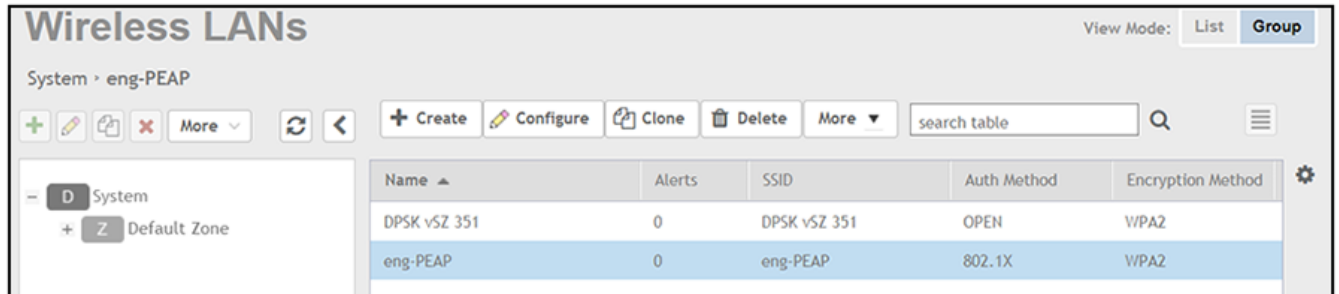
- NAS ID:** WLAN BSSID AP MAC User-defined: [Text Field]
- Delimiter:** Dash Colon
- NAS Request Timeout:** [3] Seconds
- NAS Max Number of Retries:** [2] Times
- NAS Reconnect Primary:** [5] Minute (1-60)
- Called STA ID:** WLAN BSSID AP MAC None AP GROUP
- NAS IP:** Disabled SZ Control IP User-defined: [Text Field]

11. In the Advanced Options section, there are many fields (not shown here), but you can also use all the default values.

12. Click **OK** to complete the PEAP Wireless LAN configuration.

Your newly created PEAP WLAN should now appear in the Wireless LANs List, "eng-PEAP" in this example:

FIGURE 19 Newly Created WLAN Appears in Wireless LANs List



To review the completed configuration or to make any configuration changes, click the **Configure** tab when the Wireless LAN is highlighted.

Proceed to [Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller](#) on page 20.

Configuring PEAP on Cloudpath to Integrate with the Ruckus Controller

Once you configure a PEAP WLAN on your controller, you need to add a corresponding PEAP configuration to a workflow on your Cloudpath system.

This procedure in this section includes steps for:

- Adding a PEAP Branch to Your Workflow (below)
- [Adding a PEAP Device Configuration to Your Workflow](#) on page 23
- [Configuring Cloudpath to Communicate with the External RADIUS server](#) on page 25
- [Testing the PEAP User Experience](#) on page 27
- [Troubleshooting Tips](#) on page 29

NOTE

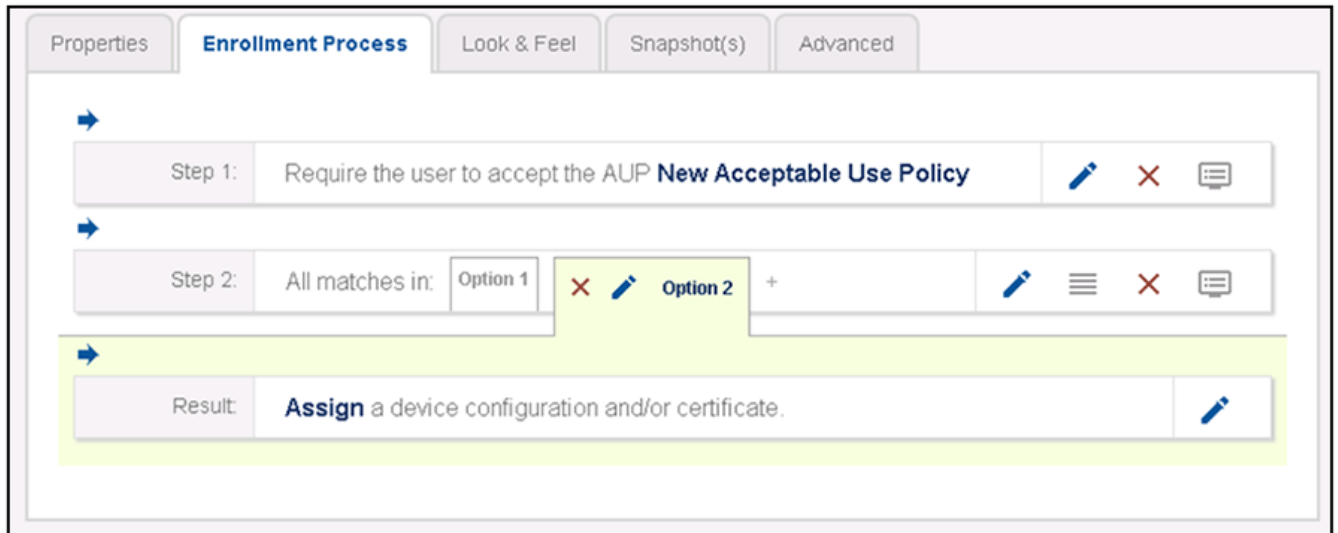
The concept of workflows and how to create one is described in detail in the *Cloudpath Deployment Guide* and the *Cloudpath Quick Start Guide*. Therefore, the purpose of the procedure in this section is to demonstrate how to add a PEAP branch to an existing workflow. The same steps included below could also be used to create a new workflow with a PEAP plugin.

Adding a PEAP Branch to Your Workflow

1. Log in to the Cloudpath user interface.
2. Go to **Configuration > Workflows**.

3. Click on a workflow to which you want to add a PEAP branch. An example of a very simple workflow before adding a PEAP branch is shown below:

FIGURE 20 Workflow Before Adding PEAP Branch



4. Click the + button to create a new branch in your workflow.

The Webpage Display Information screen is displayed, as shown below, and you add the necessary information.

FIGURE 21 Webpage Display Information Screen is Displayed When You Add a Branch to a Workflow

Webpage Display Information

Sample User Display:

Short Name: PEAP

Display Title: PEAP

Display Text:

Enabled:

Icon File:

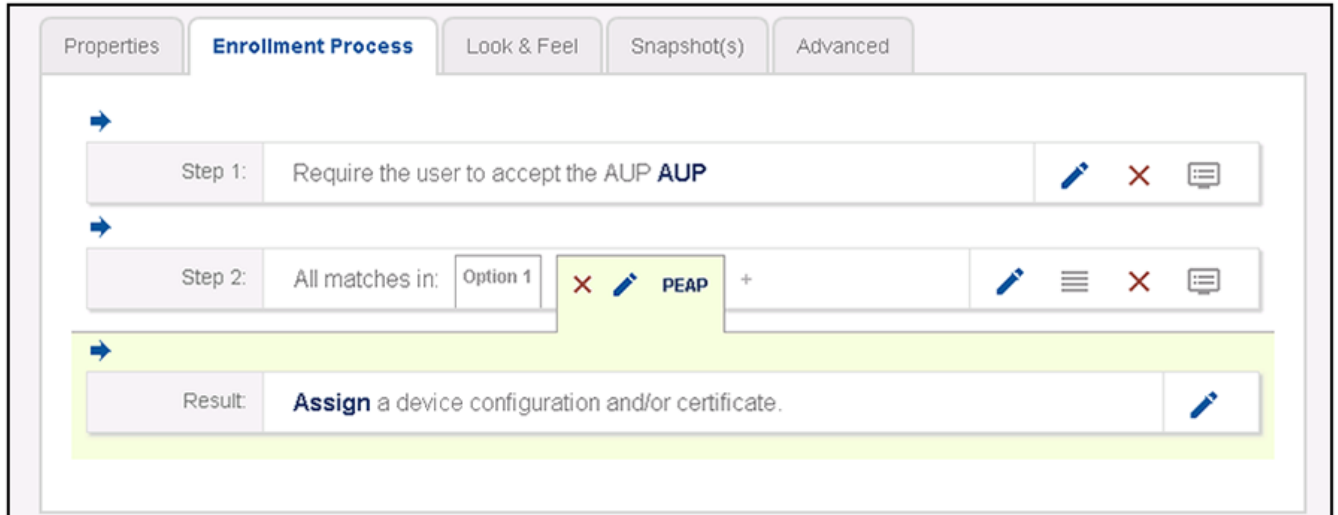
Default: Using default file. [↓](#)

Upload: No file chosen

Enter a Short Name and Display Title, and, optionally, Display Text, then click **Save**.

5. On the next screen (**Configuration > Workflows > Modify Step**), click **Done**.
The PEAP tab has been added, as shown in the following screen.

FIGURE 22 Workflow After Adding Tab for PEAP

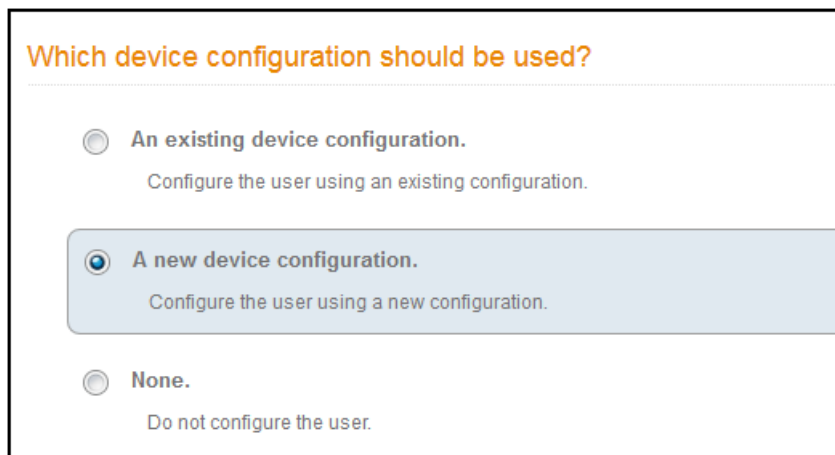


Adding a PEAP Device Configuration to Your Workflow

1. In the workflow, with the PEAP tab highlighted, click the pencil icon to the right of the Result line to "Assign a device configuration and/or certificate."

The following screen appears:

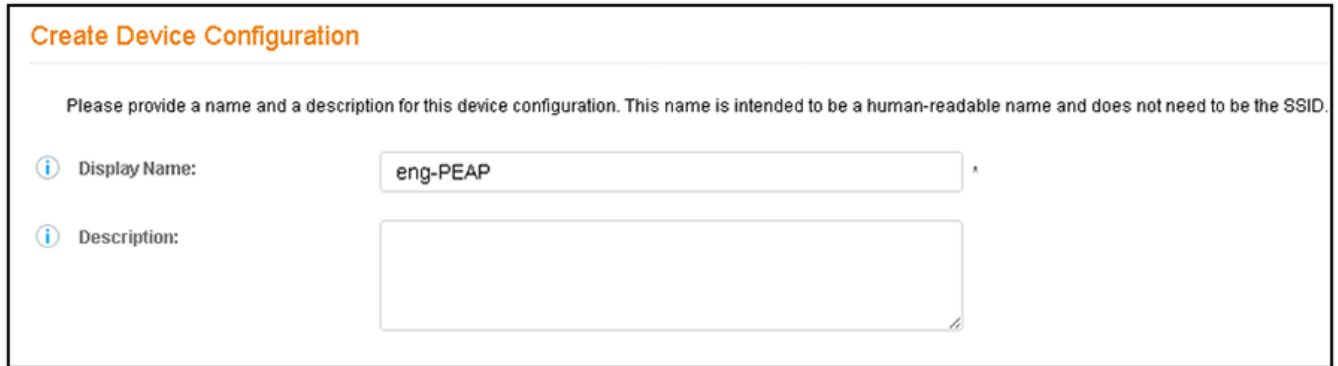
FIGURE 23 Device Configuration Selection Screen



2. Select "A new device configuration," then click **Next**.

The Create Device Configuration screen is displayed. Enter a descriptive name. The name does not need to be the same as the SSID; however it can be, as shown below.

FIGURE 24 Create Device Configuration Screen



Create Device Configuration

Please provide a name and a description for this device configuration. This name is intended to be a human-readable name and does not need to be the SSID.

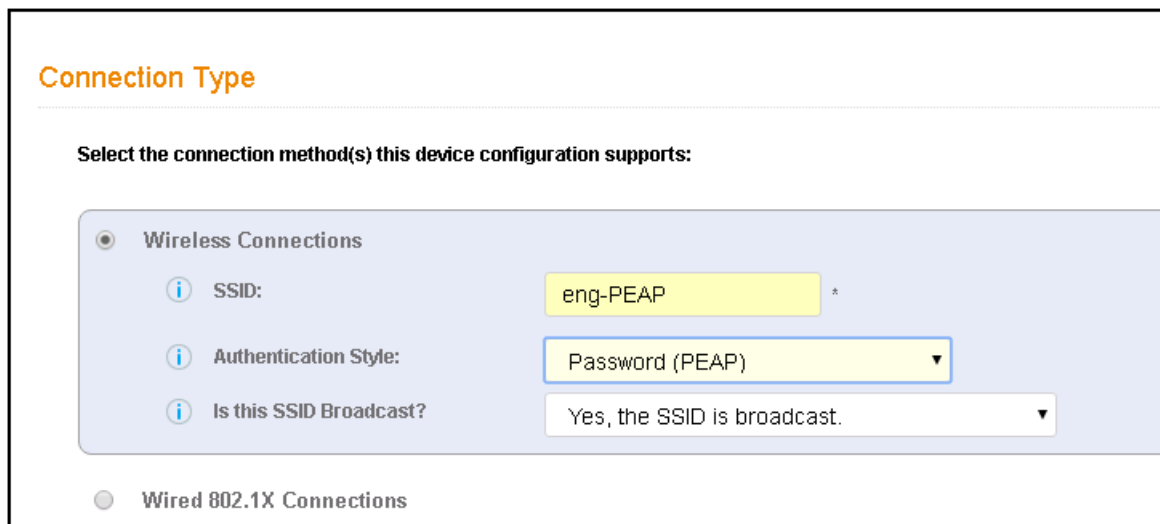
Display Name: eng-PEAP *

Description:

Click **Next**.

3. The Connection Type screen is displayed; required fields are described below the screen:

FIGURE 25 Connection Type Screen



Connection Type

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

Wireless Connections

SSID: eng-PEAP *

Authentication Style: Password (PEAP

Is this SSID Broadcast?: Yes, the SSID is broadcast.

Wired 802.1X Connections

- The Wireless Connections button must be selected.
- SSID: This name must match the PEAP SSID exactly as you configured it on the controller:
 - For a Ruckus ZoneDirector controller, it is the name configured in [Figure 4](#) on page 12.
 - For a Ruckus SmartZone controller, it is the name configured in [Figure 12](#) on page 17.
- Authentication Style: Select Password (PEAP) from the drop-down list.
- Is this SSID Broadcast?: Leave the default value of Yes, the SSID is broadcast.

Click **Next**.

Configuring Cloudpath to Communicate with the External RADIUS server

1. For the screens you are presented with next, you can keep all the default values and continue to click **Next** to progress through the screens, until you get to the following screen:

FIGURE 26 RADIUS Server Information

RADIUS Server Information

Select the RADIUS server to which the client will authenticate. This will configure server certificate validation, which is an important part of the WPA2-Enterprise and 802.1X security model. When enabled, the client device will only attempt to authenticate to a RADIUS server that provides a certificate signed by the selected certificate authorities. If server certificate validation is disabled (not recommended), the client device will attempt to authenticate to any RADIUS server. Enabling server certificate validation is a security best practice.

Client will authenticate to the onboard RADIUS server.

Client will authenticate to an external RADIUS server.

RADIUS Server: *New RADIUS Server*

Do not configure server certificate validation. (Not Recommended)

With the "Client will authenticate to an external RADIUS server" option selected, be sure that the RADIUS Server value is ***New RADIUS Server***, then, click **Next**.

2. On the screen that appears next (below), use the **Choose File** button to upload the root CA and any intermediates certificates to allow the Cloudpath system to communicate with the external RADIUS server. The following illustration is an example of the RADIUS Server Information screen after the root CA and its intermediate certificate have been uploaded.

FIGURE 27 RADIUS Server Information Screen After Uploading Certificates

RADIUS Server Information

Reference Name:

RADIUS Common Name:

Server Certificate & CAs:

✕ CPN Test A7R1 Root CA I	FFA8-387E-4E79-2055-ED18-DEBE-7CEC-FDF0-8D17
✕ CPN Test A7R1 Intermediate CA I	1444-C800-2886-3381-E447-1451-2123-AB2D-AA0F

The RADIUS server certificate and its full chain should be listed above. Clients will be configured to expect this chain and the RADIUS common name specified. The RADIUS common name will be populated automatically once the server certificate has been uploaded. If multiple RADIUS servers exist that use different common names, the RADIUS common name value may be modified to contain a wildcard.

To add additional items, select the certificate or certificate authority file below. Once selected, it will be uploaded and will appear above.

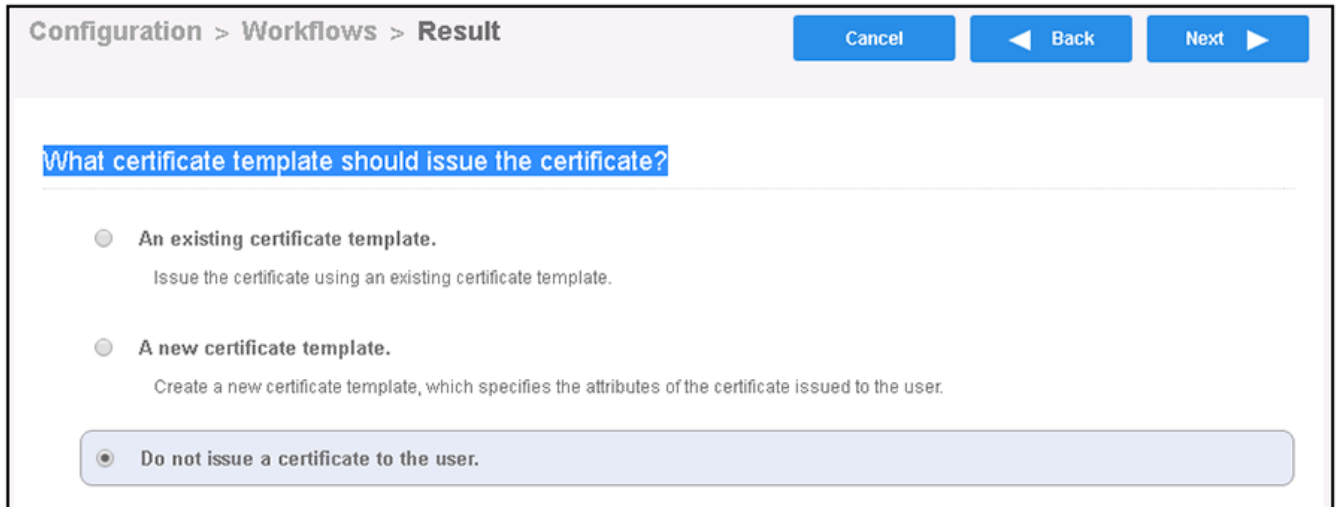
Certificate To Upload: No file chosen

The Reference Name is an internal name (typically a name for the external RADIUS server) and is not obtained from the certificate, but the RADIUS Common Name is obtained from the certificate. Both these fields can be left blank if you wish. Click **Next**.

3. On the Additional Options screen, which is displayed next, leave the default values and click **Next**.

4. On the "What certificate template should issue the certificate?" screen, select "Do not issue a certificate to the user."

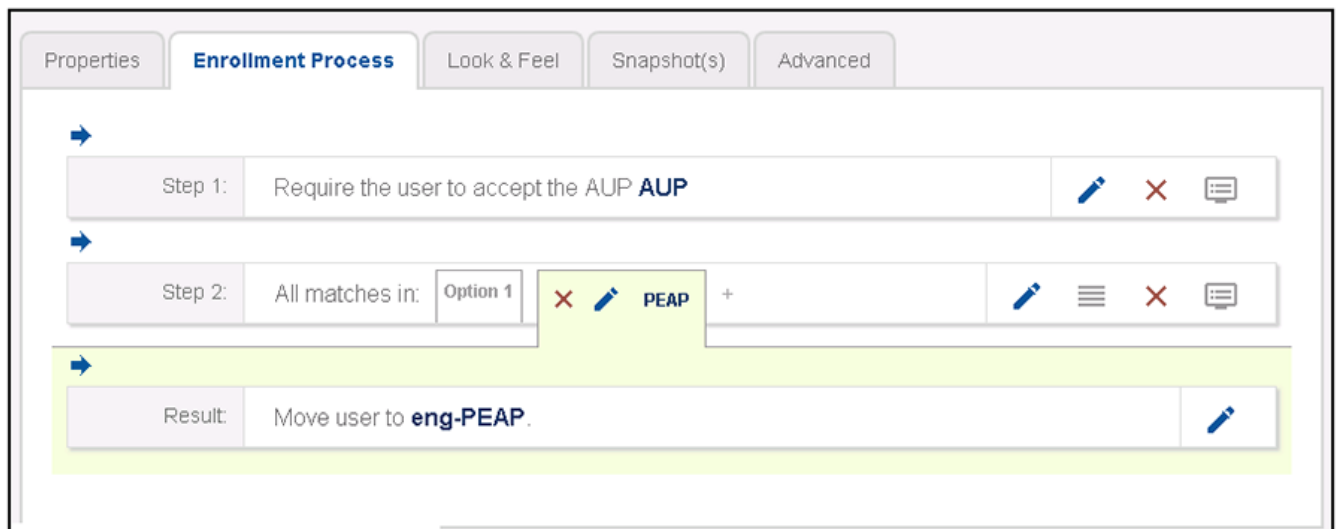
FIGURE 28 What certificate template should issue the certificate?



Click **Next**.

5. You are returned to the workflow. Make sure the Result step has been added successfully, as shown below:

FIGURE 29 Workflow After Completing the Device Configuration "Result"



Publish the workflow by clicking the **Publish** icon to the left of the workflow name at the top of the **Configuration > Workflows** screen.

Testing the PEAP User Experience

1. Test the Enrollment process by clicking on the enrollment portal URL for the workflow at the top of the **Configuration > Workflows** screen.
2. When are you presented with the with the Welcome screen, click **Start**.
3. When you are presented with various branches of your workflow, click the "PEAP" branch:

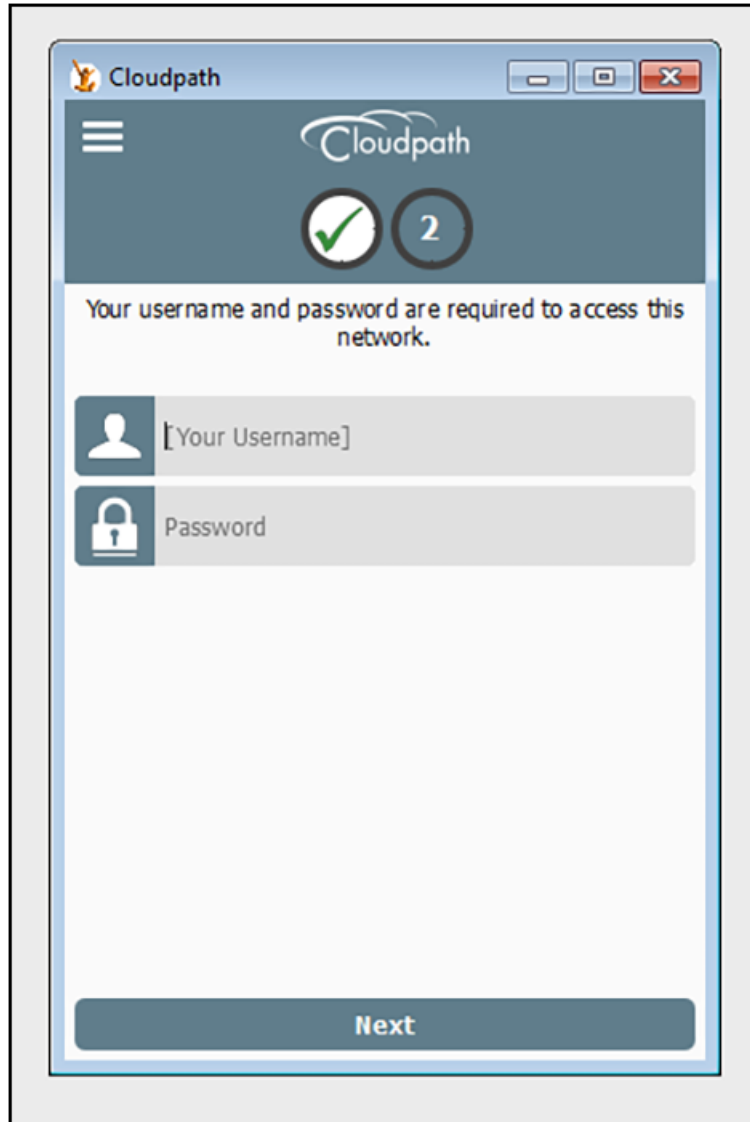
FIGURE 30 Testing the Workflow - PEAP Branch



4. Follow any prompts to continue.

5. The user is presented with a screen similar to the one shown in the following figure to enter username and password.

FIGURE 31 PEAP User Credentials Screen



Enter the credentials for the external RADIUS server, then click **Next**.

6. Proceed with the enrollment. If enrollment is successful, you will receive some status screens indicating the following status as the process is in progress:
 - "Configuring this device"
 - "Attempting to connect to the network"
 - "Congratulations! You are now connected to the network."

Troubleshooting Tips

If an error occurs during the workflow-publishing or enrollment process, check the following:

- Make sure that you have selected **Password (PEAP)** as the Authentication Style in the Cloudpath Connection Type screen.
- Make sure that you have added the correct Cloudpath PEAP SSID to the final result step in your workflow.
- Verify that the shared secret configured of your external RADIUS server matches the shared secret on the Create AAA Authentication Server configuration screen on your controller.
- Verify that the Cloudpath server can ping the external RADIUS server, and vice versa.
- Verify that you have the correct Root and any Intermediate CAs for the external RADIUS server.



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com